Skript zu den Vorlesungen

Mathematik für Informatiker I und II

(WiSe 2009/10 und SoSe 2010)

Im WiSe 2009/10 gehalten von:
Prof. Dr. Barbara Baumeister

Lehrstuhl für Algebra
Fachbereich Mathematik
Universität Dortmund

b.Baumeister@math.uni-dortmund.de

Autor: Martin Skutella
Lehrstuhl für Diskrete Optimierung
Fachbereich Mathematik
Universität Dortmund
martin.skutella@uni-dortmund.de

(Version vom 15. Oktober 2007)

Vorwort

Das vorliegende Skript entstand im Winter- und Sommersemester 2005/06 während ich die Vorlesungen „Mathematik für Informatiker I und II“ an der Universität Dortmund hielt. Ich habe versucht, die wichtigsten Punkte der behandelten Themen darin zusammen zu stellen, um den Hörerinnen und Hörern einen Leitfaden für die Nachbereitung der Vorlesung an die Hand zu geben. Das Skript erhebt nicht den Anspruch eines Lehrbuchs hinsichtlich Exaktheit, Vollständigkeit und Präsentation der Themen. Ich möchte beispielhaft auf einige Lehrbücher verweisen, die beim weiteren Studium der Materie hilfreich sein könnten.

- M. Aigner. Diskrete Mathematik. Vieweg Verlag, 2004.
- M. Brill. Mathematik für Informatiker. Hanser Verlag, 2001.
- D. Hachenberger. Mathematik für Informatiker. Pearson Studium, 2005.
- P. Hartmann. Mathematik für Informatiker. Vieweg Verlag, 2004.
- G. Rosenberger. Lineare Algebra und algebraische Strukturen für Informatiker. Shaker Verlag, 2002.
- A. Steger. Diskrete Strukturen (Band 1). Springer Verlag, 2001.
- M. Wolff, P. Hauck und W. Küchlin. Mathematik für Informatik und Bioinformatik. Springer Verlag, 2004.

Darüber hinaus gibt es natürlich eine Vielzahl weiterer Lehrbücher, auf die ich hier jedoch nicht näher eingehe.

Teile dieses Skripts basieren auf Skripten und Aufzeichnungen zu früheren Vorlesungen an der Universität Dortmund, die mir meine Kollegen freundlicherweise zur Verfügung gestellt haben. Mehr dazu findet sich zu Beginn der entsprechenden Kapitel. Die Assistenten der beiden Vorlesungen, Ronald Koch und Sammy Barkowski, haben mit zahlreichen wertvollen Text- und Bildbeiträgen, Hinweisen und Verbesserungsvorschlägen wesentlich zum Gelingen des Skripts beigetragen. Dafür sei ihnen ganz herzlich gedankt.

Aufgrund der begrenzten Zeit, die ich auf das Erstellen dieses Skripts verwenden konnte, ist es sicherlich weit davon entfernt, fehlerfrei zu sein. Für entsprechende Hinweise (am besten per Email an `martin.skutella@uni-dortmund.de`) bin ich jederzeit dankbar.

Dortmund, im Juli 2006 Martin Skutella

Inhaltsverzeichnis

Kapitel 1

Aussagen, Mengen, Abbildungen, Relationen

Das erste Kapitel dieses Vorlesungsskriptes beruht teilweise auf Skripten von Herrn Kahlhoff, Herrn Möller und Herrn Scharlau, denen ich hiermit ganz herzlich danke.

1.1 Aussagen

1.1.1 Informelle Definition von Aussagen

Im täglichen Leben ziehen Menschen mehr oder weniger korrekte Schlussfolgerungen, ohne sich der Gesetze bewusst zu sein, nach denen sich dieses Schließen vollzieht. Für wissenschaftliches, insbesondere mathematisches Arbeiten erweist sich dieses intuitive Schließen als unzureichend. Zudem zeigt sich, dass die Umgangssprache in mancher Hinsicht zu diffus ist, um mit ihr präzise einen mathematischen Sachverhalt ausdrücken zu können. Der Begriffsinhalt von Substantiven und Adjektiven ist manchmal mehrdeutig, manchmal nur unscharf abgegrenzt und zudem Schwankungen unterworfen, sowohl von Mensch zu Mensch wie auch für den einzelnen selbst im Laufe seines Lebens. Beispiele:

- Schloss — Bank — Hahn — Messe — Steuer — ...
- alter Mensch — Freiheit — groß — unerträglich — warm — kalt — ...

Bei den ersten fünf Worten liegt Mehrdeutigkeit vor (das bekannte Kinderspiel des „Teekesselratens“ beruht gerade auf solchen Mehrdeutigkeiten), die auch bei wissenschaftlichen Bezeichnungen (bedauerlicherweise) zu finden ist. Die weiteren Begriffe weisen ein diffuses, subjektives Begriffsspektrum auf. So ist eine Jugendliche geneigt, einen Vierzigjährigen schon als „alten Mann“ zu bezeichnen, während eine Achtzigjährige in diesem noch einen jungen Mann sieht. Ebenso ist

beispielsweise die Abgrenzung von „warm“ und „kalt“ nicht eindeutig an einer Temperaturgrenze festzumachen.

Auch die Satzverbindungen, die die logischen Zusammenhänge beinhalten, werden in wechselnden Bedeutungen verwendet. So etwa im Falle des Wortes „und“:

- Lena *und* Jakob sind Skifahrer.
- 3 *und* 5 sind Primzahlen.
- Lena *und* Jakob sind befreundet.
- 3 *und* 5 ist 8.
- Lena *und* Jakob haben ein Auto.
- Jakob wird krank *und* der Arzt kommt.
- Der Arzt kommt *und* Lena wird krank.
- ... na *und*?

Die somit für den wissenschaftlichen Gebrauch notwendige begriffliche Präzisierung der Sprache führt einerseits zu den in Definitionen klar umrissenen Fachausdrücken (deren Bedeutung freilich bei verschiedenen Autoren unterschiedlich sein kann) und andererseits im Falle der Satzverbindungen zu logischen Operationsvorschriften, die Einzelaussagen zu einer neuen Aussage verbinden. Was sind aber zunächst Aussagen?

Erklärung 1.1.1. Aussagen sind sprachliche Gebilde, denen genau einer der Wahrheitswerte w (wahr) oder f (falsch) zugeordnet ist.

Beispiele.

- A_1 := „Die Erde ist eine Scheibe.“ ist Aussage (Wahrheitswert f).
- A_2 := „64 ist durch 4 teilbar.“ ist Aussage (Wahrheitswert w).
- A_3 := „Diese Aussage ist falsch.“ ist keine Aussage.
- A_4 := „$2^{25964951} - 1$ ist eine Primzahl.“ ist Aussage (Wahrheitswert w).
- A_5 := „Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen.“ ist Aussage (Wahrheitswert unbekannt, Goldbachsche Vermutung, $...12 = 5 + 7...$).
- A_6 := „Es gibt unendlich viele Zahlen a, so dass a und $a + 2$ Primzahlen sind.“ ist Aussage (Wahrheitswert unbekannt, z.B. 5 und 7 oder 9629 und 9631).

1.1.2 Logische Verknüpfungen

Durch Negation und Verknüpfung (Junktion) von Aussagen erhält man neue Aussagen, die wir im Folgenden definieren.

Definition 1.1.2. Im Folgenden seien A und B zwei Aussagen.

a) Als *Negation* von A bezeichnen wir die Aussage „nicht A“ und schreiben kurz $\neg A$. Die Negation $\neg A$ hat den Wahrheitswert f, wenn A den Wahrheitswert w hat; hat umgekehrt A den Wahrheitswert f, so hat $\neg A$ den Wahrheitswert w.

Beispiel. $\neg A_2$ =„64 ist nicht durch 4 teilbar.“ (falsch)
$\neg A_5$ =„Es gibt eine gerade Zahl ≥ 4, die nicht als Summe zweier Primzahlen geschrieben werden kann.“ (Wahrheitswert unbekannt)

b) Die Verkettung der Aussagen A und B durch das logische „und“ nennen wir *Konjunktion* und schreiben kurz $A \wedge B$. Die Konjunktion $A \wedge B$ ist nur dann wahr, wenn sowohl A als auch B wahr sind.

Beispiel. $A_2 \wedge A_5$ =„64 ist durch 4 teilbar und jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen.“ (Wahrheitswert unbekannt)

c) Die Verkettung der Aussagen A und B durch das logische „oder“ nennen wir *Disjunktion* und schreiben kurz $A \vee B$. Die Disjunktion $A \vee B$ ist wahr, falls A oder B oder beide wahr sind.

Beispiel. $A_2 \vee A_5$ =„64 ist durch 4 teilbar oder jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen (oder beides).“ (wahr)

d) Die Verkettung der Aussagen A und B zu „wenn A, dann B“ nennen wir *logische Folgerung* oder *Implikation* und schreiben kurz $A \Rightarrow B$. Wir nennen A *Voraussetzung* und B *Behauptung* der Implikation. Die Implikation ist wahr, falls A falsch ist oder B wahr ist (oder A falsch und B wahr ist).

Beispiel. A :=„Jeder Tag ist ein Sonntag.“ (falsch), B :=„Der BVB ist Deutscher Meister.“ (falsch)
$(A \Rightarrow B)$=„Wenn jeder Tag ein Sonntag ist, dann ist der BVB Deutscher Meister.“ (wahr)

e) Die Verknüpfung der Aussagen A und B zu „genau dann A, wenn B“ nennen wir *Äquivalenz* und schreiben kurz $A \Leftrightarrow B$. Die Äquivalenz ist wahr, falls A und B denselben Wahrheitswert haben.

Beispiel. $(A \Leftrightarrow B)$=„Genau dann, wenn jeder Tag ein Sonntag ist, ist der BVB Deutscher Meister.“ (wahr)

Wir fassen die in Definition 1.1.2 getroffenen Vereinbarungen in der folgenden *Wahrheitstafel* zusammen:

A	B	$\neg A$	$\neg B$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	f	w	w	w	w
w	f	f	w	f	w	f	f
f	w	w	f	f	w	w	f
f	f	w	w	f	f	w	w

Definition 1.1.3. Ein logischer Ausdruck, der für beliebige Wahrheitswerte der enthaltenen Aussagen immer wahr ist, heißt *Tautologie*.

Satz 1.1.4. *Es seien A, B und C beliebige Aussagen. Dann sind die folgenden logischen Ausdrücke Tautologien:*

a) $(A \wedge f) \Leftrightarrow f$
$(A \vee w) \Leftrightarrow w$
$(A \vee f) \Leftrightarrow A$ *(Neutralität von f bzgl. $\vee$)*
$(A \wedge w) \Leftrightarrow A$ *(Neutralität von w bzgl. $\wedge$)*

b) $(A \wedge A) \Leftrightarrow A$ *(Idempotenz von $\wedge$)*
$(A \vee A) \Leftrightarrow A$ *(Idempotenz von $\vee$)*

c) $(A \wedge B) \Leftrightarrow (B \wedge A)$ *(Kommutativität von $\wedge$)*
$(A \vee B) \Leftrightarrow (B \vee A)$ *(Kommutativität von $\vee$)*

d) $((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$ *(Assoziativität von $\wedge$)*
$((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$ *(Assoziativität von $\vee$)*

e) $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$ *(Distributivität)*
$(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$ *(Distributivität)*

f) $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ *(De Morgan'sche Regel)*
$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$ *(De Morgan'sche Regel)*

g) $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$

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

i) $(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

j) $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$

Teil h) des Satzes ist Grundlage für den *Widerspruchsbeweis*: Wenn man beweisen möchte, dass unter einer Voraussetzung A eine Behauptung B gilt, dann genügt es zu beweisen, dass die Voraussetzung A nicht erfüllt ist, falls die Behauptung B nicht erfüllt ist.

Auch Teil j) ist von Bedeutung in der Beweistechnik. Wenn man beweisen möchte, dass zwei Aussagen A und B äquivalent sind, dann zeigt man das in den allermeisten Fällen in zwei Schritten: Man beweist, dass aus A die Aussage B folgt und dass aus B die Aussage A folgt.

Beweis. Wir beweisen beispielhaft den ersten Teil von f) mit Hilfe einer Wahrheitstafel. Die anderen Behauptungen des Satzes können analog bewiesen werden.

A	B	$\neg A$	$\neg B$	$\neg(A \vee B)$	$\neg A \wedge \neg B$	$\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$
w	w	f	f	f	f	w
w	f	f	w	f	f	w
f	w	w	f	f	f	w
f	f	w	w	w	w	w

Aus der letzten Spalte der Tabelle folgt, dass die Aussage $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ unabhängig von den Wahrheitswerten von A und B immer wahr ist. □

1.2 Mengen

1.2.1 Mengen und deren Beschreibungen

Wir verzichten hier auf eine formale axiomatische Einführung der Mengenlehre und beschränken uns bei der Definition des Begriffs „Menge“ auf die folgende Beschreibung, die auf Georg Cantor (1845–1918), den Begründer der Mengenlehre, zurückgeht.

Erklärung 1.2.1. Eine *Menge* ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens — welche die *Elemente* der Menge genannt werden — zu einem Ganzen.

Wir verwenden die folgenden Schreibweisen:

- $x \in M$ steht für die Aussage „x ist ein Element der Menge M.“
- Die Negation dieser Aussage bezeichnen wir mit $x \notin M$, d.h. „x ist kein Element von M.“

Beispiel. Hose $\in$ {Jacke, Hose}, Hut $\notin$ {Jacke, Hose}

Definition 1.2.2 (Standard-Bezeichnungen für Mengen)**.**

$\mathbb{N}$	$=$	$\{1, 2, 3, 4, \ldots\}$ die natürlichen Zahlen
$\mathbb{N}_0$	$=$	$\{0, 1, 2, 3, 4, \ldots\}$ die natürlichen Zahlen mit Null
$\mathbb{Z}$	$=$	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ die ganzen Zahlen
$\mathbb{Q}$	$=$	$\{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{N}\}$ die Bruchzahlen, rationalen Zahlen
$\mathbb{R}$		die reellen Zahlen
$\emptyset$		die leere Menge

Erklärung 1.2.3 (Beschreibung von Mengen)**.**

I. Durch *Aufzählung* der Elemente, z.B.

$$M = \{1, 3, 5, 6\}, \quad X = \{a, b, c, d, e, f\};$$

dieses ist prinzipiell bei endlichen Mengen möglich, unter Umständen auch bei unendlichen Mengen, wenn keine Missverständnisse zu befürchten sind:

$$\mathbb{N}_0 = \{0, 1, 2, 3, 4 \ldots\},$$

$$G = \{2, 4, 6, 8, \ldots\} \text{ die Menge der geraden Zahlen.}$$

II. In *beschreibender Form*, d.h. durch Angabe der Eigenschaften der Elemente, z.B.

$$G = \{x \mid x \in \mathbb{N} \text{ und } x \text{ ist gerade}\}.$$

Die allgemeine Form ist:

$$M = \{x \mid A(x)\},$$

dabei ist $A(x)$ eine Aussage über x, also z.B. „x ist eine natürliche Zahl und x ist gerade.“

Man kann auch schreiben:

$$G = \{x \in \mathbb{N} \mid x \text{ ist gerade}\},$$

d.h. die “Grundmenge”, in der sich die Elemente der zu definierenden Menge befinden, hier die Menge $\mathbb{N}$, wird nicht unter den Aussagen (bzw. Eigenschaften), sondern bereits vor dem Trennstrich in der Mengenklammer genannt.

III. In *abgekürzter beschreibender Form*, z.B.

$$G = \{2 \cdot m \mid m \in \mathbb{N}\}.$$

Man verzichtet hier auf einen speziellen Namen für die Elemente und gibt sofort ein *Bildungsgesetz*, z.B. einen Term oder algebraischen Ausdruck, an. Ein anderes Beispiel hierzu:

$$\begin{aligned} K &= \{1 + 3z \mid z \in \mathbb{Z}\} \\ &= \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}. \end{aligned}$$

Beispiel. Die Menge der Quadratzahlen in allen drei Beschreibungsformen:

$$\begin{aligned} Q &= \{1, 4, 9, 16, 25, \ldots\} \\ &= \{y \mid y \in \mathbb{N} \text{ und es existiert ein } x \in \mathbb{N} \text{ mit } x^2 = y\} \\ &= \{x^2 \mid x \in \mathbb{N}\} \end{aligned}$$

Kurzer Exkurs. Wir weisen an dieser Stelle darauf hin, dass ein naiver Umgang mit Mengen schnell zu scheinbar unauflösbaren Widersprüchen führen kann. Ein schönes Beispiel hierfür ist die *Russellsche Antinomie*: „Es sei M die Menge aller Mengen, die sich nicht selbst enthalten, also

$$M := \{X \mid X \notin X\} \ .“$$

Die Frage, ob M in sich selbst enthalten ist oder nicht, führt zu einem unauflösbaren Widerspruch. Ein sauberer axiomatischer Aufbau der Mengenlehre erlaubt daher keine solche Menge M.

Das beschriebene Pardoxon kann auch leicht in das tägliche Leben übersetzt werden. Man stelle sich vor, es gäbe in einer Bibliothek ein Nachschlagewerk, das alle Bücher der Bibliothek zitiert (auflistet), die sich nicht selbst zitieren. Die Frage, ob dieses Nachschlagewerk sich selbst zitiert oder nicht, führt zu demselben Paradoxon. Ein anderes bekanntes Paradoxon ist der Dorf-Barbier, der alle Männer des Dorfes rasiert, die sich nicht selbst rasieren...

1.2.2 Allquantor und Existenzquantor

Definition 1.2.4 (Allquantor und Existenzquantor)**.** Es sei M eine nichtleere Menge und für jedes $x \in M$ sei $A(x)$ eine Aussage.

a) Mit $\forall x \in M : A(x)$ bezeichnen wir die Aussage „Für alle $x \in M$ gilt $A(x)$.“

b) Mit $\exists x \in M : A(x)$ bezeichnen wir die Aussage „Es gibt ein $x \in M$, für das $A(x)$ gilt.“

c) Mit $\exists! x \in M : A(x)$ bezeichnen wir die Aussage „Es gibt genau ein $x \in M$, für das $A(x)$ gilt.“

Man nennt $\forall$ den *Allquantor* und $\exists$ den *Existenzquantor*.

Beispiel. Es sei M die Menge der Studentinnen und Studenten dieser Vorlesung und für einen Studierenden $x \in M$ sei $A(x)$ die Aussage „x fährt mit dem Fahrrad zur Uni.“ Dann steht $\forall x \in M : A(x)$ für die Aussage „Alle Studierenden dieser Vorlesung fahren mit dem Fahrrad zur Uni.“ Der Ausdruck $\exists x \in M : A(x)$ steht für „Mindestens eine(r) der Studierenden dieser Vorlesung fährt mit dem Fahrrad zur Uni.“ Schließlich steht der Ausdruck $\exists! x \in M : A(x)$ für „Genau eine(r) der Studierenden dieser Vorlesung fährt mit dem Fahrrad zur Uni.“

Lemma 1.2.5. *Es sei M eine nichtleere Menge und für jedes $x \in M$ sei $A(x)$ eine Aussage. Die Negation der Aussage $\forall x \in M : A(x)$ ist die Aussage $\exists x \in M : \neg A(x)$, d.h.*

$$\neg(\forall x \in M : A(x)) \ \Leftrightarrow \ (\exists x \in M : \neg A(x)) \ .$$

Beispiel. In Fortsetzung des Beispiels von oben stellen wir fest, dass die Negation von „Alle Studierenden dieser Vorlesung fahren mit dem Fahrrad zur Uni“ die folgende Aussage ist: „Es gibt eine Studentin oder einen Studenten dieser Vorlesung, die/der *nicht* mit dem Fahrrad zur Uni fährt.“

Lemma 1.2.5 ist die formale Rechtfertigung für den *Beweis durch Gegenbeispiel*. Wenn man etwa beweisen möchte, dass die Aussage „Alle Studentinnen und Studenten dieser Vorlesung fahren mit dem Fahrrad zur Uni“ falsch ist, so genügt es, eine Studentin oder einen Studenten zu finden, die/der nicht mit dem Fahrrad zur Uni fährt.

1.2.3 Mengenoperationen

Definition 1.2.6 (Teilmenge)**.**

a) Eine Menge X heißt *Teilmenge* einer Menge M, falls jedes Element von X auch Element von M ist (d.h.: $\forall x \in X : x \in M$). Die entsprechende Beziehung zwischen X und M heißt auch *Inklusion* (von X in M).

   Bezeichnung: $X \subseteq M$.

   Wir weisen ausdrücklich darauf hin, dass bei der Inklusion die Gleichheit der beiden Mengen erlaubt ist: Es gilt $M \subseteq M$.

b) Eine Menge X heißt *echte Teilmenge* einer Menge M, falls X Teilmenge von M und $X \neq M$ ist. Die entsprechende Beziehung zwischen X und M heißt auch *echte Inklusion* (von X in M).

   Bezeichnung: $X \subsetneq M$ oder $X \subsetneqq M$ oder $X \subset M$.

Definition 1.2.7 (Operationen mit Mengen)**.** Es seien X und Y zwei Mengen. Wir definieren:

(i) $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ (Durchschnitt)

(ii) $X \cup Y := \{x \mid x \in X \vee x \in Y\}$ (Vereinigung)

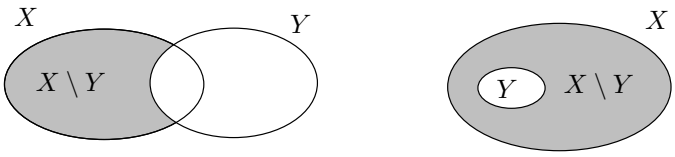
(iii) $X \setminus Y := \{x \mid x \in X \wedge x \notin Y\}$ (Differenzmenge)

Ist $X \cap Y = \emptyset$, dann sagt man, dass X und Y *disjunkt* sind.

Bemerkung. Man beachte, dass bei der Differenzmenge $X \setminus Y$ die Menge Y nicht in der Menge X enthalten sein muss. Man kann sich allerdings immer auf diesen Fall zurückziehen, denn es gilt offensichtlich

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

Veranschaulichung im sogenannten Venn-Diagramm:



Definition 1.2.8 (Komplement)**.** Ist X Teilmenge der Grundmenge M, so bezeichnen wir das *Komplement* von X in M mit $\overline{X} := M \setminus X$.

Satz 1.2.9 (Grundgesetze bei Mengenoperationen)**.** *Es seien X, Y und Z Teilmengen einer Grundmenge M. Dann gelten die folgenden Gesetze:*

a) $X \cap \emptyset = \emptyset$
$X \cup M = M$
$X \cup \emptyset = X$ *(Neutralität von $\emptyset$ bzgl. $\cup$)*
$X \cap M = X$ *(Neutralität von M bzgl. $\cap$)*

b) $X \cap X = X$ *und* $X \cup X = X$ *(Idempotenz)*

c) $X \cap Y = Y \cap X$ *und* $X \cup Y = Y \cup X$ *(Kommutativität)*

d) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ *und* $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ *(Assoziativität)*

e) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ *und* $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ *(Distributivität)*

f) $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$ *und* $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$ *(De Morgan'sche Regeln)*

Beweis. Die Gesetze folgen im Wesentlichen aus den in Satz 1.1.4 a)–f) beschriebenen Gesetzen für die Verknüpfung von Aussagen. Wir machen den Zusammenhang beispielhaft für Teil c) klar. Dazu definieren wir für $x \in M$ die Aussagen $A(x) :=$„x ist Element der Menge X.“ und $B(x) :=$„x ist Element der Menge Y.“ Die Aussagen in c) können dann wie folgt neu formuliert werden:

$$\forall x \in M : (A(x) \wedge B(x)) \Leftrightarrow (B(x) \wedge A(x))$$
$$\forall x \in M : (A(x) \vee B(x)) \Leftrightarrow (B(x) \vee A(x))$$

Aus dem entsprechenden Teil von Satz 1.1.4 folgt sofort, dass diese Aussagen wahr sind. □

Definition 1.2.10 (Kartesisches Produkt)**.**

a) Das *kartesische Produkt* zweier Mengen X und Y ist definiert als

$$\underset{\text{„}X \text{ kreuz } Y\text{“}}{X \times Y} := \{(x, y) \mid x \in X \wedge y \in Y\} .$$

Ein Element $(x, y) \in X \times Y$ heißt *geordnetes Paar*. Nach Definition gilt für beliebige $x, x' \in X$ und $y, y' \in Y$:

$$(x, y) = (x', y') \Leftrightarrow (x = x' \wedge y = y') .$$

b) Allgemeiner ist das *kartesische Produkt* von n Mengen $X_1, X_2, \ldots, X_n$ definiert als

$$X_1 \times X_2 \times \cdots \times X_n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \text{ für } i = 1, \ldots, n\} .$$

Ein Element $(x_1, x_2, \ldots, x_n) \in X_1 \times X_2 \times \cdots \times X_n$ heißt *n-Tupel*. Nach Definition gilt für beliebige $x_i, y_i \in X_i$, $i = 1, \ldots, n$:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \;\Leftrightarrow\; (x_i = y_i \text{ für } i = 1, \ldots, n) \;.$$

Zwei n-Tupel sind also nur dann gleich, wenn an entsprechenden Stellen dasselbe Element der jeweiligen Menge X_i steht. Insbesondere kommt es in geordneten Paaren auf die Reihenfolge der beiden Elemente an: Es gilt $(x, y) \neq (y, x)$, falls $x \neq y$. (Es müssen x und y beide in X und Y liegen, damit die fraglichen Paare in $X \times Y$ liegen. Wir denken bei dieser Bemerkung insbesondere an den wichtigen Fall $X = Y$.) Bezüglich Reihenfolge verhält sich also (x, y) anders als die Menge $\{x, y\}$, für die offenbar $\{x, y\} = \{y, x\}$ gilt. Übrigens sollte man die Notation $\{x, y\}$ nur benutzen, wenn $x \neq y$ ist (sonst notiert man die einelementige Menge natürlich als $\{x\}$), während ein geordnetes Paar (x, x) durchaus Sinn macht.

Bei n-Tupeln (wir nehmen hier der Einfachheit halber den Fall $X_1 = X_2 = \cdots = X_n =: X$ an) kommt es erst recht auf die Reihenfolge an: Wenn etwa x, y, z drei verschiedene Elemente aus X sind, dann können wir hieraus 6 verschiedene Tripel in $X \times X \times X$ bilden, nämlich

$$(x, y, z),\ (x, z, y),\ (y, x, z),\ (y, z, x),\ (z, x, y),\ (z, y, x) \;.$$

1.2.4 Mächtigkeit endlicher Mengen

Definition 1.2.11 (Mächtigkeit, Kardinalität)**.** Eine Menge M heißt *endlich*, wenn sie aus nur endlich vielen Elementen besteht. Andernfalls heißt sie *unendlich*. Die Anzahl der Elemente einer endlichen Menge heißt die *Mächtigkeit* oder auch *Kardinalität* von M, in Zeichen $|M|$ oder $\#M$.

In Abschnitt 1.4 kommen wir auf den Begriff der Mächtigkeit zurück und gehen dann auch auf unendliche Mengen ein.

Lemma 1.2.12. *Es seien M und N zwei endliche Mengen. Dann ist auch ihr kartesiches Produkt endlich und seine Mächtigkeit gleich dem Produkt der Mächtigkeiten von M und N:*

$$|M \times N| = |M| \cdot |N| \;.$$

Definition 1.2.13 (Potenzmenge)**.** Die Menge aller Teilmengen einer Menge M heißt *Potenzmenge* von M und wird mit $\mathcal{P}(M)$ bezeichnet:

$$\mathcal{P}(M) := \{X \mid X \subseteq M\} \;.$$

Beispiel. Es sei $M = \{x, y, z\}$. Dann ist

$$\mathcal{P}(M) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, M\} \ .$$

Lemma 1.2.14. *Wenn M eine endliche Menge ist, dann besteht $\mathcal{P}(M)$ aus $2^{|M|}$ Elementen:*

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

Definition 1.2.15 (Disjunktes Mengensystem, Partition)**.** Es sei M eine Menge und $\mathcal{S} \subseteq \mathcal{P}(M)$ ein Mengensystem über M.

a) Falls je zwei verschiedene Elemente X und Y von $\mathcal{S}$ disjunkt sind (d.h. $\forall X, Y \in \mathcal{S} : X \neq Y \Rightarrow X \cap Y = \emptyset$), so nennt man $\mathcal{S}$ ein *disjunktes Mengensystem*.

b) Ist $\mathcal{S}$ ein disjunktes Mengensystem über M, das nicht die leere Menge enthält, und ist jedes Element von M in einer (und damit in *genau* einer) Menge von $\mathcal{S}$ enthalten, dann heißt $\mathcal{S}$ *Partition* oder *Zerlegung* von M.

Beispiel. Es sei $M := \{a, b, c, d, e, f\}$. Dann ist $\mathcal{S} = \{\{c, e\}, \{b, d, f\}\}$ ein disjunktes Mengensystem und $\mathcal{S} \cup \{\{a\}\}$ ist eine Partition von M.

Das nächste Lemma folgt mit einem einfachen Abzählargument.

Lemma 1.2.16. *Ist M eine endliche Menge und $\mathcal{S}$ eine Partition von M, dann ist die Kardinalität von M die Summe der Kardinalitäten der Mengen in $\mathcal{S}$.*

1.3 Abbildungen

1.3.1 Abbildungsvorschrift, Definitions- und Bildbereich

Definition 1.3.1 (Abbildung)**.** Es seien X und Y zwei Mengen. Eine *Abbildung* von X in Y ist gegeben durch eine Vorschrift f, die jedem Element $x \in X$ genau ein Element $y \in Y$ zuordnet. Man schreibt $y = f(x)$ (lies: „f von x“). Für die gesamte Abbildung schreibt man

$$f : X \to Y \quad \text{(lies: „}f \text{ von } X \text{ nach } Y\text{“ oder „}\ldots \text{in Y“)}.$$

Für ein Element $x \in X$ benutzt man die Notation

$$x \mapsto f(x) \quad \text{(lies: „}x \text{ wird abgebildet auf } f(x)\text{“)}.$$

$f(x)$	heißt das *Bild von x unter f*.
X	heißt *Definitionsbereich*.
Y	heißt *Bildbereich* oder *Wertebereich*.

Wichtig: Zwei Abbildungen sind nur dann gleich, wenn die Vorschriften und auch die Definitions- und Bildbereiche übereinstimmen.

Die Abbildungen (1)–(3) des folgenden Beispiels sind alle verschieden, auch wenn die Vorschrift immer die gleiche, nämlich das Quadrieren einer Zahl ist.

Beispiele.

(1) $X = \mathbb{N}, \quad Y = \mathbb{N}, \quad f(x) = x^2$

(2) $X = \mathbb{Z}, \quad Y = \mathbb{N}_0, \quad f(x) = x^2$

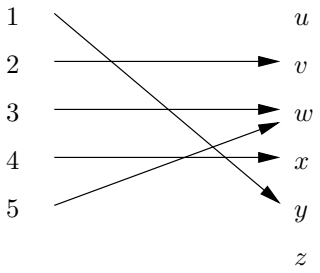
(3) $X = \mathbb{Z}, \quad Y = \mathbb{Z}, \quad f(x) = x^2$

(4) $X = Y = \mathbb{R}, \quad f(x) = e^x, \ \cos x, \ \sin x$
„Reelle Funktionen“, wie man sie in der Analysis studiert, sind ebenfalls Abbildungen.

(5) Die Menge X sei endlich. Dann kann die „Vorschrift“ als eine (endliche) Tabelle aufgefasst werden. Zum Beispiel: $X = \{1, 2, 3, 4, 5\}, \quad Y = \{u, v, w, x, y, z\}$

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

Veranschaulichung mit Pfeildiagramm:



Bei jedem Element des Definitionsbereichs X beginnt *genau ein* Pfeil.

Definition 1.3.2. Es seien X und Y zwei Mengen und $X' \subseteq X$. Die *Einschränkung* einer Abbildung $f : X \to Y$ auf X' ist die Abbildung

$$f|_{X'} : X' \to Y \qquad \text{mit} \qquad f|_{X'}(x) := f(x) \quad \text{für alle } x \in X'.$$

1.3.2 Bilder und Urbilder

Definition 1.3.3 (Bilder und Urbilder von Teilmengen)**.** Es sei $f : X \to Y$ eine Abildung.

a) Für $Z \subseteq X$ definieren wir

$$\begin{aligned} f(Z) := & \ \{y \in Y \mid \text{ es gibt ein } x \in Z \text{ mit } f(x) = y\} \\ = & \ \{f(x) \mid x \in Z\} \ . \end{aligned}$$

Wir nennen $f(Z)$ das *Bild von Z unter f*.

b) Die Menge $f(X)$ (also das Bild von ganz X unter f) heißt auch die *Bildmenge* oder einfach das *Bild* von f.

c) Für $Z \subseteq Y$ definieren wir $f^{-1}(Z) := \{x \in X \mid f(x) \in Z\}$ und nennen $f^{-1}(Z)$ das *Urbild von Z unter f*.

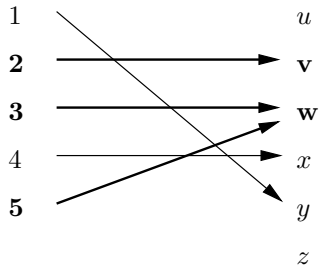
d) Für einelementiges $Z = \{z\}$ schreiben wir kurz $f^{-1}(z) := f^{-1}(\{z\})$.

Beispiele. Wir betrachten einige Beispielabbildungen von oben.

(1) $X = \mathbb{N},\ Y = \mathbb{N},\ f(x) = x^2$
$f(\{1,2,3\}) = \{1,4,9\}$
$f(\{5,7,12\}) = \{25,49,144\}$
$f^{-1}(\{25,36,49\}) = \{5,6,7\}$
$f^{-1}(\{10,11,12,\ldots,20\}) = \{4\}$
$f^{-1}(\{100,101,\ldots,200\}) = \{10,11,12,13,14\}$

(3) $X = \mathbb{Z},\ Y = \mathbb{Z},\ f(x) = x^2$
$f^{-1}(\{25\}) = \{5,-5\}$
$f^{-1}(\{25,36,49\}) = \{\pm 5, \pm 6, \pm 7\}$ (6 Elemente)
$f^{-1}(\{-1,-2,-3,\ldots\}) = \emptyset$

(5) $X = \{1,2,3,4,5\},\ Y = \{u,v,w,x,y,z\},\ f : X \to Y$



$f^{-1}(\{u,v\}) = \{2\}$
$f^{-1}(\{z\}) = \emptyset$
$f^{-1}(\{v,w\}) = \{2,3,5\}$

Lemma 1.3.4. *Ist $f : X \to Y$ eine Abbildung, so ist*

$$\mathcal{S} := \{f^{-1}(y) \mid y \in Y\} \setminus \{\emptyset\}$$

eine Partition von X.

Beweis. Wir zeigen zunächst, dass $\mathcal{S}$ ein disjunktes Mengensystem ist. Es seien $U, V \in \mathcal{S}$ mit $U \neq V$. Dann gibt es $u, v \in Y$ mit $u \neq v$, $U = f^{-1}(u)$ und $V = f^{-1}(v)$. Im Widerspruch zur Behauptung nehmen wir an, dass $x \in U \cap V$. Dann gilt $f(x) = u$, da $x \in U$, und $f(x) = v$, da $x \in V$, also $u = v$ — ein Widerspruch.

Um zu beweisen, dass $\mathcal{S}$ eine Partition ist, müssen wir noch zeigen, dass jedes $x \in X$ in einer Teilmenge aus $\mathcal{S}$ liegt. Das ist aber klar, da $x \in f^{-1}(f(x)) \in \mathcal{S}$. □

Beispiel. Wir betrachten noch einmal Beispiel (5) von oben. Hier gilt

$$\{f^{-1}(y) \mid y \in Y\} \setminus \emptyset \;=\; \{\{2\}, \{3,5\}, \{4\}, \{1\}\} \;,$$

was offenbar eine Partition der Menge $X = \{1,2,3,4,5\}$ ist.

1.3.3 Eigenschaften und Komposition von Abbildungen

Definition 1.3.5 (Injektivität, Surjektivität, Bijektivität)**.** Eine Abbildung $f : X \to Y$ heißt

a) *injektiv* $:\Longleftrightarrow$ $(\forall x, y \in X : x \neq y \Rightarrow f(x) \neq f(y))$;
d.h. verschiedene Elemente in X haben auch verschiedene Bilder unter f.

b) *surjektiv* $:\Longleftrightarrow$ $f(X) = Y$;
d.h. jedes Element in Y kommt als Bild unter f vor.

c) *bijektiv* $:\Longleftrightarrow$ f ist injektiv und surjektiv.

Im Pfeildiagramm bedeuten diese Eigenschaften:

injektiv	:	Es laufen keine zwei Pfeile zusammen.
surjektiv	:	Bei jedem $y \in Y$ endet ein Pfeil.
bijektiv	:	Bei jedem $y \in Y$ endet genau ein Pfeil.

Aus einer beliebigen Abbildung $f : X \to Y$ kann man leicht eine surjektive Abbildung konstruieren: Man ersetze nämlich Y durch die Bildmenge $f(X)$.

Definition 1.3.6 (Graph)**.** Es sei $f : X \to Y$ eine Abbildung. Der *Graph* von f ist definiert als

$$\Gamma_f := \{(x, f(x)) \mid x \in X\} \subseteq X \times Y \;.$$

Definition 1.3.7 (Komposition von Abbildungen)**.** Es seien $f : X \to Y$ und $g : Y' \to Z$ zwei Abbildungen, wobei der Wertebereich der ersten im Definitionsbereich der zweiten enthalten ist, d.h. $Y \subseteq Y'$. Die *Komposition*, *Verkettung* oder *Hintereinanderausführung*

$$g \circ f : X \to Z$$

(lies: „g nach f“) ist definiert durch

$$(g \circ f)(x) = g(f(x)) \quad \text{für alle } x \in X \;.$$

Lemma 1.3.8. *Es seien X, Y und Z Mengen und $f : X \to Y$ und $g : Y \to Z$ zwei Abbildungen.*

a) Sind f und g injektiv, so ist auch $g \circ f : X \to Z$ injektiv.

b) Sind f und g surjektiv, so ist auch $g \circ f : X \to Z$ surjektiv.

c) Sind f und g bijektiv, so ist auch $g \circ f : X \to Z$ bijektiv.

Beweis. Zu a): Es seien $x, x' \in X$ mit $x \neq x'$. Da f injektiv ist, folgt $f(x) \neq f(x')$. Da g auch injektiv ist, folgt daraus $g(f(x)) \neq g(f(x'))$, so dass also $g \circ f$ injektiv ist.

Zu b): Es sei $z \in Z$. Da g surjektiv ist, gibt es ein $y \in Y$ mit $g(y) = z$. Da f surjektiv ist, gibt es ein $x \in X$ mit $f(x) = y$. Damit gilt also $(g \circ f)(x) = g(f(x)) = g(y) = z$ und folglich ist $g \circ f$ surjektiv.

Teil c) folgt nach Definition 1.3.5 aus a) und b). □

Lemma 1.3.9. *Die Komposition von Abbildungen ist assoziativ, d.h. wenn $f : X \to Y$, $g : Y' \to Z$, $h : Z' \to W$ drei Abbildungen sind mit $Y \subseteq Y'$ und $Z \subseteq Z'$, so ist*

$$h \circ (g \circ f) = (h \circ g) \circ f \ .$$

Beweis. Für jedes beliebige Element $x \in X$ gilt

$$\begin{array}{rcccl} (h \circ (g \circ f))(x) & = & h((g \circ f)(x)) & = & h(g(f(x))) \ , \\ ((h \circ g) \circ f)(x) & = & (h \circ g)(f(x)) & = & h(g(f(x))) \ . \end{array}$$

Also sind die Abbildungsvorschriften gleich:

$$h \circ (g \circ f) = (h \circ g) \circ f \ .$$

Der Definitionsbereich X und der Zielbereich W stimmen ebenfalls überein. □

Definition 1.3.10 (Identische Abbildung)**.** Es sei X irgendeine Menge. Die *identische Abbildung*

$$\mathrm{id}_X : X \to X$$

ist definiert durch $\mathrm{id}_X(x) = x$ für alle $x \in X$.

Bemerkung. Für eine beliebige Abbildung $f : X \to Y$ gilt

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f \ .$$

1.3.4 Bijektive Abbildungen

Satz 1.3.11 (Umkehrabbildung)**.** *Es sei $f : X \to Y$ eine Abbildung.*

a) Die folgenden beiden Eigenschaften sind äquivalent:

(a1) f ist bijektiv.

(a2) Es gibt eine Abbildung $g : Y \to X$ mit
$g(f(x)) = x$ für alle $x \in X$, d.h. $g \circ f = \mathrm{id}_X$ und
$f(g(y)) = y$ für alle $y \in Y$, d.h. $f \circ g = \mathrm{id}_Y$.

Die Abbildung g ist eindeutig und heißt die zu f inverse Abbildung*, oder* Umkehrabbildung *von f. Man schreibt auch $g = f^{-1}$.*

b) Wenn $f : X \to Y$ bijektiv ist, so ist auch $f^{-1} : Y \to X$ bijektiv und es gilt $(f^{-1})^{-1} = f$.

Beweis. Zu a): Nach Satz 1.1.4 j) sind zwei Implikationen zu zeigen:

„(a1) $\Longrightarrow$ (a2)“: Zu jedem $y \in Y$ gibt es *genau ein* $x \in X$ mit $f(x) = y$, denn f ist surjektiv und injektiv. Definiere nun eine Abbildung $g : Y \to X$ gemäß $g(y) := x$. Dann gilt nach Konstruktion

$$g(f(x)) = x \quad \text{für alle } x \in X \ ,$$

wie unter (a2) als erstes behauptet. Wir zeigen nun die zweite Behauptung unter (a2). Es sei $y \in Y$ beliebig. Weil f surjektiv ist, existiert ein $x \in X$ mit $f(x) = y$. Es folgt

$$f(g(y)) = f(g(f(x))) = f(x) = y \ ,$$

wie gewünscht.

„(a2) $\Longrightarrow$ (a1)“: Wir müssen zeigen, dass f sowohl injektiv als auch surjektiv ist. Wir beginnen mit der Injektivität: Es seien $x, x' \in X$ mit $f(x) = f(x')$. Dann ist $x = g(f(x)) = g(f(x')) = x'$, wie gewünscht.

Es bleibt zu zeigen, dass f surjektiv ist: Es sei $y \in Y$ gegeben. Setze $x := g(y)$. Dann ist

$$f(x) = f(g(y)) = y \ ,$$

wie gewünscht.

Wir beweisen als nächstes die Eindeutigkeit von g: Angenommen $h : Y \to X$ hat die gleichen Eigenschaften wie g. Dann gilt

$$h = h \circ \mathrm{id}_Y = h \circ (f \circ g) = (h \circ f) \circ g = \mathrm{id}_X \circ g = g \ .$$

Teil b) des Satzes folgt schließlich aus a). □

Lemma 1.3.12. *Es seien X, Y und Z Mengen und $f : X \to Y$ und $g : Y \to Z$ bijektive Abbildungen. Dann gilt*

$$(g \circ f)^{-1} \ = \ f^{-1} \circ g^{-1} \ .$$

Beweis. Es gilt wegen Lemma 1.3.9 (Assoziativität)

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) \;=\; f^{-1} \circ ((g^{-1} \circ g) \circ f) \;=\; f^{-1} \circ (\mathrm{id}_Y \circ f) \;=\; f^{-1} \circ f \;=\; \mathrm{id}_X \;,$$

und

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) \;=\; (g \circ (f \circ f^{-1})) \circ g^{-1} \;=\; (g \circ \mathrm{id}_Y) \circ g^{-1} \;=\; g \circ g^{-1} \;=\; \mathrm{id}_Z \;.$$

Die Behauptung folgt damit aus Satz 1.3.11. □

1.4 Mächtigkeit von Mengen

Wir betrachten zunächst noch einmal endliche Mengen.

Satz 1.4.1. *Es seien X und Y endliche Mengen.*

a) Es gibt eine surjektive Abbildung von X nach Y genau dann, wenn $|X| \geq |Y|$.

b) Es gibt eine injektive Abbildung von X nach Y genau dann, wenn $|X| \leq |Y|$.

c) Es gibt eine bijektive Abbildung von X nach Y genau dann, wenn $|X| = |Y|$.

Beweis. Es seien $X = \{x_1, x_2, \ldots, x_{|X|}\}$ und $Y = \{y_1, y_2, \ldots, y_{|Y|}\}$.

Zu a): Wir nehmen zunächst an, dass $f : X \to Y$ surjektiv ist. Betrachte die Partition $\mathcal{S} = \{f^{-1}(y) \mid y \in Y\}$ von X. Da die Kardinalität von X nach Lemma 1.3.4 und Lemma 1.2.16 die Summe der Kardinalitäten der nichtleeren Mengen $f^{-1}(y)$ über alle $y \in Y$ ist, gilt

$$|X| = \underbrace{|f^{-1}(y_1)|}_{\geq 1} + \underbrace{|f^{-1}(y_2)|}_{\geq 1} + \cdots + \underbrace{|f^{-1}(y_{|Y|})|}_{\geq 1} \geq |Y| \;.$$

Ist umgekehrt $|X| \geq |Y|$, dann ist die Abbildung $f : X \to Y$ mit

$$f(x_i) := \begin{cases} y_i & \text{falls } i \leq |Y|, \\ y_{|Y|} & \text{sonst,} \end{cases}$$

nach Definition surjektiv.

Teil b) zeigt man analog. Teil c) folgt schließlich aus a) und b). □

Satz 1.4.1 c) motiviert die folgende Definition für den Fall unendlicher Mengen.

Definition 1.4.2 (Abzählbarkeit, Überabzählbarkeit)**.**

a) Zwei undendliche Mengen X und Y heißen *gleichmächtig* oder *von gleicher Kardinalität*, wenn es eine bijektive Abbildung von X nach Y (und damit auch eine bijektive Abbildung von Y nach X) gibt.

b) Eine Menge M heißt *abzählbar unendlich* oder kurz *abzählbar*, falls es eine bijektive Abbildung von $\mathbb{N}$ auf M gibt.

c) Eine unendliche Menge, die nicht abzählbar ist, heißt *überabzählbar*.

Beispiele.

(i) Die Mengen $\mathbb{N}$ und $\mathbb{N}_0$ sind gleichmächtig, da die Abbildung $\text{pred} : \mathbb{N} \to \mathbb{N}_0$ mit $\text{pred}(n) := n - 1$ bijektiv ist. (Der Name *pred* kommt von *predecessor* — Vorgänger.) Insbesondere ist also $\mathbb{N}_0$ abzählbar unendlich.

(ii) Die Mengen $\mathbb{N}_0$ und $\mathbb{Z}$ sind gleichmächtig, da die Abbildung $f : \mathbb{N}_0 \to \mathbb{Z}$ mit

$$f(n) := \begin{cases} \frac{n+1}{2} & \text{falls } n \text{ ungerade,} \\ -\frac{n}{2} & \text{falls } n \text{ gerade,} \end{cases}$$

bijektiv ist. Die Komposition der bijektiven Abbildungen pred und f zu $f \circ \text{pred} : \mathbb{N} \to \mathbb{Z}$ zeigt nach Lemma 1.3.8 c), dass auch $\mathbb{Z}$ abzählbar unendlich ist.

(iii) Es sei $J := \{x \in \mathbb{R} \mid 0 < x < 1\}$. Dann sind J und $\mathbb{R}$ gleichmächtig. Um dies zu zeigen, betrachte man die Abbildung $f : J \to \mathbb{R}$ mit

$$f(x) := \frac{x - \frac{1}{2}}{x(1-x)} \ .$$

Mit einfachen Methoden der Analysis kann man zeigen, dass f bijektiv ist.

Satz 1.4.3. *Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar.*

Beweisskizze. Der Beweis verwendet das *Diagonalisierungsschema von Cauchy*. Wir betrachten die folgende unendlich große Tabelle, in der alle Brüche $\frac{p}{q}$ mit $p, q \in \mathbb{N}$ stehen:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \cdots \\ \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Man beachte, dass jede rationale Zahl mehrfach in dieser Tabelle auftaucht. So steht beispielsweise auf der Diagonalen (von links oben nach rechts unten) überall die Zahl eins. Wir können alle Brüche dieser Tabelle aufzählen, indem wir die Tabelle wie folgt durchlaufen:

$$1 \quad 2 \quad \tfrac{1}{2} \quad \tfrac{1}{3} \quad \tfrac{2}{2} \quad 3 \quad 4 \quad \tfrac{3}{2} \quad \tfrac{2}{3} \quad \tfrac{1}{4} \quad \tfrac{1}{5} \quad \tfrac{2}{4} \quad \tfrac{3}{3} \quad \tfrac{4}{2} \quad 5 \quad 6 \quad \tfrac{5}{2} \quad \tfrac{4}{3} \quad \ldots$$

Löscht man aus dieser unendlichen Folge alle doppelten Zahlen, so erhält man die unendliche Folge

$$1 \quad 2 \quad \tfrac{1}{2} \quad \tfrac{1}{3} \quad 3 \quad 4 \quad \tfrac{3}{2} \quad \tfrac{2}{3} \quad \tfrac{1}{4} \quad \tfrac{1}{5} \quad 5 \quad 6 \quad \tfrac{5}{2} \quad \tfrac{4}{3} \quad \dots \ ,$$

in der jede positive rationale Zahl genau einmal vorkommt. Wir können daraus leicht eine bijektive Abbildung f von $\mathbb{N}$ in die positiven rationalen Zahlen konstruieren, indem wir $f(n)$ für alle $n \in \mathbb{N}$ als die n-te Zahl in dieser Folge definieren. Damit haben wir gezeigt, dass die Menge der positiven rationalen Zahlen abzählbar ist. Die modifizierte Folge

$$0 \quad 1 \quad -1 \quad 2 \quad -2 \quad \tfrac{1}{2} \quad -\tfrac{1}{2} \quad \tfrac{1}{3} \quad -\tfrac{1}{3} \quad 3 \quad -3 \quad 4 \quad -4 \quad \tfrac{3}{2} \quad -\tfrac{3}{2} \quad \tfrac{2}{3} \quad -\tfrac{2}{3} \quad \dots$$

liefert mit derselben Definition eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{Q}$. □

Man kann zeigen, dass die Menge der reellen Zahlen $\mathbb{R}$ überabzählbar ist. Da man dazu etwas Hintergrundwissen über reelle Zahlen benötigt, beweisen wir hier zunächst ein verwandtes Resultat. Die Beweisidee ist für die reelen Zahlen jedoch dieselbe.

Satz 1.4.4. *Die Menge* $\{0,1\}^{\mathbb{N}}$ *aller Abbildungen von* $\mathbb{N}$ *nach* $\{0,1\}$ *(formal:* $\{0,1\}^{\mathbb{N}} := \{\varphi \mid \varphi : \mathbb{N} \to \{0,1\}\}$*) ist überabzählbar.*

Wir können uns die Menge $\{0,1\}^{\mathbb{N}}$ als die Menge aller (unendlich langen) Folgen von Nullen und Einsen vorstellen.

Beweis. Wir führen einen Widerspruchsbeweis. Wir nehmen an, die Menge $\{0,1\}^{\mathbb{N}}$ sei abzählbar unendlich. Dann gibt es eine bijektive Abbildung $f : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Für $n \in \mathbb{N}$ sei $\varphi_n := f(n)$. Wir betrachten die folgende unendlich große Tabelle:

$$\begin{array}{cccccc}
\varphi_1(1) & \varphi_1(2) & \varphi_1(3) & \varphi_1(4) & \cdots \\
\varphi_2(1) & \varphi_2(2) & \varphi_2(3) & \varphi_2(4) & \cdots \\
\varphi_3(1) & \varphi_3(2) & \varphi_3(3) & \varphi_3(4) & \cdots \\
\varphi_4(1) & \varphi_4(2) & \varphi_4(3) & \varphi_4(4) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Die i-te Zeile entspricht der Abbildung $\varphi_i \in \{0,1\}^{\mathbb{N}}$, also einer Folge von Nullen und Einsen. Da f bijektiv und damit insbesondere surjektiv ist, muss jede mögliche Folge von Nullen und Einsen einer Zeile dieser Tabelle entsprechen. Betrachte die Abbildung $\varphi : \mathbb{N} \to \{0,1\}$, die definiert ist durch $\varphi(n) := 1 - \varphi_n(n)$ für alle $n \in \mathbb{N}$. Anschaulich gesprochen haben wir die Folge von Nullen und Einsen definiert, die man erhält, wenn man entlang der Diagonale der Tabelle von links oben nach rechts unten geht und dabei Nullen und Einsen miteinander vertauscht. Es bleibt zu zeigen, dass $\varphi \neq \varphi_k$ für alle $k \in \mathbb{N}$ und damit $\varphi \notin f(\mathbb{N})$. Das ist aber klar, da $\varphi(k) = 1 - \varphi_k(k) \neq \varphi_k(k)$.

Damit haben wir einen Widerspruch zu unserer ursprünglichen Annahme erzielt. Folglich ist die Menge $\{0,1\}^{\mathbb{N}}$ überabzählbar. □

Das im Beweis verwendete Verfahren heißt *Diagonalverfahren von Cantor*. Es findet auch im Rahmen der Komplexitätstheorie Anwendung. Man verwendet es dort um zu zeigen, dass es sogenannte nicht-entscheidbare Probleme gibt, also Probleme, die nicht von Computern gelöst werden können.

1.5 Relationen

In diesem Abschnitt werden Relationen allgemein eingeführt. Es werden verschiedene Sichtweisen des Relationsbegriffs erläutert und der Zusammenhang zu dem bekannten Begriff einer Abbildung (Funktion) geklärt. Ähnlich wie Mengen und Abbildungen gehören Relationen zum Grundhandwerkszeug der modernen Mathematik (wie auch der Informatik). Zwar gibt es keine tief liegende Theorie über allgemeine Relationen, aber sie dienen zur Beschreibung und Formalisierung von zahlreichen Problemfeldern und sind von daher allgegenwärtig.

1.5.1 Grundbegriffe und Notationen

Informelle Definition. Eine *(binäre) Relation* auf einer Menge M bezieht sich auf je zwei Elemente $a, b \in M$ (unter Beachtung der Reihenfolge). Es wird festgelegt, ob a und b „in Relation stehen“ oder nicht. *Wie* dieses festgelegt wird, hängt von der Situation ab.

Verallgemeinerungen: Die Elemente a und b können aus verschiedenen Mengen M_1 und M_2 kommen; statt zwei Elemente kann eine Relation n Elemente für ein festes n betrachten. Die folgenden einfachen Beispiele illustrieren das Konzept.

Beispiele (Relationen I)**.**

(i) Die *Gleichheitsrelation* $x = y$ auf einer beliebigen Menge M.

(ii) Die *Teilbarkeitsrelation* $a \mid b$ („a teilt b“) auf der Menge $\mathbb{Z}$.

(iii) Die Anordnung $a \leq b$ („a ist kleiner oder gleich b“) auf $\mathbb{N}$, $\mathbb{Z}$ oder $\mathbb{R}$.

(iv) Die Relation $\parallel$ („parallel“) auf der Menge $\mathcal{G}$ aller Geraden in der Ebene $\mathbb{R}^2$:

$$g \parallel h \ :\Longleftrightarrow \ (g = h \ \vee \ g \cap h = \emptyset), \text{ für } g, h \in \mathcal{G}.$$

(v) Die Relation „ist Teilmenge von“ auf der Potenzmenge $\mathcal{P}(M)$ einer gegebenen Menge M. Notation: $A \subseteq B$ für $A, B \in \mathcal{P}(M)$.

Wir sehen, dass es für übliche Relationen Standardbezeichnungen gibt; das *Relationssymbol* (z.B. $=$, $\mid$, $\leq$, $\parallel$, $\subseteq$) steht dabei zwischen den in Frage stehenden Elementen (sogenannte *Infix-Notation*). Eine allgemeine Relation würden wir

etwa mit $\mathcal{R}$ bezeichnen und dann $a\mathcal{R}b$ schreiben, wenn a und b in Relation zueinander stehen. Für jede Relation $\mathcal{R}$ auf einer Menge M können wir die Menge aller geordneten Paare aus in Relation stehenden Elementen betrachten:

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

Aus dieser Menge von Paaren kann man die Relation in offensichtlicher Weise zurückgewinnen:

$$x\mathcal{R}y \iff (x, y) \in R \ .$$

Entsprechendes gilt natürlich auch für eine Relation zwischen den Elementen von zwei verschiedenen Mengen. Diese Überlegungen motivieren die übliche mengentheoretische Definition einer Relation.

Definition 1.5.1 (Relation)**.**

a) Eine *binäre Relation* R zwischen den Mengen M_1 und M_2 ist eine Teilmenge des kartesischen Produktes $M_1 \times M_2$, also $R \subseteq M_1 \times M_2$. Im Fall $M_1 = M_2 =: M$ nennt man sie auch *Relation in* (oder *auf*) M.

   Für $(x, y) \in R$ benutzt man die Sprechweise: „x und y stehen in der Relation R“.

b) Eine *n-äre* oder *n-stellige Relation* zwischen n Mengen $M_1, M_2, \ldots, M_n$ ist eine Teilmenge von $M_1 \times M_2 \times \cdots \times M_n$.

Die Infix-Notation benutzt man auch, wenn es kein spezielles Symbol für die Relation (im Unterschied zur Paarmenge) gibt. Die Schreibweise ist dann also $xR\,y$ statt $(x, y) \in R$. Für die Negation der Relation, also $(x, y) \notin R$, schreibt man auch kurz $x\not{R}\,y$. Wir geben im Folgenden noch einige Beispiele von Relationen in Mengennotation an.

Beispiel (Relationen II)**.**

(i) $M_1 = M_2 = \mathbb{R}$, $R_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\}$.

(ii) $M_1 = M_2 = \mathbb{R}$, $R_2 = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$.

(iii) $M_1 := M$ beliebige Menge, $M_2 := \mathcal{P}(M)$ die Potenzmenge von M, $R_3 = \{(x, Y) \in M \times \mathcal{P}(M) \mid x \in Y\}$.

(iv) Die Elemente von $\mathbb{R}^2$ fassen wir wie üblich als Punkte der Ebene auf. Eine ternäre (dreistellige) Relation $R_4 \subset \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2$ ist gegeben durch

$$R_4 = \{(P_1, P_2, P_3) \mid P_1, P_2, P_3 \text{ liegen auf einer Geraden}\} \ .$$

(v) $M_1 = M_2 = M_3 = \mathbb{Z}$, $R_5 = \{(x, y, z) \in \mathbb{Z}^3 \mid x \leq y \leq z\}$.

Weiter oben haben wir den Begriff der Abbildung (Funktion) eingeführt („eindeutige Zuordnung“). Als mengentheoretisch präzise Definition gibt es den *Graphen*

$$\Gamma_f = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$$

einer Abbildung $f : X \to Y$. Der Graph ist eine Teilmenge von $X \times Y$, formal also eine Relation zwischen X und Y. Jede Abbildung stellt also insbesondere eine Relation dar. Wir fassen diese Beobachtung in der folgenden Bemerkung zusammen.

Bemerkung. Jede Abbildung $f : X \to Y$ kann als Relation aufgefasst werden: Jedes $x \in X$ steht mit seinem eindeutigen Bild $f(x)$ und keinem weiteren Element aus Y in Relation. Als Teilmenge von $X \times Y$ aufgefasst stimmt die Relation mit dem Graphen der Abbildung überein.

1.5.2 Verkettung und Inverse

Die folgende Definition der Verkettung zweier Relationen ist eine natürliche Verallgemeinerung der Verkettung von Abbildungen.

Definition 1.5.2 (Verkettung von Relationen)**.** Es seien M_1, M_2 und M_3 Mengen, R eine Relation zwischen M_1 und M_2 und S eine Relation zwischen M_2 und M_3. Das *Produkt* oder die *Komposition* $S \circ R$ von R und S ist die wie folgt definierte Relation zwischen M_1 und M_3:

$$S \circ R := \{(x, z) \in M_1 \times M_3 \mid \exists y \in M_2 : xRy \wedge ySz \}.$$

Bemerkung. Man beachte besonders die Reihenfolge der Faktoren in $S \circ R$. Diese wird wegen des (formalen) Spezialfalles der Abbildungen so definiert (Verkettung $x \mapsto g(f(x))$). Die Infix-Notation xRy, ySz würde eher die Notation $R \circ S$ nahelegen.

Definition 1.5.3 (Inverse Relation)**.** Es sei R eine Relation zwischen M_1 und M_2. Die zu R *inverse Relation* $R^{-1} \subseteq M_2 \times M_1$ ist dann wie folgt definiert:

$$R^{-1} := \{(y, x) \in M_2 \times M_1 \mid xRy\} \ .$$

Beispiele.

(i) Die Inverse der Kleiner-oder-Gleich-Relation von Zahlen $x \leq y$ ist definitionsgemäß die *Größer-oder-Gleich-Relation* $y \geq x$.

(ii) Die Inverse der Teilbarkeitsrelation $a \mid b$ in $\mathbb{Z}$ ist die *Vielfachen-Relation*.

(iii) Die Inverse einer bijektiven Abbildung, aufgefasst als Relation, ist die bekannte Umkehrabbildung (inverse Abbildung); siehe Satz 1.3.11.

Bemerkung.

a) Für eine beliebige Relation R gilt $(R^{-1})^{-1} = R$. Anders als bei bijektiven Abbildungen ist aber $R \circ R^{-1}$ in der Regel nicht die Gleichheitsrelation.

b) Unmittelbar aus der Definition der Komposition ergibt sich auch die folgende Beobachtung: Es sei R eine Relation zwischen M_1 und M_2 und S eine Relation zwischen M_2 und M_3. Dann gilt

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1} \ .$$

Für bijektive Abbildungen hatten wir das schon in Lemma 1.3.12 beobachtet.

1.5.3 Äquivalenzrelationen

Eine Relation auf einer Menge M heißt Äquivalenzrelation, wenn sie die charakteristischen Eigenschaften der Gleichheitsrelation besitzt. Nach der genauen Definition und einigen einfachen Beispielen zeigen wir, dass jede beliebige Äquivalenzrelation eine Partition von M liefert. Es gilt auch die Umkehrung: Zu einer Partition von M kann man leicht eine Relation auf M definieren, die sich als Aquivalenzrelation herausstellt.

Definition 1.5.4 (Äquivalenzrelation)**.** Es sei M eine nichtleere Menge und $\sim$ eine binäre Relation auf M mit den folgenden Eigenschaften:

(i) Für alle $x \in M$ gilt $x \sim x$ (*Reflexivität*)

(ii) Für alle $x, y \in M$ gilt: $x \sim y \ \Rightarrow \ y \sim x$ (*Symmetrie*)

(iii) Für alle $x, y, z \in M$ gilt: $(x \sim y \ \wedge \ y \sim z) \ \Rightarrow \ x \sim z$ (*Transitivität*)

Dann heißt $\sim$ eine *Äquivalenzrelation*. Für $x \in M$ nennt man die Menge $[x]_\sim := \{y \in M \mid x \sim y\}$ die *Äquivalenzklasse von* x.

Bemerkung.

(i) Die in Definition 1.5.4 (ii) geforderte Symmetrie kann man alternativ auch wie folgt definieren. Eine Relation R auf der Menge M ist *symmetrisch*, falls $R = R^{-1}$.

(ii) Aus Definition 1.5.4 (i) und (iii) folgt für eine Äquivalenzrelation R auf einer Menge M, dass $R = R \circ R$.

Beispiele.

(i) Es seien X und Y nichtleere Mengen und $f : X \to Y$ eine Abbildung. Dann ist die (binäre) Relation $\sim_f$ auf X mit

$$x \sim_f x' \ :\Leftrightarrow f(x) = f(x')$$

eine Äquivalenzrelation. Die Äquivalenzklassen sind die Urbildmengen $f^{-1}(y)$ für $y \in f(X)$.

(ii) Eine Äquivalenzrelation auf $\mathbb{Z}$ kann wie folgt definiert werden:

$$x \sim y \ :\Leftrightarrow \ x - y \text{ gerade.}$$

Die beiden verschiedenen Äquivalenzklassen sind

$$[0]_\sim = \{2k \mid k \in \mathbb{Z}\} \quad \text{und} \quad [1]_\sim = \{2k+1 \mid k \in \mathbb{Z}\} \ .$$

(iii) Es sei $M := \mathbb{Z} \times \mathbb{N}$ und $\sim$ die durch

$$(p, q) \sim (p', q') \ :\Longleftrightarrow \ p \cdot q' = p' \cdot q$$

definierte Relation. Dann ist $\sim$ eine Äquivalenzrelation. Diese Äquivalenzrelation spielt bei der formalen Definition der rationalen Zahlen eine tragende Rolle (siehe unten).

Satz 1.5.5.

a) Es sei $\sim$ eine Äquivalenzrelation auf der Menge M. Dann gilt:

(a1) Für $x, y \in M$ gilt: $[x]_\sim \neq [y]_\sim \ \Rightarrow \ [x]_\sim \cap [y]_\sim = \emptyset$.

(a2) Es sei $\mathcal{Z} := \{[x]_\sim \mid x \in M\}$ die Menge der Äquivalenzklassen. Dann ist $\mathcal{Z}$ eine Partition von M.

b) Ist M eine Menge und $\mathcal{Z} = \{Z_i \mid i \in I\}$ eine Partition von M, dann ist die durch

$$x \sim y \ :\Leftrightarrow \ x \text{ und } y \text{ liegen in derselben Teilmenge } Z_i$$

definierte Relation $\sim$ auf M eine Äquivalenzrelation, deren Äquivalenzklassen gerade die Z_i sind.

Beweis. Zu (a1): Es sei $[x]_\sim \cap [y]_\sim \neq \emptyset$. Wir müssen zeigen, dass dann $[x]_\sim = [y]_\sim$. Es sei $z \in [x]_\sim \cap [y]_\sim$ und $u \in [x]_\sim$ beliebig. Wegen Symmetrie ist $y \sim z \sim x \sim u$ und daher wegen Transitivität $y \sim u$, so dass $u \in [y]_\sim$. Damit haben wir gezeigt, dass $[x]_\sim \subseteq [y]_\sim$. Analog kann man zeigen, dass $[y]_\sim \subseteq [x]_\sim$ und damit $[x]_\sim = [y]_\sim$.

Zu (a2): Wegen (a1) ist $\mathcal{Z}$ ein disjunktes Mengensystem. Aus der Reflexivität von $\sim$ folgt, dass $x \in [x]_\sim$ für alle $x \in M$. Daher ist $\mathcal{Z}$ eine Partition von M.

Zu (b): Man überzeugt sich leicht davon, dass die so definierte Relation reflexiv, symmetrisch und transitiv ist. □

Die Äquivalenzklassen einer Äquivalenzrelation kann man als Elemente einer neuen Menge (sogenannte *Faktormenge* oder *Quotientenmenge*) auffassen. Dieses ist ein wichtiges Prinzip zur Konstruktion neuer mathematischer Objekte aus bekannten, das insbesondere bei algebraischen Strukturen genutzt wird. In diesem Zusammenhang interessiert man sich auch für sogenannte Vertretersysteme (Repräsentantensysteme) einer Klasseneinteilung bzw. Äquivalenzrelation.

Definition 1.5.6 (Repräsentantensystem)**.** Es sei $\sim$ eine Äquivalenzrelation auf der Menge M und $\mathcal{Z}$ die Menge der Äquivalenzklassen. Ist $\varrho : \mathcal{Z} \to M$ eine Abbildung mit $\varrho([x]_\sim) \in [x]_\sim$ für alle $x \in M$, dann heißt das Bild $\varrho(\mathcal{Z})$ *Repräsentantensystem* für $\sim$.

Beispiel. Wir skizzieren kurz, wie die rationalen Zahlen $\mathbb{Q}$ aus den ganzen Zahlen $\mathbb{Z}$ „konstruiert“ werden können. Dazu betrachten wir zunächst noch einmal ein Beispiel von oben: Es sei $M := \mathbb{Z} \times \mathbb{N}$ und $\sim$ die durch

$$(p,q) \sim (p',q') \;:\Longleftrightarrow\; p \cdot q' = p' \cdot q \quad \left(\iff \frac{p}{q} = \frac{p'}{q'} \right)$$

definierte Äquivalenzrelation.

Für $(p,q) \in M$ erhält man durch Kürzen des Bruches $\frac{p}{q}$ zu $\frac{p'}{q'}$ das eindeutige teilerfremde Zahlenpaar $(p',q') \in M$ mit $(p,q) \sim (p',q')$. Definiert man $\varrho([(p,q)]_\sim) := (p',q')$ so erhält man eine bijektive Abbildung zwischen der Menge der Äquivalenzklassen und den teilerfremden Zahlenpaaren in M. Letztere bilden also ein Repräsentantensystem. Man hat damit insbesondere eine bijektive Abbildung zwischen den Äquivalenzklassen und den rationalen Zahlen $\mathbb{Q}$ definiert. Die rationalen Zahlen können also mit den Äquivalenzklassen identifiziert werden. Wir werden diesen Zusammenhang im nächsten Kapitel weiter vertiefen.

1.5.4 Ordnungsrelationen

Definition 1.5.7 (Ordnungsrelation)**.**

a) Eine *Halbordnung (partielle Ordnung)* auf einer Menge M ist eine Relation $\preceq$ auf M mit

   (i) Für alle $x \in M$ gilt: $x \preceq x$ (Reflexivität)

   (ii) Für alle $x, y \in M$ gilt: $(x \preceq y \;\wedge\; y \preceq x) \;\Rightarrow\; x = y$ (Antisymmetrie)

   (iii) Für alle $x, y, z \in M$ gilt: $(x \preceq y \;\wedge\; y \preceq z) \;\Rightarrow\; x \preceq z$ (Transitivität)

   Die Menge zusammen mit der Relation $(M, \preceq)$ wird ebenfalls als Halbordnung bezeichnet, im Englischen *poset* (partially ordered set).

b) Eine *totale Ordnung* oder *lineare Ordnung* ist eine Halbordnung, in der je zwei Elemente vergleichbar sind:

$$\forall x, y \in M : x \preceq y \;\vee\; y \preceq x \;.$$

Wenn eine Halbordnung (totale Ordnung) $(M, \preceq)$ gegeben ist, sagt man auch bequem, aber etwas unpräzise: Die Menge M ist partiell (linear) geordnet. Der Begriff der „Ordnungsrelation“ oder einfach „Ordnung“ oder „Anordnung“ wird ebenfalls verwendet, ist aber nicht einheitlich definiert: Oft werden nur die Eigenschaften einer Halbordnung verlangt, anderswo ist eine Ordnung immer linear. Auch die Reflexivität (die in gewissem Sinne unwesentlich ist, siehe unten) wird nicht immer gefordert.

Beispiele.

(i) Die übliche Anordnung, also die Kleiner-oder-Gleich-Relation $x \leq y$ auf $\mathbb{N}$, $\mathbb{Z}$ oder $\mathbb{R}$ ist eine Halbordnung, sogar eine lineare Ordnung.

(ii) Die Teilbarkeitsrelation $a \mid b$ auf $\mathbb{N}$ ist eine Halbordnung.

(iii) Die Inklusions-Relation $\subseteq$ ist eine Halbordnung auf der Potenzmenge $\mathcal{P}(M)$ einer beliebigen Menge M.

Bemerkung. Wenn $\preceq$ eine Halbordnung auf M ist und wir

$$x \succeq y \;:\Leftrightarrow\; y \preceq x$$

definieren, dann ist auch $(M, \succeq)$ eine Halbordnung. Sie heißt die zu $(M, \preceq)$ *duale Halbordnung. (Man beachte, dass die hier definierte Relation $\succeq$ genau die inverse Relation zur gegebenen Relation $\preceq$ im Sinn der allgemeinen Definition 1.5.3 ist.)*

Bemerkung. Für eine gegebene Halbordnung $(M, \preceq)$ ist die durch

$$x \prec y \;:\Leftrightarrow\; x \preceq y \;\wedge\; x \neq y$$

definierte Relation $\prec$ („*strikte Ordnung*“) weiterhin antisymmetrisch und transitiv. Wenn umgekehrt eine antisymmetrische und transitive Relation $\prec$ gegeben ist, dann ist die durch

$$x \preceq y \;:\Leftrightarrow\; x \prec y \;\vee\; x = y$$

definierte Relation eine Halbordnung.

Halbordnungen lassen sich mit Hilfe von sogenannten *Hasse-Diagrammen* veranschaulichen. Dabei gilt $x \prec y$, wenn eine Verbindung zwischen x und y besteht, x aber tiefer als y liegt.

Beispiele.

(i) In Abbildung 1.1 ist das Hasse-Diagramm der Halbordnung $(\mathcal{P}(\{1,2,3\}), \subseteq)$ abgebildet.

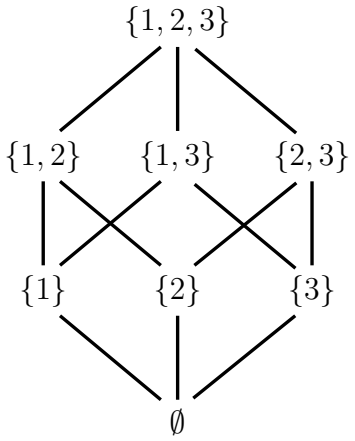


Abbildung 1.1: Das Hasse-Diagramm der Halbordnung $(\mathcal{P}(\{1,2,3\}), \subseteq)$.

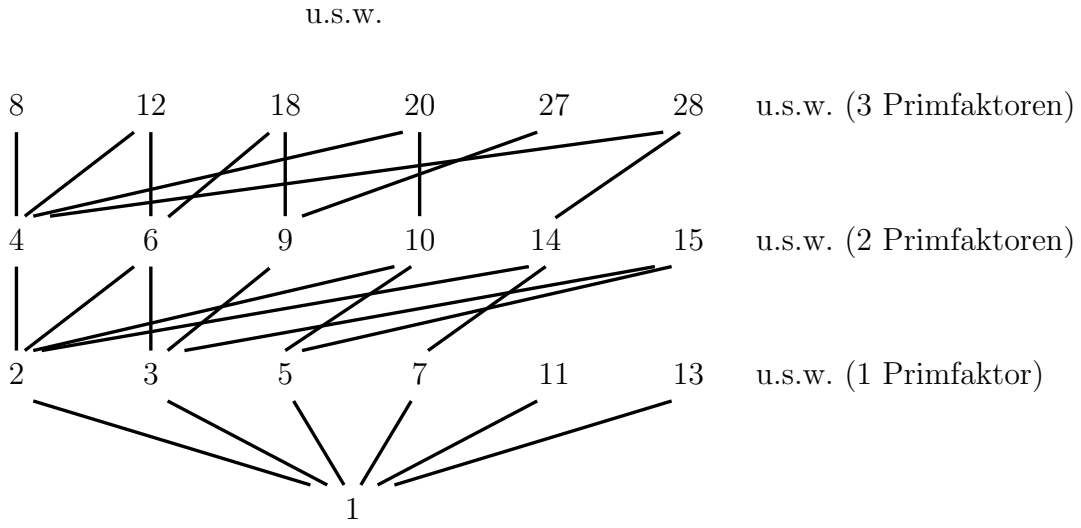


Abbildung 1.2: Das Hasse-Diagramm der Halbordnung $(\mathbb{N}, |)$.

(ii) Das Hasse-Diagramm der Halbordnung $(\mathbb{N}, \leq)$:

(iii) In Abbildung 1.2 ist das Hasse-Diagramm der Halbordnung $(\mathbb{N}, |)$ abgebildet.

Definition 1.5.8. Es sei $(M, \preceq)$ eine Halbordnung und X Teilmenge von M.

a) Ein Element $a \in X$ heißt $\left\{ \begin{array}{l} \textit{minimales} \\ \textit{maximales} \end{array} \right\}$ *Element* in X, wenn für kein $x \in X$ gilt $\left\{ \begin{array}{l} x \prec a \\ x \succ a \end{array} \right\}$.

b) Ein Element $a \in X$ heißt $\left\{ \begin{array}{l} \textit{kleinstes} \\ \textit{größtes} \end{array} \right\}$ *Element* in X, wenn für alle $x \in X$ gilt $\left\{ \begin{array}{l} a \preceq x \\ a \succeq x \end{array} \right\}$.

c) Ein Element $b \in M$ heißt $\left\{ \begin{array}{l} \textit{untere} \\ \textit{obere} \end{array} \right\}$ *Schranke* von X, wenn für alle $x \in X$ gilt $\left\{ \begin{array}{l} b \preceq x \\ b \succeq x \end{array} \right\}$.

d) Ein Element $b \in M$ heißt $\left\{ \begin{array}{l} \textit{Infimum} \\ \textit{Supremum} \end{array} \right\}$ von X, wenn b $\left\{ \begin{array}{l} \text{größtes} \\ \text{kleinstes} \end{array} \right\}$ Element der Menge aller $\left\{ \begin{array}{l} \text{unteren} \\ \text{oberen} \end{array} \right\}$ Schranken von X ist.

Ob minimale, maximale, kleinste und größte Elemente in X existieren, hängt von X und der Halbordnung ab. Genauso ist es bei Schranken und beim Supremum und Infimum.

Bemerkung.

(i) Ein kleinstes bzw. größtes Element einer Teilmenge X ist (erst recht) auch minimal bzw. maximal in X.

(ii) Bei total geordneten Mengen fallen die Begriffe zusammen.

(iii) Ein kleinstes bzw. größtes Element von X ist auch Infimum bzw. Supremum von X.

(iv) Infimum bzw. Supremum müssen nicht selbst in X liegen.

(v) Wenn ein Infimum bzw. Supremum in X liegt, dann ist es auch kleinstes bzw. größtes Element von X.

Bemerkung. Eine Teilmenge X einer Halbordnung $(M, \preceq)$ kann höchstens ein kleinstes (größtes) Element und höchstens ein Infimum (Supremum) besitzen. Falls es existiert, spricht man von dem kleinsten (größten) Element, auch *Minimum* (*Maximum*) genannt, und von dem Infimum (Supremum) der Teilmenge X. Bezeichnung

$$\min X,\ \max X,\ \inf X,\ \sup X\ .$$

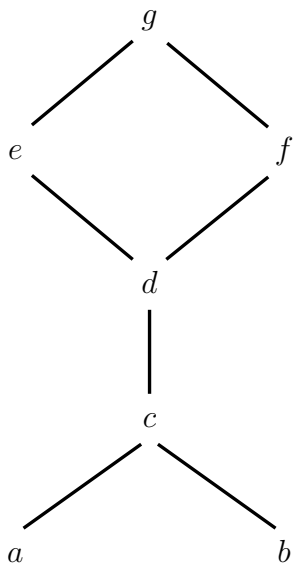


Abbildung 1.3: Hasse-Diagramm einer Halbordnung auf der Menge $\{a, b, c, d, e, f, g\}$.

Beispiel. Es sei auf $M := \{a, b, c, d, e, f, g\}$ eine Halbordnung durch das in Abbildung 1.3 gegebene Hasse-Diagramm definiert.

- Die Teilmenge $X = \{d, e, f, g\}$ besitzt d als kleinstes (und damit auch als minimales) Element.
- In $\{e, f, g\}$ sind e und f minimale Elemente, aber es gibt kein kleinstes Element.
- $\{e, f, g\}$ hat a, b, c, d als untere Schranken, d ist Infimum (größte untere Schranke).
- $\{a, b, c\}$ hat keine untere Schranke.

1.5.5 Verbände

Infimum und Supremum sind schon für zweielementige Teilmengen interessant.

Definition 1.5.9. Eine Halbordnung $(M, \preceq)$, in der für jede zweielementige Teilmenge $\{x, y\} \subseteq M$ das Infimum und das Supremum existieren, heißt *Verband*. Man schreibt dann

$$\inf\{x, y\} := x \wedge y \text{ (Englisch: } \textit{meet}\text{)}, \qquad \sup\{x, y\} := x \vee y \text{ (Englisch: } \textit{join}\text{)}.$$

Bemerkung. Das Element $s = x \wedge y$ ist definitionsgemäß charakterisiert durch die folgenden zwei Eigenschaften:

(i) $s \leq x$ und $s \leq y$ (d.h. s ist untere Schranke von x und y).

(ii) Aus $z \leq x$ und $z \leq y$ folgt $z \leq s$ (d.h. s ist größte untere Schranke).

Dualisieren gibt die analoge Beschreibung für $x \vee y$.

Beispiele.

(i) Jede total geordnete Menge $(M, \preceq)$ ist ein Verband mit $x \wedge y = \min\{x, y\}$ und $x \vee y = \max\{x, y\}$.

(ii) $\mathbb{N}$ mit der Teilbarkeitsrelation $a \mid b$ als Halbordnung ist ein Verband. Dabei ist $a \wedge b = \mathrm{ggT}(a, b)$ (größter gemeinsamer Teiler) und $a \vee b = \mathrm{kgV}(a, b)$ (kleinstes gemeinsames Vielfaches).

(iii) Die Potenzmenge $(\mathcal{P}(M), \subseteq)$ einer beliebigen Menge M ist ein Verband. Hier gilt $A \wedge B = A \cap B$ und $A \vee B = A \cup B$ für $A, B \subseteq M$.

Bemerkung. In einem Verband besitzt jede endliche Teilmenge ein Infimum und ein Supremum. Falls dieses sogar für beliebige Teilmengen gilt, spricht man von einem *vollständigen Verband*.

Aus der Definition eines Verbandes läßt sich eine Anzahl von weiteren Eigenschaften ableiten. So gilt beispielsweise der folgende Satz.

Satz 1.5.10. *Es sei $(M, \preceq)$ ein Verband. Dann gelten für $\wedge$ und $\vee$ die Gesetze*

a) $x \wedge x = x,\ x \vee x = x$ *(Idempotenz)*

b) $x \wedge y = y \wedge x,\ x \vee y = y \vee x$ *(Kommutativität)*

c) $x \wedge (y \wedge z) = (x \wedge y) \wedge z,\ x \vee (y \vee z) = (x \vee y) \vee z$ *(Assoziativität)*

d) $x \wedge (x \vee y) = x,\ x \vee (x \wedge y) = x$ *(Absorption)*

e) $x \preceq y \iff x \wedge y = x \iff x \vee y = y$ *(Konsistenz)*

Definition 1.5.11. Ein *distributiver Verband* ist ein Verband $(M, \preceq)$, in dem die folgenden beiden *Distributivgesetze* gelten:

(i) $\forall x, y, z \in M : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

(ii) $\forall x, y, z \in M : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Bemerkung. Eine total geordnete Menge ist nicht nur ein Verband, sondern sogar distributiv. Dieses ist aber nur als ein "trivialer Fall" von Distributivität anzusehen. Jeder Potenzmengenverband ist distributiv.

Kapitel 2

Zahlbereiche

Das zweite Kapitel dieses Vorlesungsskriptes beruht teilweise auf Skripten von Herrn Scharlau, dem ich hiermit ganz herzlich danke.

2.1 Natürliche Zahlen, vollständige Induktion und Rekursion

2.1.1 Axiome der natürlichen Zahlen

Die natürlichen Zahlen und ihre grundsätzlichen Eigenschaften sind uns schon von Kindheit an bekannt und wir haben einen vertrauten Umgang mit diesen Zahlen erlernt. Eine „saubere“ Beschreibung (und Definition) der Menge der natürlichen Zahlen $\mathbb{N}$ kann man wie folgt erhalten.

Definition 2.1.1 (Peano Axiome)**.** Die Menge $\mathbb{N}$ der natürlichen Zahlen wird wie folgt definiert:

(i) 1 ist eine natürliche Zahl.

(ii) Jede natürliche Zahl n hat genau einen von 1 verschiedenen Nachfolger n^+, der eine natürliche Zahl ist.

(iii) Verschiedene natürliche Zahlen haben verschiedene Nachfolger.

(iv) Ist $M \subseteq \mathbb{N}$ mit $1 \in M$ und der Eigenschaft, dass aus $n \in M$ auch $n^+ \in M$ folgt, so ist $M = \mathbb{N}$.

Die Eigenschaften (i)–(iv) heißen *Peano Axiome*[1]. Sie stehen ganz am Anfang der Theorie der natürlichen Zahlen und bilden die Grundlage für alles Weitere.

[1] Als *Axiome* werden im Allgemeinen die grundlegenden Definitionen der Mathematik bezeichnet, auf denen dann ganze Theoriegebäude aufgebaut werden. Das bedeutet, dass alle bekannten Resultate aus diesen Axiomen herleitbar sind, die Axiome selbst jedoch nicht bewiesen oder gefolgert werden können, jedoch als gegebene Grundsteine allgemein akzeptiert sind.

Mit dem in (ii) geforderten Nachfolger der natürlichen Zahl n ist offenbar die natürliche Zahl $n+1$ gemeint.

2.1.2 Vollständige Induktion

Aus dem Axiom in Definition 2.1.1 (iv) kann man jetzt unmittelbar das Beweisprinzip der vollständigen Induktion ableiten.

Satz 2.1.2 (Vollständige Induktion)**.** *Für alle $n \in \mathbb{N}$ sei $A(n)$ eine Aussage über die natürliche Zahl n. Dann gilt*

$$\Big(A(1) \wedge \big(\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)\big)\Big) \implies \big(\forall n \in \mathbb{N} : A(n)\big) \ .$$

In Worten bedeutet das: Ist die Aussage $A(1)$ wahr („Induktionsanfang“) und folgt für jedes $n \in \mathbb{N}$ aus der Aussage $A(n)$ die Aussage $A(n+1)$ („Induktionsschluss“), dann ist die Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr.

Beweis. Wir nehmen an, dass $A(1)$ wahr ist und für alle $n \in \mathbb{N}$ gilt, dass aus $A(n)$ die Aussage $A(n+1)$ folgt. Es sei $M := \{n \in \mathbb{N} \mid A(n)\}$. Aus Definition 2.1.1 (iv) folgt dann $M = \mathbb{N}$ und damit die Behauptung des Satzes. □

Als erste Anwendung des Beweisprinzips der vollständigen Induktion beweisen wir die folgende Aussage über geometrische Summen.

Lemma 2.1.3 (Geometrische Summe)**.** *Es sei $x \in \mathbb{R} \setminus \{1\}$. Dann gilt für alle $n \in \mathbb{N}$*

$$x^0 + x^1 + x^2 + \cdots + x^n \ = \ \frac{x^{n+1} - 1}{x - 1} \ . \tag{2.1}$$

Beweis. Für $n \in \mathbb{N}$ sei $A(n)$ die Aussage (2.1). Induktionsanfang: $A(1)$ ist wahr, denn

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

Induktionsschluss: Es sei jetzt $n \in \mathbb{N}$ beliebig aber fest gewählt. Ist $A(n)$ wahr, dann gilt

$$\begin{aligned} x^0 + x^1 + \cdots + x^n + x^{n+1} \ &= \ \frac{x^{n+1} - 1}{x - 1} + x^{n+1} \ = \ \frac{x^{n+1} - 1}{x - 1} + x^{n+1} \cdot \frac{x-1}{x-1} \\ &= \ \frac{x^{n+1} - 1}{x - 1} + \frac{x^{n+2} - x^{n+1}}{x - 1} \ = \ \frac{x^{n+2} - 1}{x - 1} \ . \end{aligned}$$

Damit haben wir also gezeigt, dass $A(n+1)$ wahr ist, falls $A(n)$ wahr ist (Induktionsschluss). Die Behauptung des Lemmas folgt mit vollständiger Induktion (Satz 2.1.2). □

Das Prinzip der vollständigen Induktion aus Satz 2.1.2 kann wie folgt verallgemeinert werden.

Korollar 2.1.4. *Es sei $n_0 \in \mathbb{Z}$. Für alle ganzen Zahlen $n \geq n_0$ sei $A(n)$ eine Aussage über die Zahl n. Dann gilt*

$$\Big(A(n_0) \wedge \big(\forall n \geq n_0 : A(n) \Rightarrow A(n+1)\big)\Big) \implies \big(\forall n \geq n_0 : A(n)\big) \ .$$

Wir geben im Folgenden eine weitere Verallgemeinerung des Induktionsprinzips an.

Satz 2.1.5. *Es sei $n_0 \in \mathbb{Z}$. Für alle ganzen Zahlen $n \geq n_0$ sei $A(n)$ eine Aussage über n. Dann gilt*

$$\Big(A(n_0) \wedge \big(\forall n \geq n_0 : \big(\forall n_0 \leq k \leq n : A(k)\big) \Rightarrow A(n+1)\big)\Big) \implies \big(\forall n \geq n_0 : A(n)\big) \ .$$

In Worten bedeutet das: Ist die Aussage $A(n_0)$ wahr und folgt aus den Aussagen $A(k)$ mit $n_0 \leq k \leq n$ die Aussage $A(n+1)$, dann ist die Aussage $A(n)$ für alle $n \geq n_0$ wahr.

Formal ist dieses Induktionsprinzip stärker als die Version aus Satz 2.1.2: Man darf beim Induktionsschluss mehr voraussetzen. Das verallgemeinerte Induktionsprinzip ist beispielsweise beim Beweis des folgenden Lemmas von Nutzen.

Lemma 2.1.6. *Ist $n \geq 2$ eine natürliche Zahl, so gibt es eine Primzahl p, die n teilt.*

Bevor wir das Lemma beweisen, reichen wir noch eine formale Definition des Begriffs *Primzahl* nach.

Definition 2.1.7. Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, falls sie nur von 1 und sich selbst geteilt wird, d.h. wenn gilt:

$$\forall m \in \mathbb{N} : \ (m|n \ \Rightarrow \ m \in \{1, n\}) \ .$$

Beweis von Lemma 2.1.6. Wir beweisen das Lemma mit Hilfe der verallgemeinerten vollständigen Induktion (siehe Satz 2.1.5). Induktionsanfang: Die Behauptung ist offenbar wahr für $n = 2$, da 2 eine Primzahl ist und sich selbst teilt. Induktionsschluss: Es sei $n \geq 2$ beliebig aber fest gewählt und die Behauptung gelte für alle $2 \leq k \leq n$. Ist $n+1$ eine Primzahl, so gilt die Behauptung offensichtlich auch für $n+1$. Ist $n+1$ keine Primzahl, so besitzt $n+1$ nach Definition einen Teiler q mit $2 \leq q < n+1$. Nach Induktionsvoraussetzung gibt es eine Primzahl p mit $p|q$. Da die Teilerrelation transitiv ist, gilt dann $p|(n+1)$. $\square$

2.1.3 Rekursive Abbildungen

Analog zum induktiven Beweis von Aussagen, die für alle $n \in \mathbb{N}$ gelten, kann man auch Abbildungen mit Definitionsbereich $\mathbb{N}$ „induktiv“ definieren. Hier spricht man allerdings üblicherweise von einer *rekursiven Definition*. Wir erläutern das zunächst anhand eines einfachen Beispiels.

Beispiel. Die *Fakultätsfunktion* $g : \mathbb{N}_0 \to \mathbb{N}$ mit

$$g(n) := n! := 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n$$

kann man präziser wie folgt rekursiv definieren:

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

Satz 2.1.8 (Rekursionssatz)**.** *Es sei $n_0 \in \mathbb{Z}$, $X := \{n \in \mathbb{Z} \mid n \geq n_0\}$ und Y eine beliebige, nicht leere Menge. Weiter sei $f : X \times Y \to Y$ eine Abbildung und $s \in Y$. Dann liefert die folgende rekursive Vorschrift eine eindeutige Abbildung $g : X \to Y$:*

(i) $g(n_0) := s$,

(ii) $g(n+1) := f(n, g(n))$ *für* $n \geq n_0$.

Beweis. Wir zeigen mit vollständiger Induktion, dass $g(n) \in Y$ für alle $n \geq n_0$ durch die gegebene Vorschrift eindeutig definiert ist. Induktionsanfang: $g(n_0)$ ist offenbar durch (i) eindeutig definiert. Induktionsschluss: Für ein beliebiges, fest gewähltes $n \geq 0$ sei $g(n)$ eindeutig definiert. Dann ist auch $g(n+1)$ durch (ii) eindeutig definiert. □

Beispiel.

(i) Es seien $n_0 \in \mathbb{Z}$ und $a_k \in \mathbb{R}$ für $k \geq n_0$. Für jedes $n \geq n_0$ definieren wir $\sum_{k=n_0}^{n} a_k$ durch

$$\sum_{k=n_0}^{n_0} a_k := a_{n_0} \qquad \text{und} \qquad \sum_{k=n_0}^{n+1} a_k := \sum_{k=n_0}^{n} a_k + a_{n+1} \quad \text{für } n \geq n_0.$$

Damit können wir in Zukunft die etwas unpräzise Notation

$$a_{n_0} + a_{n_0+1} + \cdots + a_n$$

vermeiden. Für $n < n_0$ definieren wir außerdem $\sum_{k=n_0}^{n} a_k := 0$.

(ii) Analog zu der Summendefinition in (i) können wir auch beliebig lange Produkte definieren. Es sei

$$\prod_{k=n_0}^{n_0} a_k := a_{n_0} \qquad \text{und} \qquad \prod_{k=n_0}^{n+1} a_k := \prod_{k=n_0}^{n} a_k \cdot a_{n+1} \quad \text{für } n \geq n_0.$$

Für $n < n_0$ definieren wir außerdem $\prod_{k=n_0}^{n} a_k := 1$.

In Abschnitt 2.1.2 haben wir neben der Grundversion der vollständigen Induktion (siehe Satz 2.1.2) auch eine verallgemeinerte Version kennen gelernt (siehe Satz 2.1.5). Ganz analog können wir auch die rekursive Definition von Fuktionen verallgemeinern. Wir verzichten hier auf eine formale Beschreibung und geben stattdessen ein illustratives Beispiel an.

Beispiel (Fibonacci-Zahlen)**.** Die Folge der *Fibonacci*[2]*-Zahlen* ist durch die folgenden Vorschriften rekursiv definiert:

$$\begin{aligned} &F(0) := 0 \ , \qquad F(1) := 1 \ , \\ &F(n) := F(n-1) + F(n-2) \qquad \text{für } n \geq 2. \end{aligned}$$

Die folgende explizite Beschreibung der Fibonacci-Zahlen kann mit Hilfe der verallgemeinerten vollständigen Induktion (Satz 2.1.5) bewiesen werden.

Lemma 2.1.9. *Für $n \in \mathbb{N}_0$ ist die n-te Fibonacci-Zahl $F(n)$ wie folgt gegeben:*

$$F(n) = \frac{1}{\sqrt{5}} \cdot (a^n - b^n) \qquad \textit{mit} \quad a := \frac{1+\sqrt{5}}{2} \quad \textit{und} \quad b := \frac{1-\sqrt{5}}{2} \ .$$

Wir lassen den Beweis des Lemmas als Übungsaufgabe.

2.2 Gruppen, Ringe, Körper

Wir studieren in diesem Abschnitt Mengen mit bestimmten Verknüpfungen, die interessante algebraische Strukturen liefern. Das Studium dieser Strukturen ist hauptsächlich durch die uns bereits bekannten Zahlbereiche der ganzen Zahlen, der rationalen Zahlen und der reellen Zahlen motiviert.

2.2.1 Halbgruppen, Monoide, Gruppen

Wir definieren zunächst den Begriff einer Verknüpfung auf einer Menge. Man kann dabei beispielsweise an „Rechenoperationen“ wie Addition, Subtraktion, Multiplikation und Division denken.

[2]Leonardo di Pisa, genannt „Fibonacci“ (ca. 1170–1250).

Definition 2.2.1 (Verknüpfungen)**.** Es sei M eine Menge. Eine *Verknüpfung* $\circ$ *auf* M ist eine Abbildung

$$\circ : M \times M \to M \ , \qquad (x, y) \mapsto x \circ y \ .$$

Die Verknüpfung heißt:

- *kommutativ*, falls $x \circ y = y \circ x$ für alle $x, y \in M$;
- *assoziativ*, falls $(x \circ y) \circ z = x \circ (y \circ z)$ für alle $x, y, z \in M$.

Mit Hilfe des Begriffs der Verknüpfung können wir jetzt einige einfache und grundlegende algebraische Strukturen definieren.

Definition 2.2.2 (Halbgruppen, Monoide, Gruppen)**.**

a) Eine Menge H zusammen mit einer assoziativen Verknüpfung $\circ$ auf H heißt *Halbruppe* $(H, \circ)$.

b) Eine Halbgruppe $(M, \circ)$ heißt *Monoid*, falls es ein $e \in M$ gibt mit

$$e \circ x \ = \ x \circ e \ = \ x \qquad \text{für alle } x \in M.$$

In diesem Fall heißt e *neutrales Element* oder *Einselement* des Monoids.

c) Ein Monoid $(G, \circ)$, in dem zu jedem $x \in G$ ein $y \in G$ existiert mit

$$x \circ y \ = \ y \circ x \ = \ e \ ,$$

heißt Gruppe. Zu gegebenem x ist das Element y dann eindeutig und heißt *zu* x *inverses Element*, in Zeichen $x^{-1} := y$.

d) Eine Gruppe $(G, \circ)$ mit kommutativer Verknüpfung $\circ$ heißt *kommutative* oder *abelsche*[3] *Gruppe*.

Beispiele.

(i) Es sei X eine beliebige Menge und M die Menge der Abbildungen von X nach X. Die in Definition 1.3.7 eingeführte Komposition $\circ$ von Abbildungen definiert eine assoziative Verknüpfung (siehe Lemma 1.3.9) auf der Menge M. Damit ist also $(M, \circ)$ eine Halbgruppe und sogar ein Monoid, da die identische Abbildung id_X neutrales Element ist. Ist M' die Teilmenge der bijektiven Abbildungen, so ist $(M', \circ)$ eine Gruppe (siehe Satz 1.3.11). Da die Komposition von Abbildungen jedoch im Allgemeinen nicht kommutativ ist, handelt es sich nicht um eine abelsche Gruppe.

[3]Niels Henrik Abel (1802–1829).

(ii) Die Addition $+$ ist eine kommutative und assoziative Verknüpfung auf $\mathbb{N}_0, \mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Die Zahl 0 ist das neutrale Element. Damit ist $(\mathbb{N}_0, +)$ ein Monoid. Außerdem sind $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ kommutative Gruppen: Das inverse Element zu x ist $-x$.

(iii) Die Multiplikation $\cdot$ ist eine kommutative und assoziative Verknüpfung auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Die Zahl 1 ist das neutrale Element. Damit sind $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ und $(\mathbb{R}, \cdot)$ Monoide. Außerdem sind $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ kommutative Gruppen: Das inverse Element zu $x \neq 0$ ist $1/x$.

(iv) Die Subtraktion und die Division sind Verknüpfungen auf $\mathbb{Q}$ und $\mathbb{R}$. Beide Verknüpfungen sind weder kommutativ noch assoziativ. Man beachte, dass die Subtraktion keine Verknüpfung auf $\mathbb{N}$ definiert und die Division weder auf $\mathbb{N}$ noch auf $\mathbb{Z}$ eine Verknüpfung definiert.

Lemma 2.2.3 (Eindeutigkeit des neutralen Elements)**.** *Ein Monoid $(M, \circ)$ hat genau ein neutrales Element.*

Beweis. Es seien $e, f \in M$ neutrale Elemente. Dann gilt

$$e \;=\; e \circ f \;=\; f \;.$$

□

Lemma 2.2.4 (Eindeutigkeit des Inversen)**.** *Ist $(G, \circ)$ eine Gruppe, dann ist das Inverse Element x^{-1} zu $x \in G$ eindeutig bestimmt.*

Beweis. Es sei $x \in G$ und $y, z \in G$ seien inverse Elemente zu x. Dann gilt:

$$y \;=\; y \circ e \;=\; y \circ (x \circ z) \;=\; (y \circ x) \circ z \;=\; e \circ z \;=\; z \;.$$

□

Aus dem Lemma folgt insbesondere, dass das neutrale Element $e \in G$ zu sich selbst invers ist, d.h. $e^{-1} = e$.

Lemma 2.2.5. *Es sei $(G, \circ)$ eine Gruppe und $x, y \in G$. Dann gilt*

$$(x \circ y)^{-1} \;=\; y^{-1} \circ x^{-1} \;.$$

Beweis. Es gilt

$$\begin{aligned}(x \circ y) \circ (y^{-1} \circ x^{-1}) \;&=\; \big(x \circ (y \circ y^{-1})\big) \circ x^{-1} \\ &=\; (x \circ e) \circ x^{-1} \;=\; x \circ x^{-1} \;=\; e\end{aligned}$$

und

$$\begin{aligned}(y^{-1} \circ x^{-1}) \circ (x \circ y) \;&=\; \big(y^{-1} \circ (x^{-1} \circ x)\big) \circ y \\ &=\; (y^{-1} \circ e) \circ y \;=\; y^{-1} \circ y \;=\; e \;.\end{aligned}$$

Da das inverse Element nach Lemma 2.2.4 eindeutig ist, folgt daraus die Behauptung. □

Eine Teilmenge einer Gruppe, die selbst wieder eine Gruppe ist, nennt man Untergruppe:

Definition 2.2.6 (Untergruppen)**.** Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e und $H \subseteq G$. Dann heißt $(H, \circ|_{H\times H})$ *Untergruppe* von $(G, \circ)$, falls gilt:

(i) $e \in H$,

(ii) $x \circ y \in H$ für alle $x, y \in H$,

(iii) $x^{-1} \in H$ für alle $x \in H$.

Lemma 2.2.7. *Eine Untergruppe einer Gruppe ist selbst eine Gruppe.*

Beispiele.

(i) Die Gruppe $(\mathbb{Z}, +)$ ist eine Untergruppe der Gruppe $(\mathbb{R}, +)$.

(ii) Die Gruppe $(\{1, -1\}, \cdot)$ ist eine Untergruppe der Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$.

(iii) Die Gruppe $(2\mathbb{Z}, +)$ ist eine Untergruppe der Gruppe $(\mathbb{Z}, +)$.

2.2.2 Ringe

Die Betrachtung der ganzen Zahlen $\mathbb{Z}$ mit den beiden Verknüpfungen Addition und Multiplikation motiviert die folgende Definition.

Definition 2.2.8 (Ringe)**.** Es sei R eine Menge mit zwei Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation), so dass gilt:

(i) $(R, +)$ ist eine kommutative Gruppe mit neutralem Element (Nullelement) 0.

(ii) $(R, \cdot)$ ist eine Halbgruppe.

(iii) Für alle $x, y, z \in R$ gilt

$$x \cdot (y + z) \;=\; x \cdot y + x \cdot z \;. \qquad \text{(Distributivität)}$$

Dann heißt $(R, +, \cdot)$ ein *Ring*. Der Ring $(R, +, \cdot)$ heißt *Ring mit Eins*, falls $(R, \cdot)$ ein Monoid ist, dessen neutrales Element 1 (Einselement) ungleich dem neutralen Element 0 (Nullelement) der Addition ist. Der Ring $(R, +, \cdot)$ heißt *kommutativ*, falls die Multiplikation kommutativ ist.

Beispiel.

(i) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.

(ii) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring (aber ohne Eins), wobei $2\mathbb{Z} := \{2z \mid z \in \mathbb{Z}\}$ ist.

(iii) Wir definieren die folgende Addition und Multiplikation auf der Menge $\{0,1,2,3,4,5\}$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

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

Dann ist $(\{0,1,2,3,4,5\},+,\cdot)$ ein kommutativer Ring mit Eins.

(iv) Es sei X eine beliebige Menge und $M := \mathbb{R}^X$ die Menge der Abbildungen von X nach $\mathbb{R}$. Wir definieren eine Addition $\oplus$ und eine Multiplikation $\odot$ auf M. Für zwei Abbildungen $f, g \in M$ sind die Summe $f \oplus g \in M$ und das Produkt $f \odot g \in M$ wie folgt definiert:

$$(f \oplus g)(x) := f(x) + g(x) \qquad \text{und} \qquad (f \odot g)(x) := f(x) \cdot g(x)$$

für alle $x \in \mathbb{R}$. Dann ist $(M, \oplus, \odot)$ ein kommutativer Ring mit Eins.

(v) Als weiteres wichtiges Beispiel eines nichtkommutativen Rings werden wir in der Linearen Algebra den Ring der $n \times n$-Matrizen über $\mathbb{R}$ kennen lernen.

Lemma 2.2.9. *Ist $(R,+,\cdot)$ ein Ring mit Nullelement 0, so gilt*

$$0 \cdot x \;=\; x \cdot 0 \;=\; 0 \qquad \textit{für alle } x \in R.$$

Beweis. Es gilt

$$0 \cdot x \;=\; (0+0) \cdot x \;=\; 0 \cdot x + 0 \cdot x \tag{2.2}$$

Wir bezeichnen mit $-(0 \cdot x)$ das zu $0 \cdot x$ inverse Element bezüglich der Addition, d.h. $(0 \cdot x) + (-(0 \cdot x)) = 0$. Dann gilt

$$\begin{aligned} 0 \cdot x \;&=\; 0 \cdot x + 0 \;=\; 0 \cdot x + (0 \cdot x + (-(0 \cdot x))) \\ &=\; (0 \cdot x + 0 \cdot x) + (-(0 \cdot x)) \\ &=\; (0+0) \cdot x + (-(0 \cdot x)) \\ &=\; 0 \cdot x + (-(0 \cdot x)) \\ &=\; 0 \ . \end{aligned}$$

Analog zeigt man, dass $x \cdot 0 = 0$ gilt. □

Analog wie bei Gruppen kann man auch bei Ringen Teilmengen betrachten, die selbst wieder Ringe sind.

Definition 2.2.10 (Unterringe)**.** Es sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$. Dann heißt $(S, +|_{S\times S}, \cdot|_{S\times S})$ *Unterring* von $(R, +, \cdot)$, falls gilt:

(i) $(S, +|_{S\times S})$ ist Untergruppe von $(R, +)$,

(ii) $x \cdot y \in S$ für alle $x, y \in S$.

Lemma 2.2.11. *Ein Unterring eines Rings ist selbst ein Ring.*

Beispiel. $(2\mathbb{Z}, +, \cdot)$ ist ein Unterring des Rings $(\mathbb{Z}, +, \cdot)$.

Polynomringe

Ein wichtiger Spezialfall von Ringen sind Polynomringe, die von der Menge aller Polynome mit Koeffizienten aus einem Ring R gebildet werden. Der Einfachheit halber kann man sich im Folgenden immer die reellen Zahlen als zugrundeliegenden Ring R vorstellen. In diesem Fall betrachtet man also die bereits aus der Schule bekannten Polynome mit Koeffizienten aus $\mathbb{R}$.

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und X eine Unbestimmte. Dann nennen wir einen Ausdruck der Form

$$a_0X^0 + a_1X^1 + \cdots + a_nX^n \qquad \text{mit } n \in \mathbb{N}_0 \text{ und } a_0, \ldots, a_n \in R$$

Polynom über R. Der *Grad* eines Polynoms $P = a_0X^0 + \cdots + a_nX^n$ ist wie folgt definiert:

$$\operatorname{grad}(P) \;:=\; \begin{cases} -1 & \text{falls } a_0 = \cdots = a_n = 0, \\ \max\{i \mid a_i \neq 0\} & \text{sonst.} \end{cases}$$

Zwei Polynome

$$a_0X^0 + a_1X^1 + \cdots + a_nX^n \qquad \text{und} \qquad b_0X^0 + b_1X^1 + \cdots + b_mX^m$$

mit $m \leq n$ sind nach Definition gleich, falls $a_i = b_i$ für alle $0 \leq i \leq m$ und $a_i = 0$ für alle $m+1 \leq i \leq n$. Die Menge aller Polynome über R bezeichnen wir mit $R[X]$. Wir definieren auf $R[X]$ die beiden folgenden Verknüpfungen:

$$\oplus : R[X] \times R[X] \to R[X] \;, \qquad \Big(\sum_{i=0}^{n} a_iX^i, \sum_{i=0}^{n} b_iX^i\Big) \mapsto \sum_{i=0}^{n} (a_i + b_i)X^i \;,$$

$$\odot : R[X] \times R[X] \to R[X] \;, \qquad \Big(\sum_{i=0}^{n} a_iX^i, \sum_{i=0}^{m} b_iX^i\Big) \mapsto \sum_{i=0}^{n+m} \Big(\sum_{j=0}^{i} a_j \cdot b_{i-j}\Big)X^i \;.$$

(Man beachte, dass es genügt, die Summe zweier Polynome für den Fall $n = m$ zu definieren. Ist nämlich beispielsweise $m < n$, so schreiben wir statt $b_0X^0 + \cdots + b_mX^m$ einfach $b_0X^0 + \cdots + b_mX^m + 0X^{m+1} + \cdots + 0X^n$.) Dann ist $(R[X], \oplus, \odot)$ ein kommutativer Ring mit Eins. Das neutrale Element der Addition (Nullelement) ist das *Nullpolynom* $0X^0$. Das neutrale Element der Multiplikation (Einselement) ist $1X^0$.

Schreibweisen. Statt $a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n$ schreibt man auch einfach $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. An Stelle von $1X^n$ kann man auch nur X^n schreiben. Terme der Form $0X^k$ kann man auch einfach weglassen, also beispielsweise $3 + 4X^3$ statt $3 + 0X + 0X^2 + 4X^3$.

Beispiel. Wir betrachten den Polynomring $\mathbb{Z}[X]$. Die Summe der beiden Polynome $3 - 2X + 4X^2$ und $-1 + 3X + 3X^2$ ist das Polynom $2 + X + 7X^2$. Das Produkt der beiden Polynome ist $-3 + 11X - X^2 + 6X^3 + 12X^4$. Wir stellen fest, dass der Grad des Produkts zweier Polynome gleich der Summe der Grade der Polynome ist.

2.2.3 Körper

Körper sind spezielle Ringe, die die Eigenschaften besitzen, die wir beispielsweise von den reellen oder rationalen Zahlen kennen.

Definition 2.2.12 (Körper)**.** Ein kommutativer Ring mit Eins $(K, +, \cdot)$, in dem jedes Element $x \neq 0$ ein multiplikatives Inverses hat, heißt *Körper*.

Beispiele.

(i) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

(ii) Wir definieren die folgende Addition und Multiplikation auf der Menge $\{0, 1\}$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Dann ist $(\{0, 1\}, +, \cdot)$ ein (endlicher) Körper mit zwei Elementen.

(iii) Wir definieren die folgende Addition und Multiplikation auf der Menge $\{0, 1, 2\}$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Dann ist $(\{0, 1, 2\}, +, \cdot)$ ein (endlicher) Körper mit drei Elementen.

(iv) Wir definieren die folgende Addition und Multiplikation auf der Menge $\{0, 1, a, b\}$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Dann ist $(\{0, 1, a, b\}, +, \cdot)$ ein (endlicher) Körper mit vier Elementen.

Bemerkung. Die Folge von Beispielen oben soll nicht suggerieren, dass es zu jedem $q \geq 2$ einen Körper mit q Elementen gibt. Man kann zeigen, dass es genau dann einen Körper mit q Elementen gibt, wenn q eine Primzahlpotenz ist, d.h. wenn $q = p^m$ für eine Primzahl p und ein $m \in \mathbb{N}$. Wir werden später noch näher auf diesen Sachverhalt eingehen.

Wir geben einige weitere Beispiele von Körpern an.

Beispiele.

(i) Es sei $K := \mathbb{Q} \times \mathbb{Q}$ mit den beiden Verknüpfungen

$$\begin{aligned} \oplus &: K \times K \to K \ , \qquad ((a,b),(a',b')) \mapsto (a + a', b + b') \ , \\ \odot &: K \times K \to K \ , \qquad ((a,b),(a',b')) \mapsto (a \cdot a' + 2b \cdot b', a \cdot b' + a' \cdot b) \ . \end{aligned}$$

Dann ist $(K, \oplus, \odot)$ ein Körper. Man bezeichnet diesen Körper auch mit $\mathbb{Q}[\sqrt{2}]$ (lies: „$\mathbb{Q}$ adjungiert Wurzel 2“), da man das Element $(a, b) \in K$ mit der reellen Zahl $a + b\sqrt{2}$ identifizieren kann.

(ii) In Fortsetzung des Beispiels nach Definition 1.5.6 in Kapitel 1 definieren wir die folgenden beiden Verknüpfungen auf der dort betrachteten Menge der Äquivalenzklassen $\mathcal{Z}$:

$$\begin{aligned} \oplus &: \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z} \ , \qquad ([p,q]_\sim, [p',q']_\sim) \mapsto [p \cdot q' + p' \cdot q, q \cdot q']_\sim \ , \\ \odot &: \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z} \ , \qquad ([p,q]_\sim, [p',q']_\sim) \mapsto [p \cdot p', q \cdot q']_\sim \ . \end{aligned}$$

Dann ist $(\mathcal{Z}, \oplus, \odot)$ ein Körper. Damit hat man den Körper der rationalen Zahlen $\mathbb{Q}$ formal definiert, indem man $[p, q]_\sim$ mit der rationalen Zahl $\frac{p}{q}$ identifiziert.

2.2.4 Homomorphismen

Wir betrachten in diesem Abschnitt sogenannte *strukturerhaltende* Abbildungen auf Gruppen und Ringen. Das sind Abbildungen, die die Verknüpfungen respektieren. Wir beginnen zunächst mit der Definition von *Gruppenhomomorphismen*.

Definition 2.2.13 (Gruppenhomomorphismen)**.** Sind $(G, \circ)$ und $(G', \bullet)$ Gruppen und $\varphi : G \to G'$ eine Abbildung, dann heißt φ *Gruppenhomomorphismus*, falls

$$\varphi(x \circ y) \;=\; \varphi(x) \bullet \varphi(y) \qquad \text{für alle } x, y \in G.$$

Beispiele.

(i) Die Abbildung $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ mit $\varphi(x) := -2 \cdot x$ ist ein Gruppenhomomorphismus zwischen den Gruppen $(\mathbb{Z}, +)$ und $(2\mathbb{Z}, +)$. Dies folgt aus dem Distributivgesetz

$$(-2) \cdot (x + y) \;=\; (-2) \cdot x + (-2) \cdot y \;\; .$$

(ii) Die Abbildung $\varphi : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ mit $\varphi(x) := 2^x$ ist ein Gruppenhomomorphismus zwischen der Gruppe $(\mathbb{R}, +)$ und der Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$. Das folgt aus der Potenzrechenregel

$$2^{x+y} \;=\; 2^x \cdot 2^y \qquad \text{für } x, y \in \mathbb{R}.$$

Lemma 2.2.14. *Sind $(G, \circ)$ und $(G', \bullet)$ Gruppen mit neutralen Elementen $e \in G$ und $f \in G'$ und ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, dann gilt $\varphi(e) = f$ und $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in G$.*

Beweis. Für das neutrale Element $e \in G$ gilt

$$\begin{aligned} \varphi(e) \;&=\; \varphi(e) \bullet f \;=\; \varphi(e) \bullet (\varphi(e) \bullet \varphi(e)^{-1}) \;=\; (\varphi(e) \bullet \varphi(e)) \bullet \varphi(e)^{-1} \\ &=\; \varphi(e \circ e) \bullet \varphi(e)^{-1} \;=\; \varphi(e) \bullet \varphi(e)^{-1} \;=\; f \;\; . \end{aligned}$$

Es sei nun $x \in G$ beliebig. Dann gilt

$$\begin{aligned} \varphi(x^{-1}) \;&=\; \varphi(x^{-1}) \bullet f \;=\; \varphi(x^{-1}) \bullet (\varphi(x) \bullet \varphi(x)^{-1}) \;=\; (\varphi(x^{-1}) \bullet \varphi(x)) \bullet \varphi(x)^{-1} \\ &=\; \varphi(x^{-1} \circ x) \bullet \varphi(x)^{-1} \;=\; \varphi(e) \bullet \varphi(x)^{-1} \;=\; f \bullet \varphi(x)^{-1} \;=\; \varphi(x)^{-1} \;\; . \end{aligned}$$

□

Lemma 2.2.15. *Sind $(G, \circ)$ und $(G', \bullet)$ Gruppen mit neutralen Elementen $e \in G$ und $f \in G'$ und ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, dann bilden die Elemente in* $\mathrm{Kern}(\varphi) := \{x \in G \mid \varphi(x) = f\} \subseteq G$ *(der* Kern *von φ) eine Untergruppe von G und die Elemente in* $\mathrm{Bild}(\varphi) := \varphi(G) \subseteq G'$ *(das* Bild *von φ) eine Untergruppe von G'.*

Beweis. Wir beweisen, dass die Elemente in $\mathrm{Kern}(\varphi)$ eine Untergruppe von G bilden. Dazu überprüfen wir die in Definition 2.2.6 geforderten Eigenschaften. Eigenschaft (i) gilt, da nach Lemma 2.2.14 $\varphi(e) = f$. Um Eigenschaft (ii) zu überprüfen, betrachten wir $x, y \in \mathrm{Kern}(\varphi)$. Dann gilt

$$\varphi(x \circ y) = \varphi(x) \bullet \varphi(y) = f \bullet f = f \;\; ,$$

so dass also $x \circ y \in \text{Kern}(\varphi)$. Eigenschaft (iii) ist schließlich erfüllt, da für $x \in \text{Kern}(\varphi)$ gilt, dass $\varphi(x^{-1}) = \varphi(x)^{-1} = f^{-1} = f$.

Den Beweis des zweiten Teils des Lemmas lassen wir als Übung. □

Wir verallgemeinern als nächstes den Begriff des Homomorphismus auf Ringe.

Definition 2.2.16 (Ringhomomorphismen)**.** Sind $(R, +, \cdot)$ und $(R', \oplus, \odot)$ Ringe und $\varphi : R \to R'$ eine Abbildung, dann heißt φ *Ringhomomorphismus*, falls

$$\varphi(x + y) = \varphi(x) \oplus \varphi(y) \qquad \text{und} \qquad \varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$$

für alle $x, y \in R$.

Beispiele.

(i) Die Abbildung $\varphi : 2\mathbb{Z} \to \mathbb{Z}$ mit $\varphi(z) = z$ ist ein Ringhomomorphismus.

(ii) Es sei $z \in \mathbb{Z}$ eine ganze Zahl. Dann ist die durch

$$\sum_{i=1}^{n} a_i X^i \;\mapsto\; \sum_{i=1}^{n} a_i z^i$$

definierte Abbildung von $\mathbb{Z}[X]$ nach $\mathbb{Z}$ ein Ringhomomorphismus. Wir sprechen hier auch von dem *Einsetzungshomomorphismus*, da die Zahl z in ein Polynom „eingesetzt“ wird.

Im Zusammenhang mit Homomorphismen (auf Gruppen oder auf Ringen) verwendet man auch die folgenden Begriffe:

Definition 2.2.17 (Monomorphismus, Epimorphismus, Isomorphismus)**.**

(i) Ein injektiver Homomorphismus heißt *Monomorphismus*.

(ii) Ein surjektiver Homomorphismus heißt *Epimorphismus*.

(iii) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

2.3 Die komplexen Zahlen

Die komplexen Zahlen sind unverzichtbar für nahezu jede Art von höherer Mathematik, z.B. für die in der Physik, der Elektrotechnik oder der Informationstechnik verwendete Mathematik. Im systematischen Aufbau der Mathematik gehören die komplexen Zahlen zum einen in die Analysis, denn viele bekannte Funktionen sind in natürlicher Weise auf der Menge $\mathbb{C}$ der komplexen Zahlen definiert. Auch wenn man vorrangig an reellen Funktionen interessiert ist, werden die Eigenschaften oft transparenter, wenn man sie (auch) als komplexe Funktionen betrachtet. Auf der

anderen Seite gehören die komplexen Zahlen genauso auch in die Algebra und Zahlentheorie: Sie stellen eine natürliche Erweiterung der üblichen Zahlbereiche dar, auf die man beim Lösen algebraischer Gleichungen geführt wird. Aufgrund ihrer generellen Bedeutung tauchen die komplexen Zahlen natürlich auch in der Informatik im Zusammenhang mit diversen konkreten algorithmischen Problemen auf.

Bevor wir eine formale Konstruktion/Definition der komplexen Zahlen als Körper angeben, beschreiben wir sie zunächst als eine Erweiterung der reellen Zahlen:

- Gegenüber den reellen Zahlen $\mathbb{R}$ sind die komplexen Zahlen $\mathbb{C}$ dadurch ausgezeichnet, dass es ein spezielles Element $i \in \mathbb{C}$ gibt mit der Eigenschaft $i^2 = i \cdot i = -1$. Die Zahl i heißt auch *imaginäre Zahl*.
- Damit können wir die komplexen Zahlen jetzt wie folgt beschreiben: $\mathbb{C} = \{a + b \cdot i \mid a, b \in \mathbb{R}\}$, wobei

$$a + b \cdot i \;=\; a' + b' \cdot i \iff (a = a' \;\wedge\; b = b') \;.$$

- Für eine komplexe Zahl $z = a + b \cdot i = a + bi$ nennen wir $\mathrm{Re}(z) := a$ den *Realteil* und $\mathrm{Im}(z) := b$ den *Imaginärteil* von z.

Mit Hilfe dieser informellen Beschreibung können wir jetzt schon mit komplexen Zahlen rechnen:

Beispiel. $2 + 3i$ und $5 - 2i := 5 + (-2)i$ sind komplexe Zahlen. Die Summe und das Produkt dieser Zahlen können wie folgt berechnet werden:

$$\begin{aligned}(2 + 3i) + (5 - 2i) &= (2 + 5) + (3i + (-2)i) \\ &= (2 + 5) + (3 + (-2))i \\ &= 7 + i\end{aligned}$$

$$\begin{aligned}(2 + 3i) \cdot (5 - 2i) &= 2 \cdot 5 + 2 \cdot (-2) \cdot i + 3 \cdot i \cdot 5 + 3 \cdot i \cdot (-2) \cdot i \\ &= 2 \cdot 5 + 2 \cdot (-2) \cdot i + 3 \cdot 5 \cdot i + 3 \cdot (-2) \cdot i \cdot i \\ &= 10 + (-6)(-1) + (-4 + 15) \cdot i \\ &= (10 + 6) + (15 - 4)i \\ &= 16 + 11i\end{aligned}$$

Wir geben jetzt eine formale Definition der komplexen Zahlen mit Addition und Multiplikation an.

Definition 2.3.1 (Komplexe Zahlen)**.** Es sei $\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$. Wir definieren auf der Menge $\mathbb{C}$ die Verknüpfungen $\oplus$ und $\odot$ wie folgt:

$$\begin{aligned}\oplus &: \mathbb{C} \times \mathbb{C} \to \mathbb{C} \;, \qquad ((a, b), (a', b')) \mapsto (a + a', b + b') \;, \\ \odot &: \mathbb{C} \times \mathbb{C} \to \mathbb{C} \;, \qquad ((a, b), (a', b')) \mapsto (a \cdot a' - b \cdot b', a \cdot b' + b \cdot a') \;.\end{aligned}$$

Satz 2.3.2 (Körper der komplexen Zahlen)**.** *Die komplexen Zahlen bilden einen Körper* $(\mathbb{C}, \oplus, \odot)$*.*

Beweisskizze. Es ist eine Fleißarbeit, sich davon zu überzeugen, dass die Verknüpfungen $\oplus$ und $\odot$ das Assoziativ-, Kommutativ- und Distributivgesetz erfüllen. Das neutrale Element der Addition (Nullelement) ist $(0,0)$ und das inverse Element zu (a,b) bezüglich der Addition ist $(-a,-b)$. Das neutrale Element der Multiplikation (Einselement) ist $(1,0)$ und das inverse Element zu $(a,b) \neq (0,0)$

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \ .$$

Damit ist $(\mathbb{C}, \oplus, \odot)$ also ein Körper. □

Anstelle der Schreibweise (a,b) für eine komplexe Zahl verwendet man normalerweise die bereits oben eingeführte Variante $a+bi$. Diese Schreibweise verdeutlicht, dass die komplexen Zahlen als Erweiterung der reellen Zahlen aufgefasst werden können. Mit anderen Worten werden die reellen Zahlen als Teilmenge der komplexen Zahlen aufgefasst, indem man die reelle Zahl a mit der komplexen Zahl $a+0i$ identifiziert. Diese Interpretation wird durch den folgenden Satz untermauert:

Satz 2.3.3. *Die Abbildung* $\varphi : \mathbb{R} \to \mathbb{C}$ *mit* $\varphi(a) := a + 0i$ *ist ein injektiver Ringhomomorphismus (Ringmonomorphismus).*

Beweis. Nach Definition gilt für $a, a' \in \mathbb{R}$:

$$\varphi(a+a') = (a+a') + 0i = (a+0i) \oplus (a'+0i) = \varphi(a) \oplus \varphi(a')$$

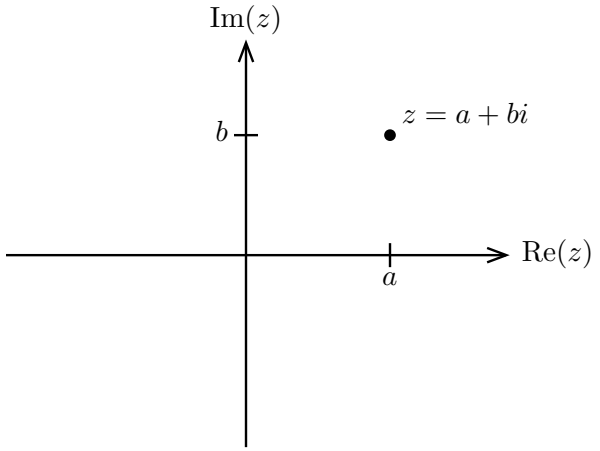
und

$$\varphi(a \cdot a') = (a \cdot a') + 0i = (a+0i) \odot (a'+0i) = \varphi(a) \odot \varphi(a') \ .$$

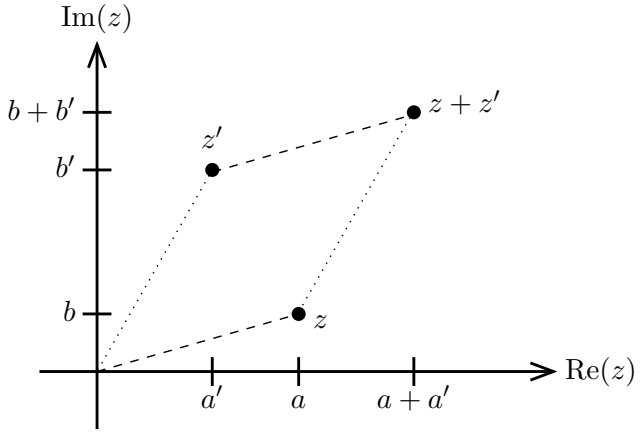
Folglich ist φ ein Homomorphismus. Außerdem ist φ injektiv, da aus $a+0i = \varphi(a) = \varphi(a') = a'+0i$ sofort $a = a'$ folgt. □

Man verwendet daher für die Addition und Multiplikation komplexer Zahlen die von den reellen Zahlen bekannten Verknüpfungssymbole $+$ und $\cdot$. Das Einselement von $\mathbb{C}$ schreibt man auch kurz als 1 (statt $1+0i$) und das Nullelement als 0 (statt $0+0i$).

Die komplexen Zahlen können als Punkte der Ebene $\mathbb{R}^2$ interpretiert werden. Die beiden Koordinaten eines Punktes sind dann durch Realteil und Imaginärteil der entsprechenden komplexen Zahl gegeben:



Die Addition zweier komplexer Zahlen entspricht dann der üblichen Addition von Vektoren:



Definition 2.3.4 (Betrag)**.** Für $z = a + bi \in \mathbb{C}$ heißt $|z| := \sqrt{a^2 + b^2}$ der *Betrag* von z.

Der Betrag einer komplexen Zahl ist also nach dem Satz des Pythagoras der Abstand des entsprechenden Punktes in der Ebene vom Nullpunkt. Die Zahl $|z|^2 = a^2 + b^2$ kann man auch als $(a+bi)(a-bi)$ schreiben. Der zweite Faktor war uns schon beim Inversen einer komplexen Zahl begegnet. Für diese Zahl gibt es einen eigenen Namen.

Definition 2.3.5 (Konjugiert-komplexe Zahl)**.** Für eine gegebene komplexe Zahl $z = a+bi,\ a, b \in \mathbb{R}$ heißt $\overline{z} := a-bi$ die *zu z konjugierte* oder *konjugiert-komplexe* Zahl. Die Abbildung $\mathbb{C} \to \mathbb{C}$ mit $z \mapsto \overline{z}$ heißt *komplexe Konjugation*.

Für die komplexe Konjugation gelten die folgenden Rechenregeln:

Lemma 2.3.6. *Es seien $z, w \in \mathbb{C}$. Dann gilt*

(i) $\overline{z + w} = \overline{z} + \overline{w}$,

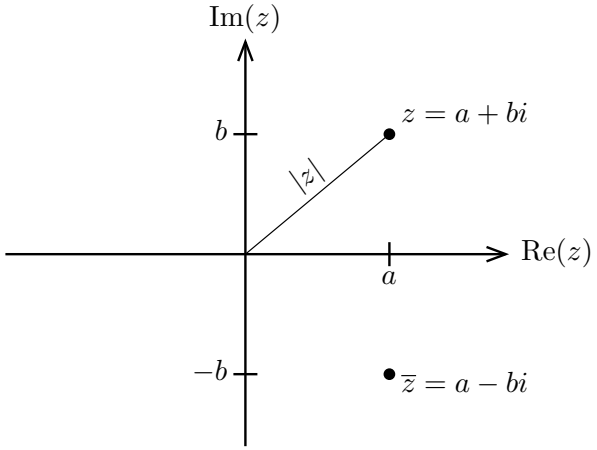
(ii) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$,

(iii) *Es seien* $z, w \in \mathbb{C}$. *Dann gilt* $|z|^2 = z \cdot \overline{z}$,

(iv) $z^{-1} = \overline{z}/|z|^2$ *falls* $z \neq 0$.

Beweis. Nachrechnen! □

Geometrisch entspricht der Übergang zur konjugiert-komplexen Zahl der Spiegelung an der reellen Achse (x-Achse).



Die Betragsfunktion hat die folgenden Eigenschaften:

Lemma 2.3.7. *Es seien* $z, w \in \mathbb{C}$. *Dann gilt*

(i) $|z| \geq 0$,

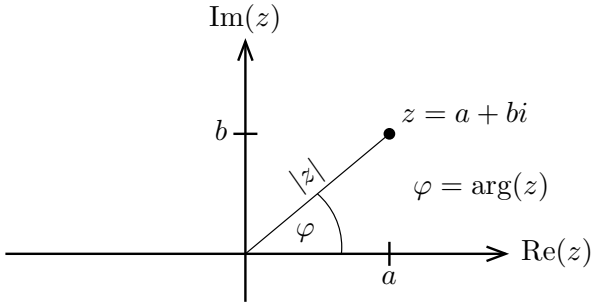
(ii) $|z| = 0 \iff z = 0$,

(iii) $|zw| = |z||w|$,

(iv) $|z + w| \leq |z| + |w|$ *(Dreiecksungleichung).*

Beweis. Nachrechnen! □

Man kann die komplexen Zahlen $z = a+bi$ statt in „kartesischen Koordinaten“ (a, b) auch in sogenannten *Polarkoordinaten* darstellen. Dazu betrachten wir den Winkel φ, den der Vektor $(a, b) \in \mathbb{R}^2$ mit der reellen Achse einschließt. Dieser Winkel wird mit $\arg(z)$ bezeichnet (*Argument von* z).



Dann gilt:

$$\cos\varphi = \frac{a}{|z|} \qquad \text{und} \qquad \sin\varphi = \frac{b}{|z|} \ .$$

Im Vorgriff auf die Analysis verwenden wir hier schon einige elementare Fakten über trigonometrische Funktionen.

Satz 2.3.8 (Polarkoordinaten-Darstellung komplexer Zahlen)**.**

a) Jede komplexe Zahl $z \neq 0$ kann eindeutig geschrieben werden als

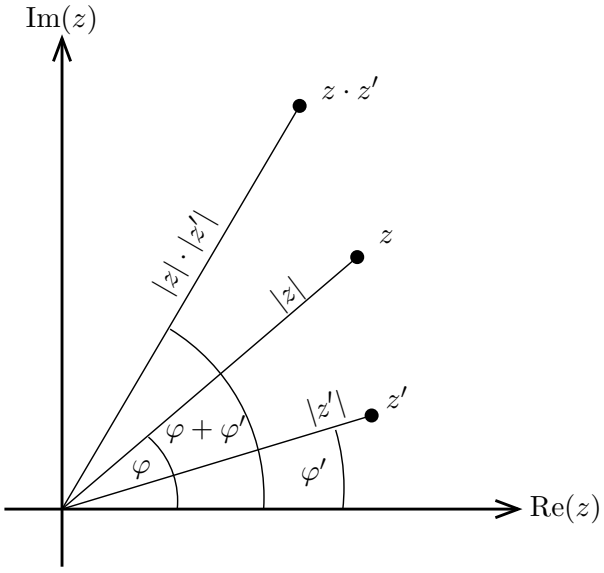
$$z = r \cdot (\cos\varphi + i \sin\varphi) \text{ mit } r \in \mathbb{R}_{\geq 0},\ \varphi \in [0, 2\pi[\ .$$

Dabei ist $r = |z|$, und φ entspricht dem Winkel zwischen z und der reellen Achse. Die Zahlen (r, φ) heißen Polarkoordinaten *von z.*

b) Für die Multiplikation komplexer Zahlen gilt

$$z \cdot z' = r \cdot r' \cdot \big(\cos(\varphi + \varphi') + i \sin(\varphi + \varphi')\big) \ .$$

Das heißt, die Beträge der beiden komplexen Zahlen werden multipliziert und die Winkel addiert.



Beispiel. Betrachte die komplexe Zahl $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{3} \cdot i$. Mit etwas Rechnung zeigt man $\omega^3 = -1,\ \omega^6 = 1$. Mit Polarkoordinaten geht dieses ohne Rechnung: Es ist $|\omega| = 1$ und $\frac{1}{2} = \cos(\frac{\pi}{3}),\ \frac{\sqrt{3}}{2} = \sin(\frac{\pi}{3})$, also

$$\omega = \cos\frac{\pi}{3} + i \sin\frac{\pi}{3} \ .$$

Also ist $\omega^3 = \cos\pi + i\sin\pi = -1,\ \omega^6 = \cos(2\pi) + i\sin(2\pi) = 1$.

Eine sehr wichtige Folgerung der Polarkoordinaten-Darstellung ist der folgende Satz.

Satz 2.3.9.

a) Jede komplexe Zahl $z = r \cdot (\cos\varphi + i \sin\varphi)$ *besitzt eine Quadratwurzel, nämlich* $\sqrt{z} := \sqrt{r} \cdot (\cos\frac{\varphi}{2} + i \sin\frac{\varphi}{2})$.

b) Allgemeiner besitzt z *auch* n*-te Wurzeln für alle* $n \in \mathbb{N}$*, also Zahlen* $c \in \mathbb{C}$ *mit* $c^n = z$*. Dieses sind die Zahlen*

$$c_k := \sqrt[n]{r} \cdot \left(\cos\frac{\varphi}{n} + i \sin\frac{\varphi}{n}\right) \cdot \left(\cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}\right), \quad k = 0, \ldots, n-1.$$

Die Zahlen

$$\omega_n^k := \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n} \qquad \text{mit} \quad k = 0, 1, \ldots, n-1$$

heißen auch n-te *Einheitswurzeln*. Sie sind die Lösungen der Gleichung $z^n = 1$. In der Tat gilt mit $\omega_n := \omega_n^1$, dass ω_n^k wirklich die k-te Potenz $(\omega_n)^k$ ist.

In Wirklichkeit gilt in $\mathbb{C}$ noch viel mehr als nur die Existenz von Wurzeln: Jede *Gleichung* n*-ten Grades*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \quad \text{mit} \quad a_k \in \mathbb{C},\ a_n \neq 0$$

besitzt in $\mathbb{C}$ wenigstens eine Lösung. Wenn man die Lösungen mit geeigneten Vielfachheiten versieht, so besitzt die Gleichung sogar n Lösungen. Die genaue Formulierung des Sachverhaltes geben wir im folgenden Satz ohne Beweis an.

Theorem 2.3.10 (Fundamentalsatz der Algebra)**.** *Jede Polynomfunktion* $f : \mathbb{C} \to \mathbb{C}$ *mit*

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$$

mit komplexen Koeffizienten a_j *und* $a_n \neq 0$ *besitzt eine Darstellung*

$$f(z) = a_n (z - c_1)(z - c_2) \cdots (z - c_n)$$

mit n *(nicht notwendig verschiedenen) komplexen Zahlen* $c_1, \ldots, c_n$.

Satz 2.3.9 b) ist in dem Theorem natürlich enthalten: Durch Lösen von

$$z^n - a = 0$$

kann man die n-ten Wurzeln einer beliebigen komplexen Zahl a finden.

2.4 Primfaktorzerlegung und der euklidische Algorithmus

Dieser und der folgende Abschnitt dieses Kapitels sind im Zusammenhang zu sehen: Sie handeln von dem Ring der ganzen Zahlen $\mathbb{Z}$ mit den Verknüpfungen Addition und Multiplikation und von daraus abgeleiteten Strukturen. Die Addition auf $\mathbb{Z}$ birgt keinerlei Geheimnisse; sie reduziert sich, wenn man so will, vollständig auf den durch die Peano-Axiome (siehe Definition 2.1.1) geregelten Prozess des „Weiterzählens“ (vergleiche auch mit dem Induktionsprinzip in Abschnitt 2.1.2), sowie auf die Konstruktion negativer Zahlen. Ganz anders ist es mit der multiplikativen Struktur von $\mathbb{Z}$, die bei näherem Hinsehen sehr viel komplizierter ist (auch wenn sie von der Definition her vollständig auf die Addition zurückgeführt werden kann). Entscheidend ist hier der Begriff *Primzahl* (siehe Definition 2.1.7), also einer Zahl, die bezüglich Multiplikation nicht weiter zerlegt werden kann. Es ist bekannt und nicht schwer zu zeigen, dass jede natürliche Zahl in ein Produkt von Primzahlen zerlegt werden kann. Deutlich schwieriger ist es, exakt und lückenlos zu begründen, dass eine solche Zerlegung eindeutig ist (bis auf die Reihenfolge der Faktoren). Ein Beweis dieser Tatsache (sogenannter “Fundamentalsatz der Arithmetik”) liegt für uns eher am Rande, zentral und wichtig ist jedoch ein dabei benutztes Konzept, nämlich der *größte gemeinsame Teiler*, kurz ggT zweier Zahlen sowie der *euklidische Algorithmus*, der den ggT berechnet. Hier liegt der Schwerpunkt des folgenden Abschnitts.

Es ist seit langem bekannt, dass der ggT in der Zahlentheorie unabhängig von der Primfaktorzerlegung der beiden in Frage stehenden Zahlen behandelt werden kann. In den letzten 30 Jahren hat sich gezeigt, dass an dieser Stelle auch der Ausgangspunkt für außerordentlich wichtige Anwendungen der Zahlentheorie in der Kryptographie liegt. Etwas verkürzt zusammengefasst kann man sagen, dass wichtige Kryptosysteme, insbesondere das bekannte RSA-Verfahren, darauf beruhen, dass der euklidische Algorithmus und gewisse andere Operationen auch für sehr große Zahlen effizient durchführbar sind, dass aber das Problem der Primfaktorzerlegung „algorithmisch schwer“ ist.

2.4.1 Division mit Rest

Wir halten zunächst eine grundlegende Eigenschaft der ganzen Zahlen fest.

Lemma 2.4.1 (Division mit Rest in $\mathbb{Z}$)**.** *Es sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, m-1\}$, so dass*

$$a = qm + r \ .$$

Die Zahl q heißt der Quotient *und r heißt der* Rest *von a bei Division durch m. Die Zahl r wird mit $a \bmod m$ oder $a \,\%\, m$ bezeichnet.*

Beweis. Es sei q die größte ganze Zahl mit $q \cdot m \leq a$. Dann gilt $0 \leq a - q \cdot m < m$ und wir können $r := a - q \cdot m$ setzen. □

Beispiele.

$$\begin{array}{lrcll} m = 6: & 23 & = & 3 \cdot 6 + 5 & \text{Rest } r = 5 \quad 23 \bmod 6 = 5 \\ & -2 & = & (-1) \cdot 6 + 4 & \text{Rest } r = 4 \quad -2 \bmod 6 = 4 \\ & 4 & = & 0 \cdot 6 + 4 & \text{Rest } r = 4 \quad 4 \bmod 6 = 4 \\ m = 17: & 100 & = & 5 \cdot 17 + 15 & \text{Rest } r = 15 \quad 100 \bmod 17 = 15 \\ & -50 & = & (-3) \cdot 17 + 1 & \text{Rest } r = 1 \quad -50 \bmod 17 = 1 \end{array}$$

Man sagt, dass a durch m *teilbar* ist, wenn die Division aufgeht, d.h. der Rest $r = 0$ ist. Dadurch wird die *Teilbarkeitsrelation* definiert, die wir bereits in Abschnitt 1.5 betrachtet hatten. Definitionsgemäß gilt also

$$b \mid a \quad :\Longleftrightarrow \quad \exists q \in \mathbb{Z} : a = q \cdot b \ .$$

2.4.2 Der euklidische Algorithmus

Wir beschreiben im Folgenden den euklidischen Algorithmus, der den größten gemeinsamen Teiler zweier positiver Zahlen x und y berechnet.

Euklidischer Algorithmus.
Eingabe: Zwei Zahlen $x, y \in \mathbb{N}$ mit $x \leq y$.
Ausgabe: Eine Zahl $d \in \mathbb{N}$.

1) Finde $q \in \mathbb{N}$ und $r \in \{0, 1, \ldots, x-1\}$ mit $y = q \cdot x + r$.
2) Ist $r = 0$, dann setze $d := x$ und STOPP.
3) Rufe den Algorithmus rekursiv mit $y := x$ und $x := r$ auf und gebe das berechnete d zurück.

Beispiel. Wir beschreiben die Berechnungen des euklidischen Algorithmus für die Eingabe $x = 221$ und $y = 1001$:

$$\begin{aligned} 1001 &= 4 \cdot 221 + 117 \\ 221 &= 1 \cdot 117 + 104 \\ 117 &= 1 \cdot 104 + 13 \\ 104 &= 8 \cdot 13 + 0 \end{aligned}$$

Der Algorithmus gibt also die Zahl $d = 13$ zurück.

Satz 2.4.2. *Es seien $x, y \in \mathbb{N}$ mit $x \leq y$. Dann terminiert der euklidische Algorithmus und die berechnete Zahl $d \in \mathbb{N}$ erfüllt die folgenden Bedingungen:*

(i) $d|x$ und $d|y$;

(ii) ist $z \in \mathbb{N}$ mit $z|x$ und $z|y$, so gilt $z|d$;

(iii) es gibt $a, b \in \mathbb{Z}$ mit $d = a \cdot x + b \cdot y$.

Definition 2.4.3. Es seien $x, y \in \mathbb{Z}$ und $d \in \mathbb{N}$, so dass d die Eigenschaften (i) und (ii) aus Satz 2.4.2 erfüllt. Dann wird d der *größte gemeinsame Teiler (ggT)* von x und y genannt. Man schreibt auch $\mathrm{ggT}(x, y) := d$.

Bemerkung. Aus technischen Gründen verlangen wir, dass der euklidische Algorithmus als Eingabe nur positive ganze Zahlen erhält. Das ist jedoch keine wirkliche Einschränkung, da für alle $x, y \in \mathbb{Z}$ gilt, dass

$$\mathrm{ggT}(x, y) \;=\; \mathrm{ggT}(-x, y) \;=\; \mathrm{ggT}(x, -y) \;=\; \mathrm{ggT}(-x, -y) \;.$$

Das liegt im Wesentlichen daran, dass für $d, z \in \mathbb{Z}$

$$d \mid z \qquad \Longleftrightarrow \qquad d \mid (-z)$$

gilt.

Als Folgerung aus Satz 2.4.2 (iii) erhalten wir das folgende Korollar.

Korollar 2.4.4 (Lemma von Bezout)**.** *Sind $x, y \in \mathbb{Z}$, so gibt es ganze Zahlen $a, b \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(x, y) \;=\; a \cdot x + b \cdot y \;.$$

Beispiele. a) Wir betrachten noch einmal das Beispiel von oben mit $x = 221$ und $y = 1001$. Der größte gemeinsame Teiler von 221 und 1001 ist 13 und es gilt $13 = (-9) \cdot 221 + 2 \cdot 1001$.

b) Es sei $x = 42$ und $y = 198$. Der euklidische Algorithmus berechnet

$$\begin{aligned} 198 &= 4 \cdot 42 + 30 && (2.3)\\ 42 &= 1 \cdot 30 + 12 && (2.4)\\ 30 &= 2 \cdot 12 + 6 && (2.5)\\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

und gibt $d = 6$ zurück. Die Menge der positiven gemeinsamen Teiler von 42 und 198 ist $\{1, 2, 3, 6\}$, so dass 6 in der Tat der größte gemeinsame Teiler ist. Außerdem gilt $6 = (-14) \cdot 42 + 3 \cdot 198$.

Wir erläutern kurz, wie man auf diese Darstellung von $d = 6$ kommt. Wegen (2.5) ist

$$6 \;=\; 1 \cdot 30 + (-2) \cdot 12 \;. \qquad (2.6)$$

Wegen (2.4) ist

$$12 \;=\; 1 \cdot 42 + (-1) \cdot 30 \;. \tag{2.7}$$

Einsetzen von (2.7) in (2.6) liefert

$$\begin{aligned} 6 \;&=\; 1 \cdot 30 + (-2) \cdot 12 \\ &=\; 1 \cdot 30 + (-2) \cdot (1 \cdot 42 + (-1) \cdot 30) \\ &=\; 3 \cdot 30 + (-2) \cdot 42 \;. \end{aligned} \tag{2.8}$$

Wegen (2.3) ist

$$30 \;=\; 1 \cdot 198 + (-4) \cdot 42 \;. \tag{2.9}$$

Einsetzen von (2.9) in (2.8) liefert schließlich

$$\begin{aligned} 6 \;&=\; 3 \cdot 30 + (-2) \cdot 42 \\ &=\; 3 \cdot (1 \cdot 198 + (-4) \cdot 42) + (-2) \cdot 42 \\ &=\; (-14) \cdot 42 + 3 \cdot 198 \;. \end{aligned}$$

Beweis von Satz 2.4.2. Wir beweisen zunächst, dass der euklidische Algorithmus für beliebige Eingaben $x, y \in \mathbb{N}$ mit $x \leq y$ terminiert. Der Beweis funktioniert mit vollständiger Induktion (siehe Satz 2.1.5) über x. Induktionsanfang: Ist $x = 1$, so gilt $y = y \cdot x + 0$ und der Algorithmus terminiert sofort in Schritt 2). Induktionsschluss: Wir nehmen an, dass für ein beliebiges aber fest gewähltes $k \in \mathbb{N}$ der Algorithmus für alle Eingaben mit $x \leq k$ terminiert. Erhält der Algorithmus als Eingabe nun $x = k + 1$ und ein $y \geq x$, so terminiert er entweder in Schritt 2) (falls $x|y$) oder er ruft sich selbst rekursiv mit der Eingabe $y := x$ und $x := r$ auf. Da $r < x$, terminiert der Algorithmus mit dieser Eingabe.

Wir zeigen als nächstes (i), also $d|x$ und $d|y$. Auch diese Behauptung zeigen wir mit vollständiger Induktion über x. Induktionsanfang: Ist $x = 1$, so terminiert der Algorithmus sofort in Schritt 2) und gibt $d = x = 1$ zurück. Offensichtlich gilt dann $d|x$ und $d|y$. Induktionsschluss: Wir nehmen an, dass für ein beliebiges aber fest gewähltes $k \in \mathbb{N}$ der Algorithmus für alle Eingaben mit $x \leq k$ eine Zahl $d \in \mathbb{N}$ mit $d|x$ und $d|y$ berechnet. Wir betrachten den Fall, dass der Algorithmus als Eingabe nun $x = k+1$ und ein $y \geq x$ erhält. Gilt $x|y$, so terminiert er in Schritt 2) und liefert $d = x$, so dass offenbar $d|x$ und $d|y$. Andernfalls ist $y = q \cdot x + r$ mit $q \in \mathbb{N}$ und $r \in \{0, 1, \ldots, x-1\}$ und der Algorithmus berechnet in Schritt (3) nach Induktion ein d mit $d|r$ (also $r = m \cdot d$ mit $m \in \mathbb{N}$) und $d|x$ (also $x = n \cdot d$ mit $n \in \mathbb{N}$). Da

$$y \;=\; q \cdot x + r \;=\; q \cdot n \cdot d + m \cdot d \;=\; (q \cdot n + m) \cdot d \;,$$

folgt auch $d|y$.

Wir zeigen als Nächstes (iii), wiederum mit vollständiger Induktion über x. Induktionsanfang: Ist $x = 1$, so terminiert der Algorithmus sofort in Schritt 2) und gibt $d = x = 1$ zurück. Dann gilt $d = 1 \cdot x + 0 \cdot y$. Induktionsschluss: Wir nehmen an, dass für ein beliebiges aber fest gewähltes $k \in \mathbb{N}$ der Algorithmus für alle Eingaben mit $x \leq k$ eine Zahl $d \in \mathbb{N}$ mit $d = a \cdot x + b \cdot y$ mit $a, b \in \mathbb{Z}$ berechnet. Wir betrachten den Fall, dass der Algorithmus als Eingabe nun $x = k + 1$ und ein $y \geq x$ erhält. Gilt $x|y$, so terminiert er in Schritt 2) und liefert $d = x$, so dass $d = 1 \cdot x + 0 \cdot y$ gilt. Andernfalls ist $y = q \cdot x + r$ mit $q \in \mathbb{N}$ und $r \in \{0, 1, \ldots, x - 1\}$ und der Algorithmus berechnet in Schritt (3) nach Induktion ein d mit $d = a' \cdot r + b' \cdot x$ mit $a', b' \in \mathbb{Z}$. Dann gilt

$$d \;=\; a' \cdot r + b' \cdot x \;=\; a' \cdot (y - q \cdot x) + b' \cdot x \;=\; (b' - a' \cdot q) \cdot x + a' \cdot y \;\; .$$

Setzt man also $a := b' - a' \cdot q \in \mathbb{Z}$ und $b := a' \in \mathbb{Z}$, so gilt $d = a \cdot x + b \cdot y$.

Zu guter Letzt zeigen wir noch (ii). Es sei $z \in \mathbb{N}$ mit $z|x$ (also $x = m \cdot z$ mit $m \in \mathbb{N}$) und $z|y$ (also $y = n \cdot z$ mit $n \in \mathbb{N}$). Wegen (iii) gibt es $a, b \in \mathbb{Z}$, so dass

$$d \;=\; a \cdot x + b \cdot y \;=\; a \cdot m \cdot z + b \cdot n \cdot z \;=\; (a \cdot m + b \cdot n) \cdot z$$

und damit $z|d$. □

Bemerkung. Es folgt aus Satz 2.4.2 und dem euklidischen Algorithmus, dass wir die Funktion $\mathrm{ggT} : \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\} \to \mathbb{N}$ wie folgt rekursiv schreiben können:

$$\mathrm{ggT}(x, y) \;=\; \begin{cases} x & \text{falls } x \mid y, \\ \mathrm{ggT}(y \bmod x, x) & \text{sonst.} \end{cases}$$

2.4.3 Primzahlen und Primfaktorzerlegung

Primzahlen sind nicht nur ein klassisches Thema der Mathematik, sondern auch für die Konstruktion algebraischer Strukturen von großer Bedeutung, mit Bezug auf die Informatik etwa für viele Fragen der Codierung und Übertragung von Daten. Das Gleiche gilt für den (theoretischen wie algorithmischen) Umgang mit beliebigen ganzen Zahlen. Es ist lohnend, sich mit dieser Grundstruktur etwas ausführlicher zu beschäftigen. Ziel dieses Unterabschnitts ist es, die Eindeutigkeit der Primfaktorzerlegung herzuleiten und zu beweisen.

Definition 2.4.5 (Relativ prim, teilerfremd)**.** Zwei Zahlen $x, y \in \mathbb{N}$ heißen *relativ prim* oder *teilerfremd*, falls $\mathrm{ggT}(x, y) = 1$.

Beispiel. Die Zahlen $143 = 11 \cdot 13$ und $119 = 7 \cdot 17$ sind relativ prim. Die Zahlen $126 = 2 \cdot 3 \cdot 3 \cdot 7$ und $231 = 3 \cdot 7 \cdot 11$ sind nicht relativ prim, da $\mathrm{ggT}(126, 231) = 3 \cdot 7 = 21$.

Aus dem Lemma von Bezout (Korollar 2.4.4) können wir die folgende alternative Charakterisierung des Begriffs „relativ prim“ folgern.

Korollar 2.4.6. *Zwei Zahlen $x, y \in \mathbb{N}$ sind genau dann relativ prim, wenn es ganze Zahlen $a, b \in \mathbb{Z}$ gibt mit $a \cdot x + b \cdot y = 1$.*

Wie wir weiter oben gesehen haben, kann man mit Hilfe des euklidischen Algorithmus nicht nur feststellen, ob x und y relativ prim sind, sondern auch die Zahlen $a, b \in \mathbb{Z}$ berechnen.

Beweis von Korollar 2.4.6. Sind x und y relativ prim, so existieren die ganzen Zahlen $a, b \in \mathbb{Z}$ wie gefordert nach Korollar 2.4.4.

Wir nehmen jetzt umgekehrt an, dass es $a, b \in \mathbb{Z}$ mit $a \cdot x + b \cdot y = 1$ gibt. Ist nun $z \in \mathbb{N}$ mit $z|x$ und $z|y$, so folgt daraus $z|1$ (vergleiche auch den Beweis von Satz 2.4.2 (ii)) und damit $z = 1$. Folglich ist der größte gemeinsame Teiler von x und y gleich 1. □

In Vorbereitung auf den Beweis der Eindeutigkeit der Primzahlzerlegung, beweisen wir zunächst das folgende wichtige Lemma.

Lemma 2.4.7. *Es seien $x, y, z \in \mathbb{N}$. Gilt $x \mid (y \cdot z)$ und sind x und y relativ prim, dann gilt $x \mid z$.*

Beweis. Da x und y relativ prim sind, gibt es nach Korollar 2.4.6 Zahlen $a, b \in \mathbb{Z}$ mit $a \cdot x + b \cdot y = 1$. Folglich gilt

$$z \;=\; (a \cdot x + b \cdot y) \cdot z \;=\; \left(a \cdot z + b \cdot \frac{y \cdot z}{x}\right) \cdot x \;. \tag{2.10}$$

Da x ein Teiler von $y \cdot z$ ist, ist $\frac{y \cdot z}{x}$ eine ganze Zahl. Folglich ist nach (2.10) die Zahl z ein ganzzahliges Vielfaches von x, so dass $x \mid z$. □

Der folgende bekannte Satz wird oft auch als der „Hauptsatz“ oder „Fundamentalsatz der Arithmetik“ bezeichnet.

Satz 2.4.8 (Eindeutigkeit der Primfaktorzerlegung)**.**

a) Jede natürliche Zahl $n > 1$ lässt sich als Produkt von Primzahlen schreiben:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r, \qquad \textit{mit} \quad p_1, p_2, \ldots, p_r \textit{ Primzahlen.}$$

b) Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren. Das heißt, wenn auch $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ ist mit q_j prim für $j = 1, \ldots, s$, so ist $r = s$, und wenn wir ferner $p_1 \leq p_2 \leq \ldots \leq p_r$ und $q_1 \leq q_2 \leq \ldots \leq q_r$ annehmen, so ist $p_i = q_i$ für $i = 1, \ldots, r$.

Beweis. Wir beweisen zunächst Teil a) des Satzes, also die Existenz einer Primfaktorzerlegung. Der Beweis benutzt vollständige Induktion über n. Induktionsanfang: Die Behauptung ist klar für $n = 2$, da 2 selbst eine Primzahl ist. Induktionsschluss: Wir nehmen an, dass die Behauptung für alle n mit $2 \leq n \leq k$ wahr ist und betrachten jetzt den Fall $n := k + 1$. Ist n eine Primzahl, so ist die Behauptung klar. Andernfalls gibt es nach Lemma 2.1.6 eine Primzahl p mit $p \mid n$. Nach Induktionsannahme gibt es eine Primfaktorzerlegung für die Zahl $\frac{n}{p}$, d.h. $\frac{n}{p} = p_1 \cdot p_2 \cdot \cdots \cdot p_r$ mit p_i Primzahl für $1 \leq i \leq r$. Daraus erhält man die folgende Primfaktorzerlegung für n:

$$n \;=\; p \cdot \frac{n}{p} \;=\; p \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_r \;\; .$$

Wir kommen jetzt zu Teil b) des Satzes, also zur Eindeutigkeit der Primfaktorzerlegung. Auch dieser Teil wird mit vollständiger Induktion bewiesen. Induktionsanfang: Die Behauptung ist klar für $n = 2$. Induktionsschluss: Wir nehmen an, dass die Behauptung für alle n mit $2 \leq n \leq k$ wahr ist und betrachten jetzt den Fall $n := k + 1$. Es seien

$$n \;=\; p_1 \cdot p_2 \cdot \cdots \cdot p_r \tag{2.11}$$

und

$$n \;=\; q_1 \cdot q_2 \cdot \cdots \cdot q_s \tag{2.12}$$

zwei Primfaktorzerlegungen von n mit $p_1 \leq p_2 \leq \cdots \leq p_r$ und $q_1 \leq q_2 \leq \cdots \leq q_s$. Gilt $p_1 = q_1$, so ist $n' := p_2 \cdot \cdots \cdot p_r = q_2 \cdot \cdots \cdot q_s$ und aus der Induktionsannahme folgt, dass die Zahl $n' < n$ eine eindeutige Primfaktorzerlegung besitzt. Daher gilt dann $r = s$ und $p_i = q_i$ für alle $1 \leq i \leq r$.

Es bleibt also nur noch zu zeigen, dass $p_1 = q_1$. Wir führen einen Widerspruchsbeweis und nehmen an, dass $p_1 < q_1$ (der Fall $p_1 > q_1$ kann völlig analog behandelt werden). Aus (2.11) folgt, dass $p_1 \mid n$. Da p_1 und q_1 verschiedene Primzahlen sind, sind sie relativ prim, so dass aus (2.12) und Lemma 2.4.7 folgt, dass $p_1 \mid q_2 \cdot \cdots \cdot q_s$. Nach Induktionsannahme besitzt die Zahl $n' = q_2 \cdot \cdots \cdot q_s$ eine eindeutige Primfaktorzerlegung. Da $p_1 \mid n'$, muss also $p_1 = q_i$ für ein i mit $2 \leq i \leq s$ gelten[4]. Dies führt jedoch zu einem Widerspruch, da $p_1 < q_1 \leq q_i$ für $2 \leq i \leq s$ gilt. □

Satz 2.4.8 sagt nur etwas über die Existenz einer eindeutigen Primfaktorzerlegung aus, nicht aber, wie man eine solche tatsächlich berechnen kann. Dazu kann das folgende Verfahren verwendet werden.

[4]Wir haben an dieser Stelle den Beweis etwas abgekürzt. Formal muss man wie folgt argumentieren: Da $p_1 \mid n'$, kann man n' als Produkt der natürlichen Zahlen p_1 und $\frac{n'}{p_1}$ schreiben. Nimmt man jetzt eine Primfaktorzerlegung von $\frac{n'}{p_1}$, so erhält man damit eine Primfaktorzerlegung von n', in der die Primzahl p_1 vorkommt. Aus der Eindeutigkeit der Primfaktorzerlegung von n' folgt dann die getroffene Behauptung.

Man schreibt sich vorbereitend die ersten Primzahlen der Größe nach geordnet in eine Liste:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots, p_k\ .$$

Dann testet man Teilbarkeit von n durch $2, 3, 5, 7, \ldots$. Sei p_i die kleinste Primzahl mit $p_i \mid n$. Ersetze n durch n/p_i und fahre so fort, beginnend nun mit der Primzahl p_i. Dieser kleinste Primteiler p_i ist tatsächlich 'klein', nämlich höchstens gleich $\sqrt{n}$, es sei denn, n ist selbst prim (warum?!). Man muss die Liste der Primzahlen also nur bis zur Größe $\sqrt{n}$ anlegen, wenn n die zu zerlegende Zahl ist.

Beispiel. Die Zahl 97 ist nicht durch $2, 3, 5, 7$ teilbar, also Primzahl. Denn nach 7 ist 11 die nächste Primzahl und $11 \cdot 11 > 97$.

Bemerkung. Der angedeutete naive Algorithmus zur Primfaktorzerlegung ist nicht besonders effizient. Wir sehen hier nur die Spitze eines Eisberges: In Wirklichkeit macht die Frage nach guten Algorithmen für die Primfaktorzerlegung und deren theoretische Analyse ein eigenes Teilgebiet der Mathematik, genauer der so genannten algorithmischen Zahlentheorie aus. Dabei spielen auch Konzepte der theoretischen Informatik (Komplexitätstheorie, probabilistische Algorithmen) eine bedeutende Rolle. Es gibt zwei weitere verwandte, aber nicht gleichwertige Fragestellungen: Das Finden großer Primzahlen, und der Beweis, dass gewisse Zahlen wirklich Primzahlen sind. Alle drei Probleme sind von großer Bedeutung für Verschlüsselungsverfahren und deren Sicherheit.

Zum Abschluss dieses Abschnitts beweisen wir noch, dass es unendlich viele Primzahlen gibt.

Satz 2.4.9 (Unendlichkeit der Menge aller Primzahlen)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir führen einen Beweis durch Widerspruch. Wir nehmen an, dass die Menge der Primzahlen endlich ist, nämlich $\{p_1, p_2, \ldots, p_r\}$. Nun betrachten wir die Zahl $n := 1 + \prod_{i=1}^{r} p_i$ und fragen uns, wie die eindeutige Primfaktorzerlegung von n aussieht. Da offenbar keine der Zahlen $p_1, \ldots, p_r$ Teiler von n ist, kann auch keine dieser Zahlen in der Primfaktorzerlegung von n vorkommen. Dies ist ein Widerspruch zu Satz 2.4.8. □

2.5 Modulare Arithmetik

Um die in der Einleitung zu Abschnitt 2.4 angedeuteten Verfahren für Datenverschlüsselung im einzelnen durchzuführen, aber auch für anders gelagerte Probleme der Speicherung und der Fehlerkorrektur von Daten, werden andere "Zahlbereiche" benötigt als die bisher bekannten. In diesem Abschnitt betrachten wir die wohl wichtigsten Beispiele solcher Rechenbereiche. Es wird zwar (auf den

ersten Blick) mit gewöhlichen ganzen Zahlen gearbeitet, genauer mit der Menge $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ für eine feste natürliche Zahl $m \geq 2$, aber die Rechenoperationen sind neu: Die Ergebnisse der gewöhnlichen Addition bzw. Multiplikation werden durch ihren jeweiligen Rest bei Division durch m ersetzt. Informell bezeichnet man diese Operationen als „modulo-m-Addition“ bzw. „modulo-m-Multiplikation“. Die resultierende Struktur $(\mathbb{Z}_m, +_m, \cdot_m)$ ist dann ein kommutativer Ring mit Eins.

2.5.1 Addition und Multiplikation modulo m

Definition 2.5.1 (mod-m-Addition und mod-m-Multiplikation)**.** Es sei $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ die Menge aller möglichen Reste modulo m. Auf $\mathbb{Z}_m$ definieren wir die beiden Verknüpfungen $+_m$ und $\cdot_m$ wie folgt:

$$\begin{aligned} x +_m y &:= (x + y) \bmod m \\ x \cdot_m y &:= (x \cdot y) \bmod m \end{aligned}$$

Wir nennen sie *Addition* bzw. *Multiplikation modulo* m, kurz *mod-m-Addition* bzw. *mod-m-Multiplikation*.

Beispiele. Wir schreiben im Folgenden die Verknüpfungstafeln beispielhaft für $m = 5$, 6 und 7 auf (siehe auch Abschnitt 2.2.2).

(i) Die Verknüpfungstafeln für $m = 5$:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(ii) Die Verknüpfungstafeln für $m = 6$:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(iii) Die Verknüpfungstafeln für $m = 7$:

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Die wesentlichen Eigenschaften der neuen Addition und Multiplikation werden in dem folgenden Satz festgehalten.

Satz 2.5.2 (Ring $\mathbb{Z}_m$)**.** *Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Eins.*

Für den Beweis des Satzes muss man vor allem eine Reihe von Rechengesetzen überprüfen. Dabei ist die folgende allgemeine Rechenregel von Nutzen.

Regel: *Man darf mehrschrittige Rechnungen in $\mathbb{Z}_m$ zunächst in $\mathbb{Z}$ führen und erst zum Schluss die Reduktion* $\bmod m$ *machen. So ist z.B.*

$$a \cdot_m x +_m b \cdot_m y = (ax + by) \bmod m\,.$$

Ähnlich ist $(a \cdot_m b) \cdot_m c = (abc) \bmod m$ und analog auch $a \cdot_m (b \cdot_m c) = (abc) \bmod m$, woraus sich die Assoziativität bereits ergibt.

Wir verzichten auf einen ausführlichen Beweis von Satz 2.5.2 und kehren stattdessen zu den obigen Verknüpfungstafeln zurück, um einige interessante Beobachtungen zu machen.

- Die Tafel für $+_m$ hat in allen Fällen eine offensichtliche „zyklische Struktur“: Jede Zeile enthält die Elemente 0 bis $m-1$ in der gleichen Reihenfolge, wobei man nach $m-1$ wieder mit der 0 beginnt; die jeweils nächste Zeile entsteht aus der vorigen, indem man sie um eins nach links verschiebt. All dies folgt direkt aus der Definition von $+_m$. Insbesondere enthält jede Zeile eine Permutation der Zahlen 0 bis $m-1$, d.h. jede dieser Zahlen kommt genau einmal vor.

- Die Struktur der Tafel für die Multiplikation ist komplizierter. Wir schauen im Augenblick nur auf die Frage der Permutation. In vielen Fällen ist die Zeile zu $a \in \mathbb{Z}_m$, d.h. die Liste der Vielfachen $a \cdot_m x$ mit $x = 0, 1, \ldots, m-1$, eine Permutation von $0, 1, \ldots, m-1$. Abgesehen von der Nullzeile zur 0 gilt das bei $m = 5$ und $m = 7$ für alle Zeilen. Bei $m = 6$ haben wir für $a = 2$, 3 und 4 keine Permutation.

2.5.2 Einheiten und Inverse

Wir fragen uns nun für allgemeines m: Für welche $a \in \{0, 1, \ldots, m-1\}$ ist die a-Zeile der Verknüpfungstafel eine Permutation von $\{0, 1, \ldots, m-1\}$? Wenn eine Permutation vorliegt, so kommt insbesondere die 1 vor, d.h. die Gleichung $a \cdot_m x = 1$ ist lösbar. Aus der Tatsache, dass wir in einem Ring arbeiten (genauer aus dem Assoziativgesetz der Multiplikation) folgt, dass auch die Umkehrung gilt: Sobald die 1 in der a-Zeile auftaucht, ist die Zeile eine Permutation. Wir entwickeln diesen Sachverhalt, der diverse Anwendungen hat, gleich in allgemeinen Ringen.

Definition 2.5.3 (Einheiten)**.** Es sei $(R, +, \cdot)$ ein Ring mit Eins. Ein Element $x \in R$ heißt *Einheit* oder *invertierbar*, falls ein $y \in R$ existiert mit

$$x \cdot y \;=\; y \cdot x \;=\; 1 \;.$$

Die Menge der Einheiten in R wird mit $R^* := \{x \in R \mid x \text{ Einheit}\}$ bezeichnet.

Wie im Fall von Gruppen (siehe Lemma 2.2.4) zeigt man, dass das *inverse Element* $y =: x^{-1}$ zu gegebener Einheit x eindeutig bestimmt ist.

Beispiele.

(i) Einheiten des Ringes $\mathbb{Z}$ sind lediglich die Zahlen 1 und -1.

(ii) Wir betrachten den Teilring $\mathbb{Z}[\sqrt{2}]$ (lies „$\mathbb{Z}$ adjungiert $\sqrt{2}$“) des Körpers $\mathbb{R}$ mit $\mathbb{Z}[\sqrt{2}] := \{x + y \cdot \sqrt{2} \mid x, y \in \mathbb{Z}\}$. In diesem Ring (mit der gewöhnlichen Addition und Multiplikation reeller Zahlen) ist $\sqrt{2}$ keine Einheit, aber $1+\sqrt{2}$ ist eine, denn $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$, und der zweite Faktor liegt wieder im betrachteten Ring.

(iii) Die Einheiten des Polynomrings $\mathbb{R}[x]$ sind die Polynome aX^0 mit $a \in \mathbb{R}\backslash\{0\}$. Das inverse Element zu aX^0 ist $a^{-1}X^0$. Da der Grad des Produkts zweier Polynome ungleich Null die Summe der Grade der beiden Polynome ist, können Polynome vom Grad größer Null keine Einheiten sein.

(iv) Das Nullelement eines beliebigen Rings R mit Eins ist keine Einheit, da nach Lemma 2.2.9 gilt: $0 \cdot x = x \cdot 0 = 0$ für alle $x \in R$.

(v) In einem beliebigen Körper $(K, +, \cdot)$ sind nach Definition alle Elemente ungleich Null Einheiten, d.h. $K^* = K \setminus \{0\}$.

Lemma 2.5.4. *Es sei $(R, +, \cdot)$ ein Ring mit Eins. Dann bilden die Einheiten von R eine multiplikative Gruppe, d.h. $(R^*, \cdot)$ ist eine Gruppe.*

Beweis. Wir müssen zunächst zeigen, dass die Multiplikation eine (assoziative) Verknüpfung auf R^* ist, das heißt, dass R^* abgeschlossen unter Multiplikation ist. Es seien also $x, y \in R^*$. Dann ist $x \cdot y \in R^*$, da

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) \;=\; (x \cdot (y \cdot y^{-1})) \cdot x^{-1} \;=\; (x \cdot 1) \cdot x^{-1} \;=\; x \cdot x^{-1} \;=\; 1$$

und

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) \;=\; (y^{-1} \cdot (x^{-1} \cdot x)) \cdot y \;=\; (y^{-1} \cdot 1) \cdot y \;=\; y^{-1} \cdot y \;=\; 1 \;.$$

Das neutrale Element der Gruppe ist natürlich $1 \in R^*$. Das inverse Element zu $x \in R^*$ ist das oben definierte x^{-1}, das nach Definition auch wieder eine Einheit und damit in R^* ist. □

Wir formulieren und beweisen nun allgemein die oben an Beispielen beobachtete Kennzeichnung von Einheiten.

Lemma 2.5.5. *Ein Element x eines Ringes $(R, +, \cdot)$ mit Eins ist genau dann Einheit, wenn die Abbildung*

$$L_x : R \to R,\; y \mapsto x \cdot y$$

bijektiv ist.

Beweis. Ist L_x, bijektiv, so gibt es ein $y \in R$ mit $1 = L_x(y) = x \cdot y$. Es bleibt zu zeigen, dass auch $y \cdot x = 1$ ist. Da die Abbildung L_x bijektiv ist, folgt dies aus

$$L_x(y \cdot x) \;=\; x \cdot (y \cdot x) \;=\; (x \cdot y) \cdot x \;=\; 1 \cdot x \;=\; x \;=\; x \cdot 1 \;=\; L_x(1) \;.$$

Folglich ist x eine Einheit.

Wir nehmen nun umgekehrt an, dass x eine Einheit ist und zeigen, dass L_x dann bijektiv ist. Zunächst ist L_x surjektiv, da

$$L_x(x^{-1} \cdot y) \;=\; x \cdot (x^{-1} \cdot y) \;=\; (x \cdot x^{-1}) \cdot y \;=\; 1 \cdot y \;=\; y \qquad \text{für alle } y \in R.$$

Weiterhin ist L_x injektiv, da für $y, z \in R$ mit $L_x(y) = L_x(z)$ gilt:

$$y \;=\; x^{-1} \cdot L_x(y) \;=\; x^{-1} \cdot L_x(z) \;=\; z \;.$$

Folglich ist L_x also bijektiv. □

Der folgende Satz klärt allgemein, welche Elemente Einheiten in $(\mathbb{Z}_m, +_m, \cdot_m)$ sind.

Satz 2.5.6 (Einheiten in $\mathbb{Z}_m$)**.** *Für $m \in \mathbb{N}$ ist ein Element $x \in \mathbb{Z}_m$ genau dann Einheit in $\mathbb{Z}_m$, wenn x und m relativ prim sind, d.h.*

$$\mathbb{Z}_m^* \;=\; \{x \in \mathbb{Z}_m \mid \mathrm{ggT}(x, m) = 1\} \;.$$

Beweis. Wenn x und m relativ prim sind, so gibt es nach Korollar 2.4.4 ganze Zahlen $a, b \in \mathbb{Z}$ mit

$$1 \;=\; \mathrm{ggT}(x, m) \;=\; a \cdot x + b \cdot m \;.$$

Es folgt

$$1 = (a \cdot x + b \cdot m) \bmod m = a \cdot x \bmod m = (a \bmod m) \cdot_m x \ .$$

Also ist x Einheit mit Inversem $a \bmod m$.

Wenn umgekehrt $x \in \mathbb{Z}_m^*$ ist, gibt es ein $a \in \mathbb{Z}_m$ mit $a \cdot_m x = 1$. Es gibt also ein Vielfaches $b \cdot m$ von m mit $a \cdot x + b \cdot m = 1$. Wegen Korollar 2.4.6 sind x und m dann relativ prim. □

Beispiele.

(i) Die Einheiten in $\mathbb{Z}_6$ sind die nicht durch 2 oder 3 teilbaren Zahlen in $\mathbb{Z}_6$, also 1 und 5, wie oben schon aus der Verknüpfungstafel abgelesen wurde.

(ii) Die Einheiten in $\mathbb{Z}_{10}$ sind 1, 3, 7 und 9.

(iii) Besonders interessant und wichtig ist der Fall, wenn $m = p$ eine Primzahl ist. Dann kann der ggT von x und m nur 1 oder m sein, und für alle Elemente $x \in \mathbb{Z}_m$ außer der Null muss er 1 sein, d.h. x ist Einheit.

Aus dem letzten Beispiel folgt der nächste Satz.

Satz 2.5.7 (Körper $\mathbb{Z}_p$)**.** *Für jede Primzahl p ist $(\mathbb{Z}_p, +_p, \cdot_p)$ ein Körper.*

2.5.3 Nullteiler

Die Einheiten eines Ringes sind diejenigen Elemente, die sich bezüglich der Multiplikation so verhalten, wie man es in einem Körper erwartet. Nun betrachten wir gewisse Elemente, die eine Abweichung vom Körper-Sein beinhalten, nämlich die sogenannten Nullteiler. In einem Körper gilt folgende, aus der Schule bekannte Regel: Wenn ein Produkt Null ist, so ist schon einer der Faktoren Null. Nullteiler sind diejenigen Elemente, die in Abweichungen von dieser Regel auftauchen. Der Einfachheit halber definieren wir sie nur in kommutativen Ringen.

Definition 2.5.8 (Nullteiler, Integritätsbereich)**.** Es sei $(R, +, \cdot)$ ein kommutativer Ring.

(i) Ein Element $x \in R$ heißt *Nullteiler*, falls $x \neq 0$ ist und ein $y \in R \setminus \{0\}$ existiert mit $x \cdot y = 0$.

(ii) Der Ring R heißt *nullteilerfrei* oder ein *Integritätsbereich*, falls R keine Nullteiler enthält.

Beispiele.

(i) Jeder Körper K ist nullteilerfrei.

(ii) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist nullteilerfrei.

(iii) Der Polynomring $\mathbb{R}[X]$ ist nullteilerfrei.

(iv) Der Ring $\mathbb{Z}_6$ besitzt Nullteiler, denn $2 \cdot_6 3 = 0$ und $2, 3 \in \mathbb{Z}_6 \setminus \{0\}$.

Beispiel (i) wird in dem folgenden Lemma verallgemeinert.

Lemma 2.5.9. *Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Eine Einheit $x \in R^*$ ist kein Nullteiler.*

Beweis. Nach Lemma 2.5.5 ist für $x \in R^*$ die Abbildung $y \mapsto x \cdot y$ bijektiv und damit injektiv. Da $x \cdot 0 = 0$ (Lemma 2.2.9) gilt also $x \cdot y \neq 0$ für alle $y \neq 0$. □

Der folgende Satz ist eine Erweiterung von Satz 2.5.7.

Satz 2.5.10. *Es sei $m \in \mathbb{N}$, $m \geq 2$. Für den Ring $(\mathbb{Z}_m, +_m, \cdot_m)$ sind die folgenden Aussagen äquivalent:*

(i) Die Zahl m ist Primzahl.

(ii) Der Ring $(\mathbb{Z}_m, +_m, \cdot_m)$ ist nullteilerfrei.

(iii) Der Ring $(\mathbb{Z}_m, +_m, \cdot_m)$ ist ein Körper.

Beweis. Wir beweisen den Satz mit einem sogenannten „Ringschluss“. Die Implikation (iii)$\Longrightarrow$(ii) folgt aus Lemma 2.5.9, da jedes Element ungleich Null in einem Körper nach Definition eine Einheit ist. Die Implikation (ii)$\Longrightarrow$(i) folgt (mittels Kontraposition) unmittelbar aus der Definition einer Primzahl. Denn wenn m keine Primzahl ist, so schreibe $m = a \cdot b$ mit $a > 1$ und $b > 1$. Dann ist $a \cdot_m b = 0$ in $\mathbb{Z}_m$, aber beide Faktoren sind ungleich 0. Die Implikation (i)$\Longrightarrow$(iii) haben wir bereits in Satz 2.5.7 festgestellt. □

2.5.4 Chinesischer Restesatz

Der chinesische Restesatz ist einer der anwendungsreichsten Sätze der elementaren Zahlentheorie. Er spielt insbesondere im Rahmen der Kryptographie eine bedeutende Rolle.

Satz 2.5.11 (Chinesischer Restesatz)**.** *Es sei $k \in \mathbb{N}$ und $m_1, \ldots, m_k \in \mathbb{N} \setminus \{1\}$ relativ prim (also $\mathrm{ggT}(m_i, m_j) = 1$ für alle $1 \leq i < j \leq k$). Dann gibt es zu beliebigen ganzen Zahlen $r_1, \ldots, r_k$ mit $0 \leq r_i < m_i$ für $i = 1, \ldots, k$ genau eine ganze Zahl x mit $0 \leq x < \prod_{i=1}^{k} m_i$, so dass*

$$x \bmod m_i \;=\; r_i \qquad \text{für } i = 1, \ldots, k.$$

Bemerkung. Die Voraussetzung, dass die Zahlen $m_1, \ldots, m_k$ relativ prim sind, ist von entscheidender Bedeutung. Ohne diese Voraussetzung ist der Satz nicht wahr.

Beispiele.

(i) Es sei $k = 2$, $m_1 = 10$ und $m_2 = 21$. Zu $r_1 = 1$ und $r_2 = 15$ gibt es genau eine Zahl $x \in \{0, 1, \ldots, 209\}$ mit

$$x \bmod 10 \;=\; 1 \qquad \text{und} \qquad x \bmod 21 \;=\; 15 \;.$$

Durch geschicktes Ausprobieren findet man heraus, dass es sich dabei um die Zahl $x = 141$ handelt.

(ii) Es sei wieder $k = 2$ und $m_1 = 10$, doch diesmal wählen wir $m_2 = 22$. Dann ist $\mathrm{ggT}(m_1, m_2) = 2$ und die beiden Zahlen sind damit nicht relativ prim. Man überzeugt sich leicht davon, dass es beispielsweise zu $r_1 = 0$ und $r_2 = 1$ keine ganze Zahl x gibt, so dass

$$x \bmod 10 \;=\; 0 \qquad \text{und} \qquad x \bmod 22 \;=\; 1 \;.$$

Aus $(x \bmod 10) = 0$ folgt nämlich insbesondere, dass die Zahl x gerade ist, während $(x \bmod 22) = 1$ impliziert, dass x ungerade ist.

Beweis von Satz 2.5.11. Es sei $n := \prod_{i=1}^{k} m_i$. Wir betrachten die beiden Mengen

$$\begin{aligned} A \;&:=\; \{0, 1, \ldots, n-1\} \qquad \text{und} \\ B \;&:=\; \{(r_1, \ldots, r_k) \in \mathbb{Z}^k \mid 0 \le r_i < m_i \text{ für } i = 1, \ldots, k\} \;. \end{aligned}$$

Nach Definition sind A und B gleichmächtig; es gilt $|A| = |B| = n$. Wir betrachten nun die Abbildung $f : A \to B$ mit

$$f(x) := (x \bmod m_1, \ldots, x \bmod m_k) \qquad \text{für } x \in A.$$

Wir werden im Folgenden zeigen, dass die Abbildung f bijektiv ist. Das bedeutet, dass es zu jedem $(r_1, \ldots, r_k) \in B$ genau ein $x \in A$ mit $f(x) = (r_1, \ldots, r_k)$ gibt. Das impliziert dann sofort die Behauptung des Satzes.

Wir zeigen zunächst, dass die Abbildung f injektiv ist. Es seien $x, y \in A$ mit $f(x) = f(y)$. Dann gilt also

$$x \bmod m_i \;=\; y \bmod m_i \qquad \text{für } i = 1, \ldots, k.$$

Wir zeigen mittels vollständiger Induktion über k, dass $n = \prod_{i=1}^{k} m_i$ ein Teiler von $x - y$ ist. Induktionsanfang: Für $k = 1$ folgt aus $(x \bmod m_1) = (y \bmod m_1)$ unmittelbar, dass $m_1 \mid (x - y)$. Induktionsschluss: Wir nehmen an, dass $\prod_{i=1}^{k-1} m_i \mid$

$(x-y)$. Außerdem gilt wegen $(x \bmod m_k) = (y \bmod m_k)$, dass $m_k \mid (x-y)$. Damit erhält man

$$m_k \;\Bigg|\; \underbrace{\prod_{i=1}^{k-1} m_i}_{\in\mathbb{Z}} \cdot \underbrace{\frac{x-y}{\prod_{i=1}^{k-1} m_i}}_{\in\mathbb{Z}} \quad .$$

Da m_k und $\prod_{i=1}^{k-1} m_i$ nach Voraussetzung des Satzes relativ prim sind, folgt mit Lemma 2.4.7, dass

$$m_k \;\Bigg|\; \frac{x-y}{\prod_{i=1}^{k-1} m_i}$$

und damit $\prod_{i=1}^{k} m_i \mid (x-y)$.

Wir haben also gezeigt, dass n ein Teiler von $x-y$ ist. Da $x, y \in A$, gilt $-n < x-y < n$ und damit folgt aus $n \mid (x-y)$ sofort $x-y = 0$, also $x = y$. Wir haben bislang gezeigt, dass $f : A \to B$ eine injektive Abbildung ist. Da außerdem $|A| = |B|$ ist, muss f sogar bijektiv sein. $\square$

Kapitel 3

Lineare Algebra

Dieses Kapitel beruht teilweise auf einer Vorlesung über Lineare Algebra, die im Wintersemester 1990/91 von Herrn Prof. Pahlings an der RWTH Aachen gehalten wurde. Gegenstand dieses Kapitels sind lineare Gleichungssysteme, Matrizen, Vektorräume und lineare Abbildungen. Lineare Gleichungssysteme treten in vielen technischen und wirtschaftlichen Zusammenhängen auf. Aus Sicht der Informatik sind sie bei zahlreichen Problemstellungen von Bedeutung, beispielsweise bei geometrischen Problemen in der graphischen Datenverarbeitung oder in der Robotik. Hier fasst man den uns umgebenden Raum als Vektorraum auf, so dass jeder Punkt des Raumes durch einen Vektor repräsentiert wird. Um räumliche Gegenstände in der Ebene darzustellen, beispielsweise auf einem Bildschirm, müssen wir lineare Abbildungen vom dreidimensionalen in den zweidimensionalen Raum durchführen. Solche lineare Abbildungen können mit Hilfe von Matrizen dargestellt werden.

Es sei im Folgenden immer $(K, +, \cdot)$ ein Körper (z.B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3 \ldots$). Die Elemente des Körpers K nennen wir auch *Skalare*.

3.1 Lineare Gleichungssysteme und Matrizen

In diesem Abschnitt beschäftigen wir uns mit linearen Gleichungssystemen und deren Lösung mit Hilfe des Gauß'schen Eliminationsverfahrens. Dabei erweisen sich Matrizen als geeignete Hilfsmittel und Rechenwerkzeuge.

Definition 3.1.1 (Lineare Gleichungssysteme)**.** Ein *lineares Gleichungssystem* über dem Körper K hat die Form

$$\begin{array}{ccccccc} a_{11}x_1 & + a_{12}x_2 & + \ldots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots & + a_{mn}x_n & = & b_m \end{array} \tag{3.1}$$

wobei alle Koeffizienten a_{ij} und b_i aus K sind (für $i = 1, \ldots, m$ und $j = 1, \ldots, n$). Gesucht sind dann Werte $x_1, x_2, \ldots, x_n \in K$, die (3.1) erfüllen.

Die *Lösungsmenge* des linearen Gleichungssystems (3.1) ist die Menge

$$L := \left\{(x_1, x_2, \ldots, x_n) \in K^n \mid x_1, x_2, \ldots, x_n \text{ erfüllen (3.1)}\right\} .$$

Beispiele.

(i) Das lineare Gleichungssystem über $\mathbb{Q}$

$$\begin{array}{rcl} x_1 + x_2 + x_3 & = & 0 \\ x_1 + x_2 + x_3 & = & 1 \end{array}$$

besitzt offenbar keine Lösung, d.h. die Lösungsmenge L ist die leere Menge.

(ii) Das lineare Gleichungssystem über $\mathbb{R}$

$$\begin{array}{rcl} x_1 + 2x_2 + x_4 & = & 1 \\ x_1 + 2x_2 + 2x_3 + 3x_4 & = & 5 \\ 2x_1 + 4x_2 + 3x_4 & = & 5 \\ 3x_3 + 2x_4 & = & 3 \end{array}$$

besitzt beispielsweise die Lösung $x_1 = -2$, $x_2 = 0$, $x_3 = -1$, $x_4 = 3$. Eine weitere Lösung ist $x_1 = 0$, $x_2 = -1$, $x_3 = -1$, $x_4 = 3$. Die gesamte Lösungsmenge L dieses linearen Gleichungssystems werden wir weiter unten bestimmen.

3.1.1 Das Gauß'sche Eliminationsverfahren

Grundlegend für die systematische Lösung linearer Gleichungssysteme ist das folgende einfache Lemma.

Lemma 3.1.2. *Die Lösungsmenge eines linearen Gleichungssystems über K ändert sich nicht, wenn man*

(i) zwei Gleichungen vertauscht;

(ii) das c-fache einer Gleichung zu einer anderen addiert ($c \in K$);

(iii) eine Gleichung mit $c \in K \setminus \{0\}$ multipliziert.

Beweis. Behauptung (i) ist klar. Um (ii) zu zeigen, muss man sich nur klar machen, dass für $c, w, x, y, z \in K$ gilt:

$$(w = x \quad \wedge \quad y = z) \quad \Longleftrightarrow \quad (w = x \quad \wedge \quad y + c \cdot w = z + c \cdot x) .$$

Teil (iii) folgt schließlich aus der Tatsache, dass für $x, y \in K$ und $c \in K \setminus \{0\}$ gilt:

$$x = y \quad \Longleftrightarrow \quad c \cdot x = c \cdot y .$$

Damit ist der Beweis abgeschlossen. □

Der Gauß'sche Algorithmus (auch *Gauß'sches Eliminationsverfahren* genannt) benutzt die Regeln aus Lemma 3.1.2 sukzessive, um ein gegebenes lineares Gleichungssystem in ein anderes zu überführen, bei dem man die Lösung direkt ablesen kann.

Beispiel. Wir betrachten noch einmal das Beispiel von oben, also das folgende lineare Gleichungssystem über $\mathbb{R}$:

$$\begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & & & + & x_4 & = & 1 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 3x_4 & = & 5 \\ 2x_1 & + & 4x_2 & & & + & 3x_4 & = & 5 \\ & & & & 3x_3 & + & 2x_4 & = & 3 \end{array}$$

Addiert man das (-1)-fache der ersten Gleichung zur zweiten Gleichung und das (-2)-fache der ersten Gleichung zur dritten, so erhält man:

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & x_4 & = & 1 \\ & & 2x_3 & + & 2x_4 & = & 4 \\ & & & & x_4 & = & 3 \\ & & 3x_3 & + & 2x_4 & = & 3 \end{array}$$

Multipliziert man jetzt die zweite Gleichung mit $1/2$ und addiert danach das (-3)-fache der zweiten Gleichung zur vierten, so erhält man:

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & x_4 & = & 1 \\ & & x_3 & + & x_4 & = & 2 \\ & & & & x_4 & = & 3 \\ & & & & -x_4 & = & -3 \end{array}$$

Addiert man schließlich die dritte Gleichung zur vierten und das (-1)-fache der dritten Gleichung zur ersten und zur zweiten, so erhält man:

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & & & = & -2 \\ & & & x_3 & & = & -1 \\ & & & & x_4 & = & 3 \\ & & & & 0 & = & 0 \end{array}$$

Daraus liest man jetzt sofort die folgende Lösungsmenge des linearen Gleichungssystems ab:

$$\begin{aligned} L &= \{(x_1, x_2, -1, 3) \in \mathbb{R}^4 \mid x_1 + 2x_2 = -2\} \\ &= \{(-2 - 2x_2, x_2, -1, 3) \mid x_2 \in \mathbb{R}\} \ . \end{aligned}$$

Bevor wir das Gauß'sche Eliminationsverfahren in voller Allgemeinheit betrachten, führen wir zunächst den Begriff der *Matrix* ein.

Definition 3.1.3 (Matrizen)**.** Es sei $(K, +, \cdot)$ ein Körper und $m, n \in \mathbb{N}$. Ein Schema der Form

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

mit $a_{ij} \in K$ für alle $i \in \{1, 2, \ldots, m\}$ und $j \in \{1, 2, \ldots, n\}$ heißt eine *Matrix*, genauer eine $m \times n$ *Matrix über* K. Dabei bezeichnet m die Anzahl der *Zeilen* der Matrix und n die Anzahl der *Spalten*. Der erste Index des Eintrages a_{ij} gibt dann die *Zeilennummer* des Eintrages an und der zweite Index die *Spaltennummer*.

Die Menge aller $m \times n$ Matrizen über dem Körper K wird mit $K^{m \times n}$ bezeichnet.

Definition 3.1.4 (Koeffizientenmatrix eines linearen Gleichungssystems)**.** Die *Koeffizientenmatrix* des linearen Gleichungssystems über K

$$\begin{array}{ccccccc} a_{11}x_1 & + a_{12}x_2 & + \ldots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots & + a_{mn}x_n & = & b_m \end{array} \tag{3.2}$$

ist die Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \in \quad K^{m \times n} \ .$$

Die *erweiterte Matrix* des linearen Gleichungssystems (3.2) ist die Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix} \quad \in \quad K^{m \times (n+1)} \ . \tag{3.3}$$

Definition 3.1.5 (Elementare Zeilenumformungen)**.** Elementare Zeilenumformungen auf $K^{m \times n}$ sind Abbildungen der folgenden Form (für $1 \leq k, \ell \leq m$):

(i) $V_{k,\ell} : K^{m \times n} \to K^{m \times n}$: „Vertausche k-te und ℓ-te Zeile."

(ii) $A_{k,\ell}(c) : K^{m \times n} \to K^{m \times n}$ für $c \in K$: „Addiere das c-Fache der k-ten Zeile zur ℓ-ten Zeile."

(iii) $M_k(c) : K^{m\times n} \to K^{m\times n}$ für $c \in K \setminus \{0\}$: „Multipliziere die k-te Zeile mit c.“

Durch elementare Zeilenumformungen kann man eine beliebige $m \times n$ Matrix auf sogenannte *Stufenform* bringen. Wir demonstrieren das zunächst anhand eines kleinen Beispiels.

Beispiel. Wir betrachten die erweiterte Matrix des linearen Gleichungssystems mit vier Variablen und vier Zeilen von oben.

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 1 & 2 & 2 & 3 & 5 \\ 2 & 4 & 0 & 3 & 5 \\ 0 & 0 & 3 & 2 & 3 \end{pmatrix} \begin{matrix} A_{1,2}(-1) \\ A_{1,3}(-2) \\ \longrightarrow \end{matrix} \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 2 & 2 & 4 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 3 & 2 & 3 \end{pmatrix}$$

$$\begin{matrix} M_2(1/2) \\ A_{2,4}(-3) \\ \longrightarrow \end{matrix} \begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & -1 & -3 \end{pmatrix} \begin{matrix} A_{3,1}(-1) \\ A_{3,2}(-1) \\ A_{3,4}(1) \\ \longrightarrow \end{matrix} \begin{pmatrix} \boxed{1} & 2 & 0 & 0 & -2 \\ 0 & 0 & \boxed{1} & 0 & -1 \\ 0 & 0 & 0 & \boxed{1} & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Die nach der letzten Umformung entstandene Matrix hat Stufenform.

Definition 3.1.6. [Stufenform] Eine Matrix $A \in K^{m\times n}$ hat *Stufenform*, wenn sie wie folgt aussieht:

$$A = \begin{pmatrix} 0\cdots 0 & \boxed{1} & *\cdots * & 0 & *\cdots * & 0 & *\cdots * & 0 & *\cdots \\ 0\cdots 0 & 0 & \cdots\ 0 & \boxed{1} & *\cdots * & 0 & *\cdots * & 0 & *\cdots \\ 0\cdots 0 & 0 & \cdots\ 0 & 0 & \cdots\ 0 & \boxed{1} & *\cdots * & 0 & *\cdots \\ 0\cdots 0 & 0 & \cdots\ 0 & 0 & \cdots\ 0 & 0 & \cdots\ 0 & \boxed{1} & *\cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} .$$

Dabei deuten die $*$-Einträge an, dass an diesen Stellen beliebige Skalare aus K stehen dürfen.

Satz 3.1.7 (Stufenform)**.** *Jede Matrix $A \in K^{m\times n}$ kann man durch elementare Zeilenumformungen auf Stufenform bringen.*

Beweis. Der Beweis des Satzes wird durch Induktion über die Anzahl der Zeilen m geführt. Induktionsanfang: Für $m = 1$ ist $A = (a_{11}, a_{12}, \ldots, a_{1n})$. Sind alle $a_{1i} = 0$ $(1 \le i \le n)$, so ist A bereits in Stufenform. Wir können also annehmen, dass nicht alle a_{1i} gleich Null sind. Es sei $j_1 := \min\{j \mid a_{1j} \neq 0\}$. Wenden wir auf A die Umformung $M_1(a_{1j_1}^{-1})$ an, so erhält man die Matrix $(0, \ldots, 0, 1, *, \ldots, *)$, die in Stufenform ist. (Dabei steht die Eins an der j_1-ten Stelle.)

Induktionsschluss: Wir nehmen an, dass die Behauptung für ein beliebiges aber fest gewähltes m gilt. Wir betrachten jetzt eine Matrix $A \in K^{(m+1)\times n}$. Enthält die Matrix nur Nullen, so ist sie bereits in Stufenform. Andernfalls sei

$$j_1 := \min\{j \mid \exists i : a_{ij} \neq 0\} \ .$$

Dann ist j_1 also der kleinste Index einer Spalte, in der es einen von Null verschiedenen Eintrag a_{ij_1} gibt.

$$\begin{pmatrix} 0\cdots 0 & * & *\cdots * \\ \vdots & \vdots & \vdots \\ 0\cdots 0 & * & *\cdots * \\ 0\cdots 0 & a_{ij_1} & *\cdots * \\ 0\cdots 0 & * & *\cdots * \\ \vdots & \vdots & \vdots \\ 0\cdots 0 & * & *\cdots * \end{pmatrix}$$

Wende jetzt die elementare Zeilenumformung $M_i(a_{ij_1}^{-1})$ und dann $A_{i,k}(-a_{kj_1})$ für alle $k \neq i$ an. Wendet man dann noch die elementare Zeilenumformung $V_{i,1}$ an, so erhält man eine Matrix der Form

$$\begin{pmatrix} 0\cdots 0 & 1 & *\cdots * \\ 0\cdots 0 & 0 & *\cdots * \\ \vdots & \vdots & \vdots \\ 0\cdots 0 & 0 & *\cdots * \end{pmatrix} \tag{3.4}$$

Es sei jetzt $B \in K^{m\times n}$ die Matrix, die aus den letzten m Zeilen in (3.4) besteht. Nach Induktionsannahme kann man B durch elementare Zeilenumformungen auf Stufenform bringen. Eliminiert man dann noch die Einträge in der ersten Zeile, die oberhalb der Stufen stehen, so erhält man damit aus (3.4) eine Matrix in Stufenform. □

Zur Illustration betrachten wir ein weiteres Beispiel.

Beispiel. Wir betrachten das folgende lineare Gleichungssystem über dem endlichen Körper mit sieben Elementen $\mathbb{Z}_7$:

$$\begin{array}{rcrcrcl} & & & & x_3 & = & 4 \\ 3x_1 & + & 6x_2 & + & 6x_3 & = & 2 \\ x_1 & + & 4x_2 & & & = & 4 \end{array}$$

Um das Gleichungssystem zu lösen, stellen wir die erweiterte Matrix auf und bringen sie durch elementare Zeilenumformungen auf Stufenform:

$$\begin{pmatrix} 0 & 0 & 1 & 4 \\ 3 & 6 & 6 & 2 \\ 1 & 4 & 0 & 4 \end{pmatrix} \xrightarrow{V_{1,2}} \begin{pmatrix} 3 & 6 & 6 & 2 \\ 0 & 0 & 1 & 4 \\ 1 & 4 & 0 & 4 \end{pmatrix} \xrightarrow[A_{1,3}(6)]{M_1(5)} \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 0 & 1 & 4 \\ 0 & 2 & 5 & 1 \end{pmatrix}$$

$$\xrightarrow{V_{2,3}} \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 2 & 5 & 1 \\ 0 & 0 & 1 & 4 \end{pmatrix} \xrightarrow[A_{2,1}(5)]{M_2(4)} \begin{pmatrix} 1 & 0 & 4 & 2 \\ 0 & 1 & 6 & 4 \\ 0 & 0 & 1 & 4 \end{pmatrix} \xrightarrow[A_{3,2}(1)]{A_{3,1}(3)} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

Die letzte Matrix entspricht dem umgeformten linearen Gleichungssystem:

$$\begin{aligned} x_1 &= 0 \\ x_2 &= 1 \\ x_3 &= 4 \end{aligned}$$

Die eindeutige Lösung des linearen Gleichungssystems ist also $x_1 = 0$, $x_2 = 1$, $x_3 = 4$ und die Lösungsmenge ist damit einelementig.

Wir wissen jetzt also, dass man die erweiterte $m \times (n+1)$ Matrix A (siehe (3.3)) eines gegebenen linearen Gleichungssystems (3.2) mit m Gleichungen und n Unbekannten durch elementare Zeilenumformungen in Stufenform bringen kann. Diese Matrix A' in Stufenform entspricht nach Lemma 3.1.2 wieder einem linearen Gleichungssystem, das zu dem gegebenen äquivalent ist.

Wir nehmen an, dass die Stufen in den Spalten $j_1 < j_2 < \cdots < j_r$ auftreten; die Spalte j_i, $i = 1, \ldots, r$, ist also die Spalte von A', in der die i-te Zeile den ersten Eintrag ungleich Null (genauer gesagt: eine Eins) enthält. Wir unterscheiden nun zwei Fälle. Ist $j_r = n+1$, dann lautet die r-te Gleichung des umgeformten linearen Gleichungssystems

$$0x_1 \; + \; 0x_2 \; + \; \ldots \; + 0x_n \; = \; 1 \; ,$$

so dass das Gleichungssystem offenbar keine Lösung besitzt.

Andernfalls (wenn $j_r \leq n$) lautet das umgeformte Gleichungssystem:

$$\begin{aligned} x_{j_1} + \sum_{\substack{j=j_1+1 \\ j \neq j_2, \ldots, j_r}}^{n} a'_{1j} x_j &= a'_{1,n+1} \\ x_{j_2} + \sum_{\substack{j=j_2+1 \\ j \neq j_3, \ldots, j_r}}^{n} a'_{2j} x_j &= a'_{2,n+1} \\ \vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\ x_{j_r} + \sum_{j=j_r+1}^{n} a'_{rj} x_j &= a'_{r,n+1} \\ 0 &= 0 \\ \vdots & \vdots \\ 0 &= 0 \end{aligned}$$

Alle x_i außer $x_{j_1}, \ldots, x_{j_r}$ sind frei wählbar; aus deren Wahl ergeben sich dann die

restlichen $x_{j_1}, \ldots, x_{j_r}$ wie folgt:

$$\begin{aligned}
x_{j_1} &:= a'_{1,n+1} - \sum_{\substack{j=j_1+1 \\ j\neq j_2,\ldots,j_r}}^{n} a'_{1j} x_j \\
x_{j_2} &:= a'_{2,n+1} - \sum_{\substack{j=j_2+1 \\ j\neq j_3,\ldots,j_r}}^{n} a'_{2j} x_j \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
x_{j_r} &:= a'_{r,n+1} - \sum_{j=j_r+1}^{n} a'_{rj} x_j
\end{aligned}$$

Damit haben wir also eine Beschreibung der Lösungsmenge des linearen Gleichungssystems.

Insbesondere ist das lineare Gleichungssystem genau dann eindeutig lösbar, wenn $\{j_1, \ldots, j_r\} = \{1, \ldots, n\}$, also falls $r = n$ gilt. Da die Anzahl der Stufen r durch die Anzahl der Zeilen m beschränkt ist, muss also $n \leq m$ sein, falls das lineare Gleichungssystem eindeutig lösbar ist.

Korollar 3.1.8. *Falls das lineare Gleichungssystem* (3.2) *eine eindeutige Lösung besitzt, so gilt* $n \leq m$.

Beispiel. Wir betrachten das folgende lineare Gleichungssystem über dem endlichen Körper mit drei Elementen $\mathbb{Z}_3$:

$$\begin{array}{rcrcrcrcrcl}
x_1 & + & 2x_2 & + & x_3 & + & x_4 & + & 2x_5 & = & 1 \\
 & & & & 2x_3 & + & x_4 & + & 2x_5 & = & 2 \\
2x_1 & + & x_2 & & & + & x_4 & & & = & 1
\end{array}$$

Wir formen die erweiterte Matrix in Stufenform um:

$$\begin{pmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \overset{\substack{A_{13}(1) \\ M_2(2)}}{\longrightarrow} \begin{pmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 2 & 2 \end{pmatrix}$$

$$\overset{\substack{A_{21}(2) \\ A_{23}(2)}}{\longrightarrow} \begin{pmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \overset{\substack{A_{31}(2) \\ A_{32}(2)}}{\longrightarrow} \begin{pmatrix} \boxed{1} & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & \boxed{1} & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 1 \end{pmatrix}$$

Das zugehörige umgeformte lineare Gleichungssystem ist

$$\begin{array}{rcrcrcrcl}
x_1 & + & 2x_2 & & + & 2x_4 & & = & 2 \\
 & & & x_3 & + & 2x_4 & & = & 0 \\
 & & & & & & x_5 & = & 1
\end{array}$$

Die Lösungsmenge ist also

$$L \;=\; \big\{(2+x_2+x_4, x_2, x_4, x_4, 1) \mid x_2, x_4 \in \mathbb{Z}_3\big\} \;.$$

Die Anzahl der verschiedenen Lösungen ist also 9.

Definition 3.1.9 (Homogene lineare Gleichungssysteme)**.** Das lineare Gleichungssystem (3.2) heißt homogen, wenn $b_1 = b_2 = \cdots = b_m = 0$. Ein homogenes lineares Gleichungssystem hat immer eine Lösung, nämlich $x_1 = x_2 = \cdots = x_n = 0$. Diese Lösung $(x_1, \ldots, x_n) = (0, \ldots, 0)$ heißt *triviale Lösung.*

Korollar 3.1.10. *Ist $m = n$ und hat das homogene lineare Gleichungssystem*

$$\begin{array}{ccccccc} a_{11}x_1 & + a_{12}x_2 & + \ldots & + a_{1n}x_n & = & 0 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots & + a_{2n}x_n & = & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots & + a_{mn}x_n & = & 0 \end{array}$$

nur die triviale Lösung, so hat (3.2) *für jede rechte Seite $b_1, \ldots, b_m$ eine eindeutig bestimmte Lösung.*

Beweis. Wir betrachten die erweiterte Matrix des homogenen linearen Gleichungssystems:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} & 0 \\ a_{21} & a_{22} & \cdots & a_{2m} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} & 0 \end{pmatrix} \;.$$

Da das homogene lineare Gleichungssystem nach Voraussetzung eine eindeutige Lösung besitzt, muss die durch elementare Zeilenumformungen entstehende Matrix in Stufenform wie folgt aussehen:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \;.$$

Bringt man durch dieselben elementaren Zeilenumformungen die erweiterte Matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2m} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} & b_m \end{pmatrix}$$

auf Stufenform, so muss diese also wie folgt aussehen (mit $b'_1, \ldots, b'_m \in K$):

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & b'_1 \\ 0 & 1 & & \vdots & b'_2 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & b'_m \end{pmatrix} .$$

Damit ist also $(x_1, \ldots, x_m) = (b'_1, \ldots, b'_m)$ die eindeutige Lösung des linearen Gleichungssystems mit rechter Seite $b_1, \ldots, b_m$. □

3.1.2 Matrizenrechnung

Auf der Menge der $m \times n$ Matrizen über einem Körper K definieren wir eine Addition und eine skalare Multiplikation mit Elementen aus dem Körper K.

Definition 3.1.11 (Matrixaddition und Multiplikation mit Skalaren)**.** Es seien $m, n \in \mathbb{N}$ und $A, B \in K^{m \times n}$. Für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ bezeichnen wir den Eintrag in der i-ten Zeile und j-ten Spalte der Matrix A mit A_{ij}. Analog seien B_{ij} die Einträge der Matrix B. Wir definieren eine Verknüpfung (Addition) „+“ auf $K^{m \times n}$ wie folgt:

$$(A + B)_{ij} \;:=\; A_{ij} + B_{ij} \qquad \text{für } i = 1, \ldots, m \text{ und } j = 1, \ldots, n.$$

Man erhält also die Einträge der Matrix $A + B \in K^{m \times n}$ durch Addition der Einträge der Matrizen A und B. Weiterhin definieren wir die skalare Multiplikation „$\cdot$“ wie folgt. Für $s \in K$ und $A \in K^{m \times n}$ sei

$$(s \cdot A)_{ij} \;:=\; s \cdot A_{ij} \qquad \text{für } i = 1, \ldots, m \text{ und } j = 1, \ldots, n.$$

Beispiel. Es sei $K = \mathbb{R}$ der Körper der reellen Zahlen. Wir betrachten 2×3 Matrizen über $\mathbb{R}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 3 \\ 5 & 4 & 7 \end{pmatrix} ,$$

$$2 \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \end{pmatrix} .$$

Das lineare Gleichungssystem

$$\begin{array}{ccccccc} a_{11}x_1 & + a_{12}x_2 & + \ldots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots & + a_{mn}x_n & = & b_m \end{array}$$

können wir jetzt alternativ wie folgt schreiben:

$$x_1 \cdot \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2 \cdot \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + x_n \cdot \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} .$$

Noch kürzer schreibt man dafür

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} .$$

Letztere Schreibweise erklärt sich durch die folgende allgemeine Definition der *Matrixmultiplikation*.

Definition 3.1.12 (Matrixmultiplikation)**.** Es seien $\ell, m, n \in \mathbb{N}$ und $A \in K^{m \times n}$, $B \in K^{n \times \ell}$. Dann ist das Produkt $A \cdot B \in K^{m \times \ell}$ wie folgt definiert:

$$(A \cdot B)_{ij} := A_{i1} \cdot B_{1j} + A_{i2} \cdot B_{2j} + \cdots + A_{in} \cdot B_{nj} = \sum_{k=1}^{n} A_{ik} \cdot B_{kj} .$$

Zur Berechnung des Eintrages in der Zeile i und Spalte j der Produktmatrix $A \cdot B$ benötigt man also die gesamte Zeile i von A sowie die gesamte Spalte j von B.

Bemerkung. Man beachte, dass das Produkt zweier Matrizen A und B nur dann definiert ist, wenn die Spaltenzahl von A gleich der Zeilenzahl von B ist.

Beispiel. Wir betrachten Matrizen über dem Körper der rationalen Zahlen $\mathbb{Q}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 1 + 3 \cdot (-1) \\ 4 \cdot 1 + 5 \cdot 1 + 6 \cdot (-1) \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} ,$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & -3 \\ 3 & 5 & -6 \end{pmatrix} .$$

Lemma 3.1.13 (Distributivgesetz der Matrixrechnung)**.** *Ist $A \in K^{m \times n}$ und $B, C \in K^{n \times q}$, dann gilt*

$$A \cdot (B + C) = A \cdot B + A \cdot C .$$

Beweis. Nach Definition der Matrixmultiplikation und -addition gilt für $1 \leq i \leq m$ und $1 \leq j \leq q$:

$$\begin{aligned}\big(A \cdot (B+C)\big)_{ij} &= \sum_{k=1}^{n} A_{ik} \cdot (B+C)_{kj} = \sum_{k=1}^{n} A_{ik} \cdot (B_{kj} + C_{kj}) \\ &= \sum_{k=1}^{n} (A_{ik} \cdot B_{kj} + A_{ik} \cdot C_{kj}) = \sum_{k=1}^{n} A_{ik} \cdot B_{kj} + \sum_{k=1}^{n} A_{ik} \cdot C_{kj} \\ &= (A \cdot B)_{ij} + (A \cdot C)_{ij} = (A \cdot B + A \cdot C)_{ij} \ .\end{aligned}$$

Damit ist die Behauptung bewiesen. □

Satz 3.1.14 (Ring der $n \times n$ Matrizen)**.** *Die Menge $K^{n\times n}$ der $n \times n$ Matrizen über einem Körper K bilden zusammen mit der oben definierten Addition und Multiplikation einen nicht-kommutativen Ring mit Eins.*

Beweisskizze. Es ist leicht zu sehen, dass $(K^{n\times n}, +)$ eine kommutative Gruppe ist. Das neutrale Element der Addition (Nullelement) ist die *Nullmatrix*, deren Einträge alle Null sind. Man kann nachrechnen, dass die Matrixmultiplikation auf $K^{n\times n}$ assoziativ ist und gemeinsam mit der Addition das Distributivgesetz erfüllt (siehe Lemma 3.1.13). Das neutrale Element der Matrixmultiplikation ist die *Einheitsmatrix* E_n, die Einsen auf der Diagonalen und sonst nur Nullen enthält:

$$E_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in K^{n\times n} \ .$$

Wir überlassen alle weiteren Beweisdetails dem Leser. □

Wir zeigen anhand eines einfachen Beispiels, dass die Matrixmultiplikation auf $K^{n\times n}$ nicht kommutativ ist.

Beispiel. Es gilt

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ ,$$

umgekehrt jedoch

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ .$$

3.2 Vektorräume

In diesem Abschnitt beschäftigen wir uns mit Vektorräumen über einem beliebigen Körper K. Vektorräume bilden die zentrale Struktur in der linearen Algebra. Es stellt sich heraus, dass beispielsweise die Lösungsmengen der im vorherigen Abschnitt diskutierten linearen Gleichungssysteme über K mit n Unbekannten einen engen Bezug zu sogenannten Teilräumen des Vektorraums K^n aufweisen. Neben der Definition und Beschreibung von Vektorräumen diskutieren wir weitere wichtige Konzepte in diesem Zusammenhang. Dazu gehören Linearkombinationen, Erzeugendensysteme, die lineare Abhängigkeit von Vektoren, Basen von Vektorräumen und schließlich der Dimensionsbegriff.

3.2.1 Definition

Wir beginnen mit einer axiomatischen Definition des Begriffs Vektorraum.

Definition 3.2.1 (K-Vektorräume)**.** Es sei $(K, +, \cdot)$ ein Körper. Ein *K-Vektorraum* ist eine Menge V zusammen mit Abbildungen

$$\begin{aligned} + :\ & V \times V \to V && (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} + \mathbf{w}\ , \\ \cdot :\ & K \times V \to V && (s, \mathbf{v}) \mapsto s \cdot \mathbf{v}\ , \end{aligned}$$

für die die folgenden Regeln gelten:

(i) $(V, +)$ ist kommutative Gruppe; das neutrale Element der Addition ist der *Nullvektor* $\mathbf{0}$. Das *inverse Element* zu $\mathbf{v}$ wird mit $-\mathbf{v}$ bezeichnet.

(ii) $1 \cdot \mathbf{v} = \mathbf{v}$ für alle $\mathbf{v} \in V$. (Dabei bezeichnet 1 das Einselement des Körpers K.)

(iii) $(s \cdot s') \cdot \mathbf{v} = s \cdot (s' \cdot \mathbf{v})$ für alle $s, s' \in K$, $\mathbf{v} \in V$.

(iv) $(s + s') \cdot \mathbf{v} = (s \cdot \mathbf{v}) + (s' \cdot \mathbf{v})$ für alle $s, s' \in K$, $\mathbf{v} \in V$.

(v) $s \cdot (\mathbf{v} + \mathbf{w}) = (s \cdot \mathbf{v}) + (s \cdot \mathbf{w})$ für alle $s \in K$, $\mathbf{v}, \mathbf{w} \in V$.

Die Elemente von V heißen *Vektoren*[1]. Ist $(K, +, \cdot)$ kein Körper sondern nur ein Ring mit Eins, so spricht man statt von einem K-Vektorraum von einem *K-Modul*.

Beispiele.

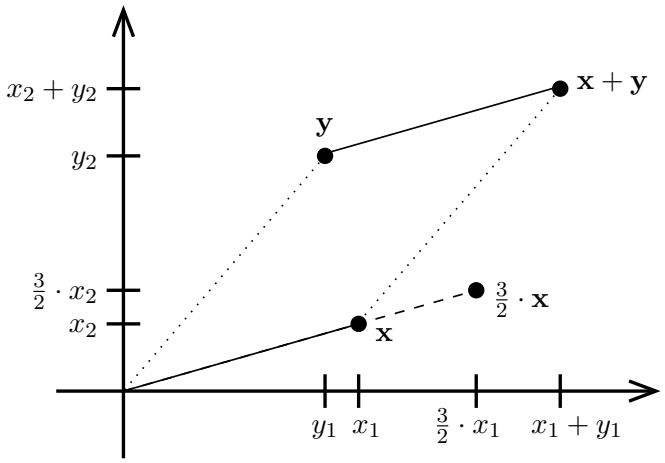
(i) Für $m, n \in \mathbb{N}$ ist die Menge $K^{m \times n}$ der $m \times n$ Matrizen über K mit der Matrixaddition und der Skalarmultiplikation (siehe Definition 3.1.11) ein K-Vektorraum.

[1] Zur besseren Unterscheidung von Skalaren drucken wir Vektoren meistens in Fettschrift.

(ii) Als Spezialfall von (i) ist $K^n := K^{n\times 1}$ mit Addition und Skalarmultiplikation ein K-Vektorraum. Addition und Skalarmultiplikation sehen in diesem Spezialfall wie folgt aus:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}, \quad s \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} s \cdot x_1 \\ s \cdot x_2 \\ \vdots \\ s \cdot x_n \end{pmatrix}.$$

(iii) Für $K = \mathbb{R}$ und $n = 2$ kann man sich den Vektorraum $\mathbb{R}^2$ als Ebene mit üblicher Vektoraddition und skalarer Multiplikation vorstellen. Wir veranschaulichen das für die beiden Vektoren $\mathbf{x} = \binom{x_1}{x_2}$ und $\mathbf{y} = \binom{y_1}{y_2}$:



Entsprechend kann man den Vektorraum $\mathbb{R}^3$ mit dem uns gut vertrauten dreidimensionalen Raum assoziieren.

(iv) Es sei M eine beliebige Menge und K ein beliebiger Körper. Dann wird die Menge K^M der Abbildungen von M nach K mit der folgenden Addition und Skalarmultiplikation zu einem Vektorraum. Für $f, g \in K^M$ und $s \in K$ definieren wir

$$\begin{aligned} (f+g)(x) &:= f(x) + g(x) && \text{für alle } x \in M, \\ (s \cdot f)(x) &:= s \cdot f(x) && \text{für alle } x \in M. \end{aligned}$$

Der Nullvektor dieses Vektorraums ist die Nullabbildung, d.h. $x \mapsto 0$ für alle $x \in M$.

(v) Es sei wie im letzten Beispiel M eine Menge und K ein Körper. Dann ist die Menge

$$K^{(M)} := \{f : M \to K \mid f(x) \neq 0 \text{ nur für endlich viele } x \in M\}$$

mit der im letzten Beispiel definierten Addition und Skalarmultiplikation ein K-Vektorraum. Dazu beachte man, dass für $f, g \in K^{(M)}$ gilt, dass auch $f + g \in K^{(M)}$. Das bedeutet, dass $K^{(M)}$ abgeschlossen ist unter der üblichen Addition von Funktionen. Dasselbe gilt für die Skalarmultiplikation.

Wir halten die folgenden allgemeingültigen Rechenregeln in Vektorräumen als Lemma fest.

Lemma 3.2.2 (Rechenregeln in Vektorräumen)**.** *Es sei $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein K-Vektorraum. Dann gilt:*

(i) $0 \cdot \mathbf{v} = \mathbf{0}$ *für alle* $\mathbf{v} \in V$.

(ii) $s \cdot \mathbf{0} = \mathbf{0}$ *für alle* $s \in K$.

(iii) Für $s \in K$ *und* $\mathbf{v} \in V$ *gilt:* $s \cdot \mathbf{v} = \mathbf{0} \iff (s = 0 \ \vee \ \mathbf{v} = \mathbf{0})$.

(iv) $(-s) \cdot \mathbf{v} = -(s \cdot \mathbf{v})$ *für alle* $s \in K$, $\mathbf{v} \in V$.

Beweis. Zu (i):

$$\begin{aligned} 0 \cdot \mathbf{v} &= 0 \cdot \mathbf{v} + \mathbf{0} = 0 \cdot \mathbf{v} + (0 \cdot \mathbf{v} + (-(0 \cdot \mathbf{v}))) \\ &= (0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}) + (-(0 \cdot \mathbf{v})) = (0 + 0) \cdot \mathbf{v} + (-(0 \cdot \mathbf{v})) \\ &= 0 \cdot \mathbf{v} + (-(0 \cdot \mathbf{v})) = \mathbf{0} \ . \end{aligned}$$

Zu (ii):

$$\begin{aligned} s \cdot \mathbf{0} &= s \cdot \mathbf{0} + \mathbf{0} = s \cdot \mathbf{0} + (s \cdot \mathbf{0} + (-(s \cdot \mathbf{0}))) \\ &= (s \cdot \mathbf{0} + s \cdot \mathbf{0}) + (-(s \cdot \mathbf{0})) = s \cdot (\mathbf{0} + \mathbf{0}) + (-(s \cdot \mathbf{0})) \\ &= s \cdot \mathbf{0} + (-(s \cdot \mathbf{0})) = \mathbf{0} \ . \end{aligned}$$

Zu (iii): Die Implikation „$\Longleftarrow$“ folgt offenbar aus (i) und (ii). Wir müssen also noch die Implikation „$\Longrightarrow$“ zeigen. Es sei also $s \cdot \mathbf{v} = 0$. Wir nehmen an, dass $s \neq 0$ gilt (andernfalls sind wir fertig) und müssen zeigen, dass dann $\mathbf{v} = \mathbf{0}$:

$$\mathbf{v} = 1 \cdot \mathbf{v} = (s^{-1} \cdot s) \cdot \mathbf{v} = s^{-1} \cdot (s \cdot \mathbf{v}) = s^{-1} \cdot \mathbf{0} = \mathbf{0} \ .$$

Zu (iv):

$$\begin{aligned} (-s) \cdot \mathbf{v} &= (-s) \cdot \mathbf{v} + \mathbf{0} = (-s) \cdot \mathbf{v} + (s \cdot \mathbf{v} + (-(s \cdot \mathbf{v}))) \\ &= (-s + s) \cdot \mathbf{v} + (-(s \cdot \mathbf{v})) = 0 \cdot \mathbf{v} + (-(s \cdot \mathbf{v})) = -(s \cdot \mathbf{v}) \ . \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

3.2.2 Teilräume

Ähnlich wie wir bei Gruppen und Ringen Untergruppen und Unterringe eingeführt haben, kann man auch bei Vektorräumen Teilmengen betrachten, die selbst wieder Vektorräume sind.

Definition 3.2.3 (Teilräume)**.** Es sei $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein K-Vektorraum. Ist $U \subseteq V$ mit

(i) $U \neq \emptyset$,

(ii) $\mathbf{v}, \mathbf{w} \in U \quad \Longrightarrow \quad (\mathbf{v} + \mathbf{w}) \in U$,

(iii) $s \in K$, $\mathbf{v} \in U \quad \Longrightarrow \quad (s \cdot \mathbf{v}) \in U$,

dann bildet U einen *Teilraum* oder *Untervektorraum* von V.

Bemerkung. Man überzeugt sich leicht von der Tatsache, dass ein Teilraum U eines K-Vektorraumes $(V, +, \cdot)$ zusammen mit der Einschränkung der Addition $+|_{U \times U}$ und Skalarmultiplikation $\cdot|_{K \times U}$ selbst K-Vektorraum ist.

Lemma 3.2.4 (Charakterisierung von Teilräumen)**.** *Es sei $(V, +, \cdot)$ ein K-Vektorraum und $U \subseteq V$. Die Teilmenge U ist genau dann ein Teilraum von V, wenn die folgenden beiden Bedingungen erfüllt sind:*

(i) $\mathbf{0} \in U$,

(ii) $s \in K$, $\mathbf{v}, \mathbf{w} \in U \quad \Longrightarrow \quad ((s \cdot \mathbf{v}) + \mathbf{w}) \in U$.

Beweis. Ist U ein Teilraum von V, so gibt es ein Element $\mathbf{v} \in U$ und es gilt $\mathbf{0} = (0 \cdot \mathbf{v}) \in U$, also (i). Ist $s \in K$ und $\mathbf{v}, \mathbf{w} \in U$, so gilt $(s \cdot \mathbf{v}) \in U$ und damit auch $((s \cdot \mathbf{v}) + \mathbf{w}) \in U$, also (ii).

Gelten umgekehrt die Eigenschaften (i) und (ii), so ist $U \neq \emptyset$, da $\mathbf{0} \in U$. Für $\mathbf{v}, \mathbf{w} \in V$ gilt $\mathbf{v} + \mathbf{w} = (1 \cdot \mathbf{v}) + \mathbf{w} \in U$. Schließlich gilt für $s \in K$ und $\mathbf{v} \in U$, dass $s \cdot \mathbf{v} = (s \cdot \mathbf{v}) + \mathbf{0} \in U$. Nach Definition 3.2.3 ist U damit also ein Teilraum von V. □

Beispiele.

(i) Die Teilmenge $\{\mathbf{0}\}$ von V und V selbst sind Teilräume von V. Man nennt sie auch die *trivialen* Teilräume. Für $\mathbf{v} \neq \mathbf{0}$ ist $\{\mathbf{v}\}$ kein Teilraum von V.

(ii) Es sei

$$A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in K^{m \times n}$$

und $U := \{\mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{0}\} \subseteq K^n$ die Lösungsmenge des homogenen linearen Gleichungssystems

$$\begin{array}{rcccl} a_{11}x_1 & + a_{12}x_2 & + \ldots & + a_{1n}x_n & = 0 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots & + a_{2n}x_n & = 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots & + a_{mn}x_n & = 0 \end{array}$$

Dann ist U ein Teilraum von K^n.

(iii) Es sei $A \in K^{m\times n}$ wie im letzten Beispiel und $\mathbf{b} \in K^m \setminus \{\mathbf{0}\}$. Die Lösungsmenge $U' := \{\mathbf{x} \in K^n \mid A\cdot\mathbf{x} = \mathbf{b}\}$ des inhomogenen linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{b}$ ist kein Teilraum von K^n. Denn offenbar wird Bedingung (i) aus Lemma 3.2.4 verletzt, da $A \cdot \mathbf{0} = \mathbf{0} \neq \mathbf{b}$ ist.

(iv) Es sei $V = \mathbb{R}^{\mathbb{R}}$ der $\mathbb{R}$-Vektorraum der Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$. Dann ist $U := \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = f(x + 2\pi) \forall x \in \mathbb{R}\}$ ein Teilraum von V (der Teilraum der 2π-periodischen Abbildungen).

Es sei nun $a \in \mathbb{R}$. Dann ist auch $U_a := \{f : \mathbb{R} \to \mathbb{R} \mid f(a) = 0\}$ ein Teilraum von V.

Andererseits ist $U' := \{f : \mathbb{R} \to \mathbb{R} \mid f(0) = 1\}$ kein Teilraum von V, da der Nullvektor (Nullfunktion) nicht in U' enthalten ist.

Auch $U'' := \{f : \mathbb{R} \to \mathbb{R} \mid f(0) = 0 \vee f(1) = 0\}$ ist kein Teilraum von V, denn die Funktion $f_1 : \mathbb{R} \to \mathbb{R}$ mit $f_1(x) := x$ und die Funktion $f_2 : \mathbb{R} \to \mathbb{R}$ mit $f_2(x) := x - 1$ sind beide in U'', nicht jedoch ihre Summe $f_1 + f_2$. Man beachte, dass U'' die Vereinigung der beiden Teilräume U_0 und U_1 ist. Die Vereinigung von zwei Teilräumen ist also im Allgemeinen kein Teilraum.

Aufgrund ihrer hohen Bedeutung halten wir die in Beispiel (ii) gemachte Beobachtung als Satz fest.

Satz 3.2.5. *Ist $A \in K^{m\times n}$, so ist die Lösungsmenge $U := \{\mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{0}\}$ des homogenen linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{0}$ ein Teilraum des K-Vektorraums K^n.*

Beweis. Es gilt $\mathbf{0} \in U$, da $A \cdot \mathbf{0} = \mathbf{0}$. Für $s \in K$ und $\mathbf{x}, \mathbf{y} \in U$ gilt

$$A \cdot ((s \cdot \mathbf{x}) + \mathbf{y}) \;=\; s \cdot (A \cdot \mathbf{x}) + A \cdot \mathbf{y} \;=\; s \cdot \mathbf{0} + \mathbf{0} \;=\; \mathbf{0} \;.$$

Die Aussage des Satzes folgt also mit Lemma 3.2.4. □

Wir diskutieren als Nächstes Teilräume, die aus anderen Teilräumen durch Schnittbildung und Addition entstehen.

Lemma 3.2.6. *Es sei $(V,+,\cdot)$ ein K-Vektorraum und U_1, U_2 zwei Teilräume von V. Dann sind auch*

$$U_1 \cap U_2 \quad \textit{und} \quad U_1 + U_2 := \{\mathbf{u}_1 + \mathbf{u}_2 \mid \mathbf{u}_1 \in U_1 \textit{ und } \mathbf{u}_2 \in U_2\}$$

Teilräume von V. Ist I eine beliebige Indexmenge und ist für alle $i \in I$ die Menge U_i ein Teilraum von V, so ist auch $\bigcap_{i\in I} U_i$ ein Teilraum von V.

Beweis. Wir beweisen zunächst die letzte Behauptung des Lemmas mit Hilfe von Lemma 3.2.4. Da U_i ein Teilraum von V ist, gilt $\mathbf{0} \in U_i$ für alle $i \in I$. Also $\mathbf{0} \in \bigcap_{i\in I} U_i$. Für $\mathbf{x}, \mathbf{y} \in \bigcap_{i\in I} U_i$ gilt offenbar $\mathbf{x}, \mathbf{y} \in U_i$ für alle $i \in I$. Folglich gilt für $s \in K$ dann $s \cdot \mathbf{x} + \mathbf{y} \in U_i$ für alle $i \in I$ und damit $s \cdot \mathbf{x} + \mathbf{y} \in \bigcap_{i\in I} U_i$.

Es bleibt zu zeigen, dass $U_1 + U_2$ ein Teilraum von V ist. Da $\mathbf{0} \in U_1$ und $\mathbf{0} \in U_2$ gilt $\mathbf{0} = \mathbf{0} + \mathbf{0} \in U_1 + U_2$. Es sei nun $s \in K$ und $\mathbf{x}, \mathbf{y} \in U_1 + U_2$. Dann gibt es $\mathbf{u}_1, \mathbf{u}_1' \in U_1$ und $\mathbf{u}_2, \mathbf{u}_2' \in U_2$ mit $\mathbf{x} = \mathbf{u}_1 + \mathbf{u}_2$ und $\mathbf{y} = \mathbf{u}_1' + \mathbf{u}_2'$. Damit gilt dann

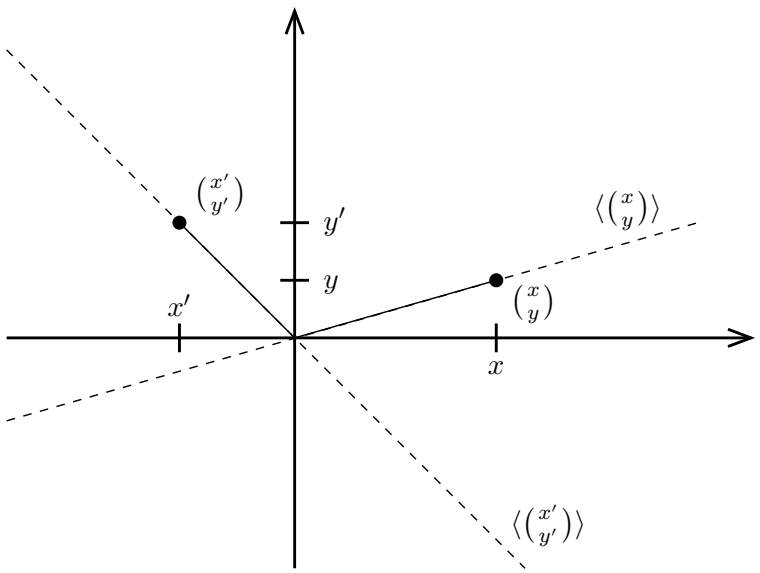
$$\begin{aligned} s \cdot \mathbf{x} + \mathbf{y} &= s \cdot (\mathbf{u}_1 + \mathbf{u}_2) + (\mathbf{u}_1' + \mathbf{u}_2') \\ &= (s \cdot \mathbf{u}_1 + \mathbf{u}_1') + (s \cdot \mathbf{u}_2 + \mathbf{u}_2') \ \in \ U_1 + U_2 \ . \end{aligned}$$

Damit ist der Beweis fertig. □

Beispiel. Es sei V ein K-Vektorraum. Für $\mathbf{v} \in V$ definieren wir

$$\langle \mathbf{v} \rangle \ := \ \{s \cdot \mathbf{v} \mid s \in K\} \ .$$

Dann ist $\langle \mathbf{v} \rangle$ ein Teilraum von V. Man nennt ihn den *von* $\mathbf{v}$ *erzeugten Teilraum*. Im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ kann man sich den von einem Vektor $\binom{x}{y} \neq \mathbf{0}$ erzeugten Teilraum als die Punkte auf der eindeutigen Geraden durch den Nullpunkt und den Punkt $\binom{x}{y}$ vorstellen:



Dann ist

$$\langle \begin{pmatrix} x \\ y \end{pmatrix} \rangle + \langle \begin{pmatrix} x' \\ y' \end{pmatrix} \rangle \;=\; \left\{ s \cdot \begin{pmatrix} x \\ y \end{pmatrix} + s' \cdot \begin{pmatrix} x' \\ y' \end{pmatrix} \mid s, s' \in \mathbb{R} \right\} \;.$$

Anschaulich überzeugt man sich leicht davon, dass dieser Teilraum von $\mathbb{R}^2$ der ganze Vektorraum $\mathbb{R}^2$ ist.

3.2.3 Linearkombinationen und Erzeugendensysteme

Eine wichtige Rolle im Zusammenhang mit Vektorräumen und Teilräumen spielen Linearkombinationen von Vektoren. Das sind neue Vektoren, die durch Skalarmultiplikation und Vektoraddition aus gegebenen Vektoren entstehen. Mit Hilfe dieser Linearkombinationen kann man einen Teilraum „von Innen heraus“ erzeugen.

Definition 3.2.7 (Linearkombinationen, Erzeugnisse)**.** Es sei $(V, +, \cdot)$ ein K-Vektorraum mit Vektoren $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$. Dann heißt der Vektor $\mathbf{v} \in V$ *Linearkombination* von $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$, wenn es $s_1, \ldots, s_n \in K$ gibt mit

$$\mathbf{v} \;=\; s_1 \cdot \mathbf{u}_1 + \cdots + s_n \cdot \mathbf{u}_n \;.$$

Ist $M \subseteq V$ eine Teilmenge von V, so definieren wir das *Erzeugnis von M* als

$$\begin{aligned} \langle M \rangle \;&:=\; \{\mathbf{v} \in V \mid \mathbf{v} \text{ ist Linearkombination endlich vieler Vektoren aus } M\} \\ &=\; \left\{ \sum_{i=1}^{n} s_i \cdot \mathbf{v}_i \;\middle|\; n \in \mathbb{N},\, s_i \in K \text{ und } \mathbf{v}_i \in M \text{ für } i = 1, \ldots, n \right\} \;. \end{aligned}$$

Das Erzeugnis der leeren Menge soll nach Definition der triviale Teilraum von V sein, der nur aus dem Nullvektor besteht, also $\langle \emptyset \rangle := \{\mathbf{0}\}$.

Lemma 3.2.8. *Es sei $(V, +, \cdot)$ ein K-Vektorraum und $M \subseteq V$ eine beliebige Teilmenge von V. Dann ist das Erzeugnis $\langle M \rangle$ von M ein Teilraum von V.*

Beweis. Ist $M = \emptyset$, so ist nach Definition $\mathbf{0} \in \langle M \rangle$. Andernfalls sei $\mathbf{v} \in M$; dann ist $\mathbf{0} = 0 \cdot \mathbf{v} \in \langle M \rangle$. Es seien nun $\mathbf{v}, \mathbf{v}' \in \langle M \rangle$. Dann gilt

$$\begin{aligned} \mathbf{v} \;&=\; \sum_{i=1}^{n} s_i \cdot \mathbf{x}_i \qquad \text{mit } n \in \mathbb{N},\, s_i \in K \text{ und } \mathbf{x}_i \in M \text{ für } i = 1, \ldots, n, \\ \mathbf{v}' \;&=\; \sum_{i=1}^{n'} s'_i \cdot \mathbf{x}'_i \qquad \text{mit } n' \in \mathbb{N},\, s'_i \in K \text{ und } \mathbf{x}'_i \in M \text{ für } i = 1, \ldots, n'. \end{aligned}$$

Folglich gilt für $t \in K$

$$t \cdot \mathbf{v} + \mathbf{v}' \;=\; \sum_{i=1}^{n} (t \cdot s_i) \cdot \mathbf{x}_i + \sum_{i=1}^{n'} s'_i \cdot \mathbf{x}'_i \;.$$

Die rechte Seite ist eine Linearkombination endlich vieler Vektoren aus M und damit in $\langle M\rangle$ enthalten. Die Behauptung folgt also mit Lemma 3.2.4. $\square$

Bemerkung.

(i) Für $M \subseteq V$ heißt $U := \langle M\rangle$ auch der *von M erzeugte Teilraum von V*. Die Menge M heißt *Erzeugendensystem* von U. Man überzeugt sich leicht davon, dass U der kleinste Teilraum (bezüglich Mengeninklusion) ist, der M enthält.

(ii) Ist die Menge M endlich, also $M = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ mit $n \in \mathbb{N}$, so sagen wir, dass $U := \langle M\rangle$ *endlich erzeugt* ist. Wir schreiben auch

$$\begin{aligned}\langle M\rangle &= \langle\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}\rangle = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n\rangle \\ &= \left\{ \sum_{i=1}^{n} s_i \cdot \mathbf{v}_i \;\middle|\; s_i \in K \text{ für } i = 1, \ldots, n \right\} .\end{aligned}$$

Insbesondere schreiben wir für $\mathbf{v} \in V$

$$\langle \mathbf{v}\rangle = \{s \cdot \mathbf{v} \mid s \in K\} .$$

Beispiele.

(i) Es sei $V = \mathbb{R}^2$ und $M = \left\{\binom{1}{1}, \binom{-1}{1}, \binom{1}{0}\right\}$. Dann ist $\langle M\rangle = \mathbb{R}^2$, denn ein beliebiger Vektor $\binom{x}{y} \in \mathbb{R}^2$ kann wie folgt als Linearkombination der Elemente von M geschrieben werden:

$$\binom{x}{y} = x \cdot \binom{1}{1} + (y - x) \cdot \binom{-1}{1} + (y - x) \cdot \binom{1}{0} .$$

Damit ist $\left\{\binom{1}{1}, \binom{-1}{1}, \binom{1}{0}\right\}$ also ein Erzeugendensystem des Vektorraums $\mathbb{R}^2$ und $\mathbb{R}^2$ ist folglich endlich erzeugt.

Bereits die kleinere Menge $\left\{\binom{1}{1}, \binom{1}{0}\right\}$ ist ein Erzeugendensystem von $\mathbb{R}^2$, da ein beliebiger Vektor $\binom{x}{y} \in \mathbb{R}^2$ geschrieben werden kann als

$$\binom{x}{y} = y \cdot \binom{1}{1} + (x - y) \cdot \binom{1}{0} .$$

(ii) Wir betrachten den K-Vektorraum K^n. Für $i = 1, \ldots, n$ sei $\mathbf{e}_i$ der Vektor, dessen i-ter Eintrag 1 ist und alle anderen Einträge 0, d.h.

$$\mathbf{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i \qquad (\mathbf{e}_i)_j = \begin{cases} 1 & \text{falls } j = i, \\ 0 & \text{sonst.} \end{cases}$$

Der Vektor $\mathbf{e}_i$ heißt *i-ter Einheitsvektor*. Dann ist $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ ein Erzeugendensystem von K^n, also $K^n = \langle \mathbf{e}_1, \ldots, \mathbf{e}_n \rangle$, denn

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \;=\; x_1 \cdot \mathbf{e}_1 + \cdots + x_n \cdot \mathbf{e}_n \qquad \text{für alle } x_1, \ldots, x_n \in K.$$

Folglich ist der Vektorraum K^n endlich erzeugt.

(iii) Es sei M eine beliebige Menge. In Verallgemeinerung des letzten Beispiels definieren wir für $y \in M$ den *Einheitsvektor* $\mathbf{e}_y \in K^{(M)}$ durch

$$\mathbf{e}_y(x) \;:=\; \begin{cases} 1 & \text{falls } x = y, \\ 0 & \text{sonst.} \end{cases}$$

Dann ist die Menge $\{\mathbf{e}_y \mid y \in M\}$ ein Erzeugendensystem von $K^{(M)}$. Betrachte eine beliebige Funktion $f \in K^{(M)}$, die nur an den Stellen $y_1, \ldots, y_n \in M$ einen Wert ungleich 0 annimmt. Dann gilt

$$f \;=\; f(y_1) \cdot \mathbf{e}_{y_1} + \cdots + f(y_n) \cdot \mathbf{e}_{y_n} \;.$$

Wir betrachten Erzeugendensysteme, die eine spezielle Eigenschaft erfüllen und *Basen* genannt werden.

Definition 3.2.9 (Basen)**.** Es sei $(V, +, \cdot)$ ein K-Vektorraum. Eine Teilmenge $M \subseteq V$ heißt *Basis von* V, wenn sich jedes $\mathbf{v} \in V$ eindeutig als Linearkombination von paarweise verschiedenen Vektoren aus M schreiben lässt. Außerdem definieren wir, dass die leere Menge $\emptyset$ eine Basis des trivialen K-Vektorraums $\{\mathbf{0}\}$ ist.

Beispiele.

(i) Es sei $(V, +, \cdot)$ ein K-Vektorraum. Die endliche Teilmenge

$$\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$$

ist Basis von V, wenn $\mathbf{v}_1, \ldots, \mathbf{v}_n$ paarweise verschieden sind und es zu jedem $\mathbf{u} \in V$ genau ein n-Tupel $(x_1, \ldots, x_n) \in K^n$ gibt mit

$$\mathbf{u} \;=\; x_1 \cdot \mathbf{v}_1 + \cdots + x_n \cdots \mathbf{v}_n \;.$$

(ii) Die Menge der Einheitsvektoren $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ ist eine Basis des K-Vektorraums K^n.

(iii) Der Nullvektor $\mathbf{0}$ kann nie Element einer Basis sein, denn

$$0 \cdot \mathbf{0} \;=\; 1 \cdot \mathbf{0} \;=\; \mathbf{0} \;,$$

so dass also die Koeffizienten der Darstellung nicht eindeutig sind.

(iv) Wie wir weiter oben beobachtet haben, gilt $\langle \binom{1}{1}, \binom{-1}{1}, \binom{1}{0} \rangle = \mathbb{R}^2$. Die Menge $\left\{ \binom{1}{1}, \binom{-1}{1}, \binom{1}{0} \right\}$ ist jedoch keine Basis von $\mathbb{R}^2$, denn

$$\begin{pmatrix} -1 \\ 1 \end{pmatrix} \;=\; 0 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

und andererseits

$$\begin{pmatrix} -1 \\ 1 \end{pmatrix} \;=\; 1 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;.$$

(v) Die Menge $\left\{ \binom{1}{1}, \binom{1}{0} \right\}$ ist Basis von $\mathbb{R}^2$, denn für $\binom{x}{y} \in \mathbb{R}^2$ gilt

$$\begin{pmatrix} x \\ y \end{pmatrix} \;=\; y \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (x - y) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;.$$

Gilt auch

$$\begin{pmatrix} x \\ y \end{pmatrix} \;=\; a \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + b \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

für $a, b \in \mathbb{R}$, so muss $x = a + b$ und $y = a$ gelten. Daraus folgt aber $a = y$ und $b = x - y$, so dass die Koeffizienten also eindeutig sind.

(vi) Der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ hat unendlich viele Basen. Man überprüft leicht, dass $\{\mathbf{e}_1, c \cdot \mathbf{e}_2\}$ für alle $c \in \mathbb{R} \setminus \{0\}$ eine Basis von $\mathbb{R}^2$ ist.

3.2.4 Lineare Abhängigkeit und lineare Unabhängigkeit

Eine Teilmenge von Vektoren eines K-Vektorraums heißt linear abhängig, falls der davon erzeugte Teilraum bereits schon von einer kleineren Teilmenge erzeugt wird. Andernfalls heißt die Teilmenge linear unabhängig.

Definition 3.2.10 (Lineare Unabhängigkeit)**.** Es sei $(V, +, \cdot)$ ein K-Vektorraum. Eine Teilmenge $M \subseteq V$ heißt *linear unabhängig*, wenn für jedes $\mathbf{v} \in M$ gilt, dass $\langle M \setminus \{\mathbf{v}\} \rangle \neq \langle M \rangle$. Die Teilmenge M heißt *linear abhängig*, wenn M nicht linear unabhängig ist, das heißt

$$M \text{ ist linear abhängig} \qquad \Longleftrightarrow \qquad \exists \mathbf{v} \in M : \; \langle M \setminus \{\mathbf{v}\} \rangle = \langle M \rangle \;.$$

Beispiele.

(i) Die leere Menge $\emptyset$ ist linear unabhängig.

(ii) Ist $\mathbf{0} \in M$, so ist M linear abhängig, da $\langle M \setminus \{\mathbf{0}\}\rangle = \langle M\rangle$.

(iii) Die Menge $\left\{\binom{1}{1}, \binom{-1}{1}, \binom{1}{0}\right\}$ ist linear abhängig, weil $\langle M\rangle = \mathbb{R}^2$ aber auch schon $\langle M \setminus \left\{\binom{-1}{1}\right\}\rangle = \mathbb{R}^2$.

Lemma 3.2.11. *Es sei V eine K-Vektorraum und $M \subseteq V$. Die folgenden Aussagen sind äquivalent:*

(i) M ist linear abhängig.

(ii) Es gibt ein $\mathbf{v} \in M$ mit $\mathbf{v} \in \langle M \setminus \{\mathbf{v}\}\rangle$.

Das Lemma sagt also aus, dass es in einer linear abhängigen Teilmenge M ein Element gibt, das als Linearkombination der anderen Elemente aus M geschrieben werden kann.

Beweis. (i)$\Longrightarrow$(ii): Da M linear abhängig ist, gibt es nach Definition ein $\mathbf{v} \in M$ mit $\langle M \setminus \{\mathbf{v}\}\rangle = \langle M\rangle$. Da $\mathbf{v} \in M$, gilt $\mathbf{v} \in \langle M\rangle = \langle M \setminus \{\mathbf{v}\}\rangle$.

(ii)$\Longrightarrow$(i): Es sei $\mathbf{v} \in M$ mit $\mathbf{v} \in \langle M \setminus \{\mathbf{v}\}\rangle$. Dann ist

$$\mathbf{v} \;=\; \sum_{i=1}^{n} s_i \cdot \mathbf{v}_i \qquad \text{mit } s_i \in K \text{ und } \mathbf{v}_i \in M \setminus \{\mathbf{v}\} \text{ für } i = 1, \ldots, n. \tag{3.5}$$

Es sei nun $\mathbf{w} \in \langle M\rangle$, also

$$\mathbf{w} \;=\; \sum_{i=1}^{m} t_i \cdot \mathbf{w}_i \qquad \text{mit } t_i \in K \text{ und } \mathbf{w}_i \in M \text{ für } i = 1, \ldots, m. \tag{3.6}$$

Wir müssen zeigen, dass $\mathbf{w} \in \langle M \setminus \{\mathbf{v}\}\rangle$. Ist $\mathbf{v} \neq \mathbf{w}_i$ für alle $i = 1, \ldots, m$, dann sind wir fertig. Andernfalls können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\mathbf{v} = \mathbf{w}_1$. Dann gilt wegen (3.6) und (3.5)

$$\mathbf{w} \;=\; t_1 \cdot \mathbf{v} + \sum_{i=2}^{m} t_i \cdot \mathbf{w}_i \;=\; \sum_{i=1}^{n} (t_1 \cdot s_i) \cdot \mathbf{v}_i + \sum_{i=2}^{m} t_i \cdot \mathbf{w}_i \;.$$

Damit ist $\mathbf{w}$ also Linearkombination endlich vieler Elemente aus $M \setminus \{\mathbf{v}\}$ und folglich $\langle M \setminus \{\mathbf{v}\}\rangle = \langle M\rangle$. □

Beispiel. Es sei $V = \mathbb{R}^3$ und

$$M \;:=\; \left\{ \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\} \;.$$

Dann ist M linear abhängig, da

$$\begin{pmatrix}1\\1\\0\end{pmatrix} \in \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle .$$

Es gilt auch

$$\begin{pmatrix}1\\0\\0\end{pmatrix} \in \left\langle \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle$$

und

$$\begin{pmatrix}0\\1\\0\end{pmatrix} \in \left\langle \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle .$$

Man beachte jedoch, dass

$$\begin{pmatrix}0\\0\\1\end{pmatrix} \notin \left\langle \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle .$$

In dem folgenden Lemma stellen wir fest, dass eine Teilmenge von Vektoren genau dann linear abhängig ist, wenn der Nullvektor als nicht-triviale Linearkombination dieser Vektoren geschrieben werden kann.

Lemma 3.2.12. *Es sei V eine K-Vektorraum und $M \subseteq V$. Die folgenden Aussagen sind äquivalent:*

(i) M ist linear abhängig.

(ii) Es gibt paarweise verschiedene Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ und zugehörige Skalare $s_1, \ldots, s_n \in K$, die nicht alle Null sind, mit

$$s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n = \mathbf{0} .$$

Beweis. (i)$\Longrightarrow$(ii): Da M linear abhängig ist, gibt es nach Lemma 3.2.11 ein $\mathbf{v}_1 \in M$ mit $\mathbf{v}_1 \in \langle M \setminus \{\mathbf{v}_1\}\rangle$. Wir unterscheiden zwei Fälle. Erster Fall: $M \setminus \{\mathbf{v}_1\} = \emptyset$. Da $\langle\emptyset\rangle = \{\mathbf{0}\}$, gilt dann $\mathbf{v}_1 = \mathbf{0}$. Wir setzen $n := 1$, $s_1 := 1$, so dass gilt $s_1 \cdot \mathbf{v}_1 = 1 \cdot \mathbf{0} = \mathbf{0}$.

Zweiter Fall: $M \setminus \{\mathbf{v}_1\} \neq \emptyset$. Dann ist nach Voraussetzung

$$\mathbf{v}_1 = s_2 \cdot \mathbf{v}_2 + \cdots + s_n \cdot \mathbf{v}_n ,$$

mit $\mathbf{v}_2, \ldots, \mathbf{v}_n \in M \setminus \{\mathbf{v}_1\}$ und $s_2, \ldots, s_n \in K$. Setzen wir $s_1 := -1 \neq 0$, dann gilt also

$$s_1 \cdot \mathbf{v}_1 + s_2 \cdot \mathbf{v}_2 + \cdots + s_n \cdot \mathbf{v}_n \;=\; \mathbf{0} \;.$$

(ii)$\Longrightarrow$(i): Es seien also $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ paarweise verschieden und $s_1, \ldots, s_n \in K$ nicht alle Null, mit

$$s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;=\; \mathbf{0} \;.$$

Durch Umnummerieren können wir ohne Beschränkung der Allgemeinheit annehmen, dass $s_1 \neq 0$. Dann gilt

$$\mathbf{v}_1 \;=\; (-s_1^{-1} \cdot s_2) \cdot \mathbf{v}_2 + \cdots + (-s_1^{-1} \cdot s_n) \cdot \mathbf{v}_n \;\in\; \langle \mathbf{v}_2, \ldots, \mathbf{v}_n \rangle \;\subseteq\; \langle M \setminus \{\mathbf{v}_1\} \rangle \;.$$

Nach Lemma 3.2.11 ist M also linear abhängig. □

Als unmittelbare Folgerung aus Lemma 3.2.12 erhalten wir das nächste Korollar.

Korollar 3.2.13. *Es sei V ein K-Vektorraum und $M \subseteq V$. Die folgenden Aussagen sind äquivalent:*

(i) M ist linear unabhängig.

(ii) Für beliebige, paarweise verschiedene Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ und beliebige Skalare $s_1, \ldots, s_n \in K$ gilt:

$$s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;=\; \mathbf{0} \quad\Longrightarrow\quad s_1 = \cdots = s_n = 0 \;.$$

Bemerkung. Aus dem Korollar folgt insbesondere, dass Teilmengen linear unabhängiger Mengen selbst wieder linear unabhängig sind.

Beispiele.

(i) Es sei $V = \mathbb{R}^3$ und

$$M \;:=\; \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} \right\} \;.$$

Um festzstellen, ob M linear abhängig ist, müssen wir nach Lemma 3.2.12 überprüfen, ob es Skalare $x_1, x_2, x_3 \in \mathbb{R}$ gibt mit $(x_1, x_2, x_3) \neq (0, 0, 0)$, so dass

$$x_1 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \;.$$

In Matrixschreibweise bedeutet das

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad .$$

Um dieses homogene lineare Gleichungssystem zu lösen, wenden wir elementare Zeilenumformungen auf die erweiterte Matrix an:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 \\ 1 & 3 & 5 & 0 \end{pmatrix} \overset{\substack{A_{12}(-1) \\ A_{13}(-1)}}{\longrightarrow} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 4 & 0 \end{pmatrix} \overset{\substack{A_{21}(-1) \\ A_{23}(-2)}}{\longrightarrow} \begin{pmatrix} \boxed{1} & 0 & -1 & 0 \\ 0 & \boxed{1} & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad .$$

Daraus lesen wir die folgende Lösungsmenge L des homogenen linearen Gleichungssystems ab:

$$\begin{aligned} L \;&=\; \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \;\middle|\; x_1 - x_3 = 0 \wedge x_2 + 2x_3 = 0 \right\} \\ &=\; \left\{ \begin{pmatrix} t \\ -2t \\ t \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\} \;=\; \left\langle \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right\rangle \quad . \end{aligned}$$

Eine Lösung (x_1, x_2, x_3) ist also zum Beispiel $(1, -2, 1)$. Folglich ist M linear abhängig.

(ii) Es sei $V = \mathbb{R}^{\mathbb{R}}$ der Vektorraum aller Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$. Wir betrachten die Teilmenge $M := \{\sin, \cos\}$ und fragen uns, ob M linear abhängig oder linear unabhängig ist. Dazu müssen wir feststellen, ob es $(s_1, s_2) \neq (0, 0)$ gibt mit

$$s_1 \cdot \sin + s_2 \cdot \cos \;=\; \mathbf{0} \quad (= \text{Nullfunktion}).$$

Das heißt, für alle $x \in \mathbb{R}$ müsste gelten, dass

$$s_1 \cdot \sin x + s_2 \cdot \cos x \;=\; 0 \quad .$$

Setzen wir in diese Gleichung beispielsweise $x = 0$ ein, so erhalten wir

$$s_1 \cdot 0 + s_2 \cdot 1 \;=\; 0 \quad ,$$

also $s_2 = 0$. Setzen wir andererseits $x = \pi/2$ ein, so ergibt sich

$$s_1 \cdot 1 + s_2 \cdot 0 \;=\; 0 \quad ,$$

also $s_1 = 0$. Folglich ist M also linear unabhängig.

3.2.5 Basen

Wir beschäftigen uns im Folgenden näher mit Basen von Vektorräumen. Zunächst beweisen wir einige alternative Charakterisierungen von Basen.

Lemma 3.2.14 (Charakterisierung von Basen)**.** *Es sei $(V, +, \cdot)$ ein K-Vektorraum und $M \subseteq V$. Dann sind die folgenden Aussagen äquivalent:*

(i) M ist Basis von V.

(ii) M ist linear unabhängiges Erzeugendensystem von V.

(iii) M ist inklusionsminimales Erzeugendensystem von V, d.h.

$$\langle M \rangle \;=\; V \qquad \textit{und} \qquad \langle M \setminus \{\mathbf{u}\} \rangle \;\neq\; V \quad \textit{für alle } \mathbf{u} \in M.$$

(iv) M ist eine inklusionsmaximale linear unabhängige Teilmenge von V, d.h. M ist linear unabhängig aber $M \cup \{\mathbf{v}\}$ ist für jedes $\mathbf{v} \in V \setminus M$ linear abhängig.

Beweis. Wir beweisen das Lemma mittels eines Ringschlusses:

(i)$\Longrightarrow$(ii): Da M Basis ist, ist M nach Definition insbesondere ein Erzeugendensystem. Wir müssen nur noch zeigen, dass M linear unabhängig ist. Dazu betrachten wir $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ paarweise verschieden und $s_1, \ldots, s_n \in K$ mit

$$s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;=\; \mathbf{0} \;=\; 0 \cdot \mathbf{v}_1 + \cdots + 0 \cdot \mathbf{v}_n \;.$$

Da M eine Basis ist, folgt aus der Eindeutigkeit der Darstellung des Nullvektors $\mathbf{0}$ als Linearkombination paarweise verschiedener Vektoren aus M, dass $s_1 = \cdots = s_n = 0$. Folglich ist M wegen Korollar 3.2.13 linear unabhängig.

(ii)$\Longrightarrow$(iii): Da M ein Erzeugendensystem von V ist, gilt $\langle M \rangle = V$. Da M linear unabhängig ist, gilt nach Definition $\langle M \setminus \{\mathbf{u}\} \rangle \neq \langle M \rangle = V$ für alle $\mathbf{u} \in M$.

(iii)$\Longrightarrow$(iv): Nach Voraussetzung ist $\langle M \setminus \{\mathbf{u}\} \rangle \neq V = \langle M \rangle$ für alle $\mathbf{u} \in M$, so dass M nach Definition linear unabhängig ist. Es bleibt zu zeigen, dass $M \cup \{\mathbf{v}\}$ für alle $\mathbf{v} \in V \setminus M$ linear abhängig ist. Wäre $M \cup \{\mathbf{v}\}$ für ein $\mathbf{v} \in V \setminus M$ linear unabhängig, so folgte daraus nach Definition

$$\langle M \rangle \;=\; \langle (M \cup \{\mathbf{v}\}) \setminus \{\mathbf{v}\} \rangle \;\neq\; V \;.$$

Dies ist aber ein Widerspruch, da nach Voraussetzung $\langle M \rangle = V$.

(iv)$\Longrightarrow$(i): Wir zeigen zunächst, dass $\langle M \rangle = V$, d.h. jeder Vektor $\mathbf{v} \in V$ kann als Linearkombination endlich vieler Vektoren aus M geschrieben werden. Das ist klar, falls $\mathbf{v} \in M$. Es sei also im Folgenden $\mathbf{v} \in V \setminus M$. Dann ist nach Voraussetzung $M \cup \{\mathbf{v}\}$ linear abhängig. Wegen Lemma 3.2.12 gibt es dann $s, s_1, \ldots, s_n \in K$ nicht alle Null und $\mathbf{v}_1, \ldots, \mathbf{v}_n \in M$ mit

$$s \cdot \mathbf{v} + s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;=\; \mathbf{0} \;.$$

Da M linear unabhängig ist, muss $s \neq 0$ gelten. Dann gilt

$$\mathbf{v} \;=\; -(s^{-1}s_1)\cdot\mathbf{v}_1 - \cdots - (s^{-1}s_n)\cdot\mathbf{v}_n \;\in\; \langle M\rangle \;.$$

Es bleibt zu zeigen, dass jeder Vektor $\mathbf{v} \in V$ eine eindeutige Darstellung als Linearkombination endlich vieler paarweise verschiedener Vektoren aus M besitzt. Es sei also

$$\mathbf{v} \;=\; s_1\mathbf{v}_1 + \cdots + s_n\mathbf{v}_n \qquad \text{und} \qquad \mathbf{v} \;=\; t_1\mathbf{w}_1 + \cdots + t_m\mathbf{w}_m \tag{3.7}$$

mit $s_1,\ldots,s_n,t_1,\ldots,t_m \in K$ und $\mathbf{v}_1,\ldots,\mathbf{v}_n,\mathbf{w}_1,\ldots,\mathbf{w}_m \in M$. Durch Umbenennen der Vektoren erhält man $\{\mathbf{v}_1,\ldots,\mathbf{v}_n,\mathbf{w}_1,\ldots,\mathbf{w}_m\} = \{\mathbf{x}_1,\ldots,\mathbf{x}_q\} \subseteq M$, wobei die $\mathbf{x}_i$ paarweise verschieden gewählt sind. Somit können wir (3.7) wie folgt schreiben:

$$\mathbf{v} \;=\; s'_1\mathbf{x}_1 + \cdots + s'_q\mathbf{x}_q \qquad \text{und} \qquad \mathbf{v} \;=\; t'_1\mathbf{x}_1 + \cdots + t'_q\mathbf{x}_q \;.$$

Durch Subtraktion der beiden Ausdrücke erhält man

$$\mathbf{0} \;=\; (s'_1 - t'_1)\mathbf{x}_1 + \cdots + (s'_q - t'_q)\mathbf{x}_q \;.$$

Da M linear unabhängig ist gilt also $s'_i = t'_i$ für $i = 1,\ldots,q$. Damit sind also die beiden Darstellungen von $\mathbf{v}$ in (3.7) identisch. □

Schon weiter oben haben wir über endlich erzeugte Vektorräume gesprochen. Der Vollständigkeit halber reichen wir eine formale Definition dieses Begriffs nach.

Definition 3.2.15 (Endlich erzeugte Vektorräume)**.** Es sei V ein K-Vektorraum. Gibt es eine endliche Teilmenge $M \subseteq V$ mit $V = \langle M\rangle$, so ist V *endlich erzeugt*.

Wir haben bislang nur an speziellen Beispielen gesehen, dass Basen von Vektorräumen tatsächlich existieren können. Der folgende Satz belegt, dass das kein Zufall ist.

Satz 3.2.16 (Existenz von Basen)**.** *Jeder endlich erzeugte K-Vektorraum besitzt eine Basis.*

Beweis. Es sei V ein K-Vektorraum mit $V = \langle\mathbf{v}_1,\ldots,\mathbf{v}_n\rangle$. Wir zeigen mittels Induktion über n, dass V eine Basis besitzt. Induktionsanfang: $n = 0$ also $V = \langle\emptyset\rangle = \{\mathbf{0}\}$. Dann ist $\emptyset$ nach Definition eine Basis von V.

Induktionsschluss: Die Behauptung sei für ein beliebiges aber fest gewähltes $n \in \mathbb{N}_0$ wahr. Es sei jetzt $V = \langle\mathbf{v}_1,\ldots,\mathbf{v}_{n+1}\rangle$. Ist die Menge $\{\mathbf{v}_1,\ldots,\mathbf{v}_{n+1}\}$ linear unabhängig, so bildet sie nach Lemma 3.2.14 eine Basis von V. Andernfalls gibt es ein $i \in \{1,\ldots,n+1\}$ mit

$$V = \langle\mathbf{v}_1,\ldots,\mathbf{v}_{n+1}\rangle = \langle\mathbf{v}_1,\ldots,\mathbf{v}_{i-1},\mathbf{v}_{i+1},\ldots,\mathbf{v}_{n+1}\rangle \;.$$

Der Vektorraum V wird also von n Vektoren erzeugt und besitzt daher nach Induktionsannahme eine Basis. □

Man kann sogar zeigen, dass jeder beliebige Vektorraum eine Basis besitzt. Der Beweis, auf den wir hier nicht näher eingehen, beruht auf dem Lemma von Zorn.

Aus dem Beweis von Satz 3.2.16 folgt das nächste Korollar.

Korollar 3.2.17. *Jedes endliche Erzeugendensystem eines Vektorraums enthält eine Basis.*

Wir wenden uns jetzt kurz dem Problem zu, für einen endlich erzeugten Vektorraum eine Basis algorithmisch zu konstruieren. Der Algorithmus beruht auf dem folgenden Lemma.

Lemma 3.2.18. *Es sei V ein K-Vektorraum und $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$.*

(i) Für $i \neq j$ und $s \in K$ gilt

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_j, \ldots, \mathbf{v}_n \rangle \;=\; \langle \mathbf{v}_1, \ldots, \mathbf{v}_j + s\mathbf{v}_i, \ldots, \mathbf{v}_n \rangle \;.$$

(ii) Für $i \in \{1, \ldots, n\}$ und $t \in K \setminus \{0\}$ gilt

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_i, \ldots, \mathbf{v}_n \rangle \;=\; \langle \mathbf{v}_1, \ldots, t\mathbf{v}_i, \ldots, \mathbf{v}_n \rangle \;.$$

(iii) $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle \;=\; \langle \mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{0} \rangle$.

Beweis. Klar. □

Wir erläutern anhand eines Beispiels, wie man mit Hilfe des Lemmas zu einem gegebenen endlich erzeugten Vektorraum eine Basis konstruieren kann.

Beispiel. Es sei $K = \mathbb{R}$ und

$$V \;:=\; \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \\ 11 \end{pmatrix} \right\rangle \;=\; \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \rangle \;.$$

Wegen Lemma 3.2.18 (i) ist dann

$$V \;=\; \langle \mathbf{v}_1, \mathbf{v}_2 - \mathbf{v}_1, \mathbf{v}_3 - \mathbf{v}_1 \rangle \;=\; \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 10 \end{pmatrix} \right\rangle \;=\; \langle \mathbf{v}_1', \mathbf{v}_2', \mathbf{v}_3' \rangle \;.$$

Durch Anwenden von Lemma 3.2.18 (i), (ii) und (iii) bekommt man

$$V \;=\; \langle \mathbf{v}_1', \tfrac{1}{2}\mathbf{v}_2', \mathbf{v}_3' - \tfrac{5}{2}\mathbf{v}_2' \rangle \;=\; \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle \;=\; \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\rangle \;.$$

Da die letzten beiden Vektoren linear unabhängig sind, bilden sie also eine Basis von V.

Wie man feststellen kann, haben wir in diesem Beispiel im Wesentlichen den Gauß'schen Algorithmus auf die Spalten der durch die erzeugenden Vektoren gebildeten Matrix angewendet. Lemma 3.2.18 besagt, dass die dabei verwendeten *elementaren Spaltenumformungen* die Eigenschaft erhalten, dass die Spaltenvektoren den Vektorraum erzeugen.

3.2.6 Dimension

Ziel dieses Unterabschnitts ist es zu zeigen, dass alle Basen eines Vektorraums dieselbe Kardinalität besitzen, die dann auch Dimension des Vektorraums genannt wird.

Im letzten Unterabschnitt haben wir gezeigt, dass jedes endliche Erzeugendensystem eines Vektorraums V eine Basis von V enthält. Der folgende Satz stellt die umgekehrte Vorgehensweise zur Konstruktion einer Basis dar.

Satz 3.2.19 (Basisergänzungssatz)**.** *Es sei V ein endlich erzeugter K-Vektorraum mit endlichem Erzeugendensystem $E \subseteq V$, also $V = \langle E \rangle$. Weiterhin sei $M \subseteq V$ linear unabhängig. Dann gibt es eine Teilmenge $E' \subseteq E$, so dass $M \cup E'$ eine Basis von V ist.*

Der Satz sagt also aus, dass man jede linear unabhängige Teilmenge von V durch Hinzunahme von geeigneten Vektoren aus einem vorgegebenen Erzeugendensystem zu einer Basis von V ergänzen kann.

Beweis. Es sei $E' \subseteq E$ inklusionsminimal mit der Eigenschaft, dass $\langle E' \cup M \rangle = V$, d.h. $\langle (E' \setminus \{\mathbf{v}\}) \cup M \rangle \neq V$ für alle $\mathbf{v} \in E'$. Wir zeigen, dass $B := E' \cup M$ eine Basis von V ist. Nach Konstruktion ist B ein Erzeugendensystem von V. Wegen Lemma 3.2.14 (ii) müssen wir nur noch zeigen, dass B linear unabhängig ist. Es seien $\mathbf{u}_1, \ldots, \mathbf{u}_n \in E'$ und $\mathbf{v}_1 \ldots, \mathbf{v}_m \in M$. Weiter seien $s_1, \ldots, s_n, t_1, \ldots, t_m \in K$ mit

$$\sum_{i=1}^{n} s_i \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j \;=\; \mathbf{0} \;. \tag{3.8}$$

Wir zeigen zunächst, dass $s_1 = \cdots = s_n = 0$. Ist $s_i \neq 0$, so ist

$$\mathbf{u}_i \;=\; -\sum_{k \neq i} ({s_i}^{-1} \cdot s_k) \cdot \mathbf{u}_k - \sum_{j=1}^{m} ({s_i}^{-1} \cdot t_j) \cdot \mathbf{v}_j \;\in\; \langle (E' \setminus \{\mathbf{u}_i\}) \cup M \rangle \;.$$

Folglich ist $V = \langle E' \cup M \rangle = \langle (E' \setminus \{\mathbf{u}_i\}) \cup M \rangle$ im Widerspruch zur Minimalität von E'. Wir haben also gezeigt, dass $s_1 = \cdots = s_n = 0$. Damit folgt aus (3.8)

$$\sum_{j=1}^{m} t_j \cdot \mathbf{v}_j \;=\; \mathbf{0} \;.$$

Da M linear unabhängig ist, folgt aus Korollar 3.2.13, dass $t_1 = \cdots = t_m = 0$. Folglich ist also $E' \cup M$ linear unabhängig (wieder wegen Korollar 3.2.13). □

Beispiel. Wir betrachten das Erzeugendensystem

$$E \;:=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

des $\mathbb{R}$-Vektorraums $\mathbb{R}^{2\times 2}$. Die Menge

$$M \;:=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

ist linear unabhängig und die Obermenge

$$B \;:=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$$

ist eine Basis von $\mathbb{R}^{2\times 2}$. Man beachte jedoch, dass

$$B' \;:=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

keine Basis von $\mathbb{R}^{2\times 2}$ ist, da diese Menge linear abhängig ist (der erste Vektor ist die Summe der beiden letzten Vektoren).

Der folgende Satz ist ein wichtiger Meilenstein auf unserem Weg, der uns schließlich zu der Einsicht führen wird, dass alle Basen eines Vektorraums dieselbe Kardinalität haben.

Satz 3.2.20 (Austauschsatz von Steinitz)**.** *Es sei V ein K-Vektorraum, I eine beliebige Indexmenge und $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ und $\{\mathbf{u}_i \mid i \in I\}$ Basen von V. Dann gibt es zu jedem $i \in \{1, \ldots, n\}$ ein $j_i \in I$, so dass*

$$\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{u}_{j_i}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$$

eine Basis von V ist.

Beweis. Da die linear unabhängige Menge $\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$ keine inklusionsmaximale linear unabhängige Menge ist, ist sie auch keine Basis, also nach Lemma 3.2.14 (ii)

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n \rangle \;\neq\; V \;.$$

Folglich gibt es also ein $j_i \in I$ mit

$$u_{j_i} \;\notin\; \langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n \rangle \;. \tag{3.9}$$

Wir zeigen, dass $B := \{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{u}_{j_i}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$ eine Basis von V ist. Zunächst zeigen wir, dass B linear unabhängig ist. Es seien

$$s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n \;\in\; K$$

mit

$$s_1\mathbf{v}_1 + \cdots + s_{i-1}\mathbf{v}_{i-1} + t\mathbf{u}_{j_i} + s_{i+1}\mathbf{v}_{i+1} + \cdots + s_n\mathbf{v}_n \;=\; \mathbf{0}\ .$$

Dann ist $t = 0$ wegen (3.9). Da die Menge $\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n\}$ linear unabhängig ist, gilt dann auch $s_1 = \cdots = s_{i-1} = s_{i+1} = \cdots = s_n = 0$. Aus Korollar 3.2.13 folgt also, dass B linear unabhängig ist.

Nach Satz 3.2.19 kann man B zu einer Basis ergänzen, das heißt es gibt $E' \subseteq E = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, so dass $B \cup E'$ eine Basis von V ist. Ist $v_i \notin E'$, so ist $B \cup E' = B$ und wir sind fertig. Andernfalls ist $B \cup E' = \{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{u}_{j_i}\}$ Basis. Da $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ Basis und damit inkusionsmaximale linear unabhängige Teilmenge ist, gilt $\mathbf{u}_{j_i} \in \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Folglich ist $B = B \cup E'$ Basis. □

Der folgende Satz enthält das wichtigste Resultat dieses Unterabschnitts und führt uns schließlich zum Begriff der Dimension.

Satz 3.2.21. *Es sei V ein K-Vektorraum und $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ eine Basis von V mit n paarweise verschiedenen Elementen, d.h. $|B| = n$. Dann gilt:*

(i) Ist B' eine beliebige Basis von V, so ist $|B'| = n$.

(ii) Ist $M \subseteq V$ linear unabhängig, so ist $|M| \leq n$.

(iii) Ist $M \subseteq V$ linear unabhängig und $|M| = n$, so ist M Basis von V.

Definition 3.2.22 (Dimension eines Vektorraums)**.** In der in Satz 3.2.21 beschriebenen Situation heißt n die *Dimension* des Vektorraums V; wir schreiben $\dim V = n$. Man sagt dann auch, dass V *endlich dimensional* ist. Besitzt ein Vektorraum V keine endliche Basis, so ist seine Dimension unendlich, also $\dim V = \infty$. Man sagt dann auch, dass V *unendlich dimensional* ist.

Bemerkung. Es folgt aus Korollar 3.2.17, dass jeder endlich erzeugte Vektorraum endlich dimensional ist.

Beweis von Satz 3.2.21. Zu (i): Es sei $B' = \{\mathbf{w}_i \mid i \in I\}$ Basis von V. Wir beweisen zunächst mittels vollständiger Induktion über k, dass es zu jedem $0 \leq k \leq n$ Indizes $j_1, \ldots, j_k \in I$ gibt, so dass die Menge

$$\{\mathbf{w}_{j_1}, \ldots, \mathbf{w}_{j_k}, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n\}$$

eine Basis von V ist. Induktionsanfang: Für $k = 0$ ist die Aussage klar, da die Menge $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ nach Voraussetzung Basis von V ist. Induktionsschluss: Die Aussage gelte für ein beliebiges, fest gewähltes k. Wir wenden den Austauschsatz von Steinitz (Satz 3.2.20) auf die beiden Basen

$$\{\mathbf{w}_{j_1}, \ldots, \mathbf{w}_{j_k}, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n\} \quad \text{und} \quad \{\mathbf{w}_i \mid i \in I\}$$

an. Der Austauschsatz besagt, dass es einen Index $j_{k+1} \in I$ gibt, so dass die Menge $\{\mathbf{w}_{j_1}, \ldots, \mathbf{w}_{j_{k+1}}, \mathbf{v}_{k+2}, \ldots, \mathbf{v}_n\}$ eine Basis von V ist. Damit ist der Induktionsbeweis fertig.

Für $k = n$ erhalten wir aus der bewiesenen Behauptung also Indizes $j_1, \ldots, j_n \in I$, so dass $\{\mathbf{w}_{j_1}, \ldots, \mathbf{w}_{j_n}\}$ Basis von V ist. Nach Lemma 3.2.14 (iv) ist $\{\mathbf{w}_{j_1}, \ldots, \mathbf{w}_{j_n}\}$ also eine inklusionsmaximale linear unabhängige Teilmenge von V. Da auch die Obermenge $\{\mathbf{w}_i \mid i \in I\}$ linear unabhängig ist, folgt also $\{j_1, \ldots, j_n\} = I$ und damit $|B'| = n$.

Zu (ii): Es sei $M \subseteq V$ linear unabhängig. Da man M nach Satz 3.2.19 zu einer Basis ergänzen kann und da jede Basis nach (i) genau n Elemente enthält, folgt also $|M| \leq n$.

Zu (iii): Ist $|M| = n$ und M linear unabhängig, so ist M selbst eine Basis, da M nach Satz 3.2.19 zu einer n-elementigen Basis ergänzt werden kann. □

Beispiele.

(i) Die Dimension des K-Vektorraums K^n ist n, da beispielsweise die Menge der Einheitsvektoren $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ eine Basis von K^n bildet.

(ii) Die Dimension des K-Vektorraums aller $m \times n$ Matrizen $K^{m \times n}$ ist $m \cdot n$. Man überzeugt sich leicht davon, dass die Menge

$$\{E_{ij} \mid 1 \leq i \leq m \text{ und } 1 \leq j \leq n\}$$

eine Basis von $K^{m \times n}$ ist. Dabei bezeichnet E_{ij} die $m \times n$ Matrix, deren Eintrag in der i-ten Zeile und j-ten Spalte eine Eins ist und die sonst nur Null-Einträge hat.

(iii) Es sei $K = \mathbb{R}$ und

$$V := \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \\ 11 \end{pmatrix} \right\rangle .$$

Wie weiter oben schon gezeigt wurde, ist $\dim V = 2$.

(iv) Es sei M eine beliebige unendliche Menge. Dann ist die Dimension des K-Vektorraums $K^{(M)}$ unendlich. Wir geben eine Basis von $K^{(M)}$ an, die aus unendlich vielen Elementen besteht. Wie in dem Beispiel vor Definition 3.2.9 betrachten wir für $x \in M$ die Funktion $\mathbf{e}_x \in K^{(M)}$ mit

$$\mathbf{e}_x(y) := \begin{cases} 1 & \text{falls } x = y, \\ 0 & \text{sonst.} \end{cases}$$

Dann ist $B := \{\mathbf{e}_x \mid x \in M\}$ eine Basis von $K^{(M)}$. Wir haben in dem Beispiel vor Definition 3.2.9 schon gezeigt, dass B den Vektorraum $K^{(M)}$

erzeugt. Es seien $\mathbf{e}_{x_1}, \ldots, \mathbf{e}_{x_n} \in B$ paarweise verschieden und $s_1, \ldots, s_n \in K$ mit

$$s_1 \cdot \mathbf{e}_{x_1} + \cdots + s_n \cdot \mathbf{e}_{x_n} \;=\; \mathbf{0} \;.$$

Dann gilt insbesondere für $i = 1, \ldots, n$, dass

$$s_i \;=\; (s_1 \cdot \mathbf{e}_{x_1} + \cdots + s_n \cdot \mathbf{e}_{x_n})(x_i) \;=\; 0 \;.$$

Folglich ist B linear unabhängig.

Die Eigenschaft eines Vektorraums, endlich dimensional zu sein, vererbt sich an alle seine Teilräume.

Korollar 3.2.23. *Ist V ein endlich dimensionaler K-Vektorraum und U ein Teilraum von V, dann ist auch U endlich dimensional und es gilt* $\dim U \leq \dim V$. *Ist* $\dim U = \dim V$, *so ist $U = V$.*

Beweis. Ist $\dim V = n$, so sind je $n+1$ Vektoren aus V linear abhängig. Insbesondere sind je $n+1$ Vektoren aus U linear abhängig, so dass eine Basis von U höchstens n Vektoren enthält, d.h. $\dim U \leq n$.

Ist $\dim U = n$, so besitzt U eine Basis B mit $|B| = n$. Dann ist B eine inklusionsmaximale linear unabhängige Teilmenge von V und damit Basis von V. Folglich ist $U = V$. □

Satz 3.2.24 (Dimensionsformel für Untervektorräume)**.** *Es sei V ein endlich erzeugter K-Vektorraum und U_1, U_2 Teilräume von V. Dann ist*

$$\dim U_1 + \dim U_2 \;=\; \dim(U_1 + U_2) + \dim(U_1 \cap U_2) \;.$$

Beweis. Es sei $B = \{\mathbf{u}_1, \ldots, \mathbf{u}_d\}$ eine Basis von $U_1 \cap U_2$, also insbesondere $\dim(U_1 \cap U_2) = d$. Dann kann man B nach Satz 3.2.19 zu einer Basis von U_1 beziehungsweise von U_2 ergänzen. Es seien also

$$B_1 \;=\; \{\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{v}_1, \ldots, \mathbf{v}_m\}$$

eine Basis von U_1 (also $\dim U_1 = d + m$) und

$$B_2 \;=\; \{\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{w}_1, \ldots, \mathbf{w}_n\}$$

eine Basis von U_2 (also $\dim U_2 = d + n$). Dann gilt

$$\dim U_1 + \dim U_2 \;=\; \dim(U_1 \cap U_2) + (d + m + n) \;.$$

Es bleibt zu zeigen, dass $\dim(U_1 + U_2) = d + m + n$. Wir zeigen, dass

$$C \;:=\; \{\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n\} \;\subseteq\; U_1 \cup U_2 \;\subseteq\; U_1 + U_2$$

eine Basis von $U_1 + U_2$ mit $d + m + n$ paarweise verschiedenen Vektoren ist. Wir überzeugen uns zunächst davon, dass C den Teilraum $U_1 + U_2$ erzeugt, also $\langle C \rangle = U_1 + U_2$. Es sei $\mathbf{x} \in U_1 + U_2$, das heißt $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$ mit $\mathbf{x}_1 \in U_1$ und $\mathbf{x}_2 \in U_2$. Dann gibt es $s_1, \ldots, s_d, t_1, \ldots, t_m \in K$ mit

$$\mathbf{x}_1 \;=\; \sum_{i=1}^{d} s_i \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j \;\;,$$

weil B_1 eine Basis von U_1 ist. Analog gibt es $s'_1, \ldots, s'_d, r_1, \ldots, r_n \in K$ mit

$$\mathbf{x}_2 \;=\; \sum_{i=1}^{d} s'_i \cdot \mathbf{u}_i + \sum_{k=1}^{n} r_k \cdot \mathbf{w}_k \;\;,$$

weil B_2 eine Basis von U_2 ist. Dann ist

$$\mathbf{x} \;=\; \mathbf{x}_1 + \mathbf{x}_2 \;=\; \sum_{i=1}^{d} (s_i + s'_i) \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j + \sum_{k=1}^{n} r_k \cdot \mathbf{w}_k \;\in\; \langle C \rangle \;\;,$$

also $\langle C \rangle = U_1 + U_2$.

Es bleibt zu zeigen, dass C linear unabhängig ist. Dazu betrachten wir Skalare $s_1, \ldots, s_d, t_1, \ldots, t_m, r_1, \ldots, r_n \in K$ mit

$$\sum_{i=1}^{d} s_i \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j + \sum_{k=1}^{n} r_k \cdot \mathbf{w}_k \;=\; \mathbf{0} \;\;.$$

Dann gilt

$$\mathbf{y} \;:=\; \underbrace{\sum_{i=1}^{d} s_i \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j}_{\in U_1} \;=\; \underbrace{-\sum_{k=1}^{n} r_k \cdot \mathbf{w}_k}_{\in U_2} \;\in\; U_1 \cap U_2 \;\;. \tag{3.10}$$

Da B eine Basis des Teilraums $U_1 \cap U_2$ ist, gibt es eindeutig bestimmte Koeffizienten $s'_1, \ldots, s'_d \in K$ mit

$$\mathbf{y} \;=\; \sum_{i=1}^{d} s'_i \cdot \mathbf{u}_i \;\;. \tag{3.11}$$

Aus (3.10) und (3.11) folgt, dass

$$\sum_{i=1}^{d} s'_i \cdot \mathbf{u}_i + \sum_{k=1}^{n} r_k \cdot \mathbf{w}_k \;=\; \mathbf{0} \;\;.$$

Da $B_2 = \{\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{w}_1, \ldots, \mathbf{w}_n\}$ linear unabhängig ist, folgt $s'_1 = \cdots = s'_d = 0$ und $r_1 = \cdots = r_n = 0$. Eingesetzt in (3.10) ergibt das

$$\sum_{i=1}^{d} s_i \cdot \mathbf{u}_i + \sum_{j=1}^{m} t_j \cdot \mathbf{v}_j \;=\; \mathbf{0} \;.$$

Da $B_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{v}_1, \ldots, \mathbf{v}_m\}$ linear unabhängig ist, folgt schließlich $s_1 = \cdots = s_d = 0$ und $t_1 = \cdots = t_m = 0$. Folglich sind die Vektoren in C paarweise verschieden und linear unabhängig. □

Beispiel. Es sei V ein dreidimensionaler K-Vektorraum und $U_1 \neq U_2$ zwei verschiedene Teilräume von V mit $\dim U_1 = \dim U_2 = 2$. Dann muss $\dim(U_1 \cap U_2) = 1$ gelten, denn für $\dim(U_1 + U_2)$ kommt nur 2 oder 3 in Betracht. Wäre $\dim(U_1 + U_2) = 2 = \dim U_i$ $(i = 1, 2)$, dann wäre $U_1 = U_1 + U_2 = U_2$ im Widerspruch zur Voraussetzung $U_1 \neq U_2$.

3.2.7 Eine Anwendung: Endliche Körper

Wir diskutieren in diesem Abschnitt einige interessante Eigenschaften endlicher Körper, die wir mit Hilfe der Theorie der Vektorräume herleiten. Dazu benötigen wir zunächst den folgenden Satz.

Satz 3.2.25. *Es sei K ein Körper mit q Elementen und V ein K-Vektorraum mit $\dim V = n$. Dann ist $|V| = q^n$.*

Beweis. Es sei $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ eine Basis von V. Dann lässt sich jeder Vektor $\mathbf{u} \in V$ eindeutig schreiben als

$$\mathbf{u} \;=\; s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n$$

mit $s_1, \ldots, s_n \in K$. Da es für jedes der s_i, $i = 1, \ldots, n$, genau q Möglichkeiten gibt, existieren insgesamt also genau q^n solcher n-Tupel $(s_1, \ldots, s_n)$. Folglich ist also $|V| = q^n$. □

Das folgende Lemma dient als Vorbereitung für die Definition der *Charakteristik* eines Körpers, die wir danach vorstellen.

Lemma 3.2.26. *Zu einem endlichen Körper K gibt es eine natürliche Zahl $p \in \mathbb{N}$ mit*

$$p \cdot 1 \;:=\; \underbrace{1 + 1 + \cdots + 1}_{p \text{ Summanden}} \;=\; 0 \;.$$

Hier bezeichnet 1 das Einselement und 0 das Nullelement aus K.

Beweis. Da K endlich ist, ist auch die Teilmenge $\{n \cdot 1 \mid n \in \mathbb{N}\}$ endlich. Folglich gibt es natürliche Zahlen $n_1 < n_2$ mit $n_1 \cdot 1 = n_2 \cdot 1$. Wie man leicht sieht, folgt daraus aber $(n_2 - n_1) \cdot 1 = 0$. □

Mit der Charakteristik eines Körpers bezeichnet man jetzt die kleinste Zahl p, die die Eigenschaft aus dem Lemma besitzt.

Definition 3.2.27 (Charakteristik eines Körpers)**.** Ist K ein beliebiger Körper, so heißt die kleinste natürliche Zahl p mit

$$p \cdot 1 \;:=\; \underbrace{1+1+\cdots+1}_{p \text{ Summanden}} \;=\; 0$$

die *Charakteristik* von K, in Zeichen $\operatorname{char} K = p$. Gibt es keine solche natürliche Zahl p, so ist die Charakteristik von K gleich null.

Beispiele.

(i) $\operatorname{char} \mathbb{R} = 0$

(ii) $\operatorname{char} \mathbb{Q} = 0$

(iii) $\operatorname{char} \mathbb{Z}_2 = 2$

(iv) $\operatorname{char} \mathbb{Z}_p = p$

Es stellt sich heraus, dass die Charakteristik eines Körpers keine beliebige natürliche Zahl sein kann.

Satz 3.2.28. *Die Charakteristik eines Körpers K ist null oder eine Primzahl.*

Beweis. Es sei K ein Körper mit $\operatorname{char} K = p \neq 0$. Dann ist $p > 1$. Wir nehmen im Widerspruch zur Behauptung an, dass p keine Primzahl ist. Dann gibt es zwei natürliche Zahlen $1 < p_1, p_2 < p$ mit $p = p_1 \cdot p_2$. Man überprüft leicht, dass dann

$$\begin{aligned} 0 \;=\; p \cdot 1 \;&=\; \underbrace{1+1+\cdots+1}_{p \text{ Summanden}} \\ &=\; (\underbrace{1+1+\cdots+1}_{p_1 \text{ Summanden}}) \cdot (\underbrace{1+1+\cdots+1}_{p_2 \text{ Summanden}}) \;=\; (p_1 \cdot 1) \cdot (p_2 \cdot 1) \;. \end{aligned}$$

Folglich gilt $p_1 \cdot 1 = 0$ oder $p_2 \cdot 1 = 0$ im Widerspruch zur Minimalität von p. □

Damit folgt insbesondere für endliche Körper, dass die Charakteristik eine Primzahl sein muss.

Korollar 3.2.29. *Ist K ein endlicher Körper, so ist* $\operatorname{char} K$ *eine Primzahl.*

Wir möchten im Folgenden herausfinden, welcher Zusammenhang zwischen der Mächtigkeit eines endlichen Körpers und seiner Charakteristik besteht.

Satz 3.2.30. *Es sei K ein endlicher Körper mit Charakteristik p. Dann ist $K_0 := \{0, 1, 1+1, \ldots, (p-1)\cdot 1\}$ mit der Einschränkung der Addition und Multiplikation von K ein Körper, also ein Teilkörper.*

Beweis. Nachrechnen. □

Bemerkung. Ist K ein Körper und $K_0 \subseteq K$ ein Teilkörper, so kann man K als K_0-Vektorraum auffassen.

Beispiele.

(i) Der Körper der komplexen Zahlen $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}$ kann als $\mathbb{R}$-Vektorraum mit Basis $\{1, i\}$ aufgefasst werden.

(ii) Die reellen Zahlen $\mathbb{R}$ bilden einen $\mathbb{Q}$-Vektorraum.

(iii) $\mathbb{Z}_5$ ist kein Teilkörper von $\mathbb{Z}_7$, weil die Addition in $\mathbb{Z}_5$ sich von der Addition in $\mathbb{Z}_7$ unterscheidet.

Mit den gesammelten Einsichten können wir jetzt das folgende wichtige Resultat über die Kardinalität endlicher Körper beweisen.

Satz 3.2.31. *Ist K ein endlicher Körper mit Charakteristik p, so gibt es ein $n \in \mathbb{N}$ mit $|K| = p^n$.*

Beweis. Nach Satz 3.2.30 ist $K_0 = \{0, 1, 1 + 1, \ldots, (p - 1) \cdot 1\}$ ein Teilkörper mit $|K_0| = p$ und K kann als (endlich dimensionaler) K_0-Vektorraum betrachtet werden. Die Behauptung folgt also aus Satz 3.2.25. □

Folglich gibt es beispielsweise keinen Körper mit 6 Elementen. Wir geben noch den folgenden Satz ohne Beweis an.

Satz 3.2.32. *Zu jeder Primzahlpotenz p^n gibt es einen Körper mit p^n Elementen.*

Beispiel. Als Beispiel stellen wir einen Körper mit 4 Elementen vor. Die Menge

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \subseteq \mathbb{Z}_2^{2\times 2}$$

bildet mit der Matrixaddition und -multiplikation einen Körper mit 4 Elementen.

3.3 Lineare Abbildungen und Matrizen

Bereits in Kapitel 2 haben wir uns kurz mit Homomorphismen von Gruppen und Ringen beschäftigt. Homomorphismen sind Abbildungen, die mit den Verknüpfungen der zugrundeliegenden Struktur (also Gruppen oder Ringen) verträglich sind. In diesem Abschnitt beschäftigen wir uns mit Homomorphismen auf Vektorräumen, die auch lineare Abbildungen genannt werden. Wie wir sehen werden, besteht ein enger Zusammenhang zwischen diesen linearen Abbildungen und Matrizen beziehungsweise linearen Gleichungssystemen.

3.3.1 Lineare Abbildungen

Im letzten Abschnitt hatten wir den Begriff der Basis eines Vektorraums ausführlich diskutiert. Dabei handelt es sich um eine linear unabhängige Menge von Vektoren, die den zugrundeliegenden Vektorraum erzeugen. Geben wir einer solchen Menge eine Ordnung, so erhalten wir eine sogenannte Basisfolge.

Definition 3.3.1 (Basisfolgen)**.** Es sei V ein K-Vektorraum und $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in V^n$. Dann heißt B *Basisfolge* oder *geordnete Basis*, wenn $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ Basis von V ist und die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ paarweise verschieden sind (also $|\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}| = n$).

Beispiel. In dem $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ sind $B_1 = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ und $B_2 = (\mathbf{e}_2, \mathbf{e}_1, \mathbf{e}_3)$ zwei unterschiedliche Basisfolgen. Man beachte, dass $B_1 \neq B_2$ aber $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\} = \{\mathbf{e}_2, \mathbf{e}_1, \mathbf{e}_3\}$ gilt.

Bemerkung. Ist $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in V^n$ eine Basisfolge des Vektorraums V, so folgt aus der Definition von Basen (Definition 3.2.9), dass es zu jedem Vektor $\mathbf{v} \in V$ eindeutige Koeffizienten $(s_1, \ldots, s_n) \in K^n$ gibt mit

$$\mathbf{v} \;=\; s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;\; .$$

Ordnen wir dem Vektor $\mathbf{v} \in V$ diese Koeffizienten zu, so erhalten wir eine Abbildung

$$\begin{aligned} c_B \;:\; V &\to K^n \;\; , \\ \mathbf{v} &\mapsto \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \;\; . \end{aligned}$$

Man überzeugt sich leicht davon, dass für alle $\mathbf{v}, \mathbf{v}' \in V$ und $s \in K$ gilt:

$$c_B(\mathbf{v} + \mathbf{v}') \;=\; c_B(\mathbf{v}) + c_B(\mathbf{v}')$$

und

$$c_B(s \cdot \mathbf{v}) \;=\; s \cdot c_B(\mathbf{v}) \;\; .$$

Aufgrund der beiden genannten Eigenschaften der Abbildung c_B nennt man sie linear oder Vektorraumhomomorphismus. Wir definieren diese Begriffe nun in voller Allgemeinheit.

Definition 3.3.2 (Lineare Abbildungen, Vektorraumhomomorphismen)**.** Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine Abbildung. Dann heißt φ *linear* oder *Vektorraumhomomorphismus*, falls

$$\varphi(\mathbf{v} + \mathbf{v}') \;=\; \varphi(\mathbf{v}) + \varphi(\mathbf{v}') \qquad \text{für alle } \mathbf{v}, \mathbf{v}' \in V$$

und

$$\varphi(s \cdot \mathbf{v}) \;=\; s \cdot \varphi(\mathbf{v}) \qquad \text{für alle } s \in K \text{ und } \mathbf{v} \in V.$$

Ein Vektorraumhomomorphismus ist also eine Abbildung zwischen zwei K-Vektorräumen, die mit der Vektoraddition und mit der skalaren Multiplikation verträglich ist. Damit haben wir also die in Kapitel 2 Abschnitt 2.2.4 eingeführte Definition von Gruppen- und Ringhomomorphismen in analoger Weise auf K-Vektorräume ausgedehnt.

Bemerkung. Sind V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung, so ist $\varphi(\mathbf{0}) = \mathbf{0}$. Denn:

$$\varphi(\mathbf{0}) \;=\; \varphi(0 \cdot \mathbf{0}) \;=\; 0 \cdot \varphi(\mathbf{0}) \;=\; \mathbf{0} \;.$$

(Diese Tatsache folgt auch schon daraus, dass eine lineare Abbildung $\varphi : V \to W$ nach Definition ein Gruppenhomomorphismus von der Gruppe $(V, +)$ in die Gruppe $(W, +)$ ist.)

Im Folgenden geben wir eine kompaktere Charakterisierung linearer Abbildungen an, indem wir die beiden in Definition 3.3.2 geforderten Eigenschaften zu einer Eigenschaft zusammenfassen. (Dazu vergleiche man auch Definition 3.2.3 für Teilräume und die entsprechende Charakterisierung in Lemma 3.2.4).

Korollar 3.3.3 (Charakterisierung linearer Abbildungen)**.** *Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine Abbildung. Die Abbildung φ ist genau dann linear, wenn*

$$\varphi(s \cdot \mathbf{v} + \mathbf{v}') \;=\; s \cdot \varphi(\mathbf{v}) + \varphi(\mathbf{v}') \qquad \textit{für alle } s \in K \textit{ und } \mathbf{v}, \mathbf{v}' \in V.$$

Den Beweis diese Korollars führt man analog zu dem Beweis des oben erwähnten Lemmas 3.2.4.

Beispiele.

(i) Sind V und W zwei K-Vektorräume, dann ist die Abbildung $\varphi : V \to W$ mit $\varphi(\mathbf{v}) := \mathbf{0}$ für alle $\mathbf{v} \in V$ linear, also ein Vektorraumhomomorphismus.

(ii) Es sei V der $\mathbb{R}$-Vektorraum aller differenzierbarer Funktionen von $\mathbb{R}$ nach $\mathbb{R}$, also

$$V \;:=\; \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ ist differenzierbar}\} \;,$$

und f' bezeichne die Ableitung der Funktion $f \in V$. Dann ist die durch $f \mapsto f'$ definierte Abbildung von V nach $\mathbb{R}^{\mathbb{R}}$ linear. Dies folgt sofort aus den bekannten Ableitungsregeln für Funktionen.

(iii) Es sei V ein K-Vektorraum und $c \in K$ ein Skalar. Dann ist die Abbildung

$$\begin{aligned} \varphi_c \;:\; & V \to V \\ & \mathbf{v} \mapsto c \cdot \mathbf{v} \end{aligned}$$

linear. Denn

$$\varphi_c(s \cdot \mathbf{v} + \mathbf{v}') \;=\; c \cdot (s \cdot \mathbf{v} + \mathbf{v}') \;=\; s \cdot (c \cdot \mathbf{v}) + c \cdot \mathbf{v}' \;=\; s \cdot \varphi_c(\mathbf{v}) + \varphi_c(\mathbf{v}')$$

für alle $s \in K$ und $\mathbf{v}, \mathbf{v}' \in V$.

(iv) Es sei $V = W = K$ und $\varphi : V \to W$ linear. Setzen wir $c := \varphi(1) \in K$, so ist

$$\varphi(x) \;=\; \varphi(x \cdot 1) \;=\; x \cdot \varphi(1) \;=\; x \cdot c \qquad \text{für alle } x \in K.$$

Folglich ist $\varphi = \varphi_c$ (siehe letztes Beispiel) und insbesondere ist die lineare Abbildung φ durch Angabe von $\varphi(1)$ eindeutig bestimmt.

Lemma 3.3.4. *Es seien U, V und W drei K-Vektorräume. Sind $\varphi : U \to V$ und $\psi : V \to W$ lineare Abbildungen, so ist die Hintereinanderausführung*

$$\begin{aligned} \psi \circ \varphi \;:\; & U \to W \\ & \mathbf{v} \mapsto \psi(\varphi(\mathbf{v})) \end{aligned}$$

ebenfalls eine lineare Abbildung.

Beweis. Für $s \in K$ und $\mathbf{v}, \mathbf{v}' \in U$ gilt

$$\begin{aligned} (\psi \circ \varphi)(s \cdot \mathbf{v} + \mathbf{v}') \;&=\; \psi(\varphi(s \cdot \mathbf{v} + \mathbf{v}')) \\ &=\; \psi(s \cdot \varphi(\mathbf{v}) + \varphi(\mathbf{v}')) \\ &=\; s \cdot \psi(\varphi(\mathbf{v})) + \psi(\varphi(\mathbf{v}')) \\ &=\; s \cdot (\psi \circ \varphi)(\mathbf{v}) + (\psi \circ \varphi)(\mathbf{v}') \;. \end{aligned}$$

Die Behauptung folgt also aus Korollar 3.3.3. □

Der folgende Satz liefert eine Erklärung für die in Beispiel (iv) gemachte Beobachtung in einem allgemeinen Kontext.

Satz 3.3.5. *Es seien V und W zwei K-Vektorräume, $(\mathbf{v}_1, \ldots, \mathbf{v}_n) \in V^n$ eine Basisfolge von V und $(\mathbf{w}_1, \ldots, \mathbf{w}_n) \in W^n$. Dann gibt es genau eine lineare Abbildung $\varphi : V \to W$ mit*

$$\varphi(\mathbf{v}_i) \;=\; \mathbf{w}_i \qquad\qquad \text{für } i = 1, \ldots, n. \tag{3.12}$$

Der Satz besagt also, dass eine lineare Abbildung durch Angabe der Bildwerte auf einer Basis des Ursprungsvektorraums V eindeutig bestimmt ist.

Beweis. Wir zeigen zunächst, dass es höchstens eine lineare Abbildung mit der geforderten Eigenschaft (3.12) gibt. Denn zu $\mathbf{v} \in V$ gibt es eindeutig bestimmte Zahlen $s_1, \ldots, s_n \in K$ mit

$$\mathbf{v} \;=\; s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n \;\; .$$

Aus (3.12) folgt dann

$$\begin{aligned} \varphi(\mathbf{v}) \;&=\; \varphi(s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n) \\ &=\; s_1 \cdot \varphi(\mathbf{v}_1) + \cdots + s_n \cdot \varphi(\mathbf{v}_n) \\ &=\; s_1 \cdot \mathbf{w}_1 + \cdots + s_n \cdot \mathbf{w}_n \;\; , \end{aligned}$$

so dass φ durch (3.12) also eindeutig bestimmt ist.

Es bleibt zu zeigen, dass eine lineare Abbildung φ mit der geforderten Eigenschaft (3.12) existiert. Dazu definieren wir für $\mathbf{v} \in V$ den Vektor $\varphi(\mathbf{v}) \in W$ wie folgt. Schreibe $\mathbf{v} = s_1 \cdot \mathbf{v}_1 + \cdots + s_n \cdot \mathbf{v}_n$ mit eindeutig bestimmten Skalaren $s_1, \ldots, s_n \in K$ und setze

$$\varphi(\mathbf{v}) \;:=\; s_1 \cdot \mathbf{w}_1 + \cdots + s_n \cdot \mathbf{w}_n \;\; .$$

Dann gilt also insbesondere (3.12). Wir müssen noch zeigen, dass die dadurch definierte Abbildung $\varphi : V \to W$ linear ist. Für $\mathbf{v}' \in V$ mit $\mathbf{v}' = s'_1 \cdot \mathbf{v}_1 + \cdots + s'_n \cdot \mathbf{v}_n$ und $t \in K$ gilt nach Definition

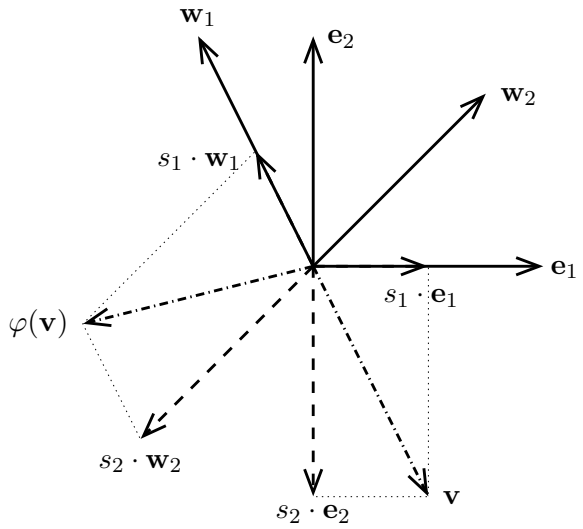
$$\begin{aligned} \varphi(t \cdot \mathbf{v} + \mathbf{v}') \;&=\; \varphi\big((t \cdot s_1 + s'_1) \cdot \mathbf{v}_1 + \cdots + (t \cdot s_n + s'_n) \cdot \mathbf{v}_n\big) \\ &=\; (t \cdot s_1 + s'_1) \cdot \mathbf{w}_1 + \cdots + (t \cdot s_n + s'_n) \cdot \mathbf{w}_n \\ &=\; t \cdot (s_1 \cdot \mathbf{w}_1 + \cdots + s_n \cdot \mathbf{w}_n) + (s'_1 \cdot \mathbf{w}_1 + \cdots + s'_n \cdot \mathbf{w}_n) \\ &=\; t \cdot \varphi(\mathbf{v}) + \varphi(\mathbf{v}') \;\; . \end{aligned}$$

Folglich ist φ linear und der Beweis abgeschlossen. □

Bemerkung. Satz 3.3.5 gilt auch für den Fall unendlicher Basen, d.h. falls eine Basisfolge $(v_i)_{i \in I}$ des Vektorraums V mit einer beliebigen Indexmenge I und Vektoren $(\mathbf{w}_i)_{i \in I}$ in W gegeben sind.

Beispiel. Wir betrachten den $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ mit der Basisfolge $(\mathbf{e}_1, \mathbf{e}_2)$. Eine lineare Abbildung $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ ist dann eindeutig durch die Bilder $\mathbf{w}_1 := \varphi(\mathbf{e}_1)$ und $\mathbf{w}_2 := \varphi(\mathbf{e}_2)$ gegeben. Für einen beliebigen Vektor $\mathbf{v} = \binom{s_1}{s_2} \in \mathbb{R}^2$ gilt dann

$$\varphi(\mathbf{v}) \;=\; s_1 \cdot \mathbf{w}_1 + s_2 \cdot \mathbf{w}_2 \;\; .$$



Das folgende Korollar beleuchtet den engen Zusammenhang zwischen linearen Abbildungen und Matrizen.

Korollar 3.3.6. *Jede lineare Abbildung $\varphi : K^n \to K^m$ ist von der Form $\varphi = \varphi_A$ für eine Matrix $A \in K^{m \times n}$, wobei*

$$\begin{aligned} \varphi_A \;:\; K^n &\to K^m \;\; , \\ \mathbf{x} &\mapsto A \cdot \mathbf{x} \;\; . \end{aligned}$$

Umgekehrt ist jede solche Abbildung φ_A mit $A \in K^{m \times n}$ linear.

Beweis. Für $A \in K^{m \times n}$ ist die Abbildung φ_A mit $A \in K^{m \times n}$ linear, da

$$A \cdot (s \cdot \mathbf{x} + \mathbf{x}') \;=\; s \cdot (A \cdot \mathbf{x}) + A \cdot \mathbf{x}'$$

für alle $s \in K$ und $\mathbf{x}, \mathbf{x}' \in K^n$.

Es sei $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ die Standardbasisfolge des Vektorraums K^n. Für eine lineare Abbildung $\varphi : K^n \to K^m$ setzen wir

$$\varphi(\mathbf{e}_i) \;=:\; \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix} \;\in\; K^m \qquad\qquad \text{für } i = 1, \ldots, n$$

und

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in K^{m\times n} .$$

Dann gilt

$$\varphi_A(\mathbf{e}_i) = A \cdot \mathbf{e}_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix} = \varphi(\mathbf{e}_i) \qquad \text{für } i = 1, \ldots, n.$$

Damit stimmen also die beiden linearen Abbildungen φ und φ_A auf der Basisfolge $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ überein. Aus Satz 3.3.5 folgt daher $\varphi = \varphi_A$. □

3.3.2 Isomorphismen

In Kapitel 2 Definition 2.2.17 haben wir bereits die Begriffe *Monomorphismus*, *Epimorphismus* und *Isomorphismus* im Zusammenhang mit Gruppen- und Ringhomomorphismen eingeführt. Wir verallgemeinern diese Definition im Folgenden für Vektorraumhomomorphismen.

Definition 3.3.7 (Monomorphismus, Epimorphismus, Isomorphismus)**.**

(i) Ein injektiver Vektorraumhomomorphismus heißt *(Vektorraum-) Monomorphismus.*

(ii) Ein surjektiver Vektorraumhomomorphismus heißt *(Vektorraum-) Epimorphismus.*

(iii) Ein bijektiver Vektorraumhomomorphismus heißt *(Vektorraum-) Isomorphismus.*

Definition 3.3.8 (Isomorphie)**.** Zwei K-Vektorräume V und W heißen *isomorph* (in Zeichen $V \cong W$), falls es einen Vektorraumisomorphismus $\varphi : V \to W$ gibt.

Satz 3.3.9 (Eigenschaften von Isomorphismen)**.** *Es seien U, V und W drei K-Vektorräume.*

(i) Ist $\varphi : U \to V$ ein Isomorphismus, so ist auch die Umkehrabbildung $\varphi^{-1} : V \to U$ ein Isomorphismus.

(ii) Sind $\varphi : U \to V$ und $\psi : V \to W$ Isomorphismen, so ist auch die Hintereinanderausführung $\psi \circ \varphi : U \to W$ ein Isomorphismus.

(iii) Die Isomorphie „$\cong$“ ist eine Äquivalenzrelation auf der Menge der K-Vektorräume.

Beweis. Um (i) zu beweisen, genügt es zu zeigen, dass $\varphi^{-1} : V \to U$ eine lineare Abbildung ist. Es seien $s \in K$ und $\mathbf{v}, \mathbf{v}' \in V$. Da φ bijektiv ist, gibt es eindeutige Vektoren $\mathbf{u}, \mathbf{u}' \in U$ mit $\varphi(\mathbf{u}) = \mathbf{v}$ und $\varphi(\mathbf{u}') = \mathbf{v}'$. Da φ linear ist, gilt $\varphi(s \cdot \mathbf{u} + \mathbf{u}') = s \cdot \mathbf{v} + \mathbf{v}'$. Damit erhält man

$$\varphi^{-1}(s \cdot \mathbf{v} + \mathbf{v}') \;=\; s \cdot \mathbf{u} + \mathbf{u}' \;=\; s \cdot \varphi^{-1}(\mathbf{v}) + \varphi^{-1}(\mathbf{v}') \;.$$

Aussage (ii) ist klar, da die Abbildung $\psi \circ \varphi$ wegen Lemma 1.3.8 c) aus Kapitel 1 bijektiv und wegen Lemma 3.3.4 linear ist.

Um Aussage (iii) zu beweisen, muss man zeigen, dass die Relation reflexiv, symmetrisch und transitiv ist. Die Reflexivität ist klar, da für einen K-Vektorraum V die identische Abbildung $\mathrm{id}_V : V \to V$ ein Isomorphismus ist. Die Symmetrie folgt aus (i) und die Transitivität aus (ii). □

Satz 3.3.10. *Je zwei endlich dimensionale K-Vektorräume derselben Dimension n sind isomorph.*

Beweis. Es sei V ein beliebiger K-Vektorraum der endlichen Dimension n. Dann hat V eine Basisfolge $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ und die Abbildung $c_B : V \to K^n$ ist ein Homomorphismus. Da jeder Vektor $\mathbf{v} \in V$ eine eindeutige Darstellung $\mathbf{v} = \sum_{i=1}^{n} s_i \cdot \mathbf{v}_i$ mit $s_1, \ldots, s_n \in K$ besitzt, ist c_B injektiv. Da für alle $s_1, \ldots, s_n \in K$ der Vektor $\sum_{i=1}^{n} s_i \cdot \mathbf{v}_i$ in V liegt, ist c_B surjektiv.

Wir haben also gezeigt, dass jeder n-dimensionale K-Vektorraum isomorph zu K^n ist. Die Behauptung folgt also aus Satz 3.3.9 (iii). □

3.3.3 Kern und Bild

Analog zu den entsprechenden Definitionen für Gruppenhomomorphismen in Kapitel 2 Abschnitt 2.2.4 definieren wir Kern und Bild einer linearen Abbildung zwischen K-Vektorräumen.

Definition 3.3.11 (Kern und Bild einer linearen Abbildung)**.** Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Dann ist

$$\mathrm{Kern}(\varphi) \;:=\; \{\mathbf{v} \in V \mid \varphi(\mathbf{v}) = \mathbf{0}\} \;\subseteq\; V$$

und

$$\mathrm{Bild}(\varphi) \;:=\; \{\varphi(\mathbf{v}) \mid \mathbf{v} \in V\} \;=\; \varphi(V) \;\subseteq\; W \;.$$

Beispiel. Wir betrachten den $\mathbb{R}$-Vektorraum $V = W = \mathbb{R}^2$ und die lineare Abbildung $\varphi : V \to W$ mit

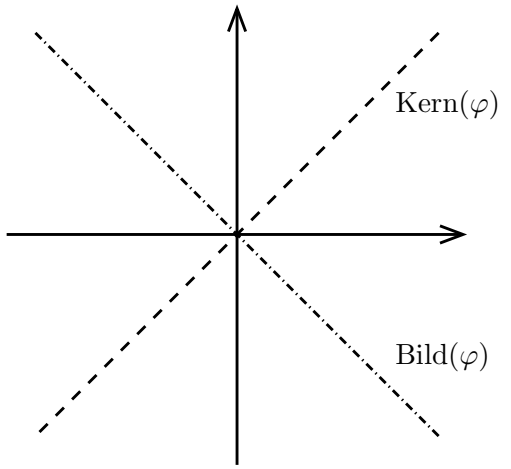
$$\varphi\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) \;:=\; \begin{pmatrix} x - y \\ y - x \end{pmatrix} \;=\; \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \;.$$

Dann ist

$$\text{Kern}(\varphi) \;=\; \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x - y = 0 \;\wedge\; y - x = 0 \right\} \;=\; \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$$

und

$$\text{Bild}(\varphi) \;=\; \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; b = -a \right\} \;=\; \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle \;.$$



Satz 3.3.12. *Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Dann gilt:*

(i) $\text{Kern}(\varphi)$ *ist Teilraum von V und*

$$\text{Kern}(\varphi) = \{\mathbf{0}\} \quad \Longleftrightarrow \quad \varphi \textit{ injektiv (Monomorphismus).}$$

(ii) $\text{Bild}(\varphi)$ *ist Teilraum von W und*

$$\text{Bild}(\varphi) = W \quad \Longleftrightarrow \quad \varphi \textit{ surjektiv (Epimorphismus).}$$

Ist $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, so ist $\text{Bild}(\varphi) = \langle \varphi(\mathbf{v}_1), \ldots, \varphi(\mathbf{v}_n) \rangle$.

(iii) Ist V endlich dimensional, so ist

$$\dim V \;=\; \dim \text{Kern}(\varphi) + \dim \text{Bild}(\varphi) \;.$$

Beweis. Zu (i): Da $\varphi(\mathbf{0}) = \mathbf{0}$ ist $\mathbf{0} \in \text{Kern}(\varphi)$. Es seien $s \in K$ und $\mathbf{v}, \mathbf{w} \in \text{Kern}(\varphi)$. Dann gilt

$$\varphi(s \cdot \mathbf{v} + \mathbf{w}) \;=\; s \cdot \varphi(\mathbf{v}) + \varphi(\mathbf{w}) \;=\; s \cdot \mathbf{0} + \mathbf{0} \;=\; \mathbf{0}$$

und damit $s \cdot \mathbf{v} + \mathbf{w} \in \text{Kern}(\varphi)$. Wegen Lemma 3.2.4 ist $\text{Kern}(\varphi)$ also ein Teilraum von V.

Ist φ injektiv, so kann außer dem Nullvektor in V kein weiteres Element auf den Nullvektor in W abgebildet werden. Daher ist $\text{Kern}(\varphi) = \{\mathbf{0}\}$.

Ist umgekehrt $\text{Kern}(\varphi) = \{\mathbf{0}\}$ und $\mathbf{v}, \mathbf{w} \in V$ mit $\varphi(\mathbf{v}) = \varphi(\mathbf{w})$, so ist

$$\varphi(\mathbf{v} - \mathbf{w}) \;=\; \varphi(\mathbf{v}) - \varphi(\mathbf{w}) \;=\; \mathbf{0}$$

und folglich $\mathbf{v} - \mathbf{w} \in \text{Kern}(\varphi) = \{\mathbf{0}\}$, also $\mathbf{v} = \mathbf{w}$.

Zu (ii): Da $\varphi(\mathbf{0}) = \mathbf{0}$ ist $\mathbf{0} \in \text{Bild}(\varphi)$. Es seien $s \in K$ und $\mathbf{v}, \mathbf{w} \in \text{Bild}(\varphi)$, also $\mathbf{v} = \varphi(\mathbf{v}')$ und $\mathbf{w} = \varphi(\mathbf{w}')$ für $\mathbf{v}', \mathbf{w}' \in V$. Dann ist

$$s \cdot \mathbf{v} + \mathbf{w} \;=\; s \cdot \varphi(\mathbf{v}') + \varphi(\mathbf{w}') \;=\; \varphi(s \cdot \mathbf{v}' + \mathbf{w}') \;\in\; \text{Bild}(\varphi) \;.$$

Wegen Lemma 3.2.4 ist $\text{Bild}(\varphi)$ also ein Teilraum von W. Die in (ii) behauptete Äquivalenz ist klar.

Ist $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, so ist $V = \{\sum_{i=1}^n s_i \cdot \mathbf{v}_i \mid s_1, \ldots, s_n \in K\}$. Folglich erhält man

$$\begin{aligned}
\text{Bild}(\varphi) \;&=\; \{\varphi(\mathbf{v}) \mid \mathbf{v} \in V\} \\
&=\; \left\{ \varphi\left(\sum_{i=1}^n s_i \cdot \mathbf{v}_i \right) \;\middle|\; s_1, \ldots, s_n \in K \right\} \\
&=\; \left\{ \sum_{i=1}^n s_i \cdot \varphi(\mathbf{v}_i) \;\middle|\; s_1, \ldots, s_n \in K \right\} \\
&=\; \big\langle \varphi(\mathbf{v}_1), \ldots, \varphi(\mathbf{v}_n) \big\rangle \;.
\end{aligned}$$

Zu (iii): Ist $\dim V = n$, so folgt aus Korollar 3.2.23 $\dim \text{Kern}(\varphi) =: d \leq n$, da $\text{Kern}(\varphi)$ ein Teilraum von V ist. Wir betrachten eine Basisfolge $(\mathbf{v}_1, \ldots, \mathbf{v}_d)$ von $\text{Kern}(\varphi)$ und ergänzen sie zu einer Basisfolge $(\mathbf{v}_1, \ldots, \mathbf{v}_d, \mathbf{v}_{d+1}, \ldots, \mathbf{v}_n)$ von V. Es genügt zu zeigen, dass $B := \big(\varphi(\mathbf{v}_{d+1}), \ldots, \varphi(\mathbf{v}_n)\big)$ eine Basisfolge von $\text{Bild}(\varphi)$ ist.

Zunächst überzeugt man sich leicht davon, dass B ein (geordnetes) Erzeugendensystem von $\text{Bild}(\varphi)$ ist, da nach (ii)

$$\begin{aligned}
\text{Bild}(\varphi) \;&=\; \big\langle \varphi(\mathbf{v}_1), \ldots, \varphi(\mathbf{v}_n) \big\rangle \\
&=\; \big\langle \mathbf{0}, \ldots, \mathbf{0}, \varphi(\mathbf{v}_{d+1}), \ldots, \varphi(\mathbf{v}_n) \big\rangle \\
&=\; \big\langle \varphi(\mathbf{v}_{d+1}), \ldots, \varphi(\mathbf{v}_n) \big\rangle \;.
\end{aligned}$$

Es bleibt zu zeigen, dass die Vektoren in B paarweise verschieden und linear unabhängig sind. Dazu betrachten wir $s_{d+1}, \ldots, s_n \in K$ mit

$$\mathbf{0} \;=\; \sum_{i=d+1}^n s_i \cdot \varphi(\mathbf{v}_i) \;=\; \varphi\left(\sum_{i=d+1}^n s_i \cdot \mathbf{v}_i \right) \;.$$

Dann ist $\sum_{i=d+1}^{n} s_i \cdot \mathbf{v}_i \in \operatorname{Kern} \varphi = \langle \mathbf{v}_1, \ldots, \mathbf{v}_d \rangle$, also

$$\sum_{i=d+1}^{n} s_i \cdot \mathbf{v}_i \;=\; \sum_{j=1}^{d} t_j \cdot \mathbf{v}_j$$

mit $t_1, \ldots, t_d \in K$. Setzt man $s_j := -t_j$ für $j = 1, \ldots, d$, so erhält man

$$\sum_{i=1}^{n} s_i \cdot \mathbf{v}_i \;=\; \mathbf{0} \;.$$

Da jedoch $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$ eine Basisfolge von V und damit linear unabhängig ist, folgt daraus $s_{d+1} = \cdots = s_n = 0$ (und auch $s_1 = \cdots = s_d = 0$). Damit ist der Beweis fertig. □

Definition 3.3.13. Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Der *Rang* von φ ist die Dimension von $\operatorname{Bild}(\varphi)$, also

$$\operatorname{Rang}(\varphi) \;:=\; \dim \operatorname{Bild}(\varphi) \;.$$

Korollar 3.3.14. *Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Ist V endlich dimensional, so gilt:*

(i) φ *surjektiv* $\iff \operatorname{Rang}(\varphi) = \dim W$*;*

(ii) φ *injektiv* $\iff \operatorname{Rang}(\varphi) = \dim V$*;*

(iii) Ist $\dim V = \dim W$*, so gilt:* φ *surjektiv* $\iff$ φ *injektiv.*

Man vergleiche den letzten Teil des Korollars mit der bekannten Tatsache, dass eine Abbildung zwischen zwei gleichmächtigen endlichen Mengen genau dann surjektiv ist, wenn sie injektiv ist.

Beweis. Zu (i): Es gilt

$$\begin{aligned} \varphi \text{ surjektiv} \quad &\iff \quad \operatorname{Bild}(\varphi) = W \\ &\iff \quad \operatorname{Rang} \varphi = \dim \operatorname{Bild}(\varphi) = \dim W \;. \end{aligned}$$

Zu (ii): Es gilt

$$\begin{aligned} \varphi \text{ injektiv} \quad &\iff \quad \operatorname{Kern}(\varphi) = \{\mathbf{0}\} \\ &\iff \quad \dim \operatorname{Kern}(\varphi) = 0 \\ &\iff \quad \dim V = \operatorname{Rang} \varphi \;. \end{aligned}$$

Behauptung (iii) folgt aus (i) und (ii). □

Das folgende Beispiel zeigt, dass Korollar 3.3.14 (iii) ohne die Voraussetzung, dass V endlich dimensional ist, nicht wahr ist.

Beispiel. Es sei $\mathcal{P}(\mathbb{R})$ der $\mathbb{R}$-Vektorraum der reellen Polynomfunktionen, d.h.

$$\mathcal{P}(\mathbb{R}) \;:=\; \left\{ f : \mathbb{R} \to \mathbb{R} \;\middle|\; \exists a_0, \ldots, a_n \in \mathbb{R} :\; f(x) = \sum_{i=0}^{n} a_i x^i \right\} \;.$$

Es sei $\varphi : \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R})$ die lineare Abbildung, die eine Funktion auf ihre Ableitung abbildet, also $\varphi(f) = f'$. Dann ist

$$\mathrm{Kern}(\varphi) \;=\; \{ f \mid \exists c \in \mathbb{R} :\; f(x) = c \;\forall x \in \mathbb{R} \} \;.$$

Folglich ist φ nicht injektiv. Andererseits ist φ jedoch surjektiv, da jede Polynomfunktion $f(x) = \sum_{i=0}^{n} a_i x^i$ eine Stammfunktion

$$F(x) \;:=\; \sum_{i=0}^{n} \frac{a_i}{i+1} x^{i+1}$$

besitzt, für die $F' = f$ gilt. Damit ist also $\varphi(F) = f$ und φ ist surjektiv.

Umgekehrt kann man leicht Beispiele linearer Abbildungen $\varphi : V \to V$ konstruieren, so dass φ injektiv jedoch nicht surjektiv ist. Wir überlassen das dem Leser als Übung.

Beispiel. Es sei A eine $m \times n$ Matrix über dem Körper K, also $A \in K^{m \times n}$ und

$$\begin{aligned} \varphi_A \;:\; K^n &\to K^m \;, \\ \mathbf{x} &\mapsto A \cdot \mathbf{x} \;. \end{aligned}$$

Dann ist $\mathrm{Kern}(\varphi_A) = \{ \mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{0} \}$ die Lösungsmenge des durch die Matrix A gegebenen homogenen linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{0}$. Wie wir wissen ist dies ein Teilraum des K-Vektorraums K^n. Es gilt

$$\dim \mathrm{Kern}(\varphi_A) \;=\; n - \mathrm{Rang}(\varphi_A) \;.$$

Für $\mathbf{b} \in K^m$ ist die Lösungsmenge $\{ \mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{b} \}$ des (inhomogenen) linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{b}$ das Urbild des Vektors $\mathbf{b}$ unter der Abbildung φ_A, also

$$\{ \mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{b} \} \;=\; {\varphi_A}^{-1}(\mathbf{b}) \;.$$

3.3.4 Homomorphiesatz

Aus dem letzten Abschnitt wissen wir, dass der Kern einer linearen Abbildung von einem K-Vektorraum V in einen K-Vektorraum W, also das Urbild des Nullvektors aus W, ein Teilraum von V ist. Wie können wir uns das Urbild eines beliebigen Vektors $\mathbf{b} \in W$ mit $\mathbf{b} \neq \mathbf{0}$ vorstellen? Und es stellt sich eine weitere Frage: Ist jeder Teilraum U von V der Kern einer linearen Abbildung von V in einen K-Vektorraum W? In diesem Abschnitt beschäftigen wir uns unter anderem mit diesen beiden Fragen. Wir beginnen mit einem Beispiel.

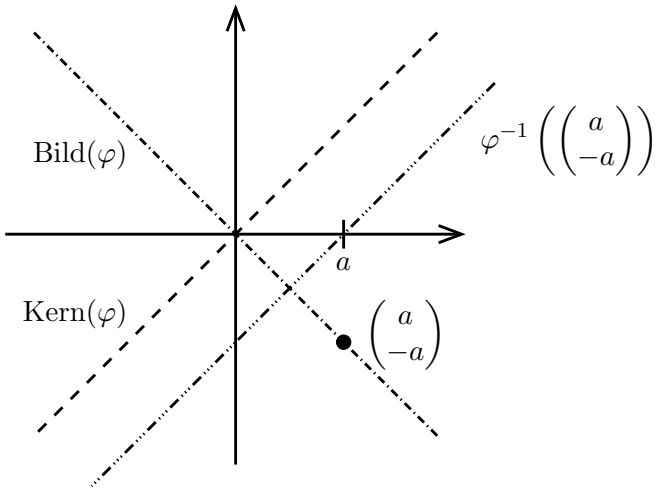


Abbildung 3.1: Die Urbildmenge eines Vektors unter einer linearen Abbildung.

Beispiel. Es sei $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ definiert durch

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x-y \\ y-x \end{pmatrix}$$

Dann ist

$$\text{Bild}(\varphi) \;=\; \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle \qquad \text{und} \qquad \text{Kern}(\varphi) \;=\; \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle \;.$$

Für einen beliebigen Vektor $\left(\begin{smallmatrix} a \\ -a \end{smallmatrix}\right) \in \text{Bild}(\varphi)$ erhält man als Urbildmenge

$$\varphi^{-1}\left(\begin{pmatrix} a \\ -a \end{pmatrix}\right) \;=\; \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \;\middle|\; y = x - a \right\} \;=\; \begin{pmatrix} a \\ 0 \end{pmatrix} + \text{Kern}(\varphi) \;.$$

Siehe auch Abbildung 3.1.

Definition 3.3.15. Ist U ein Teilraum des K-Vektorraums V und $\mathbf{v}_0 \in V$, dann sei

$$\mathbf{v}_0 + U \;:=\; \{\mathbf{v}_0 + \mathbf{u} \mid \mathbf{u} \in U\} \;.$$

Man nennt $\mathbf{v}_0 + U$ auch die *Nebenklasse* oder *Restklasse* von $\mathbf{v}_0$ nach U.

Wir können jetzt die Urbildmengen unter linearen Abbildungen durch Nebenklassen charakterisieren.

Satz 3.3.16. *Es seien V und W zwei K-Vektorräume, $\varphi : V \to W$ eine lineare Abbildung und $U := \text{Kern}(\varphi)$. Weiter seien $\mathbf{v}_0 \in V$ und $\mathbf{w} \in W$ mit $\varphi(\mathbf{v}_0) = \mathbf{w}$. Dann ist $\varphi^{-1}(\mathbf{w}) = \mathbf{v}_0 + U$.*

Beweis. Da $\varphi(\mathbf{v}_0) = \mathbf{w}$, gilt

$$\begin{aligned}
\varphi(\mathbf{v}) \;=\; \mathbf{w} \quad &\Longleftrightarrow \quad \varphi(\mathbf{v}) \;=\; \varphi(\mathbf{v}_0) \\
&\Longleftrightarrow \quad \varphi(\mathbf{v}) - \varphi(\mathbf{v}_0) \;=\; \mathbf{0} \\
&\Longleftrightarrow \quad \varphi(\mathbf{v} - \mathbf{v}_0) \;=\; \mathbf{0} \\
&\Longleftrightarrow \quad \mathbf{v} - \mathbf{v}_0 \;\in\; \mathrm{Kern}(\varphi) \\
&\Longleftrightarrow \quad \mathbf{v} \;\in\; \mathbf{v}_0 + \mathrm{Kern}(\varphi) \;\; .
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Lemma 3.3.17. *Die Menge der Nebenklassen eines Teilraums U des K-Vektorraums V bilden eine Partition der Menge V.*

Beweis. Man überzeugt sich leicht davon, dass die durch

$$\mathbf{v} \sim \mathbf{w} \quad :\Longleftrightarrow \quad \mathbf{v} - \mathbf{w} \in U$$

gegebene binäre Relation auf V reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation ist. Die Äquivalenzklasse von $\mathbf{v}$ ist die Nebenklasse $\mathbf{v} + U$. Nach Satz 1.5.5 bilden die Nebenklassen also eine Partition von V. □

Satz 3.3.18 (Restklassenraum, Faktorraum, Quotientenraum)**.** *Es sei V ein K-Vektorraum und U ein Teilraum von V. Weiter sei*

$$V/U \;:=\; \{\mathbf{v} + U \mid \mathbf{v} \in V\}$$

die Menge der Nebenklassen nach U. Definiert man für $\mathbf{v}, \mathbf{w} \in V$ und $s \in K$

$$(\mathbf{v} + U) + (\mathbf{w} + U) \;:=\; (\mathbf{v} + \mathbf{w}) + U$$

und

$$s \cdot (\mathbf{v} + U) \;:=\; (s \cdot \mathbf{v}) + U \;\; ,$$

so wird V/U ein K-Vektorraum, der Restklassenraum, Quotientenraum *oder* Faktorraum von V nach U. *Außerdem ist die Abbildung $\pi : V \to V/U$ mit $\pi(\mathbf{v}) := \mathbf{v} + U$ ein Epimorphismus mit* $\mathrm{Kern}(\pi) = U$.

Beweis. Wir müssen zunächst zeigen, dass die durch

$$(\mathbf{v} + U) + (\mathbf{w} + U) \;:=\; (\mathbf{v} + \mathbf{w}) + U$$

und

$$s \cdot (\mathbf{v} + U) \;:=\; (s \cdot \mathbf{v}) + U$$

definierten Abbildungen wohldefiniert sind. Es seien $\mathbf{v}, \mathbf{v}', \mathbf{w}, \mathbf{w}' \in V$ mit $\mathbf{v}+U = \mathbf{v}'+U$ und $\mathbf{w}+U = \mathbf{w}'+U$. Wir müssen zeigen, dass dann

$$(\mathbf{v}+\mathbf{w})+U \;=\; (\mathbf{v}'+\mathbf{w}')+U \qquad \text{und} \qquad (s\cdot\mathbf{v})+U \;=\; (s\cdot\mathbf{v}')+U$$

für alle $s \in K$ gilt. Nach Voraussetzung gilt $\mathbf{v}'-\mathbf{v} \in U$ und $\mathbf{w}'-\mathbf{w} \in U$ (siehe auch Lemma 3.3.17). Folglich ist

$$(\mathbf{v}'+\mathbf{w}')-(\mathbf{v}+\mathbf{w}) \;=\; (\mathbf{v}'-\mathbf{v})+(\mathbf{w}'-\mathbf{w}) \;\in\; U$$

und damit $(\mathbf{v}+\mathbf{w})+U = (\mathbf{v}'+\mathbf{w}')+U$. Weiterhin ist

$$s\cdot\mathbf{v}'-s\cdot\mathbf{v} \;=\; s\cdot(\mathbf{v}'-\mathbf{v}) \;\in\; U$$

und damit $(s\cdot\mathbf{v})+U = (s\cdot\mathbf{v}')+U$.

Es bleibt also zu zeigen, dass V/U mit der so definierten Addition und Skalarmultiplikation ein Vektorraum ist. Dazu müssen die Vektorraumaxiome aus Definition 3.2.1 erfüllt sein. Dies rechnet man leicht nach. Beispielsweise ist der Nullvektor in V/U gegeben durch $\mathbf{0}+U$. Wir lassen den Beweis der restlichen Vektorraumeigenschaften als Übung.

Es bleibt zu zeigen, dass π die behaupteten Eigenschaften besitzt. Zunächst einmal ist π linear, da für $\mathbf{v}, \mathbf{v}' \in V$ und $s \in K$ gilt:

$$\begin{aligned}\pi(s\cdot\mathbf{v}+\mathbf{v}') &= (s\cdot\mathbf{v}+\mathbf{v}')+U\\ &= s\cdot(\mathbf{v}+U)+(\mathbf{v}'+U)\\ &= s\cdot\pi(\mathbf{v})+\pi(\mathbf{v}')\ .\end{aligned}$$

Offensichtlich ist π surjektiv und es gilt $\pi(\mathbf{v}) = \mathbf{v}+U = \mathbf{0}+U$ genau dann, wenn $\mathbf{v} \in U$. Folglich ist $\operatorname{Kern}(\pi) = U$. □

Der folgende Satz stellt das Hauptresultat dieses Abschnitts dar.

Satz 3.3.19 (Homomorphiesatz für Vektorräume)**.** *Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Dann ist die Abbildung $\Phi : V/\operatorname{Kern}(\varphi) \to \operatorname{Bild}(\varphi)$ mit*

$$\Phi\big(\mathbf{v}+\operatorname{Kern}(\varphi)\big) \;:=\; \varphi(\mathbf{v})$$

ein Isomorphismus.

Beweis. Die Abbildung ist wohldefiniert, da für $\mathbf{v}, \mathbf{v}' \in V$

$$\begin{aligned}\mathbf{v}+\operatorname{Kern}(\varphi) \;=\; \mathbf{v}'+\operatorname{Kern}(\varphi) \quad &\Longleftrightarrow \quad \mathbf{v}-\mathbf{v}' \in \operatorname{Kern}(\varphi)\\ &\Longleftrightarrow \quad \varphi(\mathbf{v}-\mathbf{v}') \;=\; \mathbf{0}\\ &\Longleftrightarrow \quad \varphi(\mathbf{v}) \;=\; \varphi(\mathbf{v}')\ .\end{aligned}$$

Daraus folgt auch sofort, dass Φ injektiv und surjektiv, also bijektiv ist. Die Linearität der Abbildung folgt auch direkt aus der Definition. □

3.3.5 Rang einer Matrix

Nachdem wir im letzten Abschnitt den Rang einer linearen Abbildung definiert haben, beschäftigen wir uns jetzt mit dem Rang von Matrizen.

Definition 3.3.20 (Rang einer Matrix)**.** Zu einer $m \times n$ Matrix A über dem Körper K, also $A \in K^{m \times n}$, betrachten wir die zugehörige lineare Abbildung

$$\begin{aligned} \varphi_A \ : \ K^n &\to K^m \ , \\ \mathbf{x} &\mapsto A \cdot \mathbf{x} \ . \end{aligned}$$

Dann ist der *Rang der Matrix* A definiert als

$$\text{Rang}(A) \ := \ \text{Rang}(\varphi_A) \ = \ \dim(\text{Bild}(\varphi_A)) \ .$$

Definition 3.3.21 (Spaltenraum, Zeilenraum)**.** Es sei A eine $m \times n$ Matrix über dem Körper K, also

$$A \ = \ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \ \in \ K^{m \times n} \ .$$

Der Spaltenraum $SR(A)$ ist der Teilvektorraum von K^m, der durch die Spalten von A erzeugt wird, also

$$SR(A) \ := \ \left\langle \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \right\rangle \ .$$

Der Zeilenraum $ZR(A)$ ist der Teilvektorraum von $K^{1 \times n}$, der durch die Zeilen von A erzeugt wird, also

$$ZR(A) \ := \ \left\langle (a_{11}, \ldots, a_{1n}), (a_{21}, \ldots, a_{2n}), \ldots, (a_{m1}, \ldots, a_{mn}) \right\rangle \ .$$

In dem folgenden Satz charakterisieren wir den Rang einer Matrix auf verschiedene Weisen. Dabei spielen auch elementare Spaltenumformungen eine Rolle, die völlig analog zu den in Definition 3.1.5 betrachteten elementaren Zeilenumformungen definiert sind (ersetze in Definition 3.1.5 überall „Zeile“ durch „Spalte“).

Satz 3.3.22 (Charakterisierung des Rangs einer Matrix)**.** *Es sei A eine $m \times n$ Matrix über dem Körper K. Dann gilt:*

(i) $\text{Rang}(A) = \dim(SR(A))$;

(ii) Der Rang von A ändert sich durch elementare Spaltenumformungen nicht.

(iii) Der Rang von A ändert sich durch elementare Zeilenumformungen nicht.

Beweis. Zu (i): Definitionsgemäß ist der Rang der Matrix A die Dimension des Bildes der linearen Abbildung $\varphi_A : K^n \to K^m$. Es sei $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ die Standardbasisfolge von K^n. Dann ist

$$\begin{aligned} \text{Bild}(\varphi_A) &= \langle \varphi(\mathbf{e}_1), \ldots, \varphi(\mathbf{e}_n) \rangle \\ &= \langle A \cdot \mathbf{e}_1, \ldots, A \cdot \mathbf{e}_n \rangle \\ &= \left\langle \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \right\rangle = SR(A) \ . \end{aligned}$$

Behauptung (ii) gilt, da sich der Spaltenraum von A wegen Lemma 3.2.18 durch elementare Spaltenumformungen nicht ändert.

Zu (iii): Die Matrix A' gehe aus A durch elementare Zeilenumformungen hervor. Dann gilt wegen Lemma 3.1.2

$$\text{Kern}(\varphi_A) = \{\mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{0}\} = \{\mathbf{x} \in K^n \mid A' \cdot \mathbf{x} = \mathbf{0}\} = \text{Kern}(\varphi_{A'}) \ .$$

Folglich erhält man

$$\text{Rang}(A) = n - \dim\big(\text{Kern}(\varphi_A)\big) = n - \dim\big(\text{Kern}(\varphi_{A'})\big) = \text{Rang}(A') \ .$$

Damit ist der Beweis abgeschlossen. □

Bemerkung. Man beachte, dass sich durch elementare Zeilenumformungen zwar der Rang einer Matrix und damit die Dimension des Spaltenraumes nicht ändert, der Spaltenraum sich jedoch sehr wohl ändern kann.

Um den Rang einer Matrix A zu berechnen, kann man also sowohl elementare Zeilen- als auch Spaltenumformungen anwenden. Wir demonstrieren dies anhand eines Beispiels.

Beispiel. Wir berechnen den Rang der Matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 16 & 15 & 14 & 13 \\ 2 & 4 & 7 & 8 & 13 & 14 & 5 & 0 \\ 3 & 6 & 9 & 12 & 11 & 10 & 4 & 3 \end{pmatrix} \in \mathbb{R}^{3\times 8} \ .$$

Wir wenden zunächst elementare Zeilenumformungen an:

$$\begin{aligned} &\text{Rang} \begin{pmatrix} 1 & 2 & 3 & 4 & 16 & 15 & 14 & 13 \\ 2 & 4 & 7 & 8 & 13 & 14 & 5 & 0 \\ 3 & 6 & 9 & 12 & 11 & 10 & 4 & 3 \end{pmatrix} \\ \overset{\substack{A_{12}(-2) \\ A_{13}(-3)}}{=} \ &\text{Rang} \begin{pmatrix} \boxed{1} & 2 & 3 & 4 & 16 & 15 & 14 & 13 \\ 0 & 0 & \boxed{1} & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & \boxed{-37} & * & * & * \end{pmatrix} \end{aligned}$$

Durch elementare Spaltenumformungen erhält man schließlich

$$= \quad \text{Rang} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$= \quad \text{Rang} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad = \quad 3 \ .$$

Satz 3.3.23. *Es sei A eine $m \times n$ Matrix über dem Körper K. Dann gilt:*

(i) Man kann A durch elementare Zeilen- und Spaltenumformungen auf die Form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

mit r Einsen auf der Hauptdiagonalen bringen. Insbesondere erhält man dadurch $\text{Rang}(A) = r$.

(ii) $\text{Rang}(A) = \dim(SR(A)) = \dim(ZR(A))$.

Beweis. Zu (i): Nach Satz 3.1.7 kann man A durch elementare Zeilenumformungen auf Stufenform bringen:

$$A' := \begin{pmatrix} 0 \cdots 0 & \boxed{1} & * \cdots * & 0 & * \cdots * & 0 & * \cdots * & 0 & * \cdots \\ 0 \cdots 0 & 0 & \cdots & 0 & \boxed{1} & * \cdots * & 0 & * \cdots * & 0 & * \cdots \\ 0 \cdots 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \boxed{1} & * \cdots * & 0 & * \cdots \\ 0 \cdots 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \boxed{1} & * \cdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & \ddots \end{pmatrix} .$$

Durch elementare Spaltenumformungen kann man mit Hilfe der Einsen, die die Stufen von A' definieren, die restlichen Einträge den entsprechenden Zeilen zu Nullen machen. Durch Permutation der Spalten erhält man dann die beschriebene Form, wobei die Anzahl r der Einsen der Anzahl der Stufen von A' entspricht.

Zu (ii): Da sich bei elementaren Zeilenumformungen der Zeilenraum einer Matrix nicht ändert, ist $ZR(A) = ZR(A')$. In A' sind die von null verschiedenen Zeilenvektoren linear unabhängig. Folglich gilt $\dim(ZR(A)) = r = \dim(SR(A))$.
□

Wir schließen diesen Abschnitt mit dem folgenden Hauptsatz über lineare Gleichungssysteme ab.

Satz 3.3.24 (Hauptsatz über lineare Gleichungssysteme)**.** *Es sei* $A \in K^{m\times n}$ *und* $\mathbf{b} \in K^m$*.*

(i) Die Lösungsmenge

$$L := \{\mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{0}\}$$

des homogenen linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{0}$ *ist ein Teilraum von* K^n *mit*

$$\dim L \;=\; n - \mathrm{Rang}(A) \;.$$

(ii) Das inhomogene lineare Gleichungssystem $A \cdot \mathbf{x} = \mathbf{b}$ *ist genau dann lösbar, wenn*

$$\mathrm{Rang}(A) = \mathrm{Rang}([A, b]) \;,$$

wobei

$$[A, b] \;:=\; \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}$$

die erweiterte Matrix des linearen Gleichungssystems $A \cdot \mathbf{x} = \mathbf{b}$ *ist.*

(iii) Ist $\mathbf{v} \in K^n$ *mit* $A \cdot \mathbf{v} = \mathbf{b}$*, so kann die Lösungsmenge*

$$L_{\mathbf{b}} \;:=\; \{\mathbf{x} \in K^n \mid A \cdot \mathbf{x} = \mathbf{b}\}$$

geschrieben werden als

$$L_{\mathbf{b}} \;=\; \mathbf{v} + L \;=\; \{\mathbf{v} + \mathbf{w} \in K^n \mid \mathbf{w} \in L\} \;.$$

Insbesondere ist das inhomogene lineare Gleichungssystem $A \cdot \mathbf{x} = \mathbf{b}$ *genau dann eindeutig lösbar, wenn* $\mathrm{Rang}(A) = n$ *und* $L_{\mathbf{b}} \neq \emptyset$ *ist.*

Beweis. Aussage (i) folgt aus Satz 3.3.12, denn

$$\dim L \;=\; \dim\big(\mathrm{Kern}(\varphi_A)\big) \;=\; n - \dim\big(\mathrm{Bild}(\varphi_A)\big) \;=\; n - \mathrm{Rang}(A) \;.$$

Um (ii) zu beweisen stellen wir fest, dass das inhomogene lineare Gleichungssystem $A \cdot \mathbf{x} = \mathbf{b}$ genau dann eine Lösung besitzt, wenn $\mathbf{b} \in \mathrm{Bild}(\varphi_A) = SR(A)$. Letzteres ist genau dann der Fall, wenn $SR(A) = SR([A, b])$ und damit $\mathrm{Rang}(A) = \mathrm{Rang}([A, b])$ gilt.

Zu (iii): Es sei $\mathbf{v} \in K^n$ mit $A \cdot \mathbf{v} = \mathbf{b}$. Ist $\mathbf{x} \in K^n$ mit $A \cdot \mathbf{x} = \mathbf{0}$, so ist

$$A \cdot (\mathbf{v} + \mathbf{x}) \;=\; A \cdot \mathbf{v} + A \cdot \mathbf{x} \;=\; \mathbf{b} + \mathbf{0} \;=\; \mathbf{b}$$

und damit $\mathbf{v}+\mathbf{x} \in L_{\mathbf{b}}$. Wir haben also gezeigt, dass $L_{\mathbf{b}} \supseteq \mathbf{v}+L$. Ist umgekehrt $\mathbf{y} \in L_{\mathbf{b}}$, so gilt

$$A \cdot (\mathbf{y} - \mathbf{v}) \;=\; A \cdot \mathbf{y} - A \cdot \mathbf{v} \;=\; \mathbf{b} - \mathbf{b} \;=\; \mathbf{0} \;.$$

Folglich ist $\mathbf{y} - \mathbf{v} =: \mathbf{x} \in L$ und damit $\mathbf{y} = \mathbf{v} + \mathbf{x} \in \mathbf{v} + L$. Wir haben also gezeigt, dass $L_{\mathbf{b}} \subseteq \mathbf{v} + L$ und daher $L_{\mathbf{b}} = \mathbf{v} + L$. □

3.3.6 Eine Anwendung: Polynomfunktionen

Satz 3.3.25 (Vandermonde Matrix)**.** *Es seien $n \in \mathbb{N}_0$ und $c_1, \ldots, c_{n+1} \in K$ paarweise verschieden und*

$$A := \begin{pmatrix} 1 & c_1 & {c_1}^2 & \cdots & {c_1}^n \\ 1 & c_2 & {c_2}^2 & \cdots & {c_2}^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & c_{n+1} & {c_{n+1}}^2 & \cdots & {c_{n+1}}^n \end{pmatrix} \in K^{(n+1)\times(n+1)} .$$

Dann gilt $\mathrm{Rang}(A) = n+1$*. Die Matrix A heißt auch* Vandermonde Matrix*.*

Beweis. Wir führen den Beweis durch Induktion über n. Die Behauptung ist klar für $n = 0$ (und auch für $n = 1$). Addiert man für $i = n, n-1, \ldots, 1$ das $(-c_1)$-fache der i-ten Spalte auf die Spalte $i+1$, so erhält man:

$$\mathrm{Rang}(A) = \mathrm{Rang} \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & c_2 - c_1 & {c_2}^2 - c_1 c_2 & \cdots & {c_2}^n - c_1 {c_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & c_{n+1} - c_1 & {c_{n+1}}^2 - c_1 c_{n+1} & \cdots & {c_{n+1}}^n - c_1 {c_{n+1}}^{n-1} \end{pmatrix} .$$

Addiert man jetzt das (-1)-fache der ersten Zeile auf alle anderen Zeilen und multipliziert dann für $i = 1, \ldots, n+1$ die i-te Zeile mit $(c_i - c_1)^{-1}$, so erhält man:

$$\mathrm{Rang}(A) = \mathrm{Rang} \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & c_2 & \cdots & {c_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & c_{n+1} & \cdots & {c_{n+1}}^{n-1} \end{pmatrix} .$$

Jetzt folgt die Behauptung offenbar mit Induktion. □

Definition 3.3.26. Es sei K ein Körper. Dann bezeichnen wir mit $\mathcal{P}(K)$ den K-Vektorraum aller Polynomfunktionen von K nach K.

Satz 3.3.27. *Es seien $a_0, \ldots, a_n \in K$ nicht alle null und $f \in \mathcal{P}(K)$ die durch*

$$f(x) := a_0 + a_1 x + \cdots + a_n x^n$$

gegebene Polynomfunktion. Dann besitzt f höchstens n Nullstellen in K.

Beweis. Wir nehmen an, dass $c_1, \ldots, c_{n+1} \in K$ paarweise verschiedene Nullstellen von f sind. Dann ist

$$\begin{pmatrix} 1 & c_1 & {c_1}^2 & \cdots & {c_1}^n \\ 1 & c_2 & {c_2}^2 & \cdots & {c_2}^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & c_{n+1} & {c_{n+1}}^2 & \cdots & {c_{n+1}}^n \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

und wegen Satz 3.3.25 folgt daraus, dass $a_0 = \cdots = a_n = 0$. □

Satz 3.3.28. *Für $i \in \mathbb{N}_0$ sei $p_i \in \mathcal{P}(K)$ die durch $p_i(x) := x^i$ gegebene Polynomfunktion. Ist $n \in \mathbb{N}$ und hat K mindestens $n+1$ Elemente, dann ist die Menge $\{p_0, p_1, \ldots, p_n\}$ linear unabhängig.*

Beweis. Es seien $a_0, \ldots, a_n \in K$ und $a_0 p_0 + a_1 p_1 + \cdots + a_n p_n = \mathbf{0}$ die Nullabbildung. Wie im Beweis zu Satz 3.3.27 folgt dann, dass $a_0 = \cdots = a_n = 0$. Folglich ist die Menge $\{p_0, p_1, \ldots, p_n\}$ linear unabhängig. □

Korollar 3.3.29. *Besitzt der Körper K unendlich viele Elemente, so ist $(p_i)_{i\in\mathbb{N}_0}$ eine Basisfolge des K-Vektorraums $\mathcal{P}(K)$. Insbesondere gilt: Sind f und g Polynomfunktionen mit*

$$f(x) \;=\; \sum_{i=0}^{n} a_i x^i \qquad \textit{und} \qquad g(x) \;=\; \sum_{i=0}^{m} b_i x^i$$

wobei $a_n \neq 0$ und $b_m \neq 0$, so ist genau dann $f = g$, wenn $n = m$ und $a_i = b_i$ für $i = 0, \ldots, n$.

Beweis. Die Behauptung folgt direkt aus Satz 3.3.28. □

Korollar 3.3.30. *Ist K ein endlicher Körper mit q Elementen, so ist $(p_0, \ldots, p_{q-1})$ eine Basisfolge von $\mathcal{P}(K)$ und es gilt $\mathcal{P}(K) = K^K$. Jede Abbildung von K nach K ist also eine Polynomfunktion.*

Beweis. Nach Satz 3.3.28 ist $(p_0, \ldots, p_{q-1})$ linear unabhängig. Da $|K^K| = q^q$, folgt aus Satz 3.2.25, dass $\dim(K^K) = q$. Folglich ist $(p_0, \ldots, p_{q-1})$ eine Basisfolge von K^K und damit erst recht auch eine Basisfolge von $\mathcal{P}(K)$. □

3.3.7 Matrix einer linearen Abbildung

Eine lineare Abbildung zwischen zwei endlich dimensionalen Vektorräumen kann durch Angabe von Basisfolgen der Vektorräume und durch eine Matrix vollständig spezifiziert werden.

Definition 3.3.31 (Matrix einer linearen Abbildung)**.** Es seien V und W zwei K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Weiter seien $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basisfolge von V und $B' = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ eine Basisfolge von W. Dann ist nach Satz 3.3.5 die lineare Abbildung φ durch die Angabe von

$$\varphi(\mathbf{v}_j) \in W \qquad \text{für } j = 1, \ldots, n$$

vollständig bestimmt. Der Vektor $\varphi(\mathbf{v}_j)$ lässt sich eindeutig in der Basis B' ausdrücken:

$$\varphi(\mathbf{v}_j) \;=\; \sum_{i=1}^{m} a_{ij} \cdot \mathbf{w}_i \qquad \text{für } j = 1, \ldots, n,$$

wobei $a_{ij} \in K$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$. Die dadurch definierte Matrix $(a_{ij}) \in K^{m \times n}$ heißt *Matrix von φ bezüglich der Basen B und B'*, in Zeichen

$$ {}_{B'}[\varphi]_B \;=\; (a_{ij}) \;\in K^{m \times n} \;. $$

Beispiele.

(i) Wir betrachten den $\mathbb{R}$-Vektorraum $\mathcal{P}(\mathbb{R})$ der Polynomfunktionen von $\mathbb{R}$ nach $\mathbb{R}$ und den durch die Funktionen

$$ \begin{aligned} p_0(x) &:= x^0 = 1 \;, \\ p_1(x) &:= x^1 = x \;, \\ p_2(x) &:= x^2 \;, \\ p_3(x) &:= x^3 \end{aligned} $$

aufgespannten Teilraum $V := \langle p_0, p_1, p_2, p_3 \rangle$ der Polynomfunktionen vom Grad höchstens 3. Wegen Satz 3.3.28 ist $B := (p_0, p_1, p_2, p_3)$ eine Basisfolge von V. Wir betrachten die folgende Abbildung $\varphi : V \to V$ mit

$$ \varphi(f)(x) \;:=\; f(x+1) \qquad \text{für alle } x \in \mathbb{R}. $$

Diese Abbildung ist linear, denn es gilt für $s \in \mathbb{R}$ und $f, g \in V$, dass

$$ \begin{aligned} \varphi(s \cdot f + g)(x) &= (s \cdot f + g)(x+1) \\ &= s \cdot f(x+1) + g(x+1) \\ &= s \cdot \varphi(f)(x) + \varphi(g)(x) \end{aligned} $$

für alle $x \in \mathbb{R}$. Weiter gilt, dass

$$ \begin{aligned} \varphi(p_0) &= p_0 \;, \\ \varphi(p_1) &= p_0 + p_1 \;, \\ \varphi(p_2) &= p_0 + 2 \cdot p_1 + p_2 \;, \\ \varphi(p_3) &= p_0 + 3 \cdot p_1 + 3 \cdot p_2 + p_3 \;. \end{aligned} $$

Daraus erhält man die Matrix von φ bezüglich der Basis B:

$$ {}_B[\varphi]_B \;=\; \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \;. $$

(ii) Es sei $A \in K^{m \times n}$ und $\varphi_A : K^n \to K^m$ die zugehörige lineare Abbildung mit $\varphi_A(\mathbf{x}) = A \cdot \mathbf{x}$. Es seien $B = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ die Standardbasis von K^n und $B' = (\mathbf{e}'_1, \ldots, \mathbf{e}'_m)$ die Standardbasis von K^m. Dann ist

$$ \varphi_A(\mathbf{e}_j) \;=\; A \cdot \mathbf{e}_j \;=\; \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \;=\; \sum_{i=1}^{m} a_{ij} \cdot \mathbf{e}'_i \qquad \text{für } j = 1, \ldots, n. $$

Folglich ist also

$$ {}_{B'}[\varphi_A]_B \;=\; A \;. $$

Satz 3.3.32. *Es seien V und W zwei K-Vektorräume, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basisfolge von V und $B' = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ eine Basisfolge von W. Für eine lineare Abbildung $\varphi : V \to W$ gilt dann*

$$ c_{B'}\big(\varphi(\mathbf{v})\big) \;=\; {}_{B'}[\varphi]_B \cdot c_B(\mathbf{v}) \qquad \textit{für alle } \mathbf{v} \in V. $$

Beweis. Nach Definition gilt

$$ {}_{B'}[\varphi]_B \;=\; (a_{ij}) \;\in\; K^{m\times n} \;, $$

wobei $\varphi(\mathbf{v}_j) = \sum_{i=1}^{m} a_{ij}\mathbf{w}_i$ für $j = 1, \ldots, n$.

Es sei nun $\mathbf{v} \in V$ mit $\mathbf{v} = \sum_{j=1}^{n} s_j \cdot \mathbf{v}_j$, also

$$ c_B(\mathbf{v}) \;=\; \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} $$

mit $s_1, \ldots, s_n \in K$. Dann ist

$$ \begin{aligned} \varphi(\mathbf{v}) \;&=\; \sum_{j=1}^{n} s_j \cdot \varphi(\mathbf{v}_j) \\ &=\; \sum_{j=1}^{n} s_j \cdot \sum_{i=1}^{m} a_{ij} \cdot \mathbf{w}_i \\ &=\; \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \cdot s_j \right) \cdot \mathbf{w}_i \\ &=\; \sum_{i=1}^{n} \left((a_{i1}, \ldots, a_{in}) \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \right) \cdot \mathbf{w}_i \;. \end{aligned} $$

Folglich gilt also

$$ c_{B'}\big(\varphi(\mathbf{v})\big) \;=\; {}_{B'}[\varphi]_B \cdot c_B(\mathbf{v}) \;. $$

Damit ist der Beweis abgeschlossen. □

Satz 3.3.32 kann man auch wie folgt formulieren.

Korollar 3.3.33. *Es seien V und W zwei K-Vektorräume, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basisfolge von V und $B' = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ eine Basisfolge von W. Für eine lineare Abbildung $\varphi : V \to W$ gilt dann*

$$c_{B'} \circ \varphi \;=\; \varphi_A \circ c_B \;\;,$$

wobei $A :=_{B'} [\varphi]_B$.

Als weitere Folgerung können wir jetzt eine Aussage über den Rang einer linearen Abbildung mit Hilfe der ihr zugeordneten Matrix machen.

Korollar 3.3.34. *Es seien V und W zwei K-Vektorräume, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basisfolge von V und $B' = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ eine Basisfolge von W. Für eine lineare Abbildung $\varphi : V \to W$ gilt dann*

$$\mathrm{Rang}(\varphi) \;=\; \mathrm{Rang}({}_{B'}[\varphi]_B) \;\;.$$

Beweis. Es sei $A :=_{B'} [\varphi]_B \in K^{m \times n}$. Nach Definition gilt $\mathrm{Rang}(\varphi) = \dim \mathrm{Bild}(\varphi)$ und $\mathrm{Rang}(A) = \dim \mathrm{Bild}(\varphi_A)$. Es genügt daher zu zeigen, dass $\mathrm{Bild}(\varphi) \cong \mathrm{Bild}(\varphi_A)$.

Dazu betrachten wir den Isomorphismus $c_{B'} : W \to K^m$ und zeigen, dass seine Einschränkung auf $\mathrm{Bild}(\varphi)$ einen Isomorphismus von $\mathrm{Bild}(\varphi)$ auf $\mathrm{Bild}(\varphi_A)$ liefert. Wir müssen also nur zeigen, dass $c_{B'}\big(\mathrm{Bild}(\varphi)\big) = \mathrm{Bild}(\varphi_A)$. Zu „$\subseteq$“: Für $\mathbf{v} \in V$ gilt wegen Korollar 3.3.33

$$c_{B'}\big(\varphi(\mathbf{v})\big) \;=\; \varphi_A\big(c_B(\mathbf{v})\big) \;\in\; \mathrm{Bild}(\varphi_A) \;\;.$$

Zu „$\supseteq$“: Es sei

$$\begin{pmatrix} s'_1 \\ \vdots \\ s'_m \end{pmatrix} \;\in\; \mathrm{Bild}(\varphi_A) \qquad \text{also} \qquad \begin{pmatrix} s'_1 \\ \vdots \\ s'_m \end{pmatrix} \;=\; A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$$

mit $s_1, \ldots, s_n \in K$. Definieren wir $\mathbf{v} := \sum_{j=1}^{n} s_j \cdot \mathbf{v}_j$, dann gilt

$$\begin{pmatrix} s'_1 \\ \vdots \\ s'_m \end{pmatrix} \;=\; A \cdot c_B(\mathbf{v}) \;=\; c_{B'}\big(\varphi(\mathbf{v})\big) \;\in\; c_{B'}\big(\mathrm{Bild}(\varphi)\big) \;\;.$$

Damit ist der Beweis abgeschlossen. □

Satz 3.3.35. *Es seien U, V und W drei endlich-dimensionale K-Vektorräume und $\varphi : U \to V$ und $\psi : V \to W$ lineare Abbildungen. Ist B Basisfolge von U, B' Basisfolge von V und B'' Basisfolge von W, so gilt*

$${}_{B''}[\psi \circ \varphi]_B \;=\; {}_{B''}[\psi]_{B'} \cdot {}_{B'}[\varphi]_B \;\;.$$

Dieser Sachverhalt stellt die eigentliche Motivation für die Definition der Matrixmultiplikation dar.

Beweis. Es sei $B = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$, $B' = (\mathbf{v}_1, \ldots, \mathbf{v}_m)$ und $B'' = (\mathbf{w}_1, \ldots, \mathbf{w}_\ell)$. Weiter sei ${}_{B'}[\varphi]_B = A = (a_{ij}) \in K^{m \times n}$ und ${}_{B''}[\psi]_{B'} = C = (c_{ki}) \in K^{\ell \times m}$. Dann gilt also

$$\varphi(\mathbf{u}_j) \;=\; \sum_{i=1}^{m} a_{ij} \cdot \mathbf{v}_i \qquad \text{und} \qquad \psi(\mathbf{v}_i) \;=\; \sum_{k=1}^{\ell} c_{ki} \cdot \mathbf{w}_k \;\; .$$

Damit erhält man also

$$\begin{aligned}
(\psi \circ \varphi)(\mathbf{u}_j) \;&=\; \psi\big(\varphi(\mathbf{u}_j)\big) \\
&=\; \psi\left(\sum_{i=1}^{m} a_{ij} \cdot \mathbf{v}_i\right) \\
&=\; \sum_{i=1}^{m} a_{ij} \cdot \psi(\mathbf{v}_i) \\
&=\; \sum_{i=1}^{m} a_{ij} \cdot \sum_{k=1}^{\ell} c_{ki} \cdot \mathbf{w}_k \\
&=\; \sum_{k=1}^{\ell} \underbrace{\left(\sum_{i=1}^{m} c_{ki} \cdot a_{ij}\right)}_{=(C \cdot A)_{kj}} \cdot \mathbf{w}_k \;\; .
\end{aligned}$$

Damit haben wir also gezeigt, dass für $k = 1, \ldots, \ell$ und $j = 1, \ldots, m$ der Eintrag in der k-ten Zeile und j-ten Spalte der Matrix ${}_{B''}[\psi \circ \varphi]_B$ mit dem entsprechenden Eintrag der Matrix ${}_{B''}[\psi]_{B'} \cdot {}_{B'}[\varphi]_B$ übereinstimmt. □

Beispiel. Wir betrachten noch einmal den $\mathbb{R}$-Vektorraum $\mathcal{P}(\mathbb{R})$ der Polynomfunktionen von $\mathbb{R}$ nach $\mathbb{R}$ und den durch die Funktionen

$$\begin{aligned}
p_0(x) \;&:=\; x^0 \;=\; 1 \;\; , \\
p_1(x) \;&:=\; x^1 \;=\; x \;\; , \\
p_2(x) \;&:=\; x^2 \;\; , \\
p_3(x) \;&:=\; x^3
\end{aligned}$$

aufgespannten Teilraum $V := \langle p_0, p_1, p_2, p_3 \rangle$ der Polynomfunktionen vom Grad höchstens 3. Wir haben weiter oben festgestellt, dass $B := (p_0, p_1, p_2, p_3)$ eine Basisfolge von V ist. Wir betrachten wieder die folgende Abbildung $\varphi : V \to V$ mit

$$\varphi(f)(x) \;:=\; f(x+1) \qquad \text{für alle } x \in \mathbb{R}$$

und

$$ {}_B[\varphi]_B \;=\; \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \;. $$

Wir betrachten jetzt die Abbildung $\varphi^2 := \varphi \circ \varphi : V \to V$, für die gilt:

$$ \varphi^2(f)(x) \;=\; \varphi\big(\varphi(f)\big)(x) \;=\; \varphi(f)(x+1) \;=\; f(x+2) $$

für $f \in V$ und $x \in \mathbb{R}$. Wegen Satz 3.3.35 gilt

$$ {}_B[\varphi^2]_B \;=\; {}_B[\varphi]_B{}^2 \;=\; \begin{pmatrix} 1 & 2 & 4 & 8 \\ 0 & 1 & 4 & 12 \\ 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 1 \end{pmatrix} \;. $$

Dies stimmt mit der Beobachtung überein, dass für eine Funktion

$$ f(x) \;:=\; a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_3 \cdot x^3 $$

mit $a_0, a_1, a_2, a_3 \in \mathbb{R}$ gilt:

$$ \begin{aligned} f(x+2) \;=\; & (a_0 + 2a_1 + 4a_2 + 8a_3) \\ & +(a_1 + 4a_2 + 12a_3) \cdot x \\ & +(a_2 + 6a_3) \cdot x^2 \\ & +a_3 \cdot x^3 \;. \end{aligned} $$

Als Korollar aus Satz 3.3.35 können wir jetzt leicht beweisen, dass die Matrixmultiplikation assoziativ ist. (Wir hatten das bereits im Beweis von Satz 3.1.14 erwähnt, jedoch nicht explizit bewiesen.)

Korollar 3.3.36. *Die Matrixmultiplikation ist assoziativ, d.h. für $A \in K^{m\times n}$, $C \in K^{n\times p}$ und $D \in K^{p\times q}$ gilt*

$$ (A \cdot C) \cdot D \;=\; A \cdot (C \cdot D) \;. $$

Beweis. Wir betrachten die linearen Abbildungen

$$ \begin{aligned} \varphi_A \;&:\; K^n \to K^m \;, \\ \varphi_C \;&:\; K^p \to K^n \;, \\ \varphi_D \;&:\; K^q \to K^p \;. \end{aligned} $$

In Kapitel 1, Lemma 1.3.9 haben wir festgestellt, dass die Komposition von Abbildungen assoziativ ist, d.h.

$$ (\varphi_A \circ \varphi_C) \circ \varphi_D \;=\; \varphi_A \circ (\varphi_C \circ \varphi_D) \;. $$

Ist B_i die Standardbasis von K^i, so gilt ${}_{B_m}[\varphi_A]_{B_n} = A$, ${}_{B_n}[\varphi_C]_{B_p} = C$ und ${}_{B_p}[\varphi_D]_{B_q} = D$. Die Behauptung folgt also mit Satz 3.3.35. $\square$

3.3.8 Basiswechsel

Definition 3.3.37 (Basiswechselmatrix)**.** Es sei V ein K-Vektorraum mit Basisfolgen $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ und $B' = (\mathbf{v}'_1, \ldots, \mathbf{v}'_n)$. Dann heißt die Matrix $Q := {}_{B'}[\mathrm{id}_V]_B$ *Basiswechselmatrix*.

Lemma 3.3.38. *Wir betrachten die Situation aus Definition 3.3.37. Es sei* $\mathbf{v} \in V$ *mit* $\mathbf{v} = \sum_{i=1}^n s_i \mathbf{v}_i$ *und* $\mathbf{v} = \sum_{i=1}^n s'_i \mathbf{v}'_i$*, das heißt*

$$c_B(\mathbf{v}) \;=\; \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \qquad \textit{und} \qquad c_{B'}(\mathbf{v}) \;=\; \begin{pmatrix} s'_1 \\ \vdots \\ s'_n \end{pmatrix} \;.$$

Dann ist $c_{B'}(\mathbf{v}) = Q \cdot c_B(\mathbf{v})$ *und insbesondere* $\mathbf{v}_j = \sum_{i=1}^n q_{ij} \mathbf{v}'_i$ *wobei* $Q = (q_{ij})$.

Beweis. Die Behauptung folgt unmittelbar aus Satz 3.3.32, wenn man die spezielle lineare Abbildung $\varphi = \mathrm{id}_V$ betrachtet. □

Bemerkung. Wegen Satz 3.3.35 gilt

$${}_{B'}[\mathrm{id}_V]_B \cdot {}_B[\mathrm{id}_V]_{B'} \;=\; {}_{B'}[\mathrm{id}_V]_{B'} \;=\; E_n$$

und

$${}_B[\mathrm{id}_V]_{B'} \cdot {}_{B'}[\mathrm{id}_V]_B \;=\; {}_B[\mathrm{id}_V]_B \;=\; E_n \;,$$

wobei E_n die $n \times n$ *Einheitsmatrix* ist, also

$$E_n \;:=\; \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \;\in\; K^{n \times n} \;.$$

Folglich ist ${}_B[\mathrm{id}_V]_{B'} = Q^{-1}$ die zu $Q := {}_{B'}[\mathrm{id}_V]_B$ *inverse* Matrix.

Definition 3.3.39 (Invertierbar, inverse Matrix)**.** Sind $P, Q \in K^{n \times n}$ mit $P \cdot Q = Q \cdot P = E_n$, so nennt man die Matrizen P und Q *invertierbar*, *regulär* oder *nicht singulär*. Die Matrix P heißt dann auch die *zu* Q *inverse Matrix* in Zeichen $P = Q^{-1}$.

Beispiel. Es sei $V = \mathbb{R}^2$,

$$B = (\mathbf{e}_1, \mathbf{e}_2) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) \qquad \text{und} \qquad B' = (\mathbf{v}'_1, \mathbf{v}'_2) = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) \;.$$

Für einen Vektor $\mathbf{v} = \binom{x_1}{x_2} \in V$ gilt $\mathbf{v} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2$, also $c_B(\mathbf{v}) = \binom{x_1}{x_2}$. Um $c_{B'}(\mathbf{v})$ zu berechnen, bestimmen wir zunächst die Basiswechselmatrix $Q = {}_{B'}[\mathrm{id}_V]_B$. Es muss gelten

$$\binom{1}{0} \;=\; \mathbf{e}_1 \;=\; q_{11}\mathbf{v}_1' + q_{21}\mathbf{v}_2' \;=\; q_{11}\binom{1}{2} + q_{21}\binom{1}{-1}$$

und

$$\binom{0}{1} \;=\; \mathbf{e}_2 \;=\; q_{12}\mathbf{v}_1' + q_{22}\mathbf{v}_2' \;=\; q_{12}\binom{1}{2} + q_{22}\binom{1}{-1} \quad .$$

Daraus erhält man sofort $q_{11} = 1/3$, $q_{21} = 2/3$, $q_{12} = 1/3$ und $q_{22} = -1/3$, also

$$Q \;=\; \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \quad .$$

Folglich ist

$$c_{B'}(\mathbf{v}) \;=\; Q \cdot c_B(\mathbf{v}) \;=\; \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \;=\; \begin{pmatrix} \frac{1}{3}x_1 + \frac{1}{3}x_2 \\ \frac{2}{3}x_1 - \frac{1}{3}x_2 \end{pmatrix} \quad .$$

Wie man leicht sieht, ist

$$P \;=\; {}_B[\mathrm{id}_V]_{B'} \;=\; \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \;=\; Q^{-1} \quad .$$

Satz 3.3.40. *Es seien V und W zwei endlich-dimensionale K-Vektorräume und $\varphi : V \to W$ eine lineare Abbildung. Weiter seien B und B' Basisfolgen von V und C und C' Basisfolgen von W. Dann ist*

$${}_{C'}[\varphi]_{B'} \;=\; {}_{C'}[\mathrm{id}_W]_C \cdot {}_C[\varphi]_B \cdot {}_B[\mathrm{id}_V]_{B'} \quad .$$

Beweis. Die Behauptung des Satzes folgt unmittelbar aus Satz 3.3.35, da ${}_{C'}[\varphi]_{B'} = {}_{C'}[\mathrm{id}_W \circ \varphi \circ \mathrm{id}_V]_{B'}$. □

Beispiel. In Fortsetzung des Beispiels von oben betrachten wir wieder den Vektorraum $V = \mathbb{R}^2$ mit den Basisfolgen

$$B = (\mathbf{e}_1, \mathbf{e}_2) = \left(\binom{1}{0}, \binom{0}{1} \right) \qquad \text{und} \qquad B' = (\mathbf{v}_1', \mathbf{v}_2') = \left(\binom{1}{2}, \binom{1}{-1} \right) \quad .$$

Es sei $\varphi : V \to V$ die durch

$$\varphi\left(\binom{x_1}{x_2} \right) \;=\; \begin{pmatrix} -\frac{1}{3}x_1 + \frac{2}{3}x_2 \\ \frac{4}{3}x_1 + \frac{1}{3}x_2 \end{pmatrix}$$

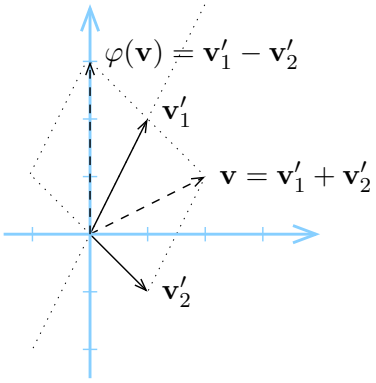


Abbildung 3.2: Geometrische Veranschaulichung der Abbildung φ.

definierte lineare Abbildung. Dann ist

$$\varphi(\mathbf{e}_1) \;=\; \begin{pmatrix} -\frac{1}{3} \\ \frac{4}{3} \end{pmatrix} \;=\; -\tfrac{1}{3}\mathbf{e}_1 + \tfrac{4}{3}\mathbf{e}_2$$

und

$$\varphi(\mathbf{e}_2) \;=\; \begin{pmatrix} \frac{2}{3} \\ \frac{1}{3} \end{pmatrix} \;=\; \tfrac{2}{3}\mathbf{e}_1 + \tfrac{1}{3}\mathbf{e}_2 \;.$$

Folglich ist

$${}_B[\varphi]_B \;=\; \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{4}{3} & \frac{1}{3} \end{pmatrix}$$

und

$$\begin{aligned} {}_{B'}[\varphi]_{B'} \;&=\; {}_{B'}[\mathrm{id}_V]_B \cdot {}_B[\varphi]_B \cdot {}_B[\mathrm{id}_V]_{B'} \\ &=\; \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{4}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \\ &=\; \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{2}{3} & \frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \;. \end{aligned}$$

Anhand dieser Darstellung sieht man leicht, dass φ geometrisch eine Schrägspiegelung an der Geraden durch $\mathbf{v}'_1 = \left(\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right)$ in Richtung $\mathbf{v}'_2 = \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$ ist. Siehe auch Abbildung 3.2.

3.3.9 Algebra der linearen Abbildungen

Definition 3.3.41 (Endomorphismen)**.** Es seien V und W zwei K-Vektorräume. Dann bezeichnen wir die Menge der linearen Abbildungen von V nach W mit

$$\mathrm{Hom}(V, W) \;:=\; \{\varphi : V \to W \mid \varphi \text{ linear}\} \;.$$

Im Spezialfall $V = W$ bezeichnen wir eine lineare Abbildung von V nach V auch als *Endomorphismus* und setzen

$$\mathrm{End}(V) \;:=\; \{\varphi : V \to V \mid \varphi \text{ linear}\} \;.$$

Satz 3.3.42. *Es seien V und W zwei K-Vektorräume.*

(i) Die Menge $\mathrm{Hom}(V,W)$ bildet einen Teilraum des K-Vektorraums $\mathrm{Abb}(V,W)$ aller Abbildungen von V nach W.

(ii) Ist $\dim(V) = n$ und $\dim(W) = m$, so ist $\mathrm{Hom}(V,W) \cong K^{m\times n}$. Insbesondere ist $\dim(\mathrm{Hom}(V,W)) = m \cdot n$.

Beweis. Ad (i): Man kann leicht verifizieren, dass $\mathrm{Abb}(V,W)$ mit der Addition

$$(f+g)(\mathbf{v}) \;:=\; f(\mathbf{v}) + g(\mathbf{v}) \qquad \text{für } f,g \in \mathrm{Abb}(V,W),\, \mathbf{v} \in V,$$

und der Skalarmultiplikation

$$(s \cdot f)(\mathbf{v}) \;:=\; s \cdot f(\mathbf{v}) \qquad \text{für } f \in \mathrm{Abb}(V,W),\, s \in K,\, \mathbf{v} \in V$$

einen K-Vektorraum bildet. Die Teilmenge der linearen Abbildungen $\mathrm{Hom}(V,W)$ bildet einen Teilraum. Die Nullabbildung $\mathbf{v} \mapsto \mathbf{0}$ ist in $\mathrm{Hom}(V,W)$ enthalten. Außerdem überprüft man leicht, dass für $\varphi, \psi \in \mathrm{Hom}(V,W)$ und $s \in K$ die Abbildung $s \cdot \varphi + \psi$ linear und daher in $\mathrm{Hom}(V,W)$ enthalten ist.

Ad (ii): Es sei $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basisfolge von V und $C = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ einen Basisfolge von W. Wir zeigen, dass für $\varphi, \psi \in \mathrm{Hom}(V,W)$ und $s \in K$

$$_C[s \cdot \varphi + \psi]_B \;=\; s \cdot {}_C[\varphi]_B + {}_C[\psi]_B \;.$$

Dazu sei

$$_C[\varphi]_B \;=\; (a_{ij}) \;, \qquad _C[\psi]_B \;=\; (b_{ij}) \qquad \text{und} \qquad _C[s \cdot \varphi + \psi]_B \;=\; (c_{ij}) \;.$$

Dann ist

$$\begin{aligned} \sum_{i=1}^{m} c_{ij}\mathbf{w}_i \;=\; (s \cdot \varphi + \psi)(\mathbf{v}_j) \;&=\; s \cdot \varphi(\mathbf{v}_j) + \psi(\mathbf{v}_j) \\ &=\; s \cdot \sum_{i=1}^{m} a_{ij}\mathbf{w}_i + \sum_{i=1}^{m} b_{ij}\mathbf{w}_i \\ &=\; \sum_{i=1}^{m} (s \cdot a_{ij} + b_{ij})\mathbf{w}_i \end{aligned}$$

und folglich $c_{ij} = s \cdot a_{ij} + b_{ij}$ für alle $i = 1, \ldots, m$ und $j = 1, \ldots, n$. Damit haben wir also gezeigt, dass die Abbildung

$$\begin{aligned} \mu_{CB} : \mathrm{Hom}(V, W) &\to K^{m \times n} \\ \varphi &\mapsto {}_C[\varphi]_B \end{aligned}$$

linear ist. Es bleibt zu zeigen, dass μ_{CB} injektiv und surjektiv ist. Zunächst überzeugt man sich leicht davon, dass $\mathrm{Kern}(\mu_{CB})$ nur aus der Nullabbildung $\mathbf{v} \mapsto \mathbf{0}$ besteht. Ist nämlich ${}_C[\varphi]_B$ die Nullmatrix, so folgt daraus sofort $\varphi(\mathbf{v}_j) = \mathbf{0}$ für alle $j = 1, \ldots, n$. Andererseits ist μ_{CB} surjektiv, da man zu einer beliebigen Matrix $(a_{ij}) \in K^{m \times n}$ eine lineare Abbildung $\varphi : V \to W$ definieren kann durch

$$\varphi(\mathbf{v}_j) \;:=\; \sum_{i=1}^{m} a_{ij} \mathbf{w}_i \qquad \text{für } j = 1, \ldots, m.$$

Dann ist aber ${}_C[\varphi]_B = (a_{ij})$. Damit ist der Beweis abgeschlossen. □

Satz 3.3.43. *Es sei V ein K-Vektorraum.*

(i) Die Menge der Endomorphismen $\mathrm{End}(V)$ *bildet mit der Addition*

$$(\varphi + \psi)(\mathbf{v}) \;:=\; \varphi(\mathbf{v}) + \psi(\mathbf{v}) \qquad \textit{für } \varphi, \psi \in \mathrm{End}(V),\ \mathbf{v} \in V$$

und der Multiplikation

$$(\varphi \circ \psi)(\mathbf{v}) \;:=\; \varphi(\psi(\mathbf{v})) \qquad \textit{für } \varphi, \psi \in \mathrm{End}(V),\ \mathbf{v} \in V$$

einen Ring mit Eins.

(ii) Ist $\dim(V) = n$ *und B eine Basisfolge von V, dann ist*

$$\begin{aligned} \mu_B : \mathrm{End}(V) &\to K^{n \times n} \\ \varphi &\mapsto {}_B[\varphi]_B \end{aligned}$$

ein Ring-Isomorphismus, das heißt μ_B ist bijektiv mit

$$\mu_B(\varphi + \psi) \;=\; \mu_B(\varphi) + \mu_B(\psi) \quad \textit{und} \quad \mu_B(\varphi \circ \psi) \;=\; \mu_B(\varphi) \cdot \mu_B(\psi)$$

für $\varphi, \psi \in \mathrm{End}(V)$.

Beweis. Ad (i): Man überprüft leicht, dass $\mathrm{End}(V)$ mit der angegebenen Addition eine kommutative Gruppe und mit der angegebenen Multiplikation ein Monoid bildet. Das Einselement ist die identische Abbildung. Außerdem gilt das Distributivgesetz, so dass $\mathrm{End}(V)$ also einen Ring mit Eins bildet.

Ad (ii): Wie im Beweis von Satz 3.3.42 gezeigt wurde ist die Abildung μ_B bijektiv und es gilt

$$\mu_B(\varphi + \psi) \;=\; \mu_B(\varphi) + \mu_B(\psi) \qquad \text{für } \varphi, \psi \in \mathrm{End}(V).$$

Außerdem ist nach Satz 3.3.35

$$\mu_B(\varphi \circ \psi) \;=\; {}_B[\varphi \circ \psi]_B \;=\; {}_B[\varphi]_B \cdot {}_B[\psi]_B \;=\; \mu_B(\varphi) \cdot \mu_B(\psi)\ .$$

Damit ist der Beweis abgeschlossen. □

Definition 3.3.44 (K-Algebra)**.** Es sei K ein Körper. Ein Ring R mit Eins, der gleichzeitig ein K-Vektorraum ist (mit derselben Addition wie im Ring), so dass außerdem noch

$$s \cdot (a \cdot b) \;=\; (s \cdot a) \cdot b \;=\; a \cdot (s \cdot b) \qquad \text{für alle } s \in K,\, a, b \in R \tag{3.13}$$

gilt, heißt eine *K-Algebra (mit Eins).*

Beispiele.

(i) Ist V ein K-Vektorraum, so ist $\mathrm{End}(V)$ eine K-Algebra. Wegen Satz 3.3.42 und Satz 3.3.43 müssen wir nur noch zeigen, dass (3.13) gilt. Es seien also $s \in K$ und $\varphi, \psi \in \mathrm{End}(V)$. Dann gilt für $\mathbf{v} \in V$

$$\begin{aligned}(s \cdot (\varphi \circ \psi))(\mathbf{v}) \;&=\; s \cdot ((\varphi \circ \psi)(\mathbf{v})) \\ &=\; s \cdot \varphi(\psi(\mathbf{v})) \;=\; ((s \cdot \varphi) \circ \psi)(\mathbf{v}) \\ &=\; \varphi(s \cdot \psi(\mathbf{v})) \\ &=\; (\varphi \circ (s \cdot \psi))(\mathbf{v})\end{aligned}$$

Damit haben wir (3.13) gezeigt.

(ii) $K^{n \times n}$ ist eine K-Algebra.

(iii) $\mathbb{C}$ ist eine $\mathbb{R}$-Algebra.

3.3.10 Die volle lineare Gruppe

Satz 3.3.45 (Volle lineare Gruppe)**.**

(i) Ist V ein K-Vektorraum, so ist

$$\mathrm{GL}(V) \;:=\; \{\varphi \in \mathrm{End}(V) \mid \varphi \textit{ ist bijektiv}\}$$

zusammen mit der Verknüpfung von Abbildungen „$\circ$“ eine Gruppe, die volle lineare Gruppe*. Die Elemente von* $\mathrm{GL}(V)$ *heißen auch* Automorphismen*.*

(ii) Für $n \in \mathbb{N}$ ist

$$\mathrm{GL}(n,K) \;:=\; \{A \in K^{n\times n} \mid A \textit{ invertierbar}\}\ ,$$

eine Gruppe, die Gruppe der regulären $n \times n$ Matrizen.

Beweis. Ad (i): Man beachte zunächst, dass die Verknüpfung von zwei bijektiven Abbildungen wieder bijektiv ist. Außerdem ist die Verknüpfung assoziativ, das neutrale Element ist id_V und zu jedem $\varphi \in \mathrm{GL}(V)$ ist φ^{-1} wegen Satz 3.3.9 auch wieder in $\mathrm{GL}(V)$. Teil (ii) beweist man analog. □

Lemma 3.3.46. *Ist V ein K-Vektorraum mit $\dim(V) = n$ und B eine Basisfolge von V, so ist*

$$\begin{aligned} \mu_B : \mathrm{GL}(V) &\longrightarrow \mathrm{GL}(n,K) \\ \varphi &\longmapsto {}_B[\varphi]_B \end{aligned}$$

ein Isomorphismus von Gruppen, das heißt μ_B ist bijektiv und

$$\mu_B(\varphi \circ \psi) \;=\; \mu_B(\varphi) \cdot \mu_B(\psi) \qquad \textit{für } \varphi, \psi \in \mathrm{GL}(V). \tag{3.14}$$

Beweis. Zunächst einmal ist μ_B wohldefiniert, da ${}_B[\varphi]_B$ für $\varphi \in \mathrm{GL}(V)$ invertierbar ist, denn

$${}_B[\varphi]_B \cdot {}_B[\varphi^{-1}]_B \;=\; {}_B[\varphi \circ \varphi^{-1}]_B \;=\; {}_B[\mathrm{id}_V]_B \;=\; E_n$$

und

$${}_B[\varphi^{-1}]_B \cdot {}_B[\varphi]_B \;=\; {}_B[\varphi^{-1} \circ \varphi]_B \;=\; {}_B[\mathrm{id}_V]_B \;=\; E_n\ .$$

Aus dem Beweis zu Satz 3.3.42 folgt, dass μ_B injektiv ist. Außerdem ist μ_B surjektiv, da für $A \in \mathrm{GL}(n,K)$ gilt, dass $\mu_B(\varphi_A) = A$ und $\varphi_A \in \mathrm{GL}(V)$, denn

$$\varphi_A \circ \varphi_{A^{-1}} \;=\; \varphi_{A^{-1}} \circ \varphi_A \;=\; \mathrm{id}_V\ .$$

Eigenschaft (3.14) folgt schließlich aus Satz 3.3.35. □

Korollar 3.3.47. *Es sei V ein K-Vektorraum mit $\dim(V) = n$, $\varphi \in \mathrm{End}(V)$ und $A \in K^{n\times n}$. Dann gilt*

$$\varphi \in \mathrm{GL}(V) \quad\Longleftrightarrow\quad \mathrm{Rang}(\varphi) \;=\; n$$

und

$$A \in \mathrm{GL}(n,K) \quad\Longleftrightarrow\quad \mathrm{Rang}(A) \;=\; n\ .$$

Bemerkung. Ist V ein K-Vektorraum mit $\dim(V) > 1$, so ist $\mathrm{GL}(V)$ nicht kommutativ.

Beweis. Es sei $B = (\mathbf{v}_1, \mathbf{v}_2, \dots)$ eine Basisfolge von V. Wir definieren zwei Endomorphismen $\varphi, \psi \in \mathrm{End}(V)$ durch

$$\varphi(\mathbf{v}_i) \;:=\; \begin{cases} \mathbf{v}_i & \text{für } i \neq 1, \\ \mathbf{v}_1 + \mathbf{v}_2 & \text{für } i = 1, \end{cases} \quad \text{und} \quad \psi(\mathbf{v}_i) \;:=\; \begin{cases} \mathbf{v}_i & \text{für } i \neq 2, \\ \mathbf{v}_1 + \mathbf{v}_2 & \text{für } i = 2. \end{cases}$$

Dann sind φ und ψ sogar Automorphismen, denn man überprüft leicht, dass

$$\varphi^{-1}(\mathbf{v}_i) \;:=\; \begin{cases} \mathbf{v}_i & \text{für } i \neq 1, \\ \mathbf{v}_1 - \mathbf{v}_2 & \text{für } i = 1, \end{cases} \quad \text{und} \quad \psi^{-1}(\mathbf{v}_i) \;:=\; \begin{cases} \mathbf{v}_i & \text{für } i \neq 2, \\ \mathbf{v}_1 - \mathbf{v}_2 & \text{für } i = 2. \end{cases}$$

Wir zeigen noch, dass $\psi \circ \varphi \neq \varphi \circ \psi$, denn

$$(\psi \circ \varphi)(\mathbf{v}_1) \;=\; \psi(\mathbf{v}_1 + \mathbf{v}_2) \;=\; 2\mathbf{v}_1 + \mathbf{v}_2$$

und

$$(\varphi \circ \psi)(\mathbf{v}_1) \;=\; \varphi(\mathbf{v}_1) \;=\; \mathbf{v}_1 + \mathbf{v}_2 \;.$$

Damit ist der Beweis abgeschlossen. □

Wir beschäftigen uns im Folgenden mit der Frage, wie man für eine gegebenen Matrix $A \in K^{n \times n}$ feststellt, ob die inverse Matrix A^{-1} existiert, und diese gegebenenfalls berechnet. Wegen Korollar 3.3.47 kann man die Frage nach er Existenz auf eine einfache Rangberechnung zurückführen. Existiert die inverse Matrix A^{-1}, so erfüllt die j-te Spalte von A^{-1} die Gleichung

$$A \cdot \mathbf{x} \;=\; \mathbf{e}_j \qquad \text{für } j = 1, \dots, n. \tag{3.15}$$

Um A^{-1} zu berechnen, muss man also die n in (3.15) gegebenen linearen Gleichungssysteme lösen. Dies kann man simultan mit dem folgenden Verfahren erledigen.

Bemerkung. Es sei $A \in \mathrm{GL}(n, K)$. Bringt man die $n \times 2n$ Matrix $[A, E_n]$ durch elementare Zeilenoperationen auf Stufenform, so erhält man eine $n \times 2n$ Matrix der Form $[E_n, X]$, wobei $X = A^{-1}$. Ist A nicht regulär, so lässt sich die Matrix $[A, E_n]$ durch elementare Zeilenoperationen nicht in diese Form bringen.

Beispiel. Es sei

$$A \;:=\; \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 3 \end{pmatrix} \in \mathbb{R}^{3 \times 3} \;.$$

Dann erhält man:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 3 & 0 & 0 & 1 \end{pmatrix} \overset{A_{1,3}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & -1 & 0 & 1 \end{pmatrix}$$

$$\overset{\substack{M_3(1/2) \\ A_{2,1}(-1)}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1/2 & 0 & 1/2 \end{pmatrix} \overset{A_{3,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1/2 & 1 & -1/2 \\ 0 & 0 & 1 & -1/2 & 0 & 1/2 \end{pmatrix}$$

Folglich ist

$$A^{-1} \;=\; \begin{pmatrix} 1 & -1 & 0 \\ 1/2 & 1 & -1/2 \\ -1/2 & 0 & 1/2 \end{pmatrix} \;.$$

Man kann die Beobachtung aus der letzten Bemerkung wie folgt verallgemeinern.

Bemerkung. Es seien $A \in \mathrm{GL}(n, K)$ und $C \in K^{n\times n}$ gegeben und eine Matrix $X \in K^{n\times n}$ mit $A \cdot X = C$ gesucht, d.h. $X = A^{-1} \cdot C$. Bringt man die $n \times 2n$ Matrix $[A, C]$ durch elementare Zeilenoperationen auf Stufenform, so erhält man eine $n \times 2n$ Matrix der Form $[E_n, X]$ mit dem gesuchten $X \in K^{n\times n}$.

Wir liefern im Folgenden eine Begründung des in den beiden letzten Bemerkungen beschriebenen Verfahrens und gleichzeitig eine neue Interpretation von elementaren Zeilenoperationen.

Satz 3.3.48. *Ist $\varepsilon : K^{n\times n} \to K^{n\times n}$ eine elementare Zeilenoperation und sind $A, B \in K^{n\times n}$, so ist*

$$\varepsilon(A \cdot B) \;=\; \varepsilon(A) \cdot B \;.$$

Beweis. Es sei $A = (a_{ij})$, $B = (b_{ij})$ und $A \cdot B = (c_{ij})$, also

$$c_{ij} \;=\; \sum_{k=1}^{n} a_{ik} b_{kj} \;.$$

Ist ε die Vertauschung der Zeilen i und ℓ, also $\varepsilon = V_{i,\ell}$, so ist

$$\big(\varepsilon(A \cdot B)\big)_{ij} \;=\; c_{\ell j} \;=\; \sum_{k=1}^{n} a_{\ell k} b_{kj} \;=\; \big(\varepsilon(A) \cdot B\big)_{ij} \;.$$

Auf diese Art zeigt man, dass in diesem Fall $\varepsilon(A \cdot B) = \varepsilon(A) \cdot B$. Noch einfacher liegt der Fall, wenn ε die Multiplikation einer Zeile mit einer Konstante s ist, also $\varepsilon = M_i(s)$, denn

$$s \cdot c_{ij} \;=\; \sum_{k=1}^{n} (s \cdot a_{ik}) b_{kj} \;.$$

Ist schließlich $\varepsilon = A_{i,\ell}(s)$, so gilt

$$c_{ij} + sc_{\ell j} \;=\; \sum k = 1^n (a_{ik} + s \cdot a_{\ell k}) b_{kj} \;\; .$$

Damit ist der Beweis abgeschlossen. □

Wir können jetzt eine exakte Begründung für die Bemerkung zur Berechnung der inversen Matrix nachliefern. Sind $\varepsilon_1, \ldots, \varepsilon_m$ elementare Zeilenoperationen mit

$$(\varepsilon_m \circ \cdots \circ \varepsilon_1)(A) \;=\; E_n \;\; ,$$

so folgt mit Satz 3.3.48, dass

$$\begin{aligned} (\varepsilon_m \circ \cdots \circ \varepsilon_1)(E_n) \;&=\; (\varepsilon_m \circ \cdots \circ \varepsilon_1)(A \cdot A^{-1}) \\ &=\; (\varepsilon_m \circ \cdots \circ \varepsilon_1)(A) \cdot A^{-1} \\ &=\; E_n \cdot A^{-1} \;=\; A^{-1} \;\; . \end{aligned}$$

Definition 3.3.49 (Elementarmatrizen)**.** Es sei $n \in \mathbb{N}$, $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ und $s \in K \setminus \{0\}$.

(i) Die *Elementarmatrix* $V_{i,j} \in \mathrm{GL}(n, K)$ entsteht aus der Einheitsmatrix E_n durch Vertauschen der i-ten und j-ten Zeile.

(ii) Die *Elementarmatrix* $M_i(s) \in \mathrm{GL}(n, K)$ entsteht aus der Einheitsmatrix E_n durch Multiplikation der i-ten Zeile mit s.

(iii) Die *Elementarmatrix* $A_{i,j}(s) \in \mathrm{GL}(n, K)$ entsteht aus der Einheitsmatrix E_n durch Addition des s-fachen der i-ten Zeile zur j-ten Zeile.

Bemerkung. Eine elementare Zeilenumformung von $A \in K^{n \times n}$ entspricht der Multiplikation von A von links mit der entsprechenden Elementarmatrix.

Lemma 3.3.50. *Die inverse Matrix einer Elementarmatrix ist selbst eine Elementarmatrix.*

Beweis. Man überprüft leicht, dass

$$V_{i,j}{}^{-1} \;=\; V_{i,j} \;\; , \qquad M_i(s)^{-1} \;=\; M_i(s^{-1}) \;\; , \qquad A_{i,j}(s)^{-1} \;=\; A_{i,j}(-s) \;\; .$$

Daraus folgt offenbar die Behauptung. □

Satz 3.3.51. *Jede Matrix $A \in \mathrm{GL}(n, K)$ ist ein Produkt von Elementarmatrizen.*

Beweis. Da man A durch elementare Zeilenumformungen in die Einheitsmatrix umformen kann, gibt es nach der Bemerkung oben Elementarmatrizen $N_1, \ldots, N_m$ mit

$$N_m \cdot \cdots \cdot N_1 \cdot A \;=\; E_n \;\; .$$

Folglich ist

$$A \;=\; N_1{}^{-1} \cdot \cdots \cdot N_m{}^{-1} \;\; .$$

Wegen Lemma 3.3.50 ist A also ein Produkt von Elementarmatrizen. □

3.4 Determinanten

3.4.1 Alternierende Multilinearformen

Definition 3.4.1. Es sei V ein K-Vektorraum und $n \geq 2$. Eine Abbildung

$$\varphi : \underbrace{V \times \cdots \times V}_{n \text{ mal}} \longrightarrow K$$

heißt *n-Multilinearform*, wenn für jedes $i \in \{1, \ldots, n\}$ und alle $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n$ die durch

$$\mathbf{v} \longmapsto \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)$$

gegebene Abbildung von V nach K linear ist, das heißt

$$\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, s \cdot \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) = s \cdot \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)$$

und

$$\begin{aligned}\varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v} + \mathbf{v}', \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) &= \\ \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) &+ \varphi(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}', \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)\end{aligned}$$

für alle $\mathbf{v}, \mathbf{v}' \in V$ und $s \in K$.

Beweis. □

Kapitel 4

Analysis

In diesem Kapitel geben wir eine Einführung in die grundlegenden Themen der Analysis. Wir beginnen mit der Behandlung von Konvergenzbetrachtungen bei Folgen und Reihen, wenden uns dann stetigen Funktionen zu, um danach die Differenzialrechnung zu behandeln. Darauf folgt ein Abschnitt über Integralrechnung und zum Schluss noch eine kurze Einführung in Differentialgleichungen.

4.1 Folgen und Reihen

4.1.1 Die Vollständigkeit der reellen Zahlen

Definition 4.1.1 (Anordnungsaxiome)**.** Ein Körper K heißt *angeordnet*, wenn es in ihm eine Teilmenge P (den *Positivbereich*) gibt, der die folgenden Eigenschaften besitzt:

(i) K ist disjunkte Vereinigung der Mengen P, $\{0\}$ und $-P := \{x \in K \mid -x \in P\}$.

(ii) Für $x, y \in P$ gilt: $x + y \in P$ und $x \cdot y \in P$.

Die Elemente aus P heißen dann *positiv* und die Elementeaus $-P$ *negativ*.

Beispiel. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ sind angeordnet. Der Positivbereich besteht aus den positiven (rationalen bzw. reellen) Zahlen.

In einem angeordneten Körper können wir die bekannte Ordnungsrelation „$\leq$“ wie folgt definieren.

Lemma 4.1.2 (Ordnungsrelation $\leq$)**.** *Es sei K ein angeordneter Körper mit Positivbereich P. Dann wird durch*

$$x \leq y \quad :\Longleftrightarrow \quad y - x \in P \cup \{0\}$$

für $x, y \in K$ eine totale Ordnung $\leq$ mit den folgenden Eigenschaften definiert. Für $w, x, y, z \in K$ gilt:

(i) Ist $x \leq y$ und $w \leq z$, dann gilt $x + w \leq y + z$.

(ii) Ist $x \leq y$ und $0 \leq z$, so ist $x \cdot z \leq y \cdot z$;
ist $x \leq y$ und $z \leq 0$, so ist $y \cdot z \leq x \cdot z$.

(iii) Falls $x \leq y$, dann ist $-y \leq -x$.

(iv) Ist $x \neq 0$ und $0 \leq x \leq y$, so ist $0 \leq y^{-1} \leq x^{-1}$.

Beweis. Wir zeigen lediglich, dass $\leq$ die Eigenschaften einer Ordnungsrelation (siehe Definition 1.5.7 in Kapitel 1) besitzt. Die weiteren Eigenschaften kann man leicht durch Nachrechnen überprüfen.

Reflexivität: Für $x \in K$ gilt nach Definition $x \leq x$, da $x - x = 0$.

Antisymmetrie: Wir betrachten zwei Elemente $x, y \in K$ mit $x \leq y$. Ist $x \neq y$, so gilt also $y - x \in P$ und daher $x - y = -(y - x) \in -P$, so dass also $y \not\leq x$.

Transitivität: Es seien $x, y, z \in K$ mit $x \leq y$ und $y \leq z$. Dann gilt also $y - x, z - y \in P$. Folglich ist auch $z - x = (z - y) + (y - x) \in P$ und damit $x \leq z$. $\square$

Wir verwenden neben dem Relationssymbol „$\leq$“ natürlich auch die bekannten Symbole „$\geq$“ ($x \geq y \ :\Leftrightarrow \ y \leq x$), „$<$“ ($x < y \ :\Leftrightarrow \ x \leq y \wedge x \neq y$) und „$>$“ ($x > y \ :\Leftrightarrow \ y < x$).

Bemerkung.

(i) Ist K ein angeordneter Körper und $x \in K$, so ist $x^2 \geq 0$. Man sieht dies leicht mit Hilfe einer Fallunterscheidung: Ist $x \geq 0$, so ist die Behauptung nach Definition klar. Ist $x < 0$, so ist $-x > 0$ und daher $x^2 = (-x) \cdot (-x) = x^2 \geq 0$.

(ii) Damit wissen wir jetzt insbesondere, dass die komplexen Zahlen $\mathbb{C}$ keinen angeordneten Körper bilden, da $1 = 1 \cdot 1$ und $-1 = i \cdot i$ andernfalls beide positiv, also in P sein müssten. Dies widerspricht aber der Tatsache, dass P und $-P$ disjunkt sein müssen.

(iii) Wir betrachten einen angeordneten Körper K und die beiden ausgezeichneten Elemente $0, 1 \in K$. Da $1 = 1 \cdot 1 > 0$, gilt

$$1 \ < \ 1+1 \ < \ 1+1+1 \ < \ 1+1+1+1 \ < \ \ldots \ < \ \underbrace{1+1+\cdots+1}_{n\text{-mal}} \ .$$

Damit sind diese Zahlen also alle verschieden und wir können sie mit der Menge der natürlichen Zahlen $\mathbb{N}$ identifizieren. Daraus kann man leicht folgern, dass auch alle ganzen Zahlen $\mathbb{Z}$ und sogar alle rationalen Zahlen $\mathbb{Q}$ in K enthalten sein müssen. Folglich ist $\mathbb{Q}$ der kleinste angeordnete Körper. Insbesondere können endliche Körper nicht angeordnet sein.

Wir werden im Folgenden sehen, dass auch die reellen Zahlen $\mathbb{R}$ einen ausgezeichneten angeordneten Körper darstellen. Dazu benötigen wir das sogenannte Vollständigkeitsaxiom. (Wir erinnern hier an Definition 1.5.8 aus Kapitel 1).

Definition 4.1.3 (Vollständigkeitsaxiom)**.** Ein angeordneter Körper K heißt *vollständig*, wenn in ihm jede Teilmenge $M \subseteq K$, die eine obere Schranke $x \in K$ besitzt (also $y \leq x$ für alle $y \in M$), auch ein Supremum besitzt.

Wir stellen im Folgenden zunächst fest, dass der Körper der rationalen Zahlen $\mathbb{Q}$ nicht vollständig ist. Dazu zeigen wir zunächst, dass sich $\mathbb{Q}$ tatsächlich von $\mathbb{R}$ unterscheidet. Das bedeutet, dass es reelle Zahlen gibt, die nicht als Bruch zweier ganzer Zahlen, also nicht als rationale Zahl geschrieben werden können.

Lemma 4.1.4. *Die Gleichung $X^2 - 2 = 0$ besitzt in $\mathbb{Q}$ keine Lösung, d.h. $\sqrt{2}$ ist keine rationale Zahl.*

Beweis. Im Widerspruch zur Behauptung nehmen wir an, dass $\left(\frac{p}{q}\right)^2 = 2$ mit $p \in \mathbb{Z}$ und $q \in \mathbb{N}$. Dann ist folglich

$$p^2 \;=\; 2 \cdot q^2 \;.$$

In der eindeutigen Primfaktorzerlegung der natürlichen Zahl p^2 kommt jeder Primfaktor mit gerader Häufigkeit vor. In der eindeutigen Primfaktorzerlegung der Zahl $2 \cdot q^2$ kommt der Primfaktor 2 jedoch ungerade oft vor. Dies ist ein Widerspruch. □

Wir wissen jetzt, dass $\sqrt{2}$ keine rationale Zahl ist. Das bedeutet, dass die Menge der rationalen Zahlen die reelle Zahlengerade nicht vollständig überdeckt, sondern Lücken wie etwa an der Stelle $\sqrt{2}$ auftreten können. Andererseits kann man leicht zeigen, dass die rationalen Zahlen „dicht“ auf der reellen Achse liegen, d.h. dass es keine „größeren“ Lücken gibt.

Lemma 4.1.5. *Sind $a, b \in \mathbb{R}$ mit $a < b$, so gibt es eine rationale Zahl $\frac{p}{q} \in \mathbb{Q}$ mit $a < \frac{p}{q} < b$.*

Beweis. Es sei $q := \left\lceil \frac{2}{b-a} \right\rceil \in \mathbb{N}$ und $p := \lceil a \cdot q \rceil + 1 \in \mathbb{Z}$. Dann ist

$$a \;=\; \frac{a \cdot q}{q} \;<\; \frac{p}{q} \;<\; \frac{a \cdot q + 2}{q} \;\leq\; a + \frac{2}{\frac{2}{b-a}} \;=\; b \;.$$

□

Wir können jetzt zeigen, dass $\mathbb{Q}$ nicht vollständig ist.

Satz 4.1.6. *Der angeordnete Körper der rationalen Zahlen $\mathbb{Q}$ ist nicht vollständig.*

Beweis. Wir betrachten die Teilmenge $M := \{x \in \mathbb{Q} \mid x^2 \leq 2\}$. Würden wir die entsprechende Teilmenge von $\mathbb{R}$ betrachten, so wäre $\sqrt{2}$ sowohl Maximum als auch Supremum dieser Menge. Da $\sqrt{2}$ wegen Lemma 4.1.4 jedoch keine rationale Zahl ist, besitzt M kein Supremum. Denn angenommen $r \in \mathbb{Q}$ wäre Supremum von M. Ist $r < \sqrt{2}$, dann gibt es nach Lemma 4.1.5 ein $r' \in M$ mit $r' > r$, so dass r keine obere Schranke ist. Folglich ist $r > \sqrt{2}$. Dann gibt es aber wiederum nach Lemma 4.1.5 ein $r'' \in \mathbb{Q}$ mit $\sqrt{2} < r'' < r$. Folglich ist r'' eine obere Schranke und r kann folglich nicht die kleinste obere Schranke sein. □

Im Gegensatz dazu ist der Körper der reellen Zahlen $\mathbb{R}$ vollständig, was eine ausgezeichnete Eigenschaft von $\mathbb{R}$ darstellt. Wir geben den folgenden Satz ohne Beweis an.

Satz 4.1.7. *Der Körper der reellen Zahlen $\mathbb{R}$ ist der einzige vollständige angeordnete Körper.*

4.1.2 Folgen

Definition 4.1.8 (Folgen)**.** Es sei M eine beliebige Menge. Eine Folge in M ist eine Abbildung $\varphi : \mathbb{N} \to M$ mit

$$n \mapsto a_n = \varphi(n) \in M \qquad \text{für } n \in \mathbb{N}.$$

Wir bezeichnen eine solche Folge mit $(a_n)_{n\in\mathbb{N}}$ oder einfach nur mit (a_n).

Manchmal beginnen Folgen nicht bei $n = 1$ sondern bei $n = 0$ oder einer anderen Zahl $n \in \mathbb{Z}$. Dann haben wir also streng genommen eine Abbildung von $\{n \in \mathbb{Z} \mid n \geq n_0\}$ nach M. Wir schreiben die Folge dann als $(a_n)_{n\in\mathbb{N}_0}$ beziehungsweise $(a_n)_{n\geq n_0}$.

Beispiele.

(i) Ist $a_n = a$ für alle $n \in \mathbb{N}$, so sprechen wir von der *konstanten Folge* (a_n).

(ii) Für $i \in \mathbb{C}$ ist $(i^n)_{n\in\mathbb{N}}$ die Folge: $i, -1, -i, 1, i, -1, -i, 1, \ldots$

(iii) $(\frac{1}{n})_{n\in\mathbb{N}}$ ist die Folge: $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \ldots$

(iv) $(\frac{1}{n^2})_{n\in\mathbb{N}}$ ist die Folge: $1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25}, \frac{1}{36}, \frac{1}{49}, \ldots$

(v) Die Folge der Fibonacci-Zahlen (siehe auch Kapitel 2, Abschnitt 2.1.3) ist rekursiv definiert durch $a_0 := 0$, $a_1 := 1$ und $a_n := a_{n-1} + a_{n-2}$ für $n \geq 2$, also: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,...

(vi) Wir betrachten die rekursiv definierte Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_1 := 1$ und $a_{n+1} := \frac{a_n}{2} + \frac{1}{a_n}$ für $n \in \mathbb{N}$, also: 1, 1.5, 1.416666..., 1.414215..., 1.414213..., ... Aufgrund der angegebenen Folgenglieder liegt der Verdacht nahe, dass sich diese Folge dem Wert $\sqrt{2}$ annähert.

Definition 4.1.9 (Konvergenz von Folgen)**.** Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge von komplexen (oder reellen) Zahlen $a_n \in \mathbb{C}$. Die Folge *konvergiert gegen den Grenzwert* $a \in \mathbb{C}$, in Zeichen $\lim_{n\to\infty} a_n = a$, wenn gilt:

$$\forall \varepsilon > 0 \; \exists n_0 \in \mathbb{N} \; \forall n > n_0 : \quad |a_n - a| \; < \; \varepsilon \; .$$

Die Folge (a_n) heißt *konvergent* (man sagt dann auch, dass die Folge *konvergiert*), falls es einen Grenzwert gibt, gegen den sie konvergiert. Falls die Folge (a_n) nicht konvergiert, dann *divergiert* sie und heißt *divergent*.

Bemerkung.

(i) Eine Folge, die gegen den Grenzwert 0 konvergiert, heißt auch *Nullfolge*.

(ii) Eine Folge komplexer Zahlen $(a_n)_{n\in\mathbb{N}}$ ist nach Definition genau dann eine Nullfolge, wenn die relle Folge $(|a_n|)_{n\in\mathbb{N}}$ eine Nullfolge ist.

(iii) Eine Folge $(a_n)_{n\in\mathbb{N}}$ konvergiert genau dann gegen den Grenzwert a, wenn die Folge $(a_n - a)_{n\in\mathbb{N}}$ eine Nullfolge ist.

(iv) Konvergiert die Folge (a_n) gegen den Grenzwert $a = \lim_{n\to\infty} a_n$, so schreiben wir auch

$$a_n \to a \quad \text{für} \quad n \to \infty \; .$$

(v) Für $\varepsilon > 0$ und $a \in \mathbb{C}$ nennen wir die Menge $\{x \in \mathbb{C} \mid |a - x| < \varepsilon\} \subseteq \mathbb{C}$ auch *ε-Umgebung* von a (analog in $\mathbb{R}$). Konvergiert eine Folge (a_n) gegen den Grenzwert a, so bedeutet das also, dass in jeder ε-Umgebung (mit $\varepsilon > 0$) von a *fast alle* Folgenglieder von (a_n) liegen. Dabei bedeutet „fast alle“ genau gesagt „alle außer endlich vielen“.

Beispiele.

(i) Die Folge $(\frac{1}{n})_{n\in\mathbb{N}}$ konvergiert gegen den Grenzwert 0, denn: Wähle zu einem beliebigen $\varepsilon > 0$ die Zahl $n_0 = \lceil \frac{1}{\varepsilon} \rceil$, so dass für $n \geq n_0$ gilt:

$$a_n \; \leq \; a_{n_0} \; = \; \frac{1}{\lceil \frac{1}{\varepsilon} \rceil} \; \leq \; \frac{1}{\frac{1}{\varepsilon}} \; = \; \varepsilon \; .$$

(ii) Man kann leicht zeigen, dass die Folge $(\frac{n}{n+1})_{n\in\mathbb{N}}$ gegen den Grenzwert 1 konvergiert.

(iii) Die komplexe Folge $(i^n)_{n\in\mathbb{N}}$ divergiert.

(iv) Die Folge $(\frac{n}{2^n})_{n\in\mathbb{N}}$ konvergiert gegen den Grenzwert 0. Mit vollständiger Induktion kann man nämlich zeigen, dass $2^n \geq n^2$ für $n \geq 4$. Folglich gilt

$$\left|\frac{n}{2^n} - 0\right| \;\leq\; \frac{n}{n^2} \;=\; \frac{1}{n} \qquad \text{für } n \geq 4.$$

Wählen wir also zu einem beliebigen $\varepsilon > 0$ die Zahl $n_0 = \max\left\{\left\lceil \frac{1}{\varepsilon} \right\rceil, 4\right\}$, so ist das Konvergenzkriterium erfüllt.

(v) Für $a \in \mathbb{C}$ betrachten wir die Folge $(a^n)_{n\in\mathbb{N}}$. Man kann zeigen, dass (a^n) für $|a| \geq 1$ und $a \neq 1$ divergent ist. Für den Fall $a = 1$ ist die Folge (a^n) konstant und konvergiert folglich gegen 1. Ist $|a| < 1$, so konvergiert die Folge (a^n) gegen 0.

(vi) Wir betrachten noch einmal die rekursiv definierte Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_1 := 1$ und $a_{n+1} := \frac{a_n}{2} + \frac{1}{a_n}$ für $n \in \mathbb{N}$. Wie weiter oben vermutet, konvergiert diese Folge gegen den Grenzwert $\sqrt{2}$. Man kann mit vollständiger Induktion leicht zeigen, dass $1 \leq a_n \leq 2$ für alle $n \in \mathbb{N}$. Weiterhin kann man leicht nachrechnen, dass

$$|a_{n+1} - \sqrt{2}| \;=\; |a_n - \sqrt{2}| \cdot \frac{|a_n - \sqrt{2}|}{2a_n} \;\leq\; |a_n - \sqrt{2}| \cdot \frac{1}{2} \;.$$

Folglich gilt nach Induktion

$$|a_n - \sqrt{2}| \;\leq\; \frac{1}{2^n} \;,$$

so dass man zu beliebigem $\varepsilon > 0$ die Zahl n_0 einfach so wählen kann, dass $\frac{1}{2^{n_0}} < \varepsilon$. Dann gilt

$$|a_n - \sqrt{2}| \;\leq\; \frac{1}{2^n} \;\leq\; \frac{1}{2^{n_0}} < \varepsilon \qquad \text{für alle } n \geq n_0.$$

Satz 4.1.10 (Eindeutigkeit des Grenzwerts)**.** *Es sei $(a_n)_{n\in\mathbb{N}}$ eine konvergente Folge mit $a_n \in \mathbb{C}$. Dann ist der Grenzwert a der Folge eindeutig bestimmt.*

Beweis. Im Widerspruch zur Behauptung nehmen wir an, dass die Folge sowohl gegen a als auch gegen $a' \neq a$ konvergiert. Wählt man $0 < \varepsilon < (a - a')/2$, dann gibt es ein $n_0 \in \mathbb{N}$, so dass

$$|a_n - a| \;<\; \varepsilon \qquad \text{für } n \geq n_0.$$

Außerdem gibt es ein $n_0' \in \mathbb{N}$, so dass

$$|a_n - a'| \;<\; \varepsilon \qquad \text{für } n \geq n_0'.$$

Folglich gilt für $n \geq \max\{n_0, n_0'\}$:

$$|a - a'| \;\leq\; |a - a_n| + |a_n - a'| \;<\; 2\varepsilon \;<\; |a - a'| \;,$$

was ein Widerspruch ist. □

Definition 4.1.11. Es sei $(a_n)_{n\in\mathbb{N}}$ eine reelle Zahlenfolge.

(i) Die Folge (a_n) *geht gegen* ∞, in Zeichen $\lim_{n\to\infty} a_n = \infty$, falls für alle $r > 0$ ein $n_0 \in \mathbb{N}$ existiert, so dass $a_n > r$ für alle $n \geq n_0$ ist.

(ii) Die Folge (a_n) *geht gegen* $-\infty$, in Zeichen $\lim_{n\to\infty} a_n = -\infty$, falls für alle $r < 0$ ein $n_0 \in \mathbb{N}$ existiert, so dass $a_n < r$ für alle $n \geq n_0$ ist.

(iii) Die Folge (a_n) heißt *nach oben (unten) beschränkt*, falls die Menge $\{a_n \mid n \in \mathbb{N}\}$ eine obere (untere) Schranke in $\mathbb{R}$ besitzt. Die Folge (a_n) heißt *beschränkt*, falls sie nach oben und nach unten beschränkt ist.

(iv) Die Folge (a_n) heißt *monoton wachsend (monoton fallend)*, wenn für alle $n \in \mathbb{N}$ gilt, dass $a_{n+1} \geq a_n$ ($a_{n+1} \leq a_n$). Ist zusätzlich $a_{n+1} \neq a_n$ für alle $n \in \mathbb{N}$, so nennen wir die Folge *streng monoton wachsend (fallend)*. Eine Folge heißt (streng) monoton, wenn sie (streng) monoton wachsend oder fallend ist.

Lemma 4.1.12. *Jede konvergente Folge reeller Zahlen ist beschränkt.*

Beweis. Es sei $(a_n)_{n\in\mathbb{N}}$ eine konvergente Folge reeller Zahlen mit Grenzwert a. Dann gibt es ein $n_0 \in \mathbb{N}$, so dass $a_n \leq a + 1$ für alle $n \geq n_0$. Dann ist (a_n) nach oben beschränkt durch $\max\{a + 1, a_1, a_2, \ldots, a_{n_0-1}\}$. Analog kann man zeigen, dass (a_n) nach unten beschränkt ist. □

Umgekehrt ist jede beschränkte reelle Zahlenfolge konvergent, falls sie monoton ist.

Lemma 4.1.13. *Es sei $(a_n)_{n\in\mathbb{N}}$ eine nach oben (unten) beschränkte, monoton wachsende (fallende) Folge reeller Zahlen. Dann ist (a_n) konvergent mit Grenzwert $\sup\{a_n \mid n \in \mathbb{N}\}$ ($\inf\{a_n \mid n \in \mathbb{N}\}$).*

Beweis. Wir zeigen, dass die monoton wachsende Folge (a_n) gegen $a := \sup\{a_n \mid n \in \mathbb{N}\}$ konvergiert. Es sei $\varepsilon > 0$ beliebig. Da a Supremum der Menge $\{a_n \mid n \in \mathbb{N}\}$ ist, gibt es ein $n_0 \in \mathbb{N}$ mit $a_{n_0} > a - \varepsilon$. Da (a_n) monoton wachsend ist gilt dann

$$|a_n - a| \;=\; a - a_n \;<\; \varepsilon \qquad \text{für alle } n \geq n_0.$$

Folglich konvergiert (a_n) gegen a. Die geklammerte Version des Lemmas beweist man analog. □

Bemerkung. Man beachte, dass die Monotonie der Folge in Lemma 4.1.13 essenziell ist. Denn die Folge $\left((-1)^n\right)_{n\in\mathbb{N}}$ ist zwar beschränkt jedoch nicht konvergent.

Satz 4.1.14 (Vergleichskriterium)**.** *Es seien (a_n), (b_n) und (c_n) reelle Zahlenfolgen mit $a_n \leq b_n \leq c_n$ für alle $n \in \mathbb{N}$.*

(i) Ist $b \in \mathbb{R}$ mit $\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n = b$, so ist $\lim_{n\to\infty} b_n = b$.

(ii) Ist $\lim_{n\to\infty} a_n = \infty$*, so ist auch* $\lim_{n\to\infty} b_n = \infty$*.*

(iii) Ist $\lim_{n\to\infty} c_n = -\infty$*, so ist auch* $\lim_{n\to\infty} b_n = -\infty$*.*

Beweis. Wir beweisen beispielhaft Teil (i). Die Beweise der restlichen Aussagen funktionieren ähnlich. Es sei $\varepsilon > 0$; dann gibt es $n_0, n_0' \in \mathbb{N}$ mit

$$|a_n - b| \ < \ \varepsilon \qquad \text{für alle } n \geq n_0$$

und

$$|c_n - b| \ < \ \varepsilon \qquad \text{für alle } n \geq n_0'.$$

Folglich gilt

$$b - \varepsilon < a_n \ \leq \ b_n \ \leq \ c_n \ \leq \ b + \varepsilon \qquad \text{für alle } n \geq \max\{n_0, n_0'\}.$$

Damit konvergiert (b_n) gegen den Grenzwert b. □

Beispiel. Wir betrachten die Folge $\left(\frac{1}{n^2}\right)_{n\in\mathbb{N}}$. Da $0 \leq \frac{1}{n^2} \leq \frac{1}{n}$ für alle $n \in \mathbb{N}$, konvergiert $\left(\frac{1}{n^2}\right)$ wie die konstante Folge $(0)_{n\in\mathbb{N}}$ und die Folge $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ gegen 0.

Korollar 4.1.15. *Es seien* (a_n) *und* (b_n) *reelle Zahlenfolgen. Ist* (a_n) *eine Nullfolge und* (b_n) *beschränkt, so ist die Folge* $(a_n \cdot b_n)_{n\in\mathbb{N}}$ *eine Nullfolge.*

Beweis. Da (b_n) beschränkt ist, gibt es ein $B > 0$ mit $|b_n| \leq B$ für alle $n \in \mathbb{N}$. Folglich gilt $0 \leq |a_n \cdot b_n| \leq B \cdot |a_n|$ für alle $n \in \mathbb{N}$. Da sowohl $(0)_{n\in\mathbb{N}}$ als auch $(B \cdot |a_n|)_{n\in\mathbb{N}}$ gegen 0 konvergieren, ist $(a_n \cdot b_n)$ nach Satz 4.1.14 (i) also eine Nullfolge. □

Lemma 4.1.16. *Es seien* (a_n) *und* (b_n) *reelle Zahlenfolgen mit* $a_n \leq b_n$ *für alle* $n \in \mathbb{N}$*. Sind* (a_n) *und* (b_n) *konvergent, so gilt* $\lim_{n\to\infty} a_n \leq \lim_{n\to\infty} b_n$*.*

Beweis. Es sei $a := \lim_{n\to\infty} a_n$ und $b := \lim_{n\to\infty} b_n$. Im Widerspruch zur Behauptung nehmen wir an, dass $b < a$. Es sei $\varepsilon := (a - b)/2$. Dann gibt es ein $n_0 \in \mathbb{N}$ mit $a_n > a - \varepsilon$ für alle $n \geq n_0$ und ein $n_0' \in \mathbb{N}$ mit $b_n < b + \varepsilon$ für alle $n \geq n_0'$. Folglich gilt für $n \geq \max\{n_0, n_0'\}$, dass

$$b_n \ < \ b + \varepsilon \ = \ a - \varepsilon \ < \ a_n \ .$$

Das ist ein Widerspruch zur Voraussetzung. □

Bemerkung. Sind (a_n) und (b_n) reelle, konvergente Zahlenfolgen mit $a_n < b_n$ für alle $n \in \mathbb{N}$, so folgt daraus nicht notwendig, dass $\lim_{n\to\infty} a_n < \lim_{n\to\infty} b_n$. Zum Beispiel sind $\left(\frac{1}{n+1}\right)_{n\in\mathbb{N}}$ und $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ zwei Nullfolgen mit $\frac{1}{n+1} < \frac{1}{n}$ für alle $n \in \mathbb{N}$.

Satz 4.1.17. *Es seien* $(a_n)_{n\in\mathbb{N}}$ *und* $(b_n)_{n\in\mathbb{N}}$ *konvergente komplexe Zahlenfolgen,* $a := \lim_{n\to\infty} a_n$ *und* $b := \lim_{n\to\infty} b_n$*. Dann gilt:*

(i) Die Folge $(a_n \pm b_n)$ *ist konvergent mit* $\lim_{n\to\infty}(a_n \pm b_n) = a \pm b$.

(ii) Die Folge $(a_n \cdot b_n)$ *ist konvergent mit* $\lim_{n\to\infty}(a_n \cdot b_n) = a \cdot b$.

(iii) Ist $c \in \mathbb{C}$*, so ist die Folge* $(c \cdot a_n)$ *konvergent mit* $\lim_{n\to\infty}(c \cdot a_n) = c \cdot a$.

(iv) Ist $b \neq 0$*, so gibt es ein* $n_0 \in \mathbb{N}$*, so dass* $b_n \neq 0$ *für alle* $n \geq n_0$*. Dann sind auch die Folgen* $\left(\frac{1}{b_n}\right)$ *und* $\left(\frac{a_n}{b_n}\right)$ *konvergent mit* $\lim_{n\to\infty}\left(\frac{1}{b_n}\right) = \frac{1}{b}$ *und* $\lim_{n\to\infty}\left(\frac{a_n}{b_n}\right) = \frac{a}{b}$.

(v) Die Folge $(|a_n|)_{n\in\mathbb{N}}$ *ist konvergent mit* $\lim_{n\to\infty}|a_n| = |a|$.

(vi) Die komplexe Folge $(a_n)_{n\in\mathbb{N}}$ *ist genau dann konvergent, wenn die beiden reellen Zahlenfolgen* $\big(\mathrm{Re}(a_n)\big)_{n\in\mathbb{N}}$ *und* $\big(\mathrm{Im}(a_n)\big)_{n\in\mathbb{N}}$ *konvergieren. In diesem Fall gilt* $\lim_{n\to\infty} a_n = \lim_{n\to\infty}\mathrm{Re}(a_n) + i\cdot\lim_{n\to\infty}\mathrm{Im}(a_n)$.

Beweis. Wir beweisen beispielhaft den ersten Teil des Satzes. Es sei $\varepsilon > 0$ beliebig gewählt. Dann gibt es zu $\varepsilon' := \varepsilon/2 > 0$ Zahlen $n_0, n_0' \in \mathbb{N}$ mit

$$|a_n - a| \;<\; \varepsilon' \qquad\qquad \text{für alle } n \geq n_0$$

und

$$|b_n - b| \;<\; \varepsilon' \qquad\qquad \text{für alle } n \geq n_0'.$$

Folglich gilt für alle $n \geq \max\{n_0, n_0'\}$:

$$\begin{aligned} |(a_n \pm b_n) - (a \pm b)| \;&=\; |(a_n - a) \pm (b_n - b)| \\ &\leq\; |a_n - a| + |b_n - b| \\ &<\; \varepsilon' + \varepsilon' \;=\; \varepsilon\ . \end{aligned}$$

Die weiteren Teile des Satzes beweist man ähnlich. □

Beispiel. Wir betrachten die Folge $\left(\frac{5n^2-2n+1}{3n^2+88n+1001}\right)_{n\in\mathbb{N}}$. Da

$$\frac{5n^2-2n+1}{3n^2+88n+1001} \;=\; \frac{5-\frac{2}{n}+\frac{1}{n^2}}{3+\frac{88}{n}+\frac{1001}{n^2}}\ ,$$

liefert Satz 4.1.17

$$\begin{aligned} \lim_{n\to\infty}\frac{5n^2-2n+1}{3n^2+88n+1001} \;&=\; \frac{\lim_{n\to\infty}(5) - \lim_{n\to\infty}(\frac{2}{n}) + \lim_{n\to\infty}(\frac{1}{n^2})}{\lim_{n\to\infty}(3) + \lim_{n\to\infty}(\frac{88}{n}) + \lim_{n\to\infty}(\frac{1001}{n^2})} \\ &=\; \frac{5\lim_{n\to\infty}(1) - 2\lim_{n\to\infty}(\frac{1}{n}) + \lim_{n\to\infty}(\frac{1}{n^2})}{3\lim_{n\to\infty}(1) + 88\lim_{n\to\infty}(\frac{1}{n}) + 1001\lim_{n\to\infty}(\frac{1}{n^2})} \\ &=\; \frac{5-2\cdot 0+0}{3+88\cdot 0+1001\cdot 0} \\ &=\; \frac{5}{3}\ . \end{aligned}$$

Wir geben schließlich ohne Beweis ein berühmtes Konvergenzkriterium von Cauchy an.

Satz 4.1.18 (Konvergenzkriterium von Cauchy)**.** *Eine Folge komplexer Zahlen $(a_n)_{n\in\mathbb{N}}$ ist genau dann konvergent, wenn*

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \ \forall p, q \geq n_0 : \quad |a_p - a_q| \ < \ \varepsilon \ .$$

Definition 4.1.19 (Teilfolgen, Häufungswerte)**.** Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen.

(i) Ist $(m_n)_{n\in\mathbb{N}}$ eine streng monoton wachsende Folge natürlicher Zahlen, so heißt die Folge $(a_{m_n})_{n\in\mathbb{N}}$ *Teilfolge* von (a_n).

(ii) Eine Zahl $a \in \mathbb{C}$ heißt *Häufungswert* von (a_n), falls es eine Teilfolge von (a_n) gibt, die gegen a konvergiert.

Beispiele.

(i) Jede Folge ist Teilfolge von sich selbst. Insbesondere ist der Grenzwert einer konvergenten Folge auch Häufungswert der Folge.

(ii) Die Folge komplexer Zahlen $(i^n)_{n\in\mathbb{N}}$ besitzt unter anderem die vier Teilfolgen $(i^{4n+1})_{n\in\mathbb{N}}$, $(i^{4n+2})_{n\in\mathbb{N}}$, $(i^{4n+3})_{n\in\mathbb{N}}$ und $(i^{4n+4})_{n\in\mathbb{N}}$, die alle vier konstant sind und insbesondere gegen die Grenzwerte i, -1, $-i$ und 1 konvergieren. Diese vier Zahlen sind also Häufungswerte der Folge $(i^n)_{n\in\mathbb{N}}$.

Wir stellen zum Schluss dieses Abschnitts über Folgen einen berühmten Satz vor (ohne Beweis).

Satz 4.1.20 (Satz von Bolzano & Weierstraß)**.** *Jede beschränkte Folge besitzt eine konvergente Teilfolge. Insbesondere besitzt also jede beschränkte Folge einen Häufungswert.*

4.1.3 Reihen

Reihen sind spezielle Folgen, die durch Aufsummieren von Folgen entstehen.

Definition 4.1.21 (Reihen)**.** Es sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Dann bezeichnet die *Reihe* $\sum_{k=1}^{\infty} a_k$ die Folge

$$(s_n)_{n\in\mathbb{N}} \ := \ \left(\sum_{k=1}^{n} a_k \right)_{n\in\mathbb{N}} \quad .$$

Konvergiert diese Folge (s_n) gegen den Grenzwert a, so *konvergiert* die Reihe und der Grenzwert a wird mit $\sum_{k=1}^{\infty} a_k$ bezeichnet. Divergiert die Folge (s_n), so sagt man auch, dass die Reihe *divergiert*. Das n-te Folgenglied $s_n = \sum_{k=1}^{n} a_k$ wird *n-te Partialsumme* genannt und die Folge (s_n) wird auch *Folge der Partialsummen* genannt.

Bemerkung.

(i) Man beachte, dass mit $\sum_{k=1}^{\infty} a_k$ zunächst keine (komplexe) Zahl identifiziert wird, sondern lediglich die spezielle Zahlenfolge (s_n). Nur wenn diese Zahlenfolge konvergiert, bezeichnet $\sum_{k=1}^{\infty} a_k$ gleichzeitig den Grenzwert.

(ii) Ähnlich wie bei Folgen müssen auch Reihen nicht mit dem Index $k = 1$ beginnen. Jede andere ganze Zahl $n_0 \in \mathbb{Z}$ ist hier denkbar. Wir schreiben dann $\sum_{k \geq n_0} a_k$. Für $n_0, n_1 \in \mathbb{Z}$ ist die Reihe $\sum_{k \geq n_0} a_k$ genau dann konvergent, wenn die Reihe $\sum_{k \geq n_1} a_k$ konvergiert.

(iii) Jede Folge $(s_n)_{n \in \mathbb{N}}$ kann als Reihe geschrieben werden. Man setzt einfach $a_1 := s_1$ und $a_{k+1} := s_{k+1} - s_k$ für $k \in \mathbb{N}$. Dann ist

$$s_n \;=\; \sum_{k=1}^{n} a_k \qquad \text{für alle } n \in \mathbb{N}.$$

Beispiele.

(i) Die „harmonische Reihe“ $\sum_{k=1}^{\infty} \frac{1}{k}$ ist nicht konvergent. Wir zeigen, dass die zugehörige Folge der Partialsummen gegen undendlich geht. Dazu betrachten wir für $m \in \mathbb{N}$ die Partialsumme $\sum_{k=1}^{2^m} \frac{1}{k}$. Es gilt

$$\begin{aligned}
\sum_{k=1}^{2^m} \frac{1}{k} \;&=\; 1 + \sum_{p=1}^{m} \sum_{k=2^{p-1}+1}^{2^p} \frac{1}{k} \\
&\geq\; 1 + \sum_{p=1}^{m} \sum_{k=2^{p-1}+1}^{2^p} \frac{1}{2^p} \\
&=\; 1 + \sum_{p=1}^{m} \frac{1}{2} \\
&=\; 1 + \frac{m}{2} \;.
\end{aligned}$$

Folglich gibt es zu jedem $r > 0$ ein $n_0 \in \mathbb{N}$ (wähle nämlich $n_0 := 2^m$ mit $1 + \frac{m}{2} > r$), so dass $\sum_{k=1}^{n} \frac{1}{k} > r$ für alle $n \geq n_0$.

(ii) Die Reihe $\sum_{k=1}^{\infty} \frac{1}{k^2}$ ist konvergent. Da die Folge der Partialsummen monoton steigend ist, genügt es nach Lemma 4.1.13 zu zeigen, dass diese Folge

beschränkt ist. Für alle $n \in \mathbb{N}$ gilt:

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k^2} &\leq 1 + \sum_{k=2}^{n} \frac{1}{k \cdot (k-1)} \\ &= 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k} \right) \\ &= 1 + \left(1 - \frac{1}{n} \right) \\ &< 2 \ .\end{aligned}$$

Man kann zeigen, dass der Grenzwert der Folge gleich $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$ ist.

(iii) Für $q \in \mathbb{C}$ mit $|q| < 1$ ist die Reihe $\sum_{k=0}^{\infty} q^k$ konvergent mit $\sum_{k=0}^{\infty} q^k = \frac{1}{1-q}$. Denn wir haben in Kapitel 2, Lemma 2.1.3 gezeigt (beachte, dass der dort geführte Beweis auch für komplexe Zahlen q funktioniert), dass für die n-te Partialsumme gilt:

$$s_n = \sum_{k=0}^{n} q^k = \frac{1 - q^{n+1}}{1 - q} \ .$$

Wie wir weiter oben festgestellt haben, ist $\lim_{n \to \infty} q^n = 0$. Folglich gilt

$$\sum_{k=0}^{\infty} q^k = \lim_{n \to \infty} s_n = \frac{1 - q \cdot \lim_{n \to \infty} q^n}{1 - q} = \frac{1}{1 - q} \ .$$

Der folgende Satz ist eine direkte Übertragung von Satz 4.1.18 für Reihen.

Satz 4.1.22 (Cauchy-Kriterium für Reihen)**.** *Es sei $(a_n)_{n \in \mathbb{N}}$ eine Folge komplexer Zahlen. Die Reihe $\sum_{k=1}^{\infty} a_k$ konvergiert genau dann, wenn*

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \ \forall p \geq n \geq n_0 : \quad \left| \sum_{k=n}^{p} a_k \right| < \varepsilon \ .$$

Beispiele.

(i) Mit Hilfe von Satz 4.1.22 können wir jetzt noch einmal sehr einfach zeigen, dass die harmonische Reihe $\sum_{k=1}^{\infty} \frac{1}{k}$ divergent ist. Denn für alle $n \in \mathbb{N}$ gilt

$$\sum_{k=n+1}^{2n} \frac{1}{k} \geq \sum_{k=n+1}^{2n} \frac{1}{2n} = \frac{1}{2} \ .$$

Folglich kann es für $\varepsilon = \frac{1}{2}$ das in Satz 4.1.22 geforderte $n_0 \in \mathbb{N}$ nicht geben.

(ii) Genauso kann man mit Hilfe von Satz 4.1.22 zeigen, dass die Reihen $\sum_{k=1}^{\infty} i^k$ und $\sum_{k=1}^{\infty}(-1)^k$ nicht konvergieren.

Mit Satz 4.1.22 erhält man sofort das folgende notwendige Kriterium für die Konvergenz einer Reihe.

Lemma 4.1.23. *Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen. Konvergiert die Reihe $\sum_{k=1}^{\infty} a_k$, so ist die Folge (a_n) eine Nullfolge.*

Beweis. Konvergiert die Reihe $\sum_{k=1}^{\infty} a_k$, so ist das Cauchy-Kriterium aus Satz 4.1.22 erfüllt. Zu einem beliebigen $\varepsilon > 0$ gibt es also ein $n_0 \in \mathbb{N}$, so dass für alle $n \geq n_0$ gilt (setze $p := n$):

$$|a_n - 0| \;=\; |a_n| \;=\; \left|\sum_{k=n}^{n} a_k\right| \;<\; \varepsilon \;.$$

Folglich ist (a_n) eine Nullfolge. □

Bemerkung. Die Bedingung, dass (a_n) eine Nullfolge sein muss ist notwendig, jedoch nicht hinreichend für die Konvergenz der Reihe $\sum_{k=1}^{\infty} a_k$. Denn die harmonische Reihe $\sum_{k=1}^{\infty} \frac{1}{k}$ ist divergent, obwohl $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ eine Nullfolge ist.

Aus unserem Wissen über die Konvergenz von Folgen aus Lemma 4.1.13 können wir sofort das folgende Kriterium für die Konvergenz einer Reihe mit nicht-negativen Summanden ableiten.

Korollar 4.1.24. *Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge nicht-negativer reeller Zahlen, dann konvergiert die zugehörige Reihe $\sum_{k=1}^{\infty} a_k$ genau dann, wenn die Folge der Partialsummen nach oben beschränkt ist.*

Definition 4.1.25 (Absolute Konvergenz)**.** Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen. Die zugehörige Reihe $\sum_{k=1}^{\infty} a_k$ heißt *absolut konvergent*, falls die Reihe $\sum_{k=1}^{\infty} |a_k|$ konvergiert.

Satz 4.1.26. *Jede absolut konvergente Reihe ist konvergent.*

Beweis. Da wegen der Dreiecksungleichung für alle $p \geq n$ gilt, dass

$$\left|\sum_{k=n}^{p} a_k\right| \;\leq\; \sum_{k=n}^{p} |a_k| \;,$$

folgt die Behauptung unmittelbar aus dem Cauchy-Kriterium in Satz 4.1.22. □

Das folgende Majorantenkriterium ist nützlich, da man damit die (absolute) Konvergenz einer Reihe auf die Konvergenz einer anderen (einfacheren) Reihe zurückführen kann.

Satz 4.1.27 (Majoranten- und Minorantenkriterium)**.** *Es seien* $(a_n)_{n\in\mathbb{N}}$ *und* $(b_n)_{n\in\mathbb{N}}$ *Folgen komplexer Zahlen.*

(i) Ist $\sum_{k=1}^{\infty} b_k$ *absolut konvergent und gibt es eine reelle Zahl* $c > 0$ *mit* $|a_n| \leq c \cdot |b_n|$ *für alle* $n \in \mathbb{N}$*, dann ist auch* $\sum_{k=1}^{\infty} a_k$ *absolut konvergent.*

(ii) Ist $\sum_{k=1}^{\infty} b_k$ *nicht absolut konvergent und gibt es eine reelle Zahl* $c > 0$ *mit* $|a_n| \geq c \cdot |b_n|$ *für alle* $n \in \mathbb{N}$*, dann ist auch* $\sum_{k=1}^{\infty} a_k$ *nicht absolut konvergent.*

Beweis. Zu (i): Wegen Korollar 4.1.24 genügt es zu zeigen, dass die Folge der Partialsummen der Reihe $\sum_{k=1}^{\infty} |a_k|$ beschränkt ist. Da $\sum_{k=1}^{\infty} |b_k|$ konvergiert, ist die Folge der Partialsummen dieser Reihe nach Lemma 4.1.12 durch eine Zahl $B > 0$ beschränkt. Folglich gilt für alle $n \in \mathbb{N}$:

$$\sum_{k=1}^{n} |a_k| \;\leq\; \sum_{k=1}^{n} c \cdot |b_k| \;=\; c \cdot \sum_{k=1}^{n} |b_k| \;\leq\; c \cdot B \;.$$

Teil (ii) beweist man analog. □

Beispiele.

(i) Die Reihe $\sum_{k=1}^{\infty} \frac{k!}{k^k}$ ist absolut konvergent. Es gilt

$$\frac{k!}{k^k} \;=\; \frac{1 \cdot 2 \cdot 3 \cdots k}{k \cdot k \cdot k \cdots k} \;\leq\; \frac{2}{k^2} \qquad \text{für } k \geq 2.$$

Folglich ist die Reihe $\sum_{k=1}^{\infty} \frac{2}{k^2}$ eine absolut konvergente Majorante.

(ii) Ist $0 < p < 1$, so divergiert die Reihe $\sum_{k=1}^{\infty} \frac{1}{k^p}$, da $\sum_{k=1}^{\infty} \frac{1}{k}$ eine divergente Minorante ist.

Das folgende Quotientenkriterium erhält man durch Anwendung des Majorantenkriteriums mit einer geometrischen Reihe als Vergleichsreihe.

Satz 4.1.28 (Quotientenkriterium)**.** *Es sei* $(a_n)_{n\in\mathbb{N}}$ *eine Folge komplexer Zahlen.*

(i) Gibt es ein $q < 1$*, so dass* $|a_{n+1}| \leq q \cdot |a_n|$ *für alle* $n \in \mathbb{N}$*, dann ist die Reihe* $\sum_{k=1}^{\infty} a_k$ *absolut konvergent.*

(ii) Gilt $|a_n| > 0$ *und* $|a_{n+1}| \geq |a_n|$ *für alle* $n \in \mathbb{N}$*, dann ist die Reihe* $\sum_{k=1}^{\infty} a_k$ *nicht absolut konvergent.*

Beweis. Zu (i): Mit vollständiger Induktion kann man leicht zeigen, dass

$$|a_n| \;\leq\; q^{n-1} \cdot |a_1| \qquad \text{für alle } n \in \mathbb{N}.$$

Folglich gilt für die n-te Partialsumme

$$\sum_{k=1}^{n} |a_k| \;\leq\; |a_1| \cdot \sum_{k=1}^{n} q^{k-1} \;=\; |a_1| \cdot \sum_{k=0}^{n-1} q^k \;=\; |a_1| \cdot \frac{1-q^n}{1-q} \;\leq\; \frac{|a_1|}{1-q} \;.$$

Die Folge der Partialsummen ist also beschränkt, so dass die Reihe nach Korollar 4.1.24 absolut konvergiert.

Zu (ii): Mit vollständiger Induktion folgt, dass $|a_n| \geq |a_1| > 0$ für alle $n \in \mathbb{N}$. Nach dem Minorantenkriterium aus Satz 4.1.27 (ii) ist die Reihe $\sum_{k=1}^{\infty} a_k$ also nicht absolut konvergent. □

Beispiele.

(i) Für $z \in \mathbb{C}$ ist die Reihe $\sum_{k=0}^{\infty} \frac{z^k}{k!}$ absolut konvergent. Dies folgt aus dem Quotientenkriterium in Satz 4.1.28, da

$$\frac{|z|^{n+1}}{(n+1)!} \;=\; \frac{|z|}{n+1} \cdot \frac{|z|^n}{n!}$$

Folglich ist die Bedingung aus dem Quotientenkriterium für alle $n \geq |z|$ erfüllt. Da die ersten n Summanden keinen Einfluss auf die Konvergenz der Reihe haben, ist die Behauptung damit gezeigt.

(ii) Obwohl die Reihe $\sum_{k=1}^{\infty} \frac{1}{k^2}$ absolut konvergent ist (siehe oben), kann man das nicht einfach mit dem Quotientenkriterium beweisen. Es gilt zwar

$$\frac{\frac{1}{(n+1)^2}}{\frac{1}{n^2}} \;=\; \left(\frac{n}{n+1}\right)^2 \;<\; 1 \;,$$

doch es gibt kein $q < 1$, so dass der Quotient für alle $n \in \mathbb{N}$ durch q nach oben beschränkt ist.

Ähnlich wie das Quotientenkriterium erhält man auch das folgende Wurzelkriterium.

Satz 4.1.29 (Wurzelkriterium)**.** *Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen.*

(i) Gibt es ein $q < 1$, so dass $\sqrt[n]{|a_n|} \leq q$ für alle $n \in \mathbb{N}$, dann ist die Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent.

(ii) Gilt $\sqrt[n]{|a_n|} \geq 1$ für alle $n \in \mathbb{N}$, dann ist die Reihe $\sum_{k=1}^{\infty} a_k$ nicht absolut konvergent.

Beweis. Behauptung (i) folgt aus dem Majorantenkriterium in Satz 4.1.27 (i), da $\sum_{k=1}^{\infty} q^k$ absolut konvergent ist. Behauptung (ii) folgt aus dem Minorantenkriterium in Satz 4.1.27 (ii), da $\sum_{k=1}^{\infty} 1^k$ divergent ist. □

Beispiel. Es sei $(a_n)_{n\in\mathbb{N}}$ die durch

$$a_n := \begin{cases} 2^{-n} & \text{falls } n \text{ gerade,} \\ 3^{-n} & \text{falls } n \text{ ungerade,} \end{cases}$$

definierte Folge. Dann ist die Reihe $\sum_{k=1}^{\infty} a_k$ nach dem Wurzelkriterium absolut konvergent. Es gilt nämlich

$$\sqrt[n]{a_n} := \begin{cases} \frac{1}{2} & \text{falls } n \text{ gerade,} \\ \frac{1}{3} & \text{falls } n \text{ ungerade.} \end{cases}$$

Folglich ist $\sqrt[n]{a_n} \leq \frac{1}{2} < 1$ für alle $n \in \mathbb{N}$.

Bemerkung. Satz 4.1.28 und Satz 4.1.29 gelten auch noch, wenn man „für alle $n \in \mathbb{N}$“ durch „für *fast* alle $n \in \mathbb{N}$“ ersetzt (mit der Bedeutung: „für alle außer endlich vielen $n \in \mathbb{N}$“).

Definition 4.1.30 (Alternierende Reihen)**.** Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge reeller Zahlen. Wir nennen die zugehörige Reihe $\sum_{k=1}^{\infty} a_k$ *alternierend*, wenn die Folgenglieder abwechselnd positiv und negativ sind.

Beispiel. Die Reihen $\sum_{k=1}^{\infty}(-1)^k$ und $\sum_{k=1}^{\infty} \frac{(-1)^k}{k}$ sind alternierend.

Satz 4.1.31 (Leibniz-Kriterium)**.** *Es sei $\sum_{k=1}^{\infty} a_k$ eine alternierende Reihe. Ist die Folge $(|a_n|)_{n\in\mathbb{N}}$ eine monoton fallende Nullfolge, dann konvergiert die Reihe $\sum_{k=1}^{\infty} a_k$.*

Beweis. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $a_1 < 0$ (den Fall $a_1 > 0$ kann man völlig analog behandeln). Dann gibt es eine Folge von nicht-negativen rellen Zahlen $(b_n)_{n\in\mathbb{N}}$ mit $a_n = (-1)^n \cdot b_n$ für alle $n \in \mathbb{N}$. Die Folge (b_n) ist nach Voraussetzung eine monoton fallende Nullfolge. Für die Partialsummen $s_n := \sum_{k=1}^{n} a_n$ der Reihe $\sum_{k=1}^{\infty} a_k$ gilt also

$$s_{2n+2} - s_{2n} = b_{2n+2} - b_{2n+1} \leq 0 \ , \tag{4.1}$$

$$s_{2n+3} - s_{2n+1} = -b_{2n+3} + b_{2n+2} \geq 0 \tag{4.2}$$

und

$$s_{2n} - s_{2n+1} = b_{2n+1} \geq 0 \tag{4.3}$$

für alle $n \in \mathbb{N}$. Folglich ist die Teilfolge $(s_{2n})_{n\in\mathbb{N}}$ wegen (4.1) monoton fallend und die Teilfolge $(s_{2n+1})_{n\in\mathbb{N}}$ ist wegen (4.2) monoton wachsend. Außerdem gilt wegen (4.3), dass $s_{2n} \geq s_{2n+1}$ für alle $n \in \mathbb{N}$. Da (b_n) eine Nullfolge ist, gibt es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ mit

$$0 \leq s_{2n} - s_{2n+1} < \varepsilon \qquad \text{für alle } n \text{ mit } 2n \geq n_0.$$

Wir zeigen jetzt mit Hilfe des Cauchy-Kriterium in Satz 4.1.22, dass die Reihe $\sum_{k=1}^{\infty} a_k$ konvergiert. Dazu genügt es zu zeigen, dass

$$\left|\sum_{k=n}^{p} a_k\right| \;<\; \varepsilon \qquad \text{für alle } p \geq n > n_0. \tag{4.4}$$

Wir nehmen im Folgenden an, dass $p = 2q$ gerade und $n = 2m+1$ ungerade ist (die anderen drei Fälle kann man analog behandeln). Dann gilt

$$\begin{aligned}
\left|\sum_{k=n}^{p} a_k\right| \;=\; \left|\sum_{k=2m+1}^{2q} a_k\right| \;&=\; s_{2m} - s_{2q} && \text{wegen (4.1)},\\
&\leq\; s_{2m} - s_{2q+1} && \text{wegen (4.3)},\\
&\leq\; s_{2m} - s_{2m+1} && \text{wegen (4.2)},\\
&<\; \varepsilon && \text{wegen (4.4)}.
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Beispiel. Die sogenannte *Leibniz-Reihe* $\sum_{k=1}^{\infty} \frac{(-1)^k}{k}$ ist nach dem Leibniz-Kriterium konvergent.

Zum Schluss dieses Abschnitts geben wir noch zwei interessante Resultate über absolut konvergente Reihen ohne Beweis an. Zunächst benötigen wir jedoch die folgende Definition der Umordnung einer Folge.

Definition 4.1.32 (Umordnung einer Folge)**.** Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen und $\pi : \mathbb{N} \to \mathbb{N}$ eine bijektive Abbildung. Dann nennt man die Folge $(a_{\pi(n)})_{n\in\mathbb{N}}$ eine *Umordnung* von (a_n).

Satz 4.1.33. *Es sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen, so dass die zugehörige Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent ist. Ist $\pi : \mathbb{N} \to \mathbb{N}$ eine bijektive Abbildung, so ist die zu der umgeordneten Folge $(a_{\pi(n)})_{n\in\mathbb{N}}$ gehörende Reihe $\sum_{k=1}^{\infty} a_{\pi(k)}$ auch absolut konvergent und die Grenzwerte der beiden Reihen stimmen überein.*

Bemerkung. Satz 4.1.33 gilt nicht, wenn man „absolut konvergent“ durch „konvergent“ ersetzt. Durch Umordnung kann aus einer konvergenten Reihe, die nicht absolut konvergent ist, sowohl eine divergente Reihe als auch eine konvergente Reihe mit verschiedenem Grenzwert entstehen.

Satz 4.1.34 (Cauchy-Produkt)**.** *Es seien $\sum_{k=0}^{\infty} a_k$ und $\sum_{k=0}^{\infty} b_k$ absolut konvergente Reihen. Für $n \in \mathbb{N}_0$ sei $c_n := \sum_{k=0}^{n} a_k b_{n-k}$. Dann konvergiert die Reihe $\sum_{n=0}^{\infty} c_n$ absolut und es gilt*

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) \;=\; \sum_{n=0}^{\infty} c_n \;=\; \left(\sum_{k=0}^{\infty} a_k\right)\cdot\left(\sum_{k=0}^{\infty} b_k\right) \;.$$

4.1.4 Potenzreihen

Wir betrachten in diesem Abschnitt Reihen, die von einer komplexen Variablen z abhängen, sogenannte Potenzreihen.

Definition 4.1.35 (Potenzreihen)**.** Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen und $z_0 \in \mathbb{C}$. Dann betrachten wir für beliebige $z \in \mathbb{C}$ die *Potenzreihe*

$$\sum_{k=0}^{\infty} a_k (z - z_0)^k \ .$$

Die komplexe Zahl z_0 heißt *Entwicklungspunkt* der Potenzreihe.

Bemerkung. Wir werden im Folgenden fast nur Potenzreihen mit dem Entwicklungspunkt $z_0 = 0$ betrachten. Wir können das ohne Beschränkung der Allgemeinheit tun, da man immer durch einen Variablenwechsel von z auf $z - z_0$ übergehen kann.

Beispiele.

(i) Wir können für $z \in \mathbb{C}$ die geometrische Reihe $\sum_{k=0}^{\infty} z^k$ als spezielle Potenzreihe mit $a_n := 1$ für alle $n \in \mathbb{N}_0$ und $z_0 := 0$ auffassen. Wie wir weiter oben gezeigt haben, konvergiert diese Potenzreihe für $|z| < 1$ und divergiert für $|z| > 1$.

(ii) Für beliebiges $z_0 \in \mathbb{C}$ konvergiert die Potenzreihe $\sum_{k=0}^{\infty} \frac{(z-z_0)^k}{k!}$ für alle $z \in \mathbb{C}$ (siehe oben).

(iii) Für den Entwicklungspunkt $z = z_0$ konvergiert eine beliebige Potenzreihe $\sum_{k=0}^{\infty} a_k (z - z_0)^k$ immer gegen den Wert a_0.

Lemma 4.1.36. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen. Konvergiert die Potenzreihe $\sum_{k=0}^{\infty} a_k z^k$ für ein $z = z_1 \in \mathbb{C}$, dann konvergiert sie absolut für alle $z \in \mathbb{C}$ mit $|z| < |z_1|$.*

Beweis. Wegen Lemma 4.1.23 ist $(a_n z_1^n)_{n\in\mathbb{N}_0}$ eine Nullfolge. Folglich gibt es ein $c > 0$ mit $|a_n z_1^n| \le c$ für alle $n \in \mathbb{N}_0$. Es sei nun $z \in \mathbb{C}$ mit $|z| < |z_1|$ und $q := \left|\frac{z}{z_1}\right| < 1$. Dann gilt

$$|a_n z^n| \ = \ \left| \left(\frac{z}{z_1}\right)^n \cdot a_n z_1^n \right| \ \le \ c \cdot \left|\frac{z}{z_1}\right|^n \ = \ c \cdot q^n \ .$$

Aufgrund des Majorantenkriteriums ist die Reihe $\sum_{k=0}^{\infty} a_k z^k$ also absolut konvergent. □

Definition 4.1.37 (Konvergenzbereich, Konvergenzradius)**.** Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen und $\sum_{k=0}^{\infty} a_k z^k$ die zugehörige Potenzreihe. Dann nennt man die Menge

$$C \;:=\; \left\{ z \in \mathbb{C} \;\middle|\; \sum_{k=0}^{\infty} a_k z^k \text{ konvergiert} \right\}$$

den *Konvergenzbereich* der Potenzreihe. Außerdem nennt man

$$\rho \;:=\; \sup\{|z| \mid z \in K\}$$

den *Konvergenzradius* der Potenzreihe.

Bemerkung. Da 0 im Konvergenzbereich jeder Potenzreihe liegt, ist der Konvergenzradius ρ immer nicht-negativ. Ist der Konvergenzradius unendlich groß, so konvergiert die Potenzreihe wegen Lemma 4.1.36 für alle $z \in \mathbb{C}$.

Satz 4.1.38. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen und $\sum_{k=0}^{\infty} a_k z^k$ die zugehörige Potenzreihe mit Konvergenzradius ρ. Dann gilt*

(i) Die Potenzreihe ist für alle $z \in \mathbb{C}$ mit $|z| < \rho$ absolut konvergent.

(ii) Die Potenzreihe ist für alle $z \in \mathbb{C}$ mit $|z| > \rho$ divergent.

Beweis. Zu (i): Es sei $z \in \mathbb{C}$ mit $|z| < \rho$. Dann gibt es nach Definition von ρ ein $z_1 \in \mathbb{C}$ mit $|z| < |z_1| < \rho$, so dass z_1 im Konvergenzbereich der Potenzreihe liegt. Die Behauptung folgt dann sofort mit Lemma 4.1.36. Teil (ii) folgt unmittelbar aus der Definition des Konvergenzradius ρ. □

Bemerkung.

(i) Satz 4.1.38 kann man wie folgt zusammenfassen. Für den Konvergenzbereich C und den Konvergenzradius ρ einer Potenzreihe gilt

$$\{z \in \mathbb{C} \mid |z| < \rho\} \;\subseteq\; C \;\subseteq\; \{z \in \mathbb{C} \mid |z| \leq \rho\} \;.$$

(ii) Betrachtet man in der Situation von Satz 4.1.38 ein $z \in \mathbb{C}$ mit $|z| = \rho$, so kann man keine allgemeingültige Aussage bezüglich der Konvergenz oder Divergenz der Potenzreihe im Punkt z machen. Wir illustrieren dies im Folgenden anhand einiger Beispiele.

Beispiele.

(i) Der Konvergenzradius der geometrischen Reihe $\sum_{k=0}^{\infty} z^k$ ist $\rho = 1$. Die geometrische Reihe divergiert jedoch für alle $z \in \mathbb{C}$ mit $|z| = \rho$, da die zugehörige Folge $(z^n)_{n\in\mathbb{N}_0}$ offenbar keine Nullfolge ist.

(ii) Wir betrachten die Potenzreihe $\sum_{k=1}^{\infty} \frac{z^k}{k}$. Für $z = -1$ erhält man die konvergente Leibnizreihe und für $z = 1$ die divergente harmonische Reihe. Daraus kann man wegen Satz 4.1.38 bereits schließen, dass der Konvergenzradius dieser Potenzreihe $\rho = 1$ ist. Insbesondere liegt hier offenbar kein einheitliches Konvergenzverhalten der Punkte $z \in \mathbb{C}$ mit $|z| = \rho$ vor.

(iii) Wir werden später zeigen, dass die Potenzreihe $\sum_{k=1}^{\infty} \frac{z^k}{k^2}$ den Konvergenzradius $\rho = 1$ hat. Da die Potenzreihe für $z = 1$ absolut konvergent ist, folgt aus dem Majorantenkriterium, dass sie für alle $z \in \mathbb{C}$ mit $|z| = \rho$ absolut konvergiert.

Zur konkreten Berechnung des Konvergenzradius einer Potenzreihe kann man das Quotienten- oder das Wurzelkriterium aus dem letzten Abschnitt verwenden. Die folgenden Sätze präzisieren diese Einsicht.

Satz 4.1.39. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen und $\sum_{k=0}^{\infty} a_k z^k$ die zugehörige Potenzreihe mit Konvergenzradius ρ. Für $n \in \mathbb{N}_0$ sei $b_n := \sqrt[n]{|a_n|}$. Dann gilt:*

(i) Geht die Folge $(b_n)_{n\in\mathbb{N}_0}$ gegen unendlich, so ist $\rho = 0$.

(ii) Konvergiert $(b_n)_{n\in\mathbb{N}_0}$ gegen den Grenzwert $b > 0$, so ist $\rho = \frac{1}{b}$.

(iii) Ist $(b_n)_{n\in\mathbb{N}_0}$ eine Nullfolge, so ist $\rho = \infty$.

Beweis. Wir beweisen nur (ii). Ist $\lim_{n\to\infty} \sqrt[n]{|a_n|} = \lim_{n\to\infty} b_n = b$, so ist

$$\lim_{n\to\infty} \sqrt[n]{|a_n z^n|} \;=\; \lim_{n\to\infty} (|z| \sqrt[n]{|a_n|}) \;=\; |z| \cdot \lim_{n\to\infty} \sqrt[n]{|a_n|} \;=\; |z| \cdot b \;.$$

Ist also $|z| < \frac{1}{b}$, so ist die Potenzreihe wegen Satz 4.1.29 (i) absolut konvergent. Ist $|z| > \frac{1}{b}$, so ist die Potenzreihe wegen Satz 4.1.29 (ii) divergent. Folglich ist der Konvergenzradius der Potenzreihe $\rho = \frac{1}{b}$. Die beiden anderen Aussagen des Satzes beweist man analog. □

Satz 4.1.40. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge komplexer Zahlen mit $a_n \neq 0$ für alle $n \in \mathbb{N}_0$ und $\sum_{k=0}^{\infty} a_k z^k$ die zugehörige Potenzreihe mit Konvergenzradius ρ. Für $n \in \mathbb{N}_0$ sei $b_n := \frac{|a_{n+1}|}{|a_n|}$. Dann gilt:*

(i) Geht die Folge $(b_n)_{n\in\mathbb{N}_0}$ gegen unendlich, so ist $\rho = 0$.

(ii) Konvergiert $(b_n)_{n\in\mathbb{N}_0}$ gegen den Grenzwert $b > 0$, so ist $\rho = \frac{1}{b}$.

(iii) Ist $(b_n)_{n\in\mathbb{N}_0}$ eine Nullfolge, so ist $\rho = \infty$.

Beweis. Wir beweisen wieder nur (ii). Ist $\lim_{n\to\infty} \frac{|a_{n+1}|}{|a_n|} = \lim_{n\to\infty} b_n = b$, so ist

$$\lim_{n\to\infty} \frac{|a_{n+1}z^{n+1}|}{|a_n z^n|} \;=\; \lim_{n\to\infty} (|z|\frac{|a_{n+1}|}{|a_n|}) \;=\; |z| \cdot \lim_{n\to\infty} \frac{|a_{n+1}|}{|a_n|} \;=\; |z| \cdot b \;.$$

Ist also $|z| < \frac{1}{b}$, so ist die Potenzreihe wegen Satz 4.1.28 (i) absolut konvergent. Ist $|z| > \frac{1}{b}$, so ist die Potenzreihe wegen Satz 4.1.28 (ii) divergent. Folglich ist der Konvergenzradius der Potenzreihe $\rho = \frac{1}{b}$. Die beiden anderen Aussagen des Satzes beweist man analog. □

Beispiele. Wir betrachten die Potenzreihe $\sum_{k=0}^{\infty} a_k z^k$.

(i) Ist $a_n = \frac{1}{n}$ für $n \in \mathbb{N}$, dann ist $\frac{|a_{n+1}|}{|a_n|} = \frac{n}{n+1}$ und die Folge $(\frac{|a_{n+1}|}{|a_n|})_{n\in\mathbb{N}}$ konvergiert gegen 1. Nach Satz 4.1.40 ist der Konvergenzradius der Potenzreihe $\rho = \frac{1}{1} = 1$ (wie bereits weiter oben festgestellt). Dasselbe Ergebnis kann man prinzipiell auch mit dem Wurzelkriterium (Satz 4.1.39) erhalten.

(ii) Ist $a_n = \frac{1}{n^2}$ für $n \in \mathbb{N}$, dann ist

$$\frac{|a_{n+1}|}{|a_n|} \;=\; \frac{n^2}{n^2+2n+1} \;=\; \frac{1}{1+\frac{2}{n}+\frac{1}{n^2}}$$

und die Folge $(\frac{|a_{n+1}|}{|a_n|})_{n\in\mathbb{N}}$ konvergiert folglich gegen 1. Nach Satz 4.1.40 ist der Konvergenzradius der Potenzreihe $\rho = \frac{1}{1} = 1$.

(iii) Ist $a_n = n^n$, so ist $\sqrt[n]{|a_n|} = n$ und die Folge $(\sqrt[n]{|a_n|})_{n\in\mathbb{N}}$ geht gegen unendlich. Folglich ist der Konvergenzradius der Potenzreihe $\rho = 0$ und der Konvergenzbereich besteht folglich nur aus dem Nullpunkt.

(iv) Ist $a_n = \frac{1}{n!}$, so ist $\frac{|a_{n+1}|}{|a_n|} = \frac{n!}{(n+1)!} = \frac{1}{n+1}$ und die Folge $(\frac{|a_{n+1}|}{|a_n|})_{n\in\mathbb{N}}$ ist eine Nullfolge. Folglich ist der Konvergenzradius der Potenzreihe unendlich und die Potenzreihe konvergiert für alle $z \in \mathbb{C}$.

Die im letzten Beispiel betrachtete Potenzreihe spielt eine besondere Rolle, da sie als Funktion aufgefasst die bekannte Exponentialfunktion definiert. Wir beschäftigen uns im folgenden Abschnitt näher mit dieser Funktion.

4.1.5 Exponentialfunktion und Logarithmus

Wir führen zunächst die Euler'sche Zahl e als Grenzwert einer Folge ein. Als technisches Hilfsmittel benötigen wir dabei die Bernoulli-Ungleichung und die Binomialformel.

Lemma 4.1.41 (Bernoulli-Ungleichung)**.** *Ist $x \in \mathbb{R}$ mit $x \geq -1$, so gilt für alle $n \in \mathbb{N}_0$*

$$(1+x)^n \;\geq\; 1 + n \cdot x \;.$$

Beweis. Wir zeigen die Behauptung mitels vollständiger Induktion. Induktionsanfang: Die Behauptung ist offenbar wahr für $n = 0$, da $(1+x)^0 = 1 = 1 + 0 \cdot x$ für alle $x \in \mathbb{R}$. Induktionsschluss: Wir nehmen an, dass die Behauptung für ein beliebiges, fest gewähltes $n \in \mathbb{N}_0$. Dann gilt

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \\
&\geq (1+n\cdot x)\cdot(1+x) \quad \text{nach Induktionsannahme und da } x \geq -1, \\
&= 1 + (n+1)\cdot x + x^2 \\
&\geq 1 + (n+1)\cdot x \qquad \text{da } x^2 \geq 0.
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Lemma 4.1.42 (Binomialformel)**.** *Es seien $x, y \in \mathbb{C}$ und $n \in \mathbb{N}$. Dann gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \ ,$$

wobei der Binomialkoeffizient $\binom{n}{k}$ *wie folgt definiert ist:*

$$\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)\cdot\cdots\cdot(n-k+2)\cdot(n-k+1)}{k\cdot(k-1)\cdot\cdots\cdot 2\cdot 1} \ .$$

Beweis. Vollständige Induktion über n. □

Satz 4.1.43 (Euler'sche Zahl e)**.** *Die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_n := \left(1+\frac{1}{n}\right)^n$ konvergiert. Der Grenzwert wird mit e bezeichnet und* Euler'sche Zahl *genannt.*

Beweis. Wir zeigen, dass die Folge (a_n) monoton steigend und beschränkt ist. Um die Monotonie zu zeigen, betrachten wir den Quotienten $\frac{a_{n+1}}{a_n}$ und zeigen, dass er immer größer als 1 ist. Denn es gilt

$$\begin{aligned}
\frac{a_{n+1}}{a_n} &= \frac{\left(1+\frac{1}{n+1}\right)^{n+1}}{\left(1+\frac{1}{n}\right)^n} \\
&= \frac{\frac{(n+2)^{n+1}}{(n+1)^{n+1}}}{\frac{(n+1)^n}{n^n}} \\
&= \frac{n+2}{n+1}\cdot\left(\frac{(n+2)\cdot n}{(n+1)^2}\right)^n \\
&= \left(1+\frac{1}{n+1}\right)\cdot\left(1-\frac{1}{(n+1)^2}\right)^n \\
&\geq \left(1+\frac{1}{n+1}\right)\cdot\left(1-\frac{n}{(n+1)^2}\right) \qquad \text{wegen Lemma 4.1.41,} \\
&= 1 + \frac{1}{n+1} - \frac{n}{(n+1)^2} - \frac{n}{(n+1)^3} \\
&= 1 + \frac{1}{(n+1)^3}
\end{aligned}$$

Es bleibt also zu zeigen, dass die Folge (a_n) beschränkt ist. Es gilt

$$a_n \;=\; \left(1+\frac{1}{n}\right)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} \;.$$

Es gilt

$$\begin{aligned} \binom{n}{k} \cdot \frac{1}{n^k} \;&=\; \frac{n \cdot (n-1) \cdot \cdots \cdot (n-k+2) \cdot (n-k+1)}{k! \cdot n^k} \\ &=\; \frac{1}{k!} \cdot \frac{n}{n} \cdot \frac{n-1}{n} \cdot \cdots \cdot \frac{n-k+1}{n} \;. \end{aligned}$$

Für $k \geq 1$ gilt daher $\binom{n}{k} \cdot \frac{1}{n^k} \leq \frac{1}{k!} \leq \frac{1}{2^{k-1}}$. Folglich gilt

$$a_n \;=\; 1+1+\sum_{k=2}^{n} \binom{n}{k} \frac{1}{n^k} \;\leq\; 1+\sum_{k=1}^{n} \frac{1}{2^{k-1}} \;<\; 1+\sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k \;=\; 3 \;.$$

Damit ist der Beweis fertig. □

Bemerkung. Aus dem Beweis von Satz 4.1.43 folgt, dass $e \leq 3$. Andererseits gilt $e \geq a_2 = \left(1+\frac{1}{2}\right)^2 = \frac{9}{4}$. Genauer gesagt ist e ungefähr 2.718282.

Lemma 4.1.44. *Die Reihe $\sum_{k=0}^{\infty} \frac{1}{k!}$ konvergiert gegen den Grenzwert e.*

Beweis. Es sei $a_n := \left(1+\frac{1}{n}\right)^n$ für alle $n \in \mathbb{N}$, so dass e nach Definition der Grenzwert der Folge (a_n) ist. Weiter sei $s_n := \sum_{k=0}^{n} \frac{1}{k!}$ die n-te Partialsumme der Reihe $\sum_{k=0}^{\infty} \frac{1}{k!}$. Dann ist die Folge (s_n) monoton steigend und wir müssen zeigen, dass sie gegen e konvergiert. Bereits im Beweis von Satz 4.1.43 haben wir gezeigt, dass $\binom{n}{k} \cdot \frac{1}{n^k} \leq \frac{1}{k!}$. Daraus folgt

$$a_n \;=\; \left(1+\frac{1}{n}\right)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} \;\leq\; \sum_{k=0}^{n} \frac{1}{k!} \;=\; s_n \;.$$

Es bleibt also zu zeigen, dass die Folge (s_n) nach oben durch e beschränkt ist. Dann folgt aus dem Vergleichskriterium in Satz 4.1.14 (i), dass sie gegen den Grenzwert e konvergiert.

Aus dem Beweis von Satz 4.1.43 folgt, dass für $m \geq n$ gilt:

$$\begin{aligned} a_m \;&=\; \sum_{k=0}^{m} \binom{m}{k} \frac{1}{m^k} \\ &=\; \sum_{k=0}^{m} \frac{1}{k!} \cdot \frac{m}{m} \cdot \frac{m-1}{m} \cdot \cdots \cdot \frac{m-k+1}{m} \\ &\geq\; \sum_{k=0}^{n} \frac{1}{k!} \cdot \frac{m}{m} \cdot \frac{m-1}{m} \cdot \cdots \cdot \frac{m-k+1}{m} \;=:\; b_m \;. \end{aligned}$$

Mit Satz 4.1.17 und Lemma 4.1.16 folgt, dass

$$s_n \;=\; \sum_{k=0}^{n} \frac{1}{k!} \;=\; \lim_{m\to\infty} b_m \;\leq\; \lim_{m\to\infty} a_m \;\leq\; e \qquad \text{für alle } n \in \mathbb{N}.$$

Damit ist der Beweis abgeschlossen. □

Wir definieren jetzt die Exponentialfunktion als spezielle Potenzreihe.

Definition 4.1.45 (Exponentialfunktion)**.** Die *Exponentialfunktion* $\exp : \mathbb{C} \to \mathbb{C}$ ist definiert durch

$$\exp(z) \;:=\; \sum_{k=0}^{\infty} \frac{z^k}{k!} \qquad \text{für alle } z \in \mathbb{C}.$$

Bemerkung.

(i) Es gilt $\exp(0) = \sum_{k=0}^{\infty} \frac{0^k}{k!} = 1$ und $\exp(1) = \sum_{k=0}^{\infty} \frac{1^k}{k!} = e$.

(ii) Die Exponentialfunktion besitzt eine sehr spezielle Eigenschaft, die im Zusammenhang mit der beschreibung von Wachstumsprozessen in der Natur von großer Bedeutung ist. Es sei $f(0) = 1$ der Bestand einer Population zum Zeitpunkt 0 und $f(t)$ der Bestand zu einem späteren Zeitpunkt $t \geq 0$. Wenn sich jedes Individuum der Population zum Zeitpunkt t weiter so vermehrt, wie das erste Individuum zum Zeitpunkt null, so ist die Population nach weiteren s Zeiteinheiten auf die Größe $f(s+t) = f(s) \cdot f(t)$ angewachsen. Man interessiert sich daher für Funktionen $f : \mathbb{C} \to \mathbb{C}$, die die folgende Funktionalgleichung erfüllen:

$$f(x+y) \;=\; f(x) \cdot f(y) \qquad \text{für alle } x, y \in \mathbb{C}. \tag{4.5}$$

Lemma 4.1.46. *Für die Exponentialfunktion* $\exp : \mathbb{C} \to \mathbb{C}$ *gilt*

$$\exp(x+y) \;=\; \exp(x) \cdot \exp(y) \qquad \textit{für alle } x, y \in \mathbb{C}.$$

Beweis. Der Beweis basiert im Wesentlichen auf Satz 4.1.34 über das Cauchy-Produkt. Für $x, y \in \mathbb{C}$ gilt:

$$\begin{aligned}
\exp(x) \cdot \exp(y) \;&=\; \left(\sum_{k=0}^{\infty} \frac{x^k}{k!}\right) \cdot \left(\sum_{k=0}^{\infty} \frac{x^k}{k!}\right) \\
&=\; \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^k}{k!} \cdot \frac{y^{n-k}}{(n-k)!} \\
&=\; \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{n!} \cdot \binom{n}{k} \cdot x^k \cdot y^{n-k} \\
&=\; \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} \\
&=\; \exp(x+y) \;.
\end{aligned}$$

Damit ist die Behauptung bewiesen. □

Bemerkung. Für $c \in \mathbb{C}$ erfüllt auch die Funktion $f : \mathbb{C} \to \mathbb{C}$ mit $f(z) := \exp(c \cdot z)$ die Funktionalgleichung (4.5). Man kann zeigen, dass jede Funktion f, die (4.5) erfüllt, von dieser Form für ein $c \in \mathbb{C}$ ist. Insbesondere ist exp die einzige Funktion, die (4.5) erfüllt und an der Stelle 1 gleich e ist.

Wir halten im folgenden Lemma einige weitere Eigenschaften der Exponentialfunktion fest.

Lemma 4.1.47. *Für die Exponentialfunktion* exp *gilt:*

(i) $\exp(z) \neq 0$ *für alle* $z \in \mathbb{C}$.

(ii) $\exp(-z) = \frac{1}{\exp(z)}$ *für alle* $z \in \mathbb{C}$.

(iii) $\exp(x) \in \mathbb{R}_{>0}$ *für alle* $x \in \mathbb{R}$.

(iv) $\exp(x) < \exp(y)$ *für alle* $x, y \in \mathbb{R}$ *mit* $x < y$, *d.h.* exp *ist auf* $\mathbb{R}$ *streng monoton wachsend.*

Beweis. Nach Lemma 4.1.46 gilt

$$1 \;=\; \exp(0) \;=\; \exp(z - z) \;=\; \exp(z) \cdot \exp(-z) \qquad \text{für alle } z \in \mathbb{C}.$$

Daraus folgen sofort Behauptung (i) und (ii).

Zu (iii): Aus der Definition der Exponentialfunktion folgt unmittelbar, dass $\exp(x) \in \mathbb{R}$ für alle $x \in \mathbb{R}$. Außerdem ist $\exp(x) \geq 0$ für alle $x \in \mathbb{R}$, da $\exp(x) = \exp(\frac{x}{2})^2$. Die Tatsache, dass sogar $\exp(x) > 0$ folgt dann unmittelbar aus (i).

Zu (iv): Da

$$\exp(y) \;=\; \exp(x) \cdot \exp(y - x) \qquad \text{und} \qquad \exp(x) > 0 \;,$$

bleibt zu zeigen, dass $\exp(r) > 1$ für $r > 0$. Dies folgt aus der Definition der Exponentialfunktion, da

$$\exp(r) \;=\; \sum_{k=0}^{\infty} \frac{r^k}{k!} \;\geq\; 1 + r \;>\; 1 \;.$$

Dabei erhält man die erste Ungleichung durch Weglassen aller Summanden mit Index $k \geq 2$. □

Satz 4.1.48. *Für jede rationale Zahl* $q \in \mathbb{Q}$ *gilt* $\exp(q) = e^q$.

Beweis. Zunächst kann man leicht durch vollständige Induktion zeigen, dass $\exp(n) = e^n$ für alle $n \in \mathbb{N}_0$. Im Induktionsschritt wendet man die Funktionalgleichung aus Lemma 4.1.46 an. Wir betrachten nun ein $m \in \mathbb{N}$:

$$e \;=\; \exp\left(\frac{m}{m}\right) \;=\; \exp\left(\sum_{k=1}^{m} \frac{1}{m}\right) \;=\; \prod_{k=1}^{m} \exp\left(\frac{1}{m}\right) \;=\; \exp\left(\frac{1}{m}\right)^m \;.$$

Folglich ist $\exp(\frac{1}{m})$ die m-te Wurzel aus e, also

$$\exp\left(\frac{1}{m}\right) \;=\; \sqrt[m]{e} \;=\; e^{\frac{1}{m}} \;.$$

Folglich gilt für jede positive rationale Zahl $\frac{n}{m}$, dass

$$\exp\left(\frac{n}{m}\right) \;=\; \exp\left(\frac{1}{m}\right)^n \;=\; \left(e^{\frac{1}{m}}\right)^n \;=\; e^{\frac{n}{m}} \;.$$

Wegen Lemma 4.1.47 (ii) gilt dann für negative rationale Zahlen

$$\exp\left(-\frac{n}{m}\right) \;=\; \exp\left(\frac{n}{m}\right)^{-1} \;=\; \left(e^{\frac{n}{m}}\right)^{-1} \;=\; e^{-\frac{n}{m}} \;.$$

Damit ist der Satz bewiesen. □

Bemerkung. Aufgrund von Satz 4.1.48 definiert man für beliebige komplexe Zahlen $z \in \mathbb{C}$:

$$e^z \;:=\; \exp(z) \;.$$

Wie wir in Lemma 4.1.47 gesehen haben, ist die Einschränkung der Exponentialfunktion auf die reellen Zahlen monoton steigend und damit insbesondere injektiv. Man kann sogar zeigen, dass sie bijektiv ist.

Satz 4.1.49. *Die Einschränkung der Exponentialfunktion auf die Menge der reellen Zahlen (*$\exp_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}_{>0}$*) definiert eine bijektive Abbildung von* $\mathbb{R}$ *nach* $\mathbb{R}_{>0}$*.*

Zur Vereinfachung der Notation bezeichnen wir die Funktion $\exp_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}_{>0}$ im Folgenden oft auch einfach nur mit exp.

Definition 4.1.50 (Natürlicher Logarithmus)**.** Die Umkehrfunktion der reellen Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ ist der *natürliche Logarithmus*, der mit $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ bezeichnet wird. Es ist also

$$\ln(x) \;=\; y \qquad \Longleftrightarrow \qquad x \;=\; e^y \;=\; \exp(y) \;.$$

Wir beweisen zunächst einige Eigenschaften des natürlichen Logarithmus.

Lemma 4.1.51. *Für den natürlichen Logarithmus* $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ *gilt:*

(i) $\ln(x) < \ln(y)$ *für alle* $0 < x < y$.

(ii) $\ln(x \cdot y) = \ln(x) + \ln(y)$ *für alle* $x, y \in \mathbb{R}_{>0}$.

(iii) $\ln(1/x) = -\ln(x)$ *für alle* $x \in \mathbb{R}_{>0}$.

(iv) $\ln(1) = 0$.

Beweis. Eigenschaft (i) folgt aus Lemma 4.1.47 (iv). Eigenschaft (ii) folgt aus Lemma 4.1.46. Eigenschaft (iii) folgt aus (ii). Und (iv) folgt schließlich aus der Tatsache, dass $\exp(0) = 1$. □

Mit Hilfe der Exponentialfunktion und des natürlichen Logarithmus können wir jetzt beliebige komplexe Potenzen reeller Zahlen definieren.

Definition 4.1.52. Es sei $a \in \mathbb{R} > 0$ und $z \in \mathbb{C}$. Dann definieren wir

$$a^z \;:=\; e^{z \cdot \ln(a)} \;=\; \exp(z \cdot \ln(a)) \;.$$

Wir nennen die durch $z \mapsto a^z$ definierte Funktion von $\mathbb{C}$ nach $\mathbb{C}$ auch *Exponentialfunktion zur Basis* a und bezeichnen sie mit $\exp_a$. Es gilt also

$$\exp_a(z) \;=\; a^z \;=\; \exp(z \ln(a)) \qquad \text{für alle } z \in \mathbb{C}.$$

Aus den Eigenschaften der Exponentialfunktion exp folgen sofort die folgenden Eigenschaften von $\exp_a$.

Lemma 4.1.53. *Es sei* $a \in \mathbb{R}_{>0}$. *Dann gilt:*

(i) $\exp_a$ *erfüllt die Funktionalgleichung* (4.5).

(ii) Die Einschränkung von $\exp_a$ *auf die reellen Zahlen ist streng monoton wachsend, falls* $a > 1$, *und streng monoton fallend, falls* $a < 1$; *für* $a = 1$ *ist sie konstant gleich* 1.

(iii) Für $a \neq 1$ *liefert* $\exp_a$ *eine Bijektion zwischen* $\mathbb{R}$ *und* $\mathbb{R}_{>0}$.

Bemerkung. Es seien $a, b \in \mathbb{R}_{>0}$. Man kann leicht zeigen, dass

$$(a^x)^y \;=\; a^{x \cdot y} \qquad \text{für alle } x, y \in \mathbb{R}.$$

Außerdem gilt

$$a^z \cdot b^z \;=\; (a \cdot b)^z \qquad \text{für alle } z \in \mathbb{C}.$$

Aufgrund der letzten Behauptung in Lemma 4.1.53 besitzt $\exp_a$ eine Umkehrfunktion von $\mathbb{R}_{>0}$ nach $\mathbb{R}$ — den Logarithmus zur Basis a.

Definition 4.1.54 (Logarithmus zur Basis a)**.** Es sei $a \in \mathbb{R}_{>0} \setminus \{1\}$. Dann nennt man die Umkehrabbildung der Einschränkung von $\exp_a$ auf die reellen Zahlen die *Logarithmusfunktion zur Basis* a und bezeichnet sie mit $\log_a : \mathbb{R}_{>0} \to \mathbb{R}$. (Insbesondere ist $\ln = \log_e$.)

Lemma 4.1.55. *Es sei $a \in \mathbb{R}_{>0} \setminus \{1\}$ und $x > 0$. dann gilt*

$$\log_a(x) \;=\; \frac{\ln(x)}{\ln(a)} \;.$$

Beweis. Es gilt

$$a^{\ln(x)/\ln(a)} \;=\; \exp_a\left(\frac{\ln(x)}{\ln(a)}\right) \;=\; \exp\bigl(\ln(x)\bigr) \;=\; x \;.$$

□

4.1.6 Landau-Symbole

In diesem Abschnitt wollen wir verschiedene Folgen miteinander vergleichen. Als Motivation dient uns dabei die folgende Problematik, die bei der Analyse von Algorithmen auftritt. Die Laufzeit (i.e., Anzahl der benötigten elementaren Rechenschritte) eines Algorithmus hängt in aller Regel von der Länge n der Eingabe (i.e., Anzahl der Bits oder Bytes, aus denen die Eingabe besteht) ab. Betrachten wir beispielsweise den Euklidischen Algorithmus aus Kapitel 2, so ist intuitiv klar, dass die Anzahl der dabei benötigten elementaren Rechenoperationen umso größer sein wird, je größer die Zahlen sind, die der Algorithmus als Eingabe erhält. Bezeichnet man die maximal mögliche Anzahl der elementaren Rechenschritte, die ein zu analysierender Algorithmus für eine Eingabe der Länge $n \in \mathbb{N}$ durchführen muss, mit f_n, so hat man dadurch eine Folge $(f_n)_{n\in\mathbb{N}}$ definiert, die das Laufzeitverhalten des Algorithmus beschreibt. Andererseits interessiert man sich natürlich nicht für die exakte Definition dieser Folge, sondern eigentlich nur für deren asymptotisches Verhalten für wachsende Werte n. Man ist beispielsweise an Aussagen der folgenden Form interessiert:

- Die Laufzeit des Algorithmus ist ungefähr proportional zur Größe der Eingabe (man sagt dann auch, dass die Laufzeit des Algorithmus *linear* mit der Länge der Eingabe wächst).

- Die Laufzeit des Algorithmus wächst ungefähr quadratisch in der Eingabelänge n, d.h. die Laufzeit ist ungefähr proportional zu n^2.

- Die Laufzeit des Algorithmus wächst mindestens exponentiell in der Eingabelänge n, d.h. die Laufzeit wächst beispielsweise wie 2^n.

- Die Laufzeit des Algorithmus ist durch ein Polynom in der Eingabelänge beschränkt, d.h. die Laufzeit ist für alle $n \in \mathbb{N}$ durch $p(n)$ beschränkt, wobei p eine beliebige Polynomfunktion ist.

Bei allen diesen Aussagen kommt es uns nicht auf konstante Faktoren an. Es ist beispielsweise nicht so interessant, ob sich die Laufzeit eines Algorithmus wie n oder wie $2n$ verhält — in beiden Fällen spricht man einfach nur von *linearer Laufzeit*. Viel interessanter ist die Frage, ob die Laufzeit proportional zu n, zu $n \log n$ oder zu n^2 wächst. Solche Betrachtungen werden durch die sogenannten *Landau-Symbole* formalisiert. Sie dienen dazu, verschiedene Folgen miteinander zu vergleichen, wobei konstante Faktoren wegabstrahiert werden.

Definition 4.1.56 (Landau-Symbole)**.** Es sei $g = (g_n) \in \mathbb{R}^{\mathbb{N}}_{>0}$ eine Folge positiver reeller Zahlen.

(i) Die Menge $O(g)$ (sprich: „Groß O von g“) enthält alle Folgen positiver reller Zahlen, die punktweise höchstens um einen konstanten Faktor größer als g sind, d.h.:

$$O(g) \;:=\; \{f = (f_n) \in \mathbb{R}^{\mathbb{N}}_{>0} \mid \exists c > 0 : f_n \leq c \cdot g_n \text{ für alle } n \in \mathbb{N}\} \;.$$

Ist $f \in O(g)$, so sagt man auch, dass f *höchstens so schnell wie g wächst.*

(ii) Die Menge $\Omega(g)$ (sprich: „Groß Omega von g“) enthält alle Folgen positiver reller Zahlen, die punktweise höchstens um einen konstanten Faktor kleiner als g sind, d.h.:

$$\Omega(g) \;:=\; \{f = (f_n) \in \mathbb{R}^{\mathbb{N}}_{>0} \mid \exists c > 0 : f_n \geq c \cdot g_n \text{ für alle } n \in \mathbb{N}\} \;.$$

Ist $f \in \Omega(g)$, so sagt man auch, dass f *mindestens so schnell wie g wächst.*

(iii) Die Menge $\theta(g)$ (sprich: „Theta von g“) enthält alle Folgen positiver reller Zahlen, die punktweise höchstens um einen konstanten Faktor von g abweichen, d.h.:

$$\theta(g) := \{f = (f_n) \in \mathbb{R}^{\mathbb{N}}_{>0} \mid \exists c \geq 1 : \tfrac{1}{c} \cdot g_n \leq f_n \leq c \cdot g_n \;\forall n \in \mathbb{N}\} \;.$$

Ist $f \in \theta(g)$, so sagt man auch, dass f *genau so schnell wie g wächst.*

(iv) Die Menge $o(g)$ (sprich: „Klein o von g“) enthält alle Folgen positiver reller Zahlen, die asymptotisch um mehr als nur einen konstanten Faktor kleiner als g sind, d.h.:

$$o(g) := \{f = (f_n) \in \mathbb{R}^{\mathbb{N}}_{>0} \mid \forall c > 0 \;\exists n_0 \in \mathbb{N} : f_n \leq c \cdot g_n \;\forall n \geq n_0\} \;.$$

Ist $f \in o(g)$, so sagt man auch, dass f *langsamer als g wächst.*

(v) Die Menge $\omega(g)$ (sprich: „Klein omega von g“) enthält alle Folgen positiver reller Zahlen, die asymptotisch um mehr als nur einen konstanten Faktor größer als g sind, d.h.:

$$\omega(g) := \{f = (f_n) \in \mathbb{R}^{\mathbb{N}}_{>0} \mid \forall c > 0\ \exists n_0 \in \mathbb{N} : f_n \geq c \cdot g_n\ \forall n \geq n_0\}\ .$$

Ist $f \in \omega(g)$, so sagt man auch, dass f *schneller als g wächst.*

Beispiele.

(i) Ist $f_n = \sum_{k=0}^{d} a_k n^k$ mit $a_0, \ldots, a_d \in \mathbb{R}$ und $a_d > 0$, so ist $f \in \theta(n^d)$.

(ii) Wir bezeichnen mit $1 = (1)_{n\in\mathbb{N}}$ die konstante Folge, deren Folgeglieder alle 1 sind. Dann ist $f \in O(1)$ genau dann, wenn f beschränkt ist.

(iii) Ist $f \in O\big(\frac{1}{n}\big)$, so ist f eine Nullfolge. Die umgekehrte Richtung gilt nicht, da die Folge $\big(\frac{1}{\sqrt{n}}\big)$ zwar eine Nullfolge ist, jedoch in $\omega\big(\frac{1}{n}\big)$ liegt.

(iv) Es gilt

$$\cdots\ \subseteq\ O\big(\frac{1}{n^2}\big)\ \subseteq\ O\big(\frac{1}{n}\big)\ \subseteq\ O(1)\ \subseteq\ O(n)\ \subseteq\ O(n^2)\ \subseteq\ \cdots$$

(v) Ist $f = (\exp(n))_{n\in\mathbb{N}}$ und $d \in \mathbb{N}$ beliebig, so ist $f \in \omega(n^d)$. Denn es gilt für $n \in \mathbb{N}$:

$$\exp(n)\ \geq\ \frac{n^{d+1}}{(d+1)!}\ =\ \frac{n}{(d+1)!} \cdot n^d$$

Wähle man also zu einem beliebigen $c > 0$ die Zahl $n_0 := c \cdot (d+1)!$, dann gilt für alle $n \geq n_0$, dass $\exp(n) \geq n^d$.

Wir haben damit gezeigt, dass die Exponentialfunktion schneller als jede Polynomfunktion wächst.

(vi) Ist $f = (\ln(n))_{n\in\mathbb{N}}$ und $d \in \mathbb{N}$ beliebig, so ist $f \in o(\sqrt[d]{n})$. Dies zeigt man analog zu der Behauptung in (v).

Es gilt also, dass die Logarithmusfunktion langsamer als jede Wurzelfunktion wächst.

Bemerkung.

(i) Aus der Definition der Landau-Symbole folgen sofort die folgenden Äquivalenzen:

$$\begin{aligned} f \in O(g) &\iff g \in \Omega(f)\ , \\ f \in o(g) &\iff g \in \omega(f)\ , \\ f \in \theta(g) &\iff \big(f \in O(g) \text{ und } f \in \Omega(g)\big)\ . \end{aligned}$$

(ii) Mit den Landau-Symbolen O, Ω, θ, o und ω verhält es sich also ähnlich wie mit den bekannten Vergleichsrelationen $\leq$, $\geq$, $=$, $<$ und $>$. Dabei gelten die folgenden anschaulichen Entsprechungen:

$$\begin{aligned} f \in O(g) \quad &\text{bedeutet} \quad „f \ \leq \ g“ \ , \\ f \in \Omega(g) \quad &\text{bedeutet} \quad „f \ \geq \ g“ \ , \\ f \in \theta(g) \quad &\text{bedeutet} \quad „f \ = \ g“ \ , \\ f \in o(g) \quad &\text{bedeutet} \quad „f \ < \ g“ \ , \\ f \in \omega(g) \quad &\text{bedeutet} \quad „f \ > \ g“ \ . \end{aligned}$$

Dabei sind die rechten Seiten natürlich nicht wirklich wörtlich zu nehmen.

(iii) Alternativ hätte man auch die folgenden zu Definition 4.1.56 äquivalenten Definitionen angeben können:

$$\begin{aligned} O(g) \ &= \ \left\{ f = (f_n) \in \mathbb{R}_{>0}^{\mathbb{N}} \mid \left(\tfrac{f_n}{g_n}\right)_{n\in\mathbb{N}} \text{ ist beschränkt} \right\} \ , \\ o(g) \ &= \ \left\{ f = (f_n) \in \mathbb{R}_{>0}^{\mathbb{N}} \mid \left(\tfrac{f_n}{g_n}\right)_{n\in\mathbb{N}} \text{ ist Nullfolge} \right\} \ . \end{aligned}$$

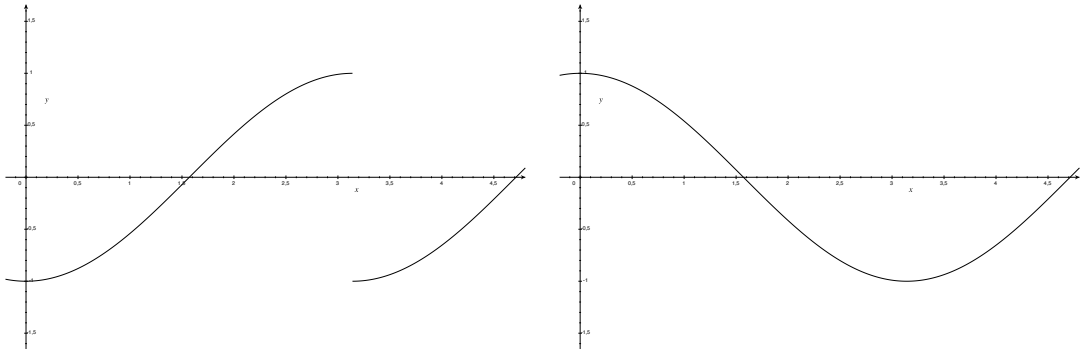
(iv) Man verwendet üblicherweise die folgenden Sprechweisen:

- Ist $f \in \theta(1)$, so ist f „*konstant*“.
- Ist $f \in \theta(n)$, so *wächst f linear*.
- Ist $f \in \theta(n^2)$, so *wächst f quadratisch*.
- Ist $f \in \theta(n^3)$, so *wächst f kubisch*.
- Ist $f \in O(n^k)$ für ein $k \in \mathbb{N}$, so ist f *polynomial beschränkt*.
- Ist $f \in \omega(c^n)$ für ein $c > 1$, so *wächst f exponentiell*.
- Ist $f \in \theta(\log n)$, so *wächst f logarithmisch*.

4.2 Stetige Funktionen

Abbildungen von einer Teilmenge der reellen Zahlen $\mathbb{R}$ in eine Teilmenge der reellen Zahlen nennt man auch *(reelle) Funktionen*. Ebenso nennt man Abbildungen von einer Teilmenge der komplexen Zahlen $\mathbb{C}$ in eine Teilmenge der komplexen Zahlen *(komplexe) Funktionen*. Wir diskutieren in diesem Abschnitt den Begriff der Stetigkeit von Funktionen. Anschaulich gesprochen heißt eine Funktion stetig, wenn sie keine Sprungstellen besitzt. Bei reellen Funktionen ist das im Wesentlichen gleichbedeutend damit, dass der Graph der Funktion ohne Absetzen des Stifts gezeichnet werden kann. (Wir geben zwei Beispiele in Abbildung 4.1.) Etwas präziser gefasst bedeutet das, dass sich bei geringfügiger Änderung des eingesetzten Wertes auch der Funktionswert nur geringfügig ändert.

Im Folgenden bezeichne $\mathbb{K}$ immer den Körper der reellen oder komplexen Zahlen, also $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.



(a) (b)

Abbildung 4.1: Der Graph einer unstetigen reellen Funktion mit Sprungstelle in (a) und der Graph einer stetigen reellen Funktion in (b).

4.2.1 Berührungspunkte

Bevor wir den Begriff der Stetigkeit formal definieren können, benötigen wir zunächst einen Begriff aus der Topologie.

Definition 4.2.1 (Berührungspunkt)**.** Es sei $D \subseteq \mathbb{K}$. Ein Element $x_0 \in \mathbb{K}$ heißt *Berührungspunkt von* D, wenn es eine Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ für alle $n \in \mathbb{N}$ gibt, so dass $\lim_{n\to\infty} x_n = x_0$.

Beispiele.

(i) Jedes Element $x_0 \in D$ ist Berührungspunkt von D, da x_0 Grenzwert der konstanten Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_n := x_0$ für alle $n \in \mathbb{N}$ ist.

(ii) Der Punkt $x_0 = 2$ ist Berührungspunkt der Menge $D = \mathbb{R}\setminus\{2\}$, da beispielsweise die durch $x_n := 2 + \frac{1}{n}$ für alle $n \in \mathbb{N}$ gegebene Folge von Elementen aus D gegen 2 konvergiert.

(iii) Alle Punkte auf dem komplexen Einheitskreis $\{z \in \mathbb{C} \mid |z| = 1\}$ sind Berührungspunkte der *offenen Kreisscheibe* $\{z \in \mathbb{C} \mid |z| < 1\}$, da für $z_0 \in \mathbb{C}$ mit $|z_0| = 1$ die durch $z_n = (1-\frac{1}{n})z_0$ gegebene komplexe Zahlenfolge gegen z_0 konvergiert. Man kann zeigen, dass alle Punkte außerhalb des Einheitskreises keine Berührungspunkte sind.

Man kann den Begriff des Berührungspunktes alternativ auch wie folgt charakterisieren.

Lemma 4.2.2. *Es sei $D \subseteq \mathbb{K}$. Dann ist $x_0 \in \mathbb{K}$ genau dann ein Berührungspunkt von D, wenn es zu jedem $\varepsilon > 0$ ein $x \in D$ mit $|x_0 - x| < \varepsilon$ gibt.*

Beweis. Es sei x_0 ein Berührungspunkt von D und $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ eine Folge mit $\lim_{n\to\infty} x_n = x_0$. Dann gibt es nach Definition 4.1.9 zu jedem $\varepsilon > 0$

ein $n_0 \in \mathbb{N}$ mit $|x_0 - x_n| < \varepsilon$ für alle $n \geq n_0$. Insbesondere gilt also $x_{n_0} \in D$ und $|x_0 - x_{n_0}| < \varepsilon$.

Um die andere Richtung zu beweisen nehmen wir nun an, dass es zu jedem $\varepsilon > 0$ ein $x \in D$ mit $|x_0 - x| < \varepsilon$ gibt. Wir definieren eine Folge $(x_n)_{n\in\mathbb{N}}$ wie folgt: Für $n \in \mathbb{N}$ wählen wir ein beliebiges $x_n \in D$ mit $|x_0 - x_n| < \frac{1}{n}$. Man sieht leicht, dass dann $\lim_{n\to\infty} x_n = x_0$ gilt, so dass x_0 Berührungspunkt von D ist. □

Beispiele.

(i) Wir betrachten die Teilmenge

$$D := \{z \in \mathbb{C} \mid 0 < \mathrm{Re}(z) \leq 1 \text{ und } \mathrm{Im}(z) = 0\} \subseteq \mathbb{C} .$$

Außer den Elementen in D ist der einzige Berührungspunkt von D der Nullpunkt. Dass 0 tatsächlich ein Berührungspunkt ist sieht man beispielsweise anhand der Nullfolge $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$, deren Folgeglieder alle in D liegen.

Betrachten wir jedoch einen Punkt $z_0 = a+bi \in \mathbb{C}\backslash(D\cup\{0\})$, dann gilt $a \neq 0$ oder $b \neq 0$. Ist $b \neq 0$, dann gibt es keinen Punkt $z \in D$ mit $|z_0 - z| < |b|$, so dass z_0 kein Berührungspunkt von D sein kann. Ist $b = 0$, so ist entweder $a < 0$ oder $a > 1$. Im ersten Fall gibt es kein $z \in D$ mit $|z_0 - z| < -a$; im zweiten Fall gibt es kein $z \in D$ mit $|z_0 - z| < a - 1$. In beiden Fällen ist also z_0 kein Berührungspunkt.

(ii) Jede reelle Zahl ist Berührungspunkt der Menge der rationalen Zahlen $\mathbb{Q}$. Dies folgt unmittelbar aus Lemma 4.2.2 und Lemma 4.1.5.

4.2.2 Grenzwerte von Funktionen

Als nächstes definieren wir den Grenzwert oder Limes einer Funktion in einem Berührungspunkt ihres Definitionsbereichs.

Definition 4.2.3 (Grenzwert, Limes einer Funktion)**.** Es sei $D \subseteq \mathbb{K}$, x_0 ein Berührungspunkt von D und $f : D \to \mathbb{K}$ eine Funktion. Weiter sei $y_0 \in \mathbb{K}$ (falls $\mathbb{K} = \mathbb{R}$ erlauben wir auch $y_0 = \infty$ und $y_0 = -\infty$).

(i) Man sagt, dass f in x_0 den *Grenzwert* y_0 hat (in Zeichen: $\lim_{x\to x_0} f(x) = y_0$), falls für alle Folgen $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ und $\lim_{n\to\infty} x_n = x_0$ gilt, dass $\lim_{n\to\infty} f(x_n) = y_0$.

(ii) Ist $\mathbb{K}$ der Körper der reellen Zahlen $\mathbb{R}$ und ist der Definitionsbereich D nach oben unbeschränkt, so ist $\lim_{x\to\infty} f(x) = y_0$, falls für alle Folgen $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ und $\lim_{n\to\infty} x_n = \infty$ gilt, dass $\lim_{n\to\infty} f(x_n) = y_0$.

(iii) Ist $\mathbb{K} = \mathbb{R}$ und ist der Definitionsbereich D nach unten unbeschränkt, so ist $\lim_{x\to-\infty} f(x) = y_0$, falls für alle Folgen $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ und $\lim_{n\to\infty} x_n = -\infty$ gilt, dass $\lim_{n\to\infty} f(x_n) = y_0$.

Bemerkung.

(i) Ist $x_0 \in D$ und besitzt die Funktion $f : D \to \mathbb{K}$ einen Grenzwert in x_0, so muss dieser gleich $f(x_0)$ sein. Denn eine möglich Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in D$ und $\lim_{n\to\infty} x_n = x_0$ ist die durch $x_n = x_0$ für alle $n \in \mathbb{N}$ definierte konstante Folge. Für diese gilt offenbar $\lim_{n\to\infty} f(x_n) = f(x_0)$.

(ii) Ist $\mathbb{K} = \mathbb{R}$ und $\lim_{x\to x_0} f(x) = \infty$ (oder $\lim_{x\to x_0} f(x) = -\infty$), so besitzt f in x_0 streng genommen keinen Grenzwert. Man sagt in diesem Fall nur, dass f für $x \to x_0$ gegen unendlich (oder minus unendlich) geht und nennt ∞ (oder $-\infty$) den *uneigentlichen Grenzwert von f in x_0*.

Beispiele.

(i) Es sei $f : \mathbb{C} \to \mathbb{C}$ definiert durch $f(z) := z^2 - 2z + 3i$. Dann existiert der Grenzwert von f in jedem Punkt $z_0 \in \mathbb{C}$. Es sei nämlich $(z_n)_{n\in\mathbb{N}}$ eine Folge mit $\lim_{n\to\infty} z_n = z_0$. Dann ist wegen Satz 4.1.17

$$\begin{aligned}\lim_{n\to\infty} f(z_n) &= \lim_{n\to\infty} ({z_n}^2) + \lim_{n\to\infty} (-2z_n) + \lim_{n\to\infty} (3i) \\ &= \Big(\lim_{n\to\infty} z_n\Big)^2 - 2 \lim_{n\to\infty} z_n + 3i \\ &= {z_0}^2 - 2z_0 + 3i \;=\; f(z_0)\ .\end{aligned}$$

(ii) Dieselbe Argumentation wie im letzten Beispiel kann man auf eine beliebige Polynomfunktion $f : \mathbb{K} \to \mathbb{K}$ anwenden, um zu zeigen, dass diese in jedem beliebigen Punkt $z_0 \in \mathbb{K}$ den Grenzwert $f(z_0)$ hat.

(iii) Es sei $D := \mathbb{C} \setminus \{3\}$ und $f : D \to \mathbb{C}$ die durch

$$f(z) \;:=\; \frac{z^2 - 9}{z - 3}$$

definierte Funktion. Dann ist 3 ein Berührungspunkt von D und die Funktion f hat in 3 den Grenzwert 6. Denn es gilt

$$f(z) \;=\; \frac{z^2 - 9}{z - 3} \;=\; \frac{(z-3)(z+3)}{z-3} \;=\; z + 3 \qquad \text{für } z \neq 3.$$

Damit folgt wie im letzten Beispiel, dass $\lim_{z\to 3} f(z) = 6$.

(iv) Wir betrachten die Signum-Funktion $\operatorname{sgn} : \mathbb{R} \to \mathbb{R}$ mit

$$\operatorname{sgn}(x) \;=\; \begin{cases} 1 & \text{falls } x > 0, \\ 0 & \text{falls } x = 0, \\ -1 & \text{falls } x < 0. \end{cases}$$

Diese Funktion besitzt im Punkt 0 keinen Grenzwert. Dazu betrachten wir zwei Folgen $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$, die beide gegen 0 konvergieren, so dass jedoch die Folgen $\big(\mathrm{sgn}(x_n)\big)_{n\in\mathbb{N}}$ und $\big(\mathrm{sgn}(y_n)\big)_{n\in\mathbb{N}}$ gegen unterschiedliche Grenzwerte konvergieren. Dazu sei $x_n := \frac{1}{n}$ und $y_n := -\frac{1}{n}$ für $n \in \mathbb{N}$. Dann ist nach Definition $\mathrm{sgn}(x_n) = 1$ und $\mathrm{sgn}(y_n) = -1$ für alle $n \in \mathbb{N}$. Folglich gilt also $\lim_{n\to\infty} \mathrm{sgn}(x_n) = 1$ und $\lim_{n\to\infty} \mathrm{sgn}(y_n) = -1$.

Man kann sogar noch eine weitere Folge $(z_n)_{n\in\mathbb{N}}$ mit $\lim_{n\to\infty} z_n = 0$ und $\lim_{n\to\infty} \mathrm{sgn}(z_n) = 0$ finden, nämlich $z_n := 0$ für alle $n \in \mathbb{N}$.

Es gibt auch Nullfolgen $(a_n)_{n\in\mathbb{N}}$, so dass die zugehörige Folge $\big(\mathrm{sgn}(a_n)\big)_{n\in\mathbb{N}}$ nicht konvergiert. Betrachte beispielsweise die Folge $\big((-1)^n \frac{1}{n}\big)_{n\in\mathbb{N}}$, für die

$$\mathrm{sgn}\big((-1)^n \tfrac{1}{n}\big) \;=\; (-1)^n \;=\; \begin{cases} 1 & \text{falls } n \text{ gerade,} \\ -1 & \text{falls } n \text{ ungerade,} \end{cases}$$

gilt.

(v) Wir betrachten die Funktion $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit $f(x) := \frac{1}{x}$. Dann ist $\lim_{x\to\infty} f(x) = 0$ und auch $\lim_{x\to-\infty} f(x) = 0$. Der Grenzwert im Punkt 0 existiert jedoch nicht. Für die Nullfolge $\big(\frac{1}{n}\big)_{n\in\mathbb{N}}$ geht die zugehörige Folge $\big(f(\frac{1}{n})\big)_{n\in\mathbb{N}}$ gegen unendlich, weil $f(\frac{1}{n}) = n$ für alle $n \in \mathbb{N}$. Für die Nullfolge $\big(-\frac{1}{n}\big)_{n\in\mathbb{N}}$ geht die zugehörige Folge $\big(f(-\frac{1}{n})\big)_{n\in\mathbb{N}}$ jedoch gegen $-\infty$.

(vi) Für die Funktion $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit $f(x) := \frac{1}{x^2}$ gilt $\lim_{x\to 0} f(x) = \infty$. Um das zu beweisen, betrachten wir eine beliebige Nullfolge $(x_n)_{n\in\mathbb{N}}$. Wir müssen zeigen, dass es zu jedem $r > 0$ ein $n_0 \in \mathbb{N}$ gibt mit $f(x_n) > r$ für alle $n \geq n_0$. Da (x_n) eine Nullfolge ist, gibt es ein $n_0 \in \mathbb{N}$ mit $x_n < \frac{1}{\sqrt{r}}$ für alle $n \geq n_0$. Folglich ist $f(x_n) = \frac{1}{{x_n}^2} > r$ für alle $n \geq n_0$.

(vii) Wir betrachten die *Dirichlet'sche Funktion* $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(x) \;:=\; \begin{cases} 1 & \text{falls } x \in \mathbb{Q}, \\ 0 & \text{falls } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

Diese Funktion besitzt in keinem Punkt $x_0 \in \mathbb{R}$ einen Grenzwert. Wir erläutern das beispielhaft für den Punkt $x_0 = 0$. Dazu betrachten wir die beiden Nullfolgen $\big(\frac{1}{n}\big)_{n\in\mathbb{N}}$ und $\big(\frac{\sqrt{2}}{n}\big)_{n\in\mathbb{N}}$. Da $\frac{1}{n} \in \mathbb{Q}$ und $\frac{\sqrt{2}}{n} \notin \mathbb{Q}$, konvergiert die erste Folge gegen 1 und die zweite gegen 0.

Bemerkung. Um zu zeigen, dass der Grenzwert einer Funktion in einem Punkt x_0 *nicht* existiert, genügt es, zwei gegen x_0 konvergente Folgen zu finden, so dass die zugehörigen Funktionswerte gegen unterschiedliche Grenzwerte konvergieren. Alternativ reicht es auch, eine einzelne gegen x_0 konvergente Folge aufzuzeigen, deren Funktionswerte nicht konvergieren. Es scheint jedoch viel schwieriger zu

zeigen, dass der Grenzwert einer Funktion in einem Punkte x_0 tatsächlich existiert, da man dazu laut Definition alle gegen x_0 konvergenten Folgen betrachten muss. Abhilfe verschafft hier die folgende alternative Charakterisierung.

Lemma 4.2.4. *[ε-δ-Kriterium für Grenzwert einer Funktion] Es sei $D \subseteq \mathbb{K}$, x_0 ein Berührungspunkt von D und $f : D \to \mathbb{K}$ eine Funktion. Dann besitzt f in x_0 genau dann den Grenzwert $y_0 \in \mathbb{K}$, wenn es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für alle $x \in D$ mit $|x_0 - x| < \delta$ stets $|y_0 - f(x)| < \varepsilon$ gilt.*

Beweis. Wir zeigen zunächst, dass das ε-δ-Kriterium hinreichend für die Existenz des Grenzwertes ist. Wir nehmen also an, dass es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für alle $x \in D$ mit $|x_0 - x| < \delta$ stets $|y_0 - f(x)| < \varepsilon$ gilt. Es sei nun $(x_n)_{n\in\mathbb{N}}$ eine beliebige Folge mit $x_n \in D$ und $\lim_{n\to\infty} x_n = x_0$. Wir betrachten ein beliebiges $\varepsilon > 0$ und das zugehörige $\delta > 0$. Da die Folge $(x_n)_{n\in\mathbb{N}}$ gegen x_0 konvergiert, gibt es ein $n_0 \in \mathbb{N}$ mit $|x_0 - x_n| < \delta$ für alle $n \geq n_0$. Betrachten wir jetzt die Folge $\big(f(x_n)\big)_{n\in\mathbb{N}}$, dann gilt also $|y_0 - f(x_n)| < \varepsilon$ für alle $n \geq n_0$. Folglich konvergiert $\big(f(x_n)\big)_{n\in\mathbb{N}}$ gegen y_0.

Wir beweisen noch die Notwendigkeit des Kriteriums. Dazu nehmen wir an, dass es nicht erfüllt ist und zeigen, dass f dann nicht den Grenzwert y_0 besitzen kann. Es sei also $\varepsilon > 0$, so dass es für jedes $\delta > 0$ ein $x \in D$ mit $|x_0 - x| < \delta$ und $|y_0 - f(x)| > \varepsilon$ gibt. Wir konstruieren eine gegen x_0 konvergente Folge $(x_n)_{n\in\mathbb{N}}$ wie folgt: Für jedes $n \in \mathbb{N}$ wählen wir eine $x_n \in D$ mit $|x_0 - x_n| < \frac{1}{n}$ und $|y_0 - f(x_n)| > \varepsilon$. Dann konvergiert die Folge $(x_n)_{n\in\mathbb{N}}$ offenbar gegen x_0, die Folge der Funktionswerte $\big(f(x_n)\big)_{n\in\mathbb{N}}$ jedoch nicht gegen y_0, da $|y_0 - f(x_n)| > \varepsilon$ für alle $n \in \mathbb{N}$. □

Um die Existenz des Grenzwertes einer Funktion in einem Punkt x_0 zu zeigen, sind die Rechenregeln für konvergente Folgen aus Satz 4.1.17 oft nützlich. Wir formulieren sie hier neu für Grenzwerte von Funktionen.

Satz 4.2.5. *Es sei $D \subseteq \mathbb{K}$, x_0 eine Berührungspunkt von D und $f, g : D \to \mathbb{K}$ zwei Funktionen mit $\lim_{x\to x_0} f(x) = y_0 \in \mathbb{K}$ und $\lim_{x\to x_0} g(x) = z_0 \in \mathbb{K}$. Dann gilt:*

(i) $\lim_{x\to x_0}\big(f(x) \pm g(x)\big) = y_0 \pm z_0$.

(ii) $\lim_{x\to x_0}\big(f(x) \cdot g(x)\big) = y_0 \cdot z_0$.

(iii) Für $\lambda \in \mathbb{K}$ ist $\lim_{x\to x_0}\big(\lambda \cdot f(x)\big) = \lambda \cdot y_0$.

(iv) Ist $z_0 \neq 0$, so ist $\lim_{x\to x_0}\big(f(x)/g(x)\big) = y_0/z_0$.

(v) $\lim_{x\to x_0} |f(x)| = |y_0|$.

(vi) Ist $\mathbb{K} = \mathbb{C}$, so gilt genau dann $\lim_{x\to x_0} f(x) = y_0$, *wenn*

$$\lim_{x\to x_0} \mathrm{Re}\big(f(x)\big) = \mathrm{Re}(y_0) \qquad \textit{und} \qquad \lim_{x\to x_0} \mathrm{Im}\big(f(x)\big) = \mathrm{Im}(y_0) \ .$$

Bemerkung. In Satz 4.2.5 (iv) betrachtet man streng genommen die Funktion $h : D' \to \mathbb{K}$ mit $h(x) := f(x)/g(x)$, deren Definitionsbereich durch $D' = \{x \in D \mid g(x) \neq 0\}$ gegeben ist. Man kann zeigen, dass x_0 auch ein Berührungspunkt von D' ist.

Beispiel. Wir betrachten die Funktion $h : \mathbb{C} \setminus \{3\} \to \mathbb{C}$ mit

$$h(z) \;:=\; \frac{z^2 + z + 1}{z - 3} \;.$$

Dann existiert für $z_0 \neq 3$ der Grenzwert von h in z_0 und es gilt $\lim_{z \to z_0} h(z) = h(z_0)$.

Satz 4.2.6. *Es seien $D, E \subseteq \mathbb{K}$, x_0 ein Berührungspunkt von D und $f : D \to E$ mit $\lim_{x \to x_0} f(x) = y_0$. Ist $g : E \to \mathbb{K}$ mit $\lim_{y \to y_0} g(y) = z_0$, dann ist $\lim_{x \to x_0} g\big(f(x)\big) = z_0$.*

Beweis. Wir betrachten eine beliebige Folge $(x_n)_{n \in \mathbb{N}}$ mit $x_n \in D$ und $\lim_{n \to \infty} x_n = x_0$. Dann ist $f(x_n) \in E$ und die Folge $\big(f(x_n)\big)_{n \in \mathbb{N}}$ konvergiert nach Voraussetzung gegen y_0. (Insbesondere ist also y_0 ein Berührungspunkt von E.) Da $\lim_{y \to y_0} g(y) = z_0$, gilt also $\lim_{n \to \infty} g\big(f(x_n)\big) = z_0$. Folglich ist $\lim_{x \to x_0} g\big(f(x)\big) = z_0$. □

Als nächstes betrachten wir für den Spezialfall reeller Funktionen noch sogenannte rechtsseitige und linksseitige Grenzwerte.

Definition 4.2.7 (Rechtsseitiger und linksseitiger Grenzwert)**.** Es sei $D \subseteq \mathbb{R}$, x_0 ein Berührungspunkt von D und $f : D \to \mathbb{R}$ eine reelle Funktion. Weiter sei $y_0 \in \mathbb{R} \cup \{\infty, -\infty\}$.

(i) Man sagt, dass f in x_0 den *rechtsseitigen Grenzwert* y_0 hat (in Zeichen: $\lim_{x \to x_0^+} f(x) = y_0$), falls für alle Folgen $(x_n)_{n \in \mathbb{N}}$ mit $x_n \in D$, $x_n > x_0$ und $\lim_{n \to \infty} x_n = x_0$ gilt, dass $\lim_{n \to \infty} f(x_n) = y_0$.

(ii) Man sagt, dass f in x_0 den *linksseitigen Grenzwert* y_0 hat (in Zeichen: $\lim_{x \to x_0^-} f(x) = y_0$), falls für alle Folgen $(x_n)_{n \in \mathbb{N}}$ mit $x_n \in D$, $x_n < x_0$ und $\lim_{n \to \infty} x_n = x_0$ gilt, dass $\lim_{n \to \infty} f(x_n) = y_0$.

Bemerkung. Ist $y_0 \in \{\infty, -\infty\}$, so spricht man wieder nur von *uneigentlichen* (rechtsseitigen oder linksseitigen) Grenzwerten.

Beispiel. Die Signumfunktion besitzt an der Stelle 0 den rechtsseitigen Grenzwert $\lim_{x \to 0^+} \operatorname{sgn}(x) = 1$ und den linksseitigen Grenzwert $\lim_{x \to 0^-} \operatorname{sgn}(x) = -1$. Man beachte jedoch, dass keiner dieser Grenzwerte dem tatsächlichen Funktionswert $\operatorname{sgn}(0) = 0$ entspricht.

4.2.3 Stetigkeit

Wir können jetzt den Begriff der Stetigkeit formal definieren.

Definition 4.2.8. [Stetigkeit] Es sei $D \subseteq \mathbb{K}$ und $f : D \to \mathbb{K}$ eine Funktion.

(i) Die Funktion f heißt *stetig in* $x_0 \in D$, falls ihr Grenzwert in x_0 existiert (also $\lim_{x \to x_0} f(x) = f(x_0)$).

(ii) Die Funktion f heißt *rechtsseitig (linksseitig) stetig in* $x_0 \in D$, falls gilt, dass $\lim_{x \to x_0^+} f(x) = f(x_0)$ ($\lim_{x \to x_0^-} f(x) = f(x_0)$).

(iii) Die Funktion f heißt *stetig*, falls sie in allen Punkten $x_0 \in D$ stetig ist.

(iv) Ist $x_0 \in \mathbb{K} \backslash D$ ein Berührungspunkt von D und existiert der Grenzwert von f in x_0, so heißt f *stetig ergänzbar in* x_0. Die Funktion $\bar{f} : D \cup \{x_0\} \to \mathbb{K}$ mit

$$\bar{f}(x) \;=\; \begin{cases} f(x) & \text{falls } x \in D, \\ \lim_{x' \to x_0} f(x') & \text{falls } x = x_0, \end{cases}$$

heißt *stetige Ergänzung von* f *in* x_0.

Beispiele.

(i) Wie schon weiter oben bemerkt, existiert der Grenwert einer (reellen oder komplexen) Polynomfunktion in jedem Punkt von $\mathbb{K}$. Folglich sind Polynomfunktionen also stetig.

(ii) Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := \lceil x \rceil$ (hier bezeichnet $\lceil x \rceil$ die kleinste ganze Zahl, die größer oder gleich x ist, also $\lceil x \rceil := \min\{n \in \mathbb{Z} \mid x \leq n\}$) ist in allen Punkten $x_0 \in \mathbb{R}$ linksseitig stetig, jedoch in keinem ganzzahligen Punkt $x_0 \in \mathbb{Z}$ rechtsseitig stetig. Wir beweisen nur letztere Behauptung.

Für $x_0 \in \mathbb{Z}$ betrachten wir die Folge $(x_n)_{n \in \mathbb{N}}$ mit $x_n := x_0 + \frac{1}{n}$ für alle $n \in \mathbb{N}$. Dann gilt $\lceil x_n \rceil = x_0 + 1$ und daher $\lim_{n \to \infty} \lceil x_n \rceil = x_0 + 1 \neq \lceil x_0 \rceil$.

(iii) Sei $D := \mathbb{C} \setminus \{3\}$ und $f : D \to \mathbb{C}$ die durch $f(z) := (z^2 - 9)/(z - 3)$ definierte Funktion. Wie weiter oben gezeigt wurde, ist f im Punkt 3 stetig ergänzbar (mit Funktionswert 6).

Mit Hilfe der Definition 4.2.8 können wir jetzt Satz 4.2.5 wie folgt formulieren.

Korollar 4.2.9. *Es sei $D \subseteq \mathbb{K}$, x_0 eine Berührungspunkt von D und $f, g : D \to \mathbb{K}$ zwei Funktionen, die in x_0 stetig (falls $x_0 \in D$) beziehungsweise stetig ergänzbar (falls $x_0 \notin D$) sind. Dann gilt:*

(i) Die auf D definierten Funktionen $f \pm g$, $f \cdot g$, $\lambda \cdot f$ (für beliebiges $\lambda \in \mathbb{K}$) und $|f|$ sind stetig (ergänzbar) in x_0.

(ii) Ist $\lim_{x\to x_0} g(x) \neq 0$*, so ist die auf* $\{x \in D \mid g(x) \neq 0\}$ *definierte Funktion* f/g *stetig (ergänzbar) in* x_0*.*

(iii) Ist $\mathbb{K} = \mathbb{C}$*, so ist die Funktion* $f : D \to \mathbb{C}$ *genau dann stetig (ergänzbar) in* x_0*, wenn die beiden Funktion* $\mathrm{Re}(f), \mathrm{Im}(f) : D \to \mathbb{R}$ *stetig (ergänzbar) in* x_0 *sind.*

Bemerkung. Als Spezialfall von Korollar 4.2.9 (ii) können wir festhalten, dass die Funktion $x \mapsto 1/f(x)$ stetig im Punkt x_0 ist, falls die Funktion f in x_0 stetig ist und $\lim_{x\to x_0} f(x) \neq 0$.

Beispiel. Es seien $f, g : \mathbb{K} \to \mathbb{K}$ Polynomfunktionen und $D := \{x \in \mathbb{K} \mid g(x) \neq 0\}$. Dann ist die gebrochen rationale Funktion $h : D \to \mathbb{K}$ mit $h(x) := f(x)/g(x)$ stetig.

Das nächste Korollar ist eine unmittelbare Folgerung aus Satz 4.2.6.

Korollar 4.2.10. *Es seien* $D, E \subseteq \mathbb{K}$*,* x_0 *ein Berührungspunkt von* D *und* $f : D \to E$ *stetig (ergänzbar) in* x_0*. Ist die Funktion* $g : E \to \mathbb{K}$ *stetig (ergänzbar) in dem Punkt* $\lim_{x\to x_0} f(x)$*, so ist auch die Komposition* $g \circ f : D \to \mathbb{K}$ *stetig (ergänzbar) in* x_0*.*

Wir geben das folgende Resultat ohne Beweis an.

Satz 4.2.11. *Es seien* $a, b \in \mathbb{R} \cup \{-\infty, \infty\}$ *mit* $a < b$ *und* $I \subseteq \mathbb{R}$ *ein Intervall der Form*[1] $[a, b]$*,* $(a, b]$*,* $[a, b)$ *oder* (a, b)*. Ist* $f : I \to M$ *mit* $M \subseteq \mathbb{R}$ *eine bijektive stetige Funktion, so ist auch die Umkehrabbildung* $f^{-1} : M \to I$ *stetig.*

Beispiele.

(i) Die Abbildung $f : [0, \infty) \to [0, \infty)$ mit $f(x) = x^2$ ist stetig und streng monoton steigend und damit bijektiv. Folglich ist die Umkehrabbildung (Wurzelfunktion) $f^{-1} : [0, \infty) \to [0, \infty)$ mit $f^{-1}(x) = \sqrt{x}$ auch stetig.

(ii) In Verallgemeinerung des letzten Beispiels betrachten wir für beliebiges $n \in \mathbb{N}$ die bijektive, stetige Abbildung $f : [0, \infty) \to [0, \infty)$ mit $f(x) = x^n$. Die Umkehrfunktion von f ist offenbar die Funktion, die ein $x \in [0, \infty)$ auf seine n-te Wurzel $\sqrt[n]{x}$ abbildet. Diese Funktion ist nach Satz 4.2.11 also auch stetig.

Aus dem ε-δ-Kriterium in Lemma 4.2.4 können wir die folgende alternative Charakterisierung von Stetigkeit folgern.

Korollar 4.2.12. *Es sei* $D \subseteq \mathbb{K}$ *und* $x_0 \in D$*. Eine Funktion* $f : D \to \mathbb{K}$ *ist genau dann stetig in* x_0*, wenn es für alle* $\varepsilon > 0$ *ein* $\delta > 0$ *gibt, so dass für alle* $x \in D$ *mit* $|x_0 - x| < \delta$ *folgt, dass* $|f(x_0) - f(x)| < \varepsilon$*.*

[1] Wir verwenden hier die folgende Konvention: $[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$, $(a, b] := \{x \in \mathbb{R} \mid a < x \leq b\}$, $[a, b) := \{x \in \mathbb{R} \mid a \leq x < b\}$ und $(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$.

Beweis. Folgt unmittelbar aus Lemma 4.2.4. □

Bemerkung. Wir stellen fest, dass Stetigkeit im Punkt x_0 eine *lokale Eigenschaft* einer Funktion f ist, die nur von dem Verhalten von f in unmittelbarer Umgebung von x_0 abhängt.

Wir führen im Folgenden noch zwei weitere, stärkere Stetigkeitsbegriffe ein, die im Gegensatz zur gewöhnlichen Stetigkeit nicht mehr nur lokal sondern global definiert sind.

Definition 4.2.13 (Gleichmäßige Stetigkeit)**.** Es sei $D \subseteq \mathbb{K}$. Eine Funktion $f : D \to \mathbb{K}$ heißt *gleichmäßig stetig* auf D, falls es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für alle $x, y \in D$ mit $|x - y| < \delta$ folgt, dass $|f(x) - f(y)| < \varepsilon$.

Bemerkung. Aus Definition 4.2.13 und Korollar 4.2.12 folgt, dass jede gleichmäßig stetige Funktion insbesondere stetig ist.

Beispiele.

(i) Die Wurzelfunktion $f : [0, \infty) \to \mathbb{R}$ mit $f(x) := \sqrt{x}$ ist gleichmäßig stetig. Wählt man zu einem gegebenen $\varepsilon > 0$ das zugehörige $\delta := \varepsilon^2$, dann gilt für alle $x, y \geq 0$ mit $|x - y| < \delta$, dass

$$|f(x) - f(y)| \;=\; |\sqrt{x} - \sqrt{y}| \;\leq\; \sqrt{|x - y|} \;<\; \sqrt{\delta} \;\leq\; \varepsilon \;.$$

Für die erste Ungleichung haben wir die folgende Abschätzung verwendet: Für $x \geq y \geq 0$ gilt

$$\sqrt{x} - \sqrt{y} \;\leq\; \sqrt{x - y} \;.$$

Diese Ungleichung ist genau dann erfüllt, wenn die durch Quadrieren beider Seiten entstehende Ungleichung erfüllt ist (das liegt daran, dass die Funktion $z \mapsto z^2$ streng monoton wachsend[2] auf $[0, \infty)$ ist):

$$x + y - 2\sqrt{x}\sqrt{y} \;\leq\; x - y \;.$$

Diese Ungleichung ist erfüllt, da $\sqrt{x} \geq \sqrt{y}$ gilt.

(ii) Die Funktion $f : [0, \infty) \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht gleichmäßig stetig. Denn andernfalls müsste es zu $\varepsilon = 1$ ein $\delta > 0$ geben, so dass $x^2 - y^2 < 1$ für alle $x \geq y \geq 0$ mit $x - y < \delta$. Dies führt zu dem folgenden Widerspruch, wenn wir $y = 1/\delta$ und $x = y + \delta/2$ wählen:

$$x^2 - y^2 \;=\; (x + y)(x - y) \;=\; (2/\delta + \delta/2)\delta/2 \;=\; 1 + \delta^2/4 \;>\; 1 \;.$$

[2] Ähnlich wie bei Folgen definiert man die Begriffe (streng) monoton wachsend bzw. fallend auch für reelle Funktionen. Ist $D \subseteq \mathbb{R}$ und $f : D \to \mathbb{R}$, dann heißt f *monoton wachsend*, falls $f(x) \leq f(y)$ für alle $x, y \in D$ mit $x \leq y$. Die Funktion heißt *streng monoton wachsend*, falls man „$\leq$“ durch „$<$“ ersetzen kann. Die Funktion f heißt *(streng) monoton fallend*, falls $-f$ (streng) monoton wachsend ist.

Bemerkung. Anhand der beiden Beispiele sieht man, dass Satz 4.2.11 nicht mehr gilt, wenn wir Stetigkeit durch gleichmäßige Stetigkeit ersetzen.

Definition 4.2.14 (Lipschitz-Stetigkeit)**.** Es sei $D \subseteq \mathbb{K}$. Eine Funktion $f : D \to \mathbb{K}$ heißt *Lipschitz-stetig* auf D, falls es eine Konstante $L \geq 0$ gibt, so dass für alle $x, y \in D$ gilt, dass $|f(x) - f(y)| \leq L \cdot |x - y|$. Dann heißt L *Lipschitz-Konstante*. Ist f Lipschitz-stetig mit Lipschitz-Konstante $L < 1$, so nennt man f auch eine *Kontraktion*.

Beispiele.

(i) Für $a, b \in \mathbb{C}$ ist die komplexe Funktion $f : \mathbb{C} \to \mathbb{C}$ mit $f(z) := a \cdot z + b$ Lipschitz-stetig mit Lipschitz-Konstante $L := |a|$. Denn es gilt für $x, y \in \mathbb{C}$, dass

$$|f(x) - f(y)| \;=\; |(a \cdot x + b) - (a \cdot y + b)| \;=\; |a| \cdot |x - y| \;.$$

(ii) Die Wurzelfunktion $f : [0, \infty) \to \mathbb{R}$ mit $f(x) := \sqrt{x}$ ist nicht Lipschitz-stetig. Widerspruchsbeweis: Angenommen f ist Lipschitz-stetig mit Lipschitz-Konstante $L > 0$. Wähle $x := 4/(16L^2)$ und $y := 1/(16L^2)$, dann gilt

$$|\sqrt{x} - \sqrt{y}| \;=\; \frac{|x - y|}{\sqrt{x} + \sqrt{y}} \;=\; \tfrac{4}{3} L \cdot |x - y| \;>\; L \cdot |x - y| \;.$$

Lemma 4.2.15. *Es sei $D \subseteq \mathbb{K}$. Eine Lipschitz-stetige Funktion $f : D \to \mathbb{K}$ ist insbesondere gleichmäßig stetig.*

Beweis. Es sei $f : D \to \mathbb{K}$ eine Lipschitz-stetige Funktion mit zugehöriger Lipschitz-Konstante $L > 0$. Wählt man zu einem beliebigen $\varepsilon > 0$ dann $\delta = \varepsilon / L$, so gilt für beliebige $x, y \in D$ mit $|x - y| < \delta$, dass

$$|f(x) - f(y)| \;\leq\; L \cdot |x - y| \;<\; L \cdot \delta \;=\; \varepsilon \;.$$

Damit ist der Beweis abgeschlossen □

4.2.4 Elementare Funktionen: exp, ln, cos, sin, tan etc.

Wir gehen in diesem Abschnitt noch einmal auf die Exponentialfunktion und dazu verwandte Funktionen ein. Wir beginnen mit der Feststellung, dass die Exponentialfunktion stetig ist.

Satz 4.2.16. *Die Exponentialfunktion $\exp : \mathbb{C} \to \mathbb{C}$ ist stetig.*

Beweis. Wir beweisen zunächst, dass exp im Nullpunkt stetig ist. Dazu betrachten wir eine beliebige Nullfolge $(z_n)_{n\in\mathbb{N}}$ und zeigen, dass $\lim_{n\to\infty} \exp(z_n) = \exp(0) = 1$ ist. Für $|z_n| < 1$ gilt:

$$0 \;\leq\; |\exp(z_n) - 1| \;=\; \left|\sum_{k=1}^{\infty} \frac{{z_n}^k}{k!}\right| \;\leq\; \sum_{k=1}^{\infty} \frac{|z_n|^k}{k!} \;\leq\; \sum_{k=1}^{\infty} |z_n|^k \;=\; \frac{|z_n|}{1-|z_n|} \;.$$

Da $\lim_{n\to\infty} z_n = 0$, konvergiert auch die rechte Seite dieser Ungleichung gegen 0 (wegen Satz 4.1.17). Folglich gilt $\lim_{n\to\infty} |\exp(z_n) - 1| = 0$ und damit auch $\lim_{n\to\infty} \exp(z_n) = 1$.

Damit können wir jetzt leicht zeigen, dass exp auch in jedem beliebigen Punkt $z_0 \in \mathbb{C}$ stetig ist. Dazu betrachten wir eine Folge $(z_n)_{n\in\mathbb{N}}$ mit $\lim_{n\to\infty} z_n = z_0$. Das bedeutet, dass $\lim_{n\to\infty}(z_n - z_0) = 0$. Folglich gilt wegen Lemma 4.1.46

$$\begin{aligned}
\lim_{n\to\infty} \exp(z_n) &= \lim_{n\to\infty} \big(\exp(z_0) \cdot \exp(z_n - z_0)\big) \\
&= \exp(z_0) \cdot \lim_{n\to\infty} \exp(z_n - z_0) \\
&= \exp(z_0) \cdot 1 \;=\; \exp(z_0) \;.
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Satz 4.2.16 folgt auch aus einem allgemeinen Stetigkeitsresultat über Potenzreihen, das wir hier ohne Beweis angeben.

Satz 4.2.17 (Stetigkeit von Potenzreihen)**.** *Es sei $\sum_{k=0}^{\infty} a_k z^k$ eine Potenzreihe mit Konvergenzradius $\rho > 0$. Wir betrachten die zugehörige komplexe Funktion*

$$f : \{z \in \mathbb{C} \mid |z| < \rho\} \to \mathbb{C} \quad \textit{mit} \quad f(z) \;:=\; \sum_{k=0}^{\infty} a_k z^k \;.$$

Dann ist die Funktion f stetig.

Da die Einschränkung einer stetigen Funktion auf eine Teilmenge ihres Definitionsbereichs immer noch stetig ist (dies folgt sofort aus der Definition der Stetigkeit oder alternativ aus Korollar 4.2.12), ist auch die reelle Exponentialfunktion $\exp_{\mathbb{R}}$ stetig. Folglich ist auch die Logarithmusfunktion stetig.

Korollar 4.2.18. *Der natürliche Logarithmus $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ ist stetig.*

Beweis. Folgt aus Satz 4.2.16 und Satz 4.2.11. □

Wie wir schon in Abschnitt 4.1.6 erwähnt haben, wächst die Exponentialfunktion schneller als jede Polynomfunktion und die Logarithmusfunktion wächst langsamer als die n-te Wurzel für alle $n \in \mathbb{N}$.

Lemma 4.2.19. *Es sei $p : \mathbb{R} \to \mathbb{R}$ eine beliebige Polynomfunktion. Dann gilt*

$$\lim_{x\to\infty} \frac{p(x)}{\exp(x)} \;=\; 0 \;.$$

Für beliebiges $n \in \mathbb{N}$ gilt

$$\lim_{x\to\infty} \frac{\ln(x)}{\sqrt[n]{x}} \;=\; 0 \;.$$

Beweis. Siehe Beispiel nach Definition 4.1.56 und Übung. □

Mit Hilfe der Exponentialfunktion können wir die trigonometrischen Funktionen Sinus (sin) und Cosinus (cos) einführen. Dazu benötigen wir zunächst die folgende Eigenschaft.

Lemma 4.2.20. *Die Exponentialfunktion* $\exp : \mathbb{C} \to \mathbb{C}$ *besitzt die folgenden Eigenschaften:*

(i) $\exp(\bar{z}) = \overline{\exp(z)}$ *für alle* $z \in \mathbb{C}$.

(ii) $|\exp(x+iy)| = \exp(x)$ *für alle* $x, y \in \mathbb{R}$. *Insbesondere ist* $|\exp(iy)| = 1$ *für alle* $y \in \mathbb{R}$.

Beweis. Teil (i) folgt im Wesentlichen aus Satz 4.1.17 (vi). Für (ii) genügt es zu zeigen, dass $|\exp(iy)| = 1$ für alle $y \in \mathbb{R}$. Denn daraus folgt

$$|\exp(x+iy)| \;=\; |\exp(x)\cdot\exp(iy)| \;=\; |\exp(x)|\cdot|\exp(iy)| \;=\; |\exp(x)|$$

für alle $x, y \in \mathbb{R}$. Wegen Lemma 2.3.6 (iii) gilt

$$\begin{aligned} |\exp(iy)|^2 &= \exp(iy)\cdot\overline{\exp(iy)} \\ &= \exp(iy)\cdot\exp(\overline{iy}) \\ &= \exp(iy)\cdot\exp(-iy) \\ &= \exp(iy-iy) \\ &= \exp(0) \;=\; 1 \;. \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Bemerkung. Aus Lemma 4.2.20 (ii) folgt insbesondere, dass die komplexe Zahl $\exp(iy)$ für $y \in \mathbb{R}$ auf dem komplexen Einheitskreis liegt. Man kann zeigen, dass $\exp(iy)$ genau einmal entgegen dem Uhrzeigersinn um den Einheitskreis wandert, wenn man y von 0 bis 2π erhöht. Die komplexe Zahl $\exp(i\phi)$ mit $\phi \in \mathbb{R}$ schließt also mit der positiven reellen Achse den Winkel ϕ ein (siehe Abbildung 4.2). Insbesondere gilt $\exp(i2\pi) = \exp(0) = 1$ und folglich $\exp\big(i(\phi+2\pi k)\big) = \exp(i\phi)$ für alle $\phi \in \mathbb{R}$ und $k \in \mathbb{Z}$.

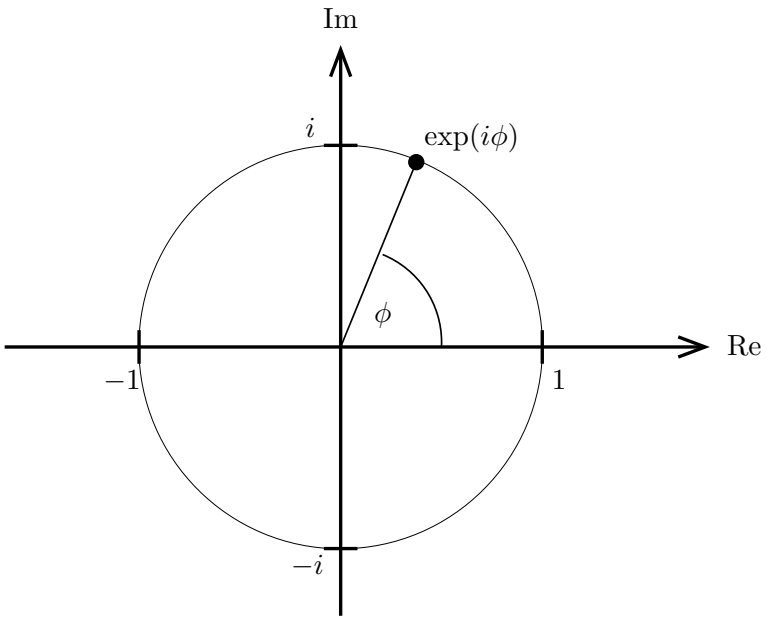


Abbildung 4.2: Das Verhalten der Funktion $\phi \mapsto \exp(i\phi)$ für $\phi \in [0, 2\pi]$.

Lemma 4.2.21. *Die Funktion* $f : \mathbb{R} \to \mathbb{C}$ *mit* $f(\phi) := \exp(i\phi)$ *ist* 2π-periodisch*, das heißt*

$$\exp\big(i(\phi + 2\pi)\big) \;=\; \exp(i\phi) \qquad \textit{für alle } \phi \in \mathbb{R}.$$

Betrachtet man Abbildung 4.2, so sieht man sehr leicht, dass der Realteil der komplexen Zahl $\exp(i\phi)$ dem Cosinus des Winkels ϕ und der Imaginärteil dem Sinus des Winkels ϕ entspricht. Da wir die Cosinus- und die Sinus-Funktion bislang nicht formal definiert haben, holen wir das an dieser Stelle nach.

Definition 4.2.22 (Cosinus und Sinus)**.** Für $\phi \in \mathbb{R}$ definieren wir

$$\cos(\phi) \;:=\; \mathrm{Re}\big(\exp(i\phi)\big) \qquad \text{und} \qquad \sin(\phi) \;:=\; \mathrm{Im}\big(\exp(i\phi)\big)\;.$$

Die dadurch definierten Funktionen $\cos : \mathbb{R} \to \mathbb{R}$ und $\sin : \mathbb{R} \to \mathbb{R}$ nennt man *Cosinus-* und *Sinus-Funktion.*

Aus den Eigenschaften der Exponentialfunktion kann man die folgenden Eigenschaften von cos und sin herleiten.

Satz 4.2.23 (Eigenschaften von Cosinus und Sinus)**.**

(i) Cosinus und Sinus sind 2π*-periodisch und es gilt für alle* $k \in \mathbb{Z}$*:*

$$\begin{aligned} \cos\big(2k\pi\big) \;=\; \sin\big(2k\pi + \pi/2\big) \;&=\; 1\;, \\ \cos\big(k\pi + \pi/2\big) \;=\; \sin\big(k\pi\big) \;&=\; 0\;, \\ \cos\big((2k+1)\pi\big) \;=\; \sin\big(2k\pi + 3\pi/2\big) \;&=\; -1\;. \end{aligned}$$

Außerdem ist $\cos(\phi) = \sin(\phi + \pi/2)$ *für alle* $\phi \in \mathbb{R}$*.*

(ii) Cosinus und Sinus sind stetige Funktionen.

(iii) $\big(\cos(x)\big)^2 + \big(\sin(x)\big)^2 = 1$ *für alle* $x \in \mathbb{R}$.

(iv) $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$ *für alle* $x, y \in \mathbb{R}$.

(v) $\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y)$ *für alle* $x, y \in \mathbb{R}$.

Die Gleichungen in (iv) *und* (v) *bezeichnet man auch als* Additionstheoreme für Cosinus und Sinus.

Beweis. Die Eigenschaften in (i) folgen unmittelbar aus den oben besprochenen Eigenschaften der Funktion $\phi \mapsto \exp(i\phi)$. Teil (ii) folgt aus Korollar 4.2.9 (iii). Teil (iii) gilt, da für $x \in \mathbb{R}$

$$\begin{aligned}\big(\cos(x)\big)^2 + \big(\sin(x)\big)^2 &= \big(\mathrm{Re}\big(\exp(i\phi)\big)\big)^2 + \big(\mathrm{Im}\big(\exp(i\phi)\big)\big)^2 \\ &= |\exp(i\phi)|^2 = 1\end{aligned}$$

wegen Lemma 4.2.20 (ii). Die Additionstheoreme in (iv) und (v) erhält man wie folgt. Für $x, y \in \mathbb{R}$ ist einerseits

$$\begin{aligned}\exp\big(i(x+y)\big) &= \exp(ix)\cdot\exp(iy) \\ &= \big(\cos(x) + i\sin(x)\big)\cdot\big(\cos(y) + i\sin(y)\big) \\ &= \big(\cos(x)\cos(y) - \sin(x)\sin(y)\big) \\ &\quad + i\big(\sin(x)\cos(y) + \cos(x)\sin(y)\big)\end{aligned}$$

Andererseits ist

$$\exp\big(i(x+y)\big) = \cos(x+y) + i\sin(x+y)\ .$$

Vergleicht man Real- und Imaginärteile der beiden Ausdrücke, so erhält man daraus (iv) und (v). □

Satz 4.2.24 (Reihenentwicklung von cos und sin)**.** *Die Funktionen* cos *und* sin *lassen sich wie folgt als Potenzreihen darstellen. Es gilt*

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} x^{2k}$$

und

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1}\ .$$

Beweis. Nach Definition der Exponentialfunktion ist

$$\exp(ix) \;=\; \sum_{k=0}^{\infty} \frac{(ix)^k}{k!} \;.$$

Wegen Satz 4.1.17 (vi) gilt dann

$$\cos(x) \;=\; \mathrm{Re}\big(\exp(ix)\big) \;=\; \sum_{k=0}^{\infty} \mathrm{Re}\left(\frac{(ix)^k}{k!}\right)$$

und

$$\sin(x) \;=\; \mathrm{Im}\big(\exp(ix)\big) \;=\; \sum_{k=0}^{\infty} \mathrm{Im}\left(\frac{(ix)^k}{k!}\right) \;.$$

Für $k \in \mathbb{N}_0$ ist

$$\mathrm{Re}\left(\frac{(ix)^k}{k!}\right) \;=\; \begin{cases} \frac{(-1)^{k/2}}{k!} x^k & \text{falls } k \text{ gerade,} \\ 0 & \text{falls } k \text{ ungerade,} \end{cases}$$

und

$$\mathrm{Im}\left(\frac{(ix)^k}{k!}\right) \;=\; \begin{cases} 0 & \text{falls } k \text{ gerade,} \\ \frac{(-1)^{(k-1)/2}}{k!} x^k & \text{falls } k \text{ ungerade.} \end{cases}$$

Daraus folgt die Behauptung. □

Wir erwähnen schließlich noch eine Eigenschaft von Cosinus und Sinus ohne Beweis.

Lemma 4.2.25. *Die Einschränkung der Cosinus-Funktion auf das Intervall* $[0, \pi]$ *definiert eine Bijektion zwischen* $[0, \pi]$ *und* $[-1, 1]$*. Analog dazu definiert die Einschränkung der Sinus-Funktion auf* $[-\pi/2, \pi/2]$ *eine Bijektion zwischen dem Intervall* $[-\pi/2, \pi/2]$ *und* $[-1, 1]$*.*

Die Umkehrfunktionen von Cosinus und Sinus heißen Arcuscosinus und Arcussinus und werden im Folgenden definiert.

Definition 4.2.26 (Arcuscosinus und Arcussinus)**.** Die Umkehrfunktionen der in Lemma 4.2.25 betrachteten Einschränkungen von Cosinus und Sinus werden *Arcuscosinus* und *Arcussinus* genannt und wie folgt bezeichnet:

$$\arccos : [-1, 1] \to [0, \pi] \qquad \text{und} \qquad \arcsin : [-1, 1] \to [-\pi/2, \pi/2] \;.$$

Schließlich definieren wir noch die Funktionen Tangens und Cotangens.

Definition 4.2.27 (Tangens, Cotangens)**.** Für $x \in \mathbb{R} \setminus \{\pi/2 + k\pi \mid k \in \mathbb{Z}\}$ ist die *Tangens-Funktion* definiert als

$$\tan(x) := \frac{\sin(x)}{\cos(x)} .$$

Für $x \in \mathbb{R} \setminus \{k\pi \mid k \in \mathbb{Z}\}$ ist die *Cotangens-Funktion* definiert als

$$\cot(x) := \frac{\cos(x)}{\sin(x)} .$$

4.2.5 Nullstellensatz und Zwischenwertsatz

Wir zeigen in diesem Abschnitt einige wichtige Eigenschaften stetiger Funktionen. Zunächst beschäftigen wir uns mit dem Nullstellensatz, der unter gewissen Bedingungen die Existenz einer Nullstelle garantiert.

Satz 4.2.28 (Nullstellensatz)**.** *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : [a, b] \to \mathbb{R}$ eine stetige Funktion. Haben $f(a)$ und $f(b)$ verschiedene Vorzeichen, dann gibt es ein $x \in [a, b]$ mit $f(x) = 0$. Wir nennen x* Nullstelle von f*.*

Der Satz ist relativ einleuchtend, wenn man sich vor Augen führt, dass man den Graphen der stetigen Funktion f ohne Absetzen des Stiftes zeichnen können muss. Da nämlich $f(a)$ und $f(b)$ verschiedene Vorzeichen haben, muss man beim Zeichnen offenbar (mindestens) einmal die horizontale x-Achse überqueren. An der Stelle, an der der Graph die x-Achse berührt, liegt dann eine Nullstelle von f vor. Wir führen im Folgenden einen formalen Beweis, der auf dem wichtigen Prinzip der *Intervallschachtelung* beruht.

Beweis. Wir betrachten den Fall, dass $f(a) < 0$ und $f(b) > 0$. Der dazu symmetrische Fall kann völlig analog behandelt werden. Wir definieren rekursiv eine Folge von Intervallen $[a_n, b_n]$ für alle $n \in \mathbb{N}_0$ mit den folgenden Eigenschaften:

(i) $f(a_n) \leq 0$ und $f(b_n) \geq 0$ für alle $n \in \mathbb{N}_0$;

(ii) $[a_n, b_n] \supseteq [a_{n+1}, b_{n+1}]$ für alle $n \in \mathbb{N}_0$;

(iii) $b_n - a_n = (b - a)/2^n$ für alle $n \in \mathbb{N}_0$.

Dazu setzen wir $a_0 := a$ und $b_0 := b$. Zu gegebenem a_n und b_n betrachten wir den Mittelpunkt $(a_n + b_n)/2$ des Intervalls $[a_n, b_n]$. Gilt $f\big((a_n + b_n)/2\big) \leq 0$, so setzen wir $a_{n+1} := (a_n + b_n)/2$ und $b_{n+1} := b_n$. Anderfalls, wenn $f\big((a_n + b_n)/2\big) > 0$, setzen wir $a_{n+1} := a_n$ und $b_{n+1} := (a_n + b_n)/2$. Man kann mit vollständiger Induktion leicht zeigen, dass dann die Eigenschaften (i), (ii) und (iii) erfüllt sind.

Wegen (ii) ist die Folge $(a_n)_{n\in\mathbb{N}}$ monoton wachsend und die Folge $(b_n)_{n\in\mathbb{N}}$ ist monoton fallend. Außerdem sind beide Folgen beschränkt und daher konvergent. Wegen (iii) ist die Folge $(b_n - a_n)_{n\in\mathbb{N}}$ eine Nullfolge, so dass also $x := \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n \in [a, b]$. Weil f stetig ist, gilt dann $f(x) = \lim_{n\to\infty} f(a_n) = \lim_{n\to\infty} f(b_n)$. Wegen (i) gilt $f(x) \leq 0$ und $f(x) \geq 0$ also $f(x) = 0$. □

Das folgende Korollar stellt eine wichtige Anwendung des Nullstellensatzes dar.

Korollar 4.2.29. *Ist p ein Polynom über $\mathbb{R}$ mit ungeradem Grad, so besitzt die zugehörige reelle Polynomfunktion $x \mapsto p(x)$ eine Nullstelle.*

Beweis. Siehe Übung. □

Als nächstes stellen wir den Zwischenwertsatz vor, der unmittelbar aus dem oben besprochenen Nullstellensatz folgt.

Satz 4.2.30 (Zwischenwertsatz)**.** *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : [a, b] \to \mathbb{R}$ eine stetige Funktion. Ist $f(a) \leq y \leq f(b)$ oder $f(a) \geq y \geq f(b)$, dann gibt es ein $x \in [a, b]$ mit $f(x) = y$.*

Beweis. Wir betrachten die Funktion $g[a, b] \to \mathbb{R}$ mit $g(z) := f(z) - y$. Da f stetig ist, ist auch g stetig und besitzt nach Satz 4.2.28 eine Nullstelle $x \in [a, b]$. Dann gilt $f(x) = g(x) + y = y$. □

Eine Konsequenz des Zwischenwertsatzes ist das folgende Resultat über injektive Funktionen.

Korollar 4.2.31. *Es sei $I \subseteq \mathbb{R}$ ein Intervall und $f : I \to \mathbb{R}$ eine stetige Funktion. Dann ist f genau dann injektiv, wenn f streng monoton wachsend oder fallend ist.*

Beweis. Ist f streng monoton wachsend oder fallend, so ist f nach Definition injektiv.

Wir nehmen im Folgenden im Widerspruch zur Behauptung an, dass f injektiv jedoch weder streng monoton wachsend noch fallend ist. Dann gibt es $x_1, x_2, x_3 \in I$ mit $x_1 < x_2 < x_3$ und

$$f(x_1) < f(x_2) \wedge f(x_2) > f(x_3) \qquad \text{oder} \qquad f(x_1) > f(x_2) \wedge f(x_2) < f(x_3) \ .$$

Wir beschränken uns im Folgenden auf ersteren Fall; der zweite Fall kann völlig analog behandelt werden. Wir wählen $y \in \mathbb{R}$ mit $\max\{f(x_1), f(x_3)\} < y < f(x_2)$. Nach Satz 4.2.30 gibt es dann ein $x \in [x_1, x_2]$ und ein $x' \in [x_2, x_3]$ mit $f(x) = y = f(x')$. Da $f(x_2) > y$ gilt $x \neq x_2 \neq x'$ und daher $x < x'$. Folglich ist f im Widerspruch zur Annahme nicht injektiv. □

Wir geben schließlich noch den folgenden Satz ohne Beweis an.

Satz 4.2.32. *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : [a, b] \to \mathbb{R}$ eine stetige Funktion. Dann gibt es $y, z \in [a, b]$ mit*

$$f(y) \ = \ \max\{f(x) \mid x \in [a, b]\}$$

und

$$f(z) \ = \ \min\{f(x) \mid x \in [a, b]\} \ .$$

Bemerkung. Die Aussage von Satz 4.2.32 gilt nicht mehr, falls wir ein Intervall der Form $(a, b]$, $[a, b)$ oder (a, b) betrachten. Ein Gegenbeispiel ist hier die Funktion $f : (0, 1] \to \mathbb{R}$ mit $f(x) := 1/x$, die offenbar unbeschränkt ist und daher kein Maximum annimmt.

Bemerkung. In allen in diesem Abschnitt vorgestellten Resultaten ist die Voraussetzung der Stetigkeit der Funktion f unabdingbar. Man kann zu jedem dieser Resultate leicht Beispiele unstetiger Funktionen konstruieren, für die das entsprechende Resultat nicht gilt. Wir lassen das als Übungsaufgabe.

4.3 Differenzialrechnung

Wir beschäftigen uns in diesem Abschnitt mit der Differenzialrechnung von (reellen) Funktionen. Im Folgenden bezeichnet $\mathbb{K}$ wieder den Körper der reellen oder komplexen Zahlen, also $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

4.3.1 Differenzierbarkeit und Ableitung von Funktionen

Wir betrachten eine reelle Funktion f. Wenn wir uns den Graphen von f vornehmen, haben wir eine gute Vorstellung davon, was es bedeuten soll, dass eine Funktion an einer stelle x_0 „glatt“ ist. Anschaulich gesprochen meinen wir damit, dass der Graph der Funktion an dieser Stelle keine „Ecke“ aufweist. Etwas mathematischer formuliert heißt das, dass die Funktion f an der Stelle x_0 eine Tangente besitzt, die sich an die Funktion „anschmiegt“.

Wie fasst man diese Vorstellung in eine formale Definition? Wir können uns dem Begriff der Tangente einer Funktion mit Hilfe des Begriffs der Sekante nähern.

Definition 4.3.1 (Sekante, Steigung)**.** Es sei $D \subseteq \mathbb{R}$ und $f : D \to \mathbb{R}$ eine reelle Funktion. Sind $x_0, x \in D$ mit $x_0 \neq x$, dann heißt die eindeutige Gerade durch die Punkte $\big(x_0, f(x_0)\big)$ und $\big(x, f(x)\big)$ *Sekante* des Graphen der Funktion f. Die *Steigung* der Sekante ist durch den Ausdruck

$$\frac{f(x) - f(x_0)}{x - x_0}$$

gegeben. Dieser Ausdruck wird auch *Differenzenquotient* genannt.

Anschaulich gesprochen erhält man die Tangente der Funktion f an der Stelle x_0 (falls die Funktion überhaupt eine Tangente an dieser Stelle besitzt), indem man den Punkt x immer näher an den Punkt x_0 heranrücken lässt und dabei die Sekante betrachtet.

Definition 4.3.2 (Differenzierbarkeit, Ableitung)**.** Es sei $D \subseteq \mathbb{R}$ und $f : D \to \mathbb{R}$ eine reelle Funktion.

(i) Ist $x_0 \in D$ und existiert der Grenzwert

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} \ , \tag{4.6}$$

so sagt man, dass f *in* x_0 *differenzierbar* ist. In diesem Fall bezeichnet man den Grenzwert (4.6) mit $f'(x_0)$ und nennt ihn die *Ableitung von* f *an der Stelle* x_0.

(ii) Ist die Funktion f an jeder Stelle $x_0 \in D$ differenzierbar, so heißt f *differenzierbar*. In diesem Fall nennt man die Funktion

$$f' : D \to \mathbb{R} \qquad \text{mit} \qquad x \mapsto f'(x)$$

die *Ableitung von* f.

Bemerkung.

(i) Existiert die Ableitung von f an der Stelle x_0, so wird die Tangente von f in x_0 durch die Funktion $x \mapsto f(x_0) + f'(x_0) \cdot (x - x_0)$ beschrieben.

(ii) Eine notwendige Voraussetzung für die Existenz des Grenzwertes (4.6) ist, dass x_0 ein Berührungspunkt von $D \setminus \{x_0\}$ ist. Das heißt, dass x_0 kein isolierter Punkt des Definitionsbereichs D sein kann. Dies entspricht auch unserer Anschauung, nach der eine reelle Funktion in einem isolierten Punkt ihres Definitionsbereichs keine Tangente besitzt.

(iii) Den Grenzwert (4.6) kann man, falls er existiert, alternativ auch wie folgt schreiben:

$$f'(x_0) \ = \ \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h} \ .$$

(iv) Definition 4.3.2 kann unmittelbar auf den Fall komplexwertiger Funktionen $f : D \to \mathbb{C}$ mit $D \subseteq \mathbb{R}$ erweitert werden. In diesem Fall ist auch f' eine komplexwertige Funktion.

(v) Die Ableitung von f an der Stelle x_0 wird manchmal auch mit $\frac{df}{dx}(x_0)$ bezeichnet.

Der folgende Satz stellt eine alternative Charakterisierung der Differenzierbarkeit einer Funktion f dar. Diese Charakterisierung ist durch die in der Bemerkung diskutierte Tangentenfunktion $x \mapsto f(x_0) + f'(x_0) \cdot (x - x_0)$ motiviert.

Satz 4.3.3. *Es sei $D \subseteq \mathbb{R}$ und $f : D \to \mathbb{K}$ eine Funktion. Weiter seien $x_0 \in D$ und $s \in \mathbb{K}$. Dann sind die beiden folgenden Aussagen äquivalent:*

(i) Die Funktion f ist in x_0 differenzierbar mit Ableitung $f'(x_0) = s$.

(ii) Es gibt eine Funktion $\varphi : D \to \mathbb{K}$ *mit* $\lim_{x\to x_0} \varphi(x) = 0$ *und*

$$f(x) \;=\; f(x_0) + s \cdot (x - x_0) + \varphi(x) \cdot (x - x_0) \qquad \textit{für alle } x \in D.$$

Beweis. Gilt (ii), so ist der Differenzenquotient gegeben durch

$$\frac{f(x) - f(x_0)}{x - x_0} \;=\; s + \varphi(x) \;\; .$$

Folglich existiert die Ableitung von f in x_0 und es gilt

$$\lim_{x\to x_0} \frac{f(x) - f(x_0)}{x - x_0} \;=\; s + \lim_{x\to x_0} \varphi(x) \;=\; s \;\; .$$

Ist umgekehrt f in x_0 differenzierbar mit $f'(x_0) = s$, so können wir die Funktion $\varphi : D \to \mathbb{K}$ wie folgt definieren:

$$\varphi(x) \;:=\; \begin{cases} \frac{f(x)-f(x_0)}{x-x_0} - s & \text{für } x \in D \setminus \{x_0\}, \\ 0 & \text{für } x = x_0. \end{cases}$$

Dann gilt $\lim_{x\to x_0} \varphi(x) = 0$, da $\lim_{x\to x_0} \frac{f(x)-f(x_0)}{x-x_0} = s$, und nach Definition von φ ist (ii) erfüllt. □

Beispiel. Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := (x+1)^2$ ist differenzierbar und es gilt $f'(x_0) = 2x_0 + 2$ für alle $x_0 \in \mathbb{R}$. Dies folgt unmittelbar aus Satz 4.3.3, denn man kann f für jedes beliebige $x_0 \in \mathbb{R}$ wie folgt schreiben:

$$\begin{aligned} f(x) \;&=\; (x+1)^2 \\ &=\; (x_0+1)^2 + (2x_0+2) \cdot (x - x_0) + (x - x_0) \cdot (x - x_0) \end{aligned}$$

für alle $x \in \mathbb{R}$. Setzt man also $\varphi(x) := x - x_0$, so ist die Bedingung aus Satz 4.3.3 (ii) erfüllt.

Eine wichtige Konsequenz von Satz 4.3.3 ist, dass aus der Differenzierbarkeit von f in x_0 insbesondere die Stetigkeit von f in x_0 folgt.

Satz 4.3.4. *Es sei* $D \subseteq \mathbb{R}$ *und* $f : D \to \mathbb{K}$ *eine Funktion. Ist* $x_0 \in D$ *und ist* f *in* x_0 *differenzierbar, so ist* f *in* x_0 *auch stetig.*

Beweis. Ist f in x_0 differenzierbar, so gilt nach Satz 4.3.3

$$\begin{aligned} \lim_{x\to x_0} f(x) \;&=\; f(x_0) + f'(x_0) \cdot \lim_{x\to x_0} (x - x_0) + \lim_{x\to x_0} \big(\varphi(x) \cdot (x - x_0)\big) \\ &=\; f(x_0) \;\; . \end{aligned}$$

Folglich ist f in x_0 stetig. □

Bemerkung. Die Umkehrung von Satz 4.3.4 gilt im Allgemeinen nicht. Ein Gegenbeispiel ist die Betragsfunktion $x \mapsto |x|$, die im Punkt 0 zwar stetig, jedoch nicht differenzierbar ist. Denn es gilt

$$\lim_{x \to 0^+} \frac{|x| - |0|}{x - 0} \;=\; 1 \qquad \text{und} \qquad \lim_{x \to 0^-} \frac{|x| - |0|}{x - 0} \;=\; -1 \;.$$

Folglich existiert der Grenzwert des Differenzenquotienten an der Stelle 0 nicht.

Beispiele.

(i) Ist $c \in \mathbb{C}$, so ist die konstante Funktion $f : \mathbb{R} \to \mathbb{C}$ mit $f(x) = c$ für alle $x \in \mathbb{R}$ differenzierbar und die Ableitung ist überall null.

(ii) Sind $a, b \in \mathbb{C}$ und ist $f : \mathbb{R} \to \mathbb{C}$ mit $f(x) = a \cdot x + b$, so ist

$$f'(x_0) \;=\; \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} \;=\; \lim_{x \to x_0} \frac{a \cdot (x - x_0)}{x - x_0} \;=\; a$$

für alle $x_0 \in \mathbb{R}$. Insbesondere ist f differenzierbar.

(iii) Ist $n \in \mathbb{N}$ und $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^n$ für alle $x \in \mathbb{R}$, so ist f differenzierbar und es gilt $f'(x) = n \cdot x^{n-1}$ für alle $x \in \mathbb{R}$. Denn wegen Lemma 4.1.42 gilt

$$\frac{(x+h)^n - x^n}{h} \;=\; \frac{\sum_{k=0}^{n} \binom{n}{k} h^k x^{n-k} - x^n}{h} \;=\; \sum_{k=1}^{n} \binom{n}{k} h^{k-1} x^{n-k} \;.$$

Folglich ist

$$\lim_{h \to 0} \frac{(x+h)^n - x^n}{h} \;=\; \binom{n}{1} x^{n-1} \;=\; n \cdot x^{n-1} \;.$$

Satz 4.3.5. *Die reelle Exponentialfunktion* $\exp : \mathbb{R} \to \mathbb{R}$ *ist differenzierbar und es gilt* $\exp' = \exp$.

Beweis. Wir zeigen zunächst, dass die reelle Exponentialfunktion an der Stelle 0 differenzierbar ist und $\exp'(0) = \exp(0) = 1$ gilt. Dazu betrachten wir für $x \neq 0$ den Differenzenquotienten

$$\frac{\exp(x) - \exp(0)}{x - 0} - 1 \;=\; \frac{1}{x} \sum_{k=1}^{\infty} \frac{x^k}{k!} - 1 \;=\; \sum_{k=1}^{\infty} \frac{x^{k-1}}{k!} - 1 \;=\; \sum_{k=2}^{\infty} \frac{x^{k-1}}{k!} \;.$$

Es genügt also zu zeigen, dass

$$\lim_{x \to 0} \sum_{k=2}^{\infty} \frac{x^{k-1}}{k!} \;=\; 0 \;.$$

Dies folgt, da für x mit $|x| < 1$ gilt, dass

$$0 \;\leq\; \left|\sum_{k=2}^{\infty} \frac{x^{k-1}}{k!}\right| \;\leq\; \sum_{k=2}^{\infty} \frac{|x|^{k-1}}{k!} \;\leq\; \sum_{k=2}^{\infty} |x|^{k-1} \;=\; \sum_{\ell=1}^{\infty} |x|^{\ell} \;=\; \frac{|x|}{1-|x|} \;.$$

Wir zeigen schließlich noch, dass $\exp'(x) = \exp(x)$ auch für $x \neq 0$ gilt. Dies folgt jetzt unmittelbar, da

$$\frac{\exp(x+h) - \exp(x)}{h} \;=\; \exp(x) \cdot \frac{\exp(h) - \exp(0)}{h}$$

und daher

$$\begin{aligned} \lim_{h\to 0} \frac{\exp(x+h) - \exp(x)}{h} \;&=\; \exp(x) \cdot \lim_{h\to 0} \frac{\exp(h) - \exp(0)}{h} \\ &=\; \exp(x) \cdot \exp'(0) \;=\; \exp(x) \cdot 1 \;. \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

In Verallgemeinerung von Satz 4.3.5 kann man das folgende Resultat zeigen.

Korollar 4.3.6. *Für $c \in \mathbb{C}$ ist die Funktion $f : \mathbb{R} \to \mathbb{C}$ mit $f(x) := \exp(c \cdot x)$ differenzierbar mit Ableitung $f'(x) = c \cdot f(x) = c \cdot \exp(c \cdot x)$.*

Satz 4.3.5 folgt auch aus einem allgemeinen Differenzierbarkeitsresultat über Potenzreihen, das wir hier ohne Beweis angeben.

Satz 4.3.7 (Differenzierbarkeit von Potenzreihen)**.** *Es sei $\sum_{k=0}^{\infty} a_k z^k$ eine Potenzreihe mit Konvergenzradius $\rho > 0$. Wir betrachten die komplexwertige Funktion*

$$f : (-\rho, \rho) \to \mathbb{C} \quad \textit{mit} \quad f(x) \;:=\; \sum_{k=0}^{\infty} a_k x^k \;.$$

Dann ist die Funktion f differenzierbar. Die Potenzreihe $\sum_{k=1}^{\infty} k a_k z^{k-1}$ hat auch den Konvergenzradius ρ und es gilt

$$f'(x) \;=\; \sum_{k=1}^{\infty} k a_k x^{k-1} \qquad\qquad \textit{für alle } x \in (-\rho, \rho).$$

4.3.2 Ableitungsregeln

Wir geben in diesem Abschnitt die wichtigsten Ableitungsregeln an, die sich bei der Bestimmung der Ableitung von Funktionen als nützlich erweisen.

Satz 4.3.8. *Es sei $D \subseteq \mathbb{R}$, $x_0 \in D$ und $f, g : D \to \mathbb{K}$ zwei Funktionen, die in x_0 differenzierbar sind. Weiter seien $\lambda, \mu \in \mathbb{K}$. Dann gilt:*

(i) Die Funktion $\lambda \cdot f + \mu \cdot g : D \to \mathbb{K}$ ist in x_0 differenzierbar mit

$$(\lambda \cdot f + \mu \cdot g)'(x_0) \;=\; \lambda \cdot f'(x_0) + \mu \cdot g'(x_0) \quad (\text{„Linearität der Ableitung“}).$$

(ii) Die Funktion $f \cdot g : D \to \mathbb{K}$ ist in x_0 differenzierbar mit

$$(f \cdot g)'(x_0) \;=\; f'(x_0) \cdot g(x_0) + f(x_0) \cdot g'(x_0) \quad (\text{„Leibniz'sche Produktregel“}).$$

(iii) Ist $g(x_0) \neq 0$, so ist die Funktion f/g in x_0 differenzierbar mit

$$\left(\frac{f}{g}\right)'(x_0) \;=\; \frac{f'(x_0) \cdot g(x_0) - f(x_0) \cdot g'(x_0)}{g(x_0)^2} \qquad (\text{„Quotientenregel“}).$$

(iv) Ist $D' \subseteq \mathbb{R}$, $y_0 \in D'$ und $h : D' \to D$ eine Funktion mit $h(y_0) = x_0$, die in y_0 differenzierbar ist. Dann ist die Funktion $f \circ h : D' \to \mathbb{K}$ in y_0 differenzierbar mit

$$(f \circ h)'(y_0) \;=\; f'\big(h(y_0)\big) \cdot h'(y_0) \qquad (\text{„Kettenregel“}).$$

Beweis. Die Linearität der Ableitung (i) folgt direkt aus der Definition der Ableitung und Satz 4.2.5 (i) und (iii).

Die Produktregel (ii) gilt, da

$$\begin{aligned}
(f \cdot g)'(x_0) &= \lim_{x \to x_0} \frac{(f \cdot g)(x) - (f \cdot g)(x_0)}{x - x_0} \\
&= \lim_{x \to x_0} \frac{f(x) \cdot g(x) - f(x_0) \cdot g(x_0) - f(x_0) \cdot g(x) + f(x_0) \cdot g(x)}{x - x_0} \\
&= \lim_{x \to x_0} \left(\frac{f(x) - f(x_0)}{x - x_0} \cdot g(x) + f(x_0) \cdot \frac{g(x) - g(x_0)}{x - x_0} \right) \\
&= \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} \cdot \lim_{x \to x_0} g(x) + f(x_0) \cdot \lim_{x \to x_0} \frac{g(x) - g(x_0)}{x - x_0} \\
&= f'(x_0) \cdot g(x_0) + f(x_0) \cdot g'(x_0) \;.
\end{aligned}$$

Die Quotientenregel (iii) kann relativ leicht mit Hilfe der Produktregel und der Kettenregel bewiesen werden. Wir lassen diesen Teil als Übung.

Die Kettenregel (iv) kann man beispielsweise mit Hilfe von Satz 4.3.3 beweisen. Wir gehen hier nicht auf die Details des Beweises ein. □

Beispiele.

(i) Es seien $a_0, \ldots, a_k \in \mathbb{C}$ und $p : \mathbb{R} \to \mathbb{C}$ die durch $p(x) := \sum_{i=0}^{k} a_i x^i$ gegebene Polynomfunktion. Dann ist p differenzierbar mit Ableitung $p'(x) = \sum_{i=1}^{k} i a_i x^{i-1}$.

(ii) Nach Korollar 4.3.6 gilt für die Funktion $f : \mathbb{R} \to \mathbb{C}$ mit $f(x) := \exp(i \cdot x)$, dass

$$f'(x) \;=\; i \cdot \exp(i \cdot x) \;=\; i \cdot \cos(x) + i^2 \cdot \sin(x) \;=\; -\,sin(x) + i \cdot \cos(x) \;.$$

Andererseits gilt nach Satz 4.3.8 (i), dass

$$f'(x) \;=\; (\cos + i \cdot \sin)'(x) \;=\; cos'(x) + i \cdot \sin'(x) \;.$$

Vergleicht man Real- und Imaginärteil der beiden Ausdrücke, so erhält man $\cos' = -\sin$ und $\sin' = \cos$.

(iii) Für $n \in \mathbb{N}$ ist die Funktion $f : \mathbb{R}\backslash\{0\}$ mit $f(x) := 1/x^n$ wegen Satz 4.3.8 (iii) differenzierbar mit Ableitung

$$f'(x) \;=\; \frac{0 \cdot x^n - 1 \cdot n \cdot x^{n-1}}{(x^n)^2} \;=\; -\,\frac{n}{x^{n+1}} \;.$$

(iv) Die Tangens-Funktion tan ist wegen Satz 4.3.8 (iii) auf ihrem gesamten Definitionsbereich differenzierbar und es gilt

$$\begin{aligned} \tan'(x) \;&=\; \left(\frac{\sin}{\cos}\right)'(x) \;=\; \frac{\sin'(x)\cos(x) - \sin(x)\cos'(x)}{\cos^2(x)} \\ &=\; \frac{\cos^2(x) + \sin^2(x)}{\cos^2(x)} \;=\; \frac{1}{\cos^2(x)} \;. \end{aligned}$$

(v) Wegen Satz 4.3.8 (iv) ist für $n \in \mathbb{N}$ die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := \sin^n(x)$ differenzierbar mit Ableitung

$$f'(x) \;=\; n \cdot \sin^{n-1}(x) \cdot \cos(x) \;.$$

Satz 4.3.9 (Ableitung der Umkehrfunktion)**.** *Es sei $I \subseteq \mathbb{R}$ ein Intervall, $x_0 \in I$ und $f : I \to \mathbb{R}$ eine stetige und streng monotone Funktion, die in x_0 differenzierbar ist mit $f'(x_0) \neq 0$. Dann ist die Umkehrfunktion $f^{-1} : f(I) \to I$ in $f(x_0)$ differenzierbar und es gilt*

$$(f^{-1})'\big(f(x_0)\big) \;=\; \frac{1}{f'(x_0)} \;.$$

Beweis. Es sei $y_0 := f(x_0)$ und $y \in f(I)$. Da f in $x_0 = f^{-1}(y_0)$ differenzierbar ist, gibt es nach Satz 4.3.3 eine Funktion $\varphi : I \to \mathbb{R}$ mit $\lim_{x \to x_0} \varphi(x) = 0$, so dass

$$\begin{aligned} y - y_0 \;&=\; f\big(f^{-1}(y)\big) - f\big(f^{-1}(y_0)\big) \\ &=\; \big(f'\big(f^{-1}(y_0)\big) + \varphi\big(f^{-1}(y)\big)\big) \cdot \big(f^{-1}(y) - f^{-1}(y_0)\big) \;. \end{aligned}$$

Folglich hat der Differenzenquotient von f^{-1} die folgende Gestalt:

$$\frac{f^{-1}(y) - f^{-1}(y_0)}{y - y_0} \;=\; \frac{1}{f'\big(f^{-1}(y_0)\big) + \varphi\big(f^{-1}(y)\big)} \;.$$

Daher ist

$$\begin{aligned}
(f^{-1})'\big(f(x_0)\big) \;&=\; \lim_{y \to y_0} \frac{f^{-1}(y) - f^{-1}(y_0)}{y - y_0} \\
&=\; \lim_{y \to y_0} \frac{1}{f'\big(f^{-1}(y_0)\big) + \varphi\big(f^{-1}(y)\big)} \\
&=\; \frac{1}{f'\big(f^{-1}(y_0)\big) + \lim_{y \to y_0} \varphi\big(f^{-1}(y)\big)} \\
&=\; \frac{1}{f'\big(f^{-1}(y_0)\big)} \;=\; \frac{1}{f'(x_0)} \;.
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Beispiele.

(i) Die Logarithmus-Funktion ist die Umkehrfunktion der Exponentialfunktion. Daher ist sie differenzierbar und für die Ableitung gilt

$$\ln'(x) \;=\; \frac{1}{\exp'\big(\ln(x)\big)} \;=\; \frac{1}{\exp\big(\ln(x)\big)} \;=\; \frac{1}{x}$$

für alle $x \in \mathbb{R}_{>0}$.

(ii) Es sei $n \in \mathbb{N}$ und $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ mit $f(x) = \sqrt[n]{x}$ die n-te Wurzelfunktion. Da f die Umkehrfunktion von $y \mapsto y^n$ ist, gilt für $x > 0$

$$f'(x) \;=\; \frac{1}{n \cdot (\sqrt[n]{x})^{n-1}} \;=\; \frac{1}{n \cdot x^{1-1/n}} \;=\; \frac{1}{n} \cdot x^{1/n-1} \;.$$

(iii) Die in Definition 4.2.26 eingeführte Umkehrfunktion der Sinusfunktion ist die Funktion $\arcsin : [-1, 1] \to [-\pi/2, \pi/2]$. Für $x \in [-1, 1]$ gilt

$$\arcsin'(x) \;=\; \frac{1}{\sin'\big(\arcsin(x)\big)} \;.$$

Da $\sin' = \cos$ und $\cos(y) = \sqrt{1 - \sin^2(y)}$ für $y \in [-\pi/2, \pi/2]$, folgt

$$\arcsin'(x) \;=\; \frac{1}{\sqrt{1 - \sin^2\big(\arcsin(x)\big)}} \;=\; \frac{1}{\sqrt{1 - x^2}} \;.$$

Zum Abschluss dieses Abschnittes betrachten wir noch Ableitungen höherer Ordnung.

Definition 4.3.10. Es sei $I \subseteq \mathbb{R}$ ein Intervall, $x_0 \in I$ und $f : I \to \mathbb{K}$ eine Funktion.

(i) Die Funktion f heißt *einmal differenzierbar (in x_0)*, falls f (in x_0) differenzierbar ist. Die Ableitung $f'(x_0)$ bezeichnet man dann auch als *erste Ableitung* und schreibt dafür $f^{(1)}(x_0)$.

(ii) Ist f differenzierbar und ist die erste Ableitung $f^{(1)}$ (in x_0) differenzierbar, so sagt man, dass f *(in x_0) zweimal differenzierbar* ist. Man nennt dann $f^{(2)}(x_0) := (f^{(1)})'(x_0)$ die *zweite Ableitung von f* (in x_0).

(iii) Es sei $n \in \mathbb{N}$. Ist f n-mal differenzierbar und ist die n-te Ableitung $f^{(n)}$ (in x_0) differenzierbar, so sagt man, dass f *(in x_0) $n+1$-mal differenzierbar* ist. Man nennt dann $f^{(n+1)}(x_0) := (f^{(n)})'(x_0)$ die *$(n+1)$-te Ableitung von f* (in x_0).

(iv) Es sei $n \in \mathbb{N}$. Ist f n-mal differenzierbar und ist $f^{(n)}$ stetig, so heißt f *n-mal stetig differenzierbar*.

(v) Ist f n-mal differenzierbar für alle $n \in \mathbb{N}$, so heißt f *unendlich oft differenzierbar* oder *beliebig oft differenzierbar*.

Bemerkung. Die zweite Ableitung von f bezeichnet man auch mit f'' oder $\frac{d^2 f}{dx^2}$, die dritte mit f''' oder $\frac{d^3 f}{dx^3}$, u.s.w.

Beispiele.

(i) Wegen $\exp' = \exp$ ist die Exponentialfunktion unendlich oft differenzierbar und es gilt $\exp^{(n)} = \exp$ für alle $n \in \mathbb{N}$.

(ii) Die durch eine beliebige Potenzreihe mit Konvergenzradius $\rho > 0$ definierte Funktion auf dem Intervall $(-\rho, \rho)$ ist nach Satz 4.3.7 unendlich oft differenzierbar.

(iii) Cosinus und Sinus sind unendlich oft differenzierbar. Für $n \in \mathbb{N}$ gilt

$$\cos^{(n)} = \begin{cases} \cos & \text{falls } n \bmod 4 = 0, \\ -\sin & \text{falls } n \bmod 4 = 1, \\ -\cos & \text{falls } n \bmod 4 = 2, \\ \sin & \text{falls } n \bmod 4 = 3, \end{cases}$$

und

$$\sin^{(n)} \;=\; \begin{cases} \sin & \text{falls } n \bmod 4 = 0, \\ \cos & \text{falls } n \bmod 4 = 1, \\ -\sin & \text{falls } n \bmod 4 = 2, \\ -\cos & \text{falls } n \bmod 4 = 3. \end{cases}$$

(iv) Ist $f : \mathbb{R} \to \mathbb{C}$ eine Polynomfunktion vom Grad k mit

$$f(x) \;=\; a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0 \;\;,$$

so ist f unendlich oft differenzierbar. Die k-te Ableitung $f^{(k)}$ ist konstant, nämlich $f^{(k)}(x) = k! \cdot a_k$ für alle $x \in \mathbb{R}$, und jede höhere Ableitung $f^{(n)}$ mit $n > k$ ist die Nullfunktion.

(v) Die Logarithmus-Funktion $\ln : (0, \infty) \to \mathbb{R}$ ist unendlich oft differenzierbar. Es gilt

$$\ln'(x) \;=\; \frac{1}{x}\;, \qquad \ln''(x) \;=\; -\frac{1}{x^2}\;, \qquad \ln'''(x) \;=\; \frac{2}{x^3}$$

und allgemeiner

$$\ln^{(n)}(x) \;=\; (-1)^{n-1} \frac{(n-1)!}{x^n} \qquad \text{für } n \in \mathbb{N}.$$

(vi) Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x \cdot |x|$ ist differenzierbar. Es gilt

$$f(x) \;=\; \begin{cases} -x^2 & \text{für } x < 0, \\ x^2 & \text{für } x \geq 0, \end{cases} \quad \text{und} \quad f'(x) \;=\; \begin{cases} -2x & \text{für } x < 0, \\ 2x & \text{für } x > 0. \end{cases}$$

Die Ableitung an der Stelle 0 bestimmen wir mit Hilfe des Differenzenquotienten:

$$f'(0) \;=\; \lim_{x \to 0} \frac{x|x| - 0}{x - 0} \;=\; \lim_{x \to 0} |x| \;=\; 0 \;\;.$$

Es gilt also, dass $f'(x) = 2|x|$ für alle $x \in \mathbb{R}$. Folglich ist f sogar stetig differenzierbar, jedoch nicht zweimal differenzierbar, da f' an der Stelle 0 nicht differenzierbar ist.

(vii) Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(x) \;:=\; \begin{cases} x^2 \sin(1/x) & \text{für } x \neq 0, \\ 0 & \text{für } x = 0, \end{cases}$$

ist differenzierbar, jedoch nicht stetig differenzierbar. Wir lassen den Beweis als Übung.

Bemerkung. „Im Herbst 1972 verkündete Präsident Nixon, die Beschleunigungsrate der Inflation nehme ab. Dies war das erste Mal, dass ein amtierender Präsident zugunsten seiner Wiederwahl die dritte Ableitung ins Feld führte." (Zitat des Mathematikers Hugo Rossi)

4.3.3 Mittelwertsätze und Extrema

Wir gehen in diesem Abschnitt zunächst auf die Nützlichkeit der Differenzierbarkeit bei der Lösung von Extremwertaufgaben ein.

Definition 4.3.11 (Globale und lokale Extremwerte)**.** Es sei $D \subseteq \mathbb{R}$, $x_0 \in D$ und $f : D \to \mathbb{R}$ eine reelle Funktion.

(i) x_0 heißt *globales Maximum von* f, wenn $f(x) \leq f(x_0)$ für alle $x \in D$.

(ii) x_0 heißt *lokales Maximum von* f, wenn es ein $\varepsilon > 0$ gibt mit $f(x) \leq f(x_0)$ für alle $x \in D$ mit $|x - x_0| < \varepsilon$.

Globale und lokale *Minima* werden analog definiert, indem man „$\leq$" durch „$\geq$" ersetzt. Ein (globales oder lokales) Maximum oder Minimum heißt auch *(globales oder lokales) Extremum.*

Bemerkung. Ein globales Maximum (Minimum) ist immer auch ein lokales Maximum (Minimum).

Wir zeigen zunächst das folgende notwendige Kriterium für lokale Extrema einer differenzierbaren Funktion.

Lemma 4.3.12. *Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$, $a < x_0 < b$ und $f : (a, b) \to \mathbb{R}$ eine in x_0 differenzierbare Funktion. Ist x_0 ein lokales Extremum von f, so ist $f'(x_0) = 0$.*

Beweis. Wir nehmen im Folgenden an, dass x_0 ein lokales Minimum ist. Den Fall eines lokalen Maximums kann man völlig analog behandeln. Es sei $\varepsilon > 0$ mit $a < x_0 - \varepsilon < x_0 + \varepsilon < b$ und $f(x) \geq f(x_0)$ für alle x mit $|x - x_0| < \varepsilon$. Dann gilt für den Differenzenquotienten

$$\frac{f(x) - f(x_0)}{x - x_0} \begin{cases} \geq 0 & \text{falls } x > x_0, \\ \leq 0 & \text{falls } x < x_0. \end{cases}$$

Folglich ist der rechtsseitige Grenzwert des Differenzenquotienten nicht-negativ und der linksseitige Grenzwert ist nicht-positiv. Daher muss der Grenzwert $f'(x_0)$ gleich null sein. □

Bemerkung. Die Umkehrung der Aussage von Lemma 4.3.12 gilt im Allgemeinen nicht. Die Funktion $x \mapsto x^3$ besitzt an der Stelle $x_0 = 0$ offenbar kein lokales Extremum. Ihre Ableitung ist dort aber null.

Wir werden sehen, dass die Umkehrung der Aussage von Lemma 4.3.12 jedoch unter gewissen Zusatzbedingungen gilt. Dazu benötigen wir zunächst den Mittelwertsatz.

Satz 4.3.13 (Mittelwertsatz der Differentialrechnung)**.** *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : [a, b] \to \mathbb{R}$ eine stetige Funktion, die in jedem Punkt $x \in (a, b)$ differenzierbar ist. Dann gibt es ein $x_0 \in (a, b)$ mit*

$$\frac{f(b) - f(a)}{b - a} \;=\; f'(x_0) \;\; .$$

Bevor wir den Mittelwertsatz beweisen, formulieren wir zunächst ein einfaches Korollar, das unter dem Namen „Satz von Rolle“ bekannt ist.

Korollar 4.3.14 (Satz von Rolle)**.** *Es seien $a, b \in \mathbb{R}$ und $f : [a, b] \to \mathbb{R}$ eine stetige Funktion, die in jedem Punkt $x \in (a, b)$ differenzierbar ist. Ist $f(a) = f(b)$, so gibt es ein $x_0 \in (a, b)$ mit $f'(x_0) = 0$.*

Beweis von Satz 4.3.13. Wir beweisen zunächst den Spezialfall aus Korollar 4.3.14. Ist f konstant, so ist $f'(x) = 0$ für alle $x \in [a, b]$. Andernfalls besitzt f gemäß Satz 4.2.32 ein globales Maximum x_0 und ein globales Minimum x_1. Da f nicht konstant ist, muss mindestens einer der beiden Funktionswerte $f(x_0)$ und $f(x_1)$ von $f(a) = f(b)$ verschieden sein. Dann gilt also $x_0 \in (a, b)$ oder $x_1 \in (a, b)$. Außerdem ist die Ableitung an dieser Stelle nach Lemma 4.3.12 gleich null. Damit ist der Satz von Rolle bewiesen.

Der allgemeine Mittelwertsatz folgt jetzt sofort daraus, wenn man die Funktion $h : [a, b] \to \mathbb{R}$ mit

$$h(x) \;:=\; f(x) - \frac{f(b) - f(a)}{b - a}(x - a)$$

betrachtet. Denn offenbar gilt

$$h(a) = h(b) = f(a) \qquad \text{und} \qquad h'(x) = f'(x) - \frac{f(b) - f(a)}{b - a} \;\; .$$

Damit ist der Beweis abgeschlossen. □

Als Konsequenz aus dem Mittelwertsatz können wir das folgende Monotoniekriterium formulieren.

Lemma 4.3.15 (Monotoniekriterien)**.** *Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$ und $f : (a, b) \to \mathbb{R}$ eine differenzierbare Funktion.*

(i) Es gilt genau dann $f'(x) \geq 0$ ($f'(x) \leq 0$) für alle $x \in (a, b)$, wenn f monoton wachsend (fallend) ist.

(ii) Ist $f'(x) > 0$ ($f'(x) < 0$) für alle $x \in (a,b)$, so ist f streng monoton wachsend (fallend).

(iii) Es gilt genau dann $f'(x) = 0$ für alle $x \in (a,b)$, wenn f konstant ist.

Beweisskizze. Für (i) bis (iii) folgt die Implikation „$\Rightarrow$“ unmittelbar aus dem Mittelwertsatz 4.3.13. Die Implikation „$\Leftarrow$“ in (i) und (iii) folgt direkt aus der Definition der Ableitung mit Hilfe des Differenzenquotienten. □

Korollar 4.3.16. *Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$ und $f, g : (a,b) \to \mathbb{R}$ zwei differenzierbare Funktionen mit $f'(x) = g'(x)$ für alle $x \in (a,b)$. Dann gibt es ein $c \in \mathbb{R}$ mit $f(x) = g(x) + c$ für alle $x \in (a,b)$.*

Beweis. Die Ableitung der Funktion $f - g$ ist nach Voraussetzung überall null, so dass $f - g$ nach Lemma 4.3.15 (iii) konstant ist. □

Auch das nächste Korollar folgt direkt aus Lemma 4.3.15.

Korollar 4.3.17. *Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$ und $f : (a,b) \to \mathbb{R}$ eine differenzierbare Funktion. Weiter seien $\alpha, \beta, x_0 \in \mathbb{R}$ mit $a \le \alpha < x_0 < \beta \le b$ und $f'(x_0) = 0$. Gilt $f'(x) \ge 0$ ($f'(x) \le 0$) für alle $x \in (\alpha, x_0)$ und $f'(x) \le 0$ ($f'(x) \ge 0$) für alle $x \in (x_0, \beta)$, so hat f in x_0 ein lokales Maximum (Minimum).*

Ist f zweimal differenzierbar, so erhält man ein einfacheres Kriterium.

Satz 4.3.18. *Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$ und $f : (a,b) \to \mathbb{R}$. Weiter sei $x_0 \in (a,b)$ und f sei in x_0 zweimal differenzierbar. Ist $f'(x_0) = 0$ und $f''(x_0) < 0$ ($f''(x_0) > 0$), so besitzt f in x_0 ein lokales Maximum (Minimum).*

Beweis. Es sei $f'(x_0) = 0$ und $f''(x_0) < 0$. Nach Definition der zweiten Ableitung gilt

$$0 \;>\; f''(x_0) \;=\; \lim_{x \to x_0} \frac{f'(x) - f'(x_0)}{x - x_0} \;=\; \lim_{x \to x_0} \frac{f'(x)}{x - x_0} \;,$$

so dass also $f'(x)/(x - x_0) < 0$ in einer kleinen Umgebung von x_0. Folglich sind die Voraussetzungen von Korollar 4.3.17 erfüllt und x_0 ist ein lokales Maximum. Der Beweis für den Fall eines lokalen Minimums funktioniert völlig analog. □

Beispiele.

(i) Es seien $a, b, c \in \mathbb{R}$ mit $a \neq 0$ und $f(x) := ax^2 + bx + c$ eine Polynomfunktion vom Grad zwei. Dann besitzt die Ableitung $f'(x) = 2ax + b$ eine eindeutige Nullstelle bei $x_0 = -b/(2a)$. Ist $a > 0$ ($a < 0$), so gilt $f'(x) < 0$ ($f'(x) > 0$) für $x < x_0$ und $f'(x) > 0$ ($f'(x) < 0$) für $x > x_0$. Folglich ist x_0 nach Korollar 4.3.17 ein lokales Minimum (Maximum) von f. Noch einfacher erkennt man das mit Hilfe von Satz 4.3.18, da $f''(x_0) = 2a$. Man kann sich überlegen, dass x_0 sogar ein globales Minimum (Maximum) von f ist.

(ii) Wir betrachten die Funktion $f : (0, \infty) \to \mathbb{R}$ mit $f(x) := x^x = \exp\big(x \ln(x)\big)$. Dann ist

$$f'(x) \;=\; \big(x \ln(x)\big)' \exp\big(x \ln(x)\big) \;=\; \big(\ln(x) + 1\big) x^x$$

und

$$f''(x) \;=\; \frac{1}{x} x^x + \big(\ln(x) + 1\big)^2 x^x \;\; .$$

Die einzige Nullstelle von f' ist $1/e$ und es gilt $f''(1/e) > 0$. Folglich ist $1/e$ ein lokales (und sogar das globale) Minimum.

Zum Abschluss dieses Abschnittes stellen wir die Regeln von de L'Hôpital vor. Dazu benötigen wir zunächst den folgenden verallgemeinerten Mittelwertsatz.

Satz 4.3.19 (Verallgemeinerter Mittelwertsatz)**.** *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f, g : [a, b] \to \mathbb{R}$ zwei stetige Funktion, die in jedem Punkt $x \in (a, b)$ differenzierbar sind. Weiter gelte $g'(x) \neq 0$ für alle $x \in (a, b)$. Dann gibt es ein $x_0 \in (a, b)$ mit*

$$\frac{f(b) - f(a)}{g(b) - g(a)} \;=\; \frac{f'(x_0)}{g'(x_0)} \;\; .$$

Bemerkung. Setzt man $g(x) := x$ in Satz 4.3.19, so erhält man den bereits bekannten Mittelwertsatz 4.3.13.

Beweis. Es sei $h : [a, b] \to \mathbb{R}$ mit

$$h(x) \;:=\; f(x) - \frac{f(b) - f(a)}{g(b) - g(a)} \big(g(x) - g(a)\big) \;\; .$$

Nach Definition ist h stetig und in jedem Punkt $x \in (a, b)$ differenzierbar. Außerdem ist $h(a) = h(b) = f(a)$. Folglich gibt es nach Korollar 4.3.14 ein $x_0 \in (a, b)$ mit $h'(x_0) = 0$. Da

$$h'(x) \;=\; f'(x) - \frac{f(b) - f(a)}{g(b) - g(a)} g'(x)$$

folgt die Behauptung. □

Satz 4.3.20 (Regeln von de L'Hôpital)**.** *Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f, g : (a, b] \to \mathbb{R}$ zwei differenzierbare Funktion mit $g(x) \neq 0$ und $g'(x) \neq 0$ für alle $x \in (a, b]$.*

(i) Gilt $\lim_{x \to a} f(x) = \lim_{x \to a} g(x) = 0$ und existiert der (uneigentliche) Grenzwert $\lim_{x \to a} \big(f'(x)/g'(x)\big) \in \mathbb{R} \cup \{-\infty, \infty\}$, so gilt

$$\lim_{x \to a} \frac{f(x)}{g(x)} \;=\; \lim_{x \to a} \frac{f'(x)}{g'(x)} \;\; .$$

(ii) Gilt $\lim_{x\to a} f(x) = \pm\infty$ *und* $\lim_{x\to a} g(x) = \pm\infty$ *und existiert der (uneigentliche) Grenzwert* $\lim_{x\to a}\big(f'(x)/g'(x)\big) \in \mathbb{R} \cup \{-\infty, \infty\}$*, so gilt*

$$\lim_{x\to a} \frac{f(x)}{g(x)} \;=\; \lim_{x\to a} \frac{f'(x)}{g'(x)} \;.$$

Bemerkung. Der Satz gilt natürlich auch, wenn wir das Intervall $(a, b]$ durch $[b, a)$ (für $b < a$) ersetzen. Außerdem gilt er auch für den Fall, dass $a = -\infty$ bzw. $a = +\infty$ ist.

Beweisskizze. Wir beweisen nur (i): Nach Voraussetzung kann man f und g durch $f(a) = g(a) = 0$ stetig ergänzen. Nach Satz 4.3.19 gibt es dann zu jedem $x \in (a, b)$ ein $x_0 \in (a, x)$ mit

$$\frac{f(x)}{g(x)} \;=\; \frac{f(x) - f(a)}{g(x) - g(a)} \;=\; \frac{f'(x_0)}{g'(x_0)} \;.$$

Lassen wir nun x gegen a konvergieren, so konvergiert auch x_0 gegen a, so dass

$$\lim_{x\to a} \frac{f(x)}{g(x)} \;=\; \lim_{x_0\to a} \frac{f'(x_0)}{g'(x_0)} \;.$$

□

Beispiele.

(i) Es seien $f(x) = x^2$ und $g(x) = \sqrt{x^2+1} - 1$ für $x \geq 0$. Dann ist $f(0) = g(0) = 0$ und $f'(x) = 2x$, $g'(x) = 2x/(2\sqrt{x^2+1})$. Es gilt

$$\lim_{x\to 0} \frac{f'(x)}{g'(x)} \;=\; \lim_{x\to 0} 2\sqrt{x^2+1} \;=\; 2$$

und daher auch

$$\lim_{x\to 0} \frac{f(x)}{g(x)} \;=\; 2 \;.$$

(ii) Wir betrachten noch einmal f und g aus dem letzten Beispiel. Offenbar gilt $\lim_{x\to\infty} f(x) = \infty$ und $\lim_{x\to\infty} g(x) = \infty$. Da

$$\lim_{x\to\infty} \frac{f'(x)}{g'(x)} \;=\; \lim_{x\to\infty} 2\sqrt{x^2+1} \;=\; \infty \;,$$

folgt auch

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} \;=\; \infty \;.$$

(iii) Es sei $f(x) = \sin(x)$ und $g(x) = x$ für $x \in \mathbb{R}$. Dann gilt $f(0) = g(0) = 0$, $f'(x) = \cos(x)$ und $g'(x) = 1$. Folglich ist

$$\lim_{x\to 0} \frac{\sin(x)}{x} \;=\; \lim_{x\to 0} \frac{\cos(x)}{1} \;=\; 1 \;.$$

(iv) Es sei $f(x) = \exp(x) - \exp(-x)$ und $g(x) = \sin(x)$ für $x \in \mathbb{R}$. Dann gilt $f(0) = g(0) = 0$, $f'(x) = \exp(x) + \exp(-x)$ und $g'(x) = \cos(x)$. Folglich ist

$$\lim_{x\to 0} \frac{e^x - e^{-x}}{\sin(x)} \;=\; \lim_{x\to 0} \frac{e^x + e^{-x}}{\cos(x)} \;=\; 2 \;.$$

(v) Bei der Berechnung des Grenzwertes $\lim_{x\to 0} x\ln(x)$ führt es nicht zum Ziel, die Regel von de L'Hôpital auf die beiden Funktionen $f(x) = x$ und $g(x) = 1/\ln(x)$ anzuwenden. Denn es gilt $f'(x) = 1$ und $g'(x) = -1/(x\ln^2(x))$, so dass $f'(x)/g'(x) = -x\ln^2(x)$. Über den Grenzwert des letzten Terms für x gegen 0 kann man wieder keine direkte Aussage treffen.

Setzt man jedoch $f(x) = \ln(x)$ und $g(x) = 1/x$, so erhält man $f'(x) = 1/x$ und $g'(x) = -1/x^2$ und daher

$$\lim_{x\to 0} x\ln(x) \;=\; \lim_{x\to 0} \frac{\frac{1}{x}}{-\frac{1}{x^2}} \;=\; \lim_{x\to 0} -x \;=\; 0 \;.$$

(vi) Man kann die Regel von de L'Hôpital auch rekursiv anwenden, wie das folgende Beispiel zeigt. Für $n \in \mathbb{N}$ gilt

$$\begin{aligned}\lim_{x\to\infty} \frac{e^x}{x^n} \;&=\; \lim_{x\to\infty} \frac{e^x}{n\cdot x^{n-1}} \;=\; \lim_{x\to\infty} \frac{e^x}{n(n-1)\cdot x^{n-2}} \\ &=\; \cdots \;=\; \lim_{x\to\infty} \frac{e^x}{n!} \;=\; \infty \;.\end{aligned}$$

Die dadurch getroffene Aussage, dass die Exponentialfunktion schneller als jede Polynomfunktion wächst, hatten wir schon früher kennengelernt.

(vii) Auch der folgende Grenzwert ist uns eigentlich schon bekannt.Für $n \in \mathbb{N}$ ist

$$\lim_{x\to\infty} \frac{\ln(x)}{\sqrt[n]{x}} \;=\; \lim_{x\to\infty} \frac{\frac{1}{x}}{\frac{1}{n}x^{1/n-1}} \;=\; \lim_{x\to\infty} \frac{1}{\frac{1}{n}\sqrt[n]{x}} \;=\; 0 \;.$$

4.3.4 Taylorreihen

Bei der Einführung der Differentialrechnung haben wir die Interpretation der Ableitung als Steigung der Tangente der Funktion genutzt. Man kann sagen, dass

die Tangente an eine Funktion f in der Stelle x_0 die Funktion in einer Umgebung von x_0 approximiert. Die Tangente ist durch die folgende Funktion g gegeben:

$$g(x) \ := \ f(x_0) + f'(x_0) \cdot (x - x_0) \ .$$

In Satz 4.3.3 haben wir gezeigt, dass für den Fehlerterm $f(x) - g(x)$ gilt, dass er sich besser verhält als $(x - x_0)$, das heißt

$$\lim_{x \to x_0} \frac{f(x) - g(x)}{x - x_0} \ = \ 0 \ .$$

Ist die Funktion f an der Stelle x_0 mehr als einmal differenzierbar, so kann man versuchen, mit Hilfe höherer Ableitungen eine bessere Approximation von f in einer Umgebung von x_0 zu bekommen.

Definition 4.3.21 (Taylorpolynom)**.** Es sei $D \subseteq \mathbb{R}$, $x_0 \in D$ und $f : D \to \mathbb{K}$ eine Funktion, die an der Stelle x_0 mindestens n-mal differenzierbar ist für ein $n \in \mathbb{N}$. Dann heißt das Polynom

$$T_{f,n}(x, x_0) \ := \ \sum_{i=0}^{n} \frac{f^{(i)}(x_0)}{i!}(x - x_0)^i$$

n-tes Taylorpolynom von f mit Entwicklungspunkt x_0.

Bemerkung. Das erste Taylorpolynom $T_{f,1}(x, x_0)$ beschreibt offenbar die Tangente an f im Punkt x_0.

Beispiel. Es sei $f(x) = \sin(x)$. Das erste Taylorpolynom von sin mit Entwicklungspunkt 0 ist

$$T_{\sin,1}(x, 0) \ = \ \sin(0) + sin'(0)x \ = \ x \ .$$

Da $\sin''(0) = -\sin(0) = 0$, stimmt das zweite mit dem ersten Taylorpolynom überein, also $T_{\sin,2}(x, 0) = T_{\sin,1}(x, 0) = x$ für alle $x \in \mathbb{R}$. Für das dritte Taylorpolynom gilt

$$T_{\sin,3}(x, 0) \ = \ x - \tfrac{1}{6}x^3 \ .$$

Allgemeiner gilt für das $(2n + 1)$-te Taylorpolynom

$$T_{\sin,2n+1}(x, 0) \ = \ \sum_{k=0}^{n} \frac{(-1)^k}{(2k + 1)!}x^{2k+1} \ .$$

Man beachte, dass es sich hierbei um die ersten $n + 1$ Summanden der Reihenentwicklung der Sinus-Funktion handelt (siehe Satz 4.2.24).

Lemma 4.3.22. *Es sei $D \subseteq \mathbb{R}$, $x_0 \in D$ und $f : D \to \mathbb{K}$ eine Funktion, die an der Stelle x_0 n-mal differenzierbar ist für ein $n \in \mathbb{N}$. Dann ist das Taylorpolynom $T_{f,n}(x, x_0)$ die einzige Polynomfunktion $p : D \to \mathbb{K}$ vom Grad höchstens n mit $p^{(k)}(x_0) = f^{(k)}(x_0)$ für $k = 0, \ldots, n$.*

Beweis. Man rechnet leicht nach, dass das Taylorpolynom $T_{f,n}(x, x_0)$ aufgrund seiner Definition die geforderte Eigenschaft besitzt.

Um die Eindeutigkeit zu beweisen, betrachten wir die Basisfolge $\big(1, x-x_0, (x-x_0)^2, \ldots, (x-x_0)^n\big)$ des Vektorraums aller Polynome vom Grad höchstens n. Es sei p ein Polynom vom grad höchstens n mit der geforderten Eigenschaft. Wir können p schreiben als

$$p(x) \;=\; \sum_{i=0}^{n} a_i (x - x_0)^i \qquad \text{mit } a_0, \ldots, a_n \in \mathbb{K}.$$

Nach Voraussetzung gilt dann für $k = 0, \ldots, n$

$$f^{(k)}(x_0) \;=\; p^{(k)}(x_0) \;=\; k! \cdot a_k \;\;,$$

so dass $a_k = f^{(k)}(x_0)/k!$. Folglich stimmt p mit dem Taylorpolynom überein. □

Der folgende Satz von Taylor liefert eine genaue Beschreibung der Abweichung zwischen einer Funktion f und ihrem Taylorpolynom. Mit Hilfe dieses Satzes kann man also abschätzen, wie groß der Fehler ist, den man in Kauf nimmt, wenn man statt einer (komplizierten) Funktion ihr Taylorpolynom auswertet.

Satz 4.3.23 (Satz von Taylor)**.** *Es sei $n \in \mathbb{N}$, $a < b$ und $f : [a, b] \to \mathbb{R}$ eine n-mal stetig differenzierbare Funktion, die auf dem offenen Intervall (a, b) mindestens $(n+1)$-mal differenzierbar ist. Dann gibt es zu jedem $x \in (a, b]$ ein $y \in (a, x)$ mit*

$$f(x) \;=\; T_{f,n}(x, a) + \frac{f^{(n+1)}(y)}{(n+1)!}(x - a)^{n+1} \;\;. \tag{4.7}$$

Den zweiten Summanden auf der rechten Seite von (4.7) *nennt man* Restglied*.*

Beweis. Wir betrachten die Funktion $g : (a, b) \to \mathbb{R}$ mit

$$g(z) \;:=\; f(z) - T_{f,n}(z, a) - \frac{f(x) - T_{f,n}(x, a)}{(x - a)^{n+1}} \cdot (z - a)^{n+1} \;\;.$$

Dann ist g mindestens $(n + 1)$-mal differenzierbar und, da die Polynomfunktion $z \mapsto T_{f,n}(z, a)$ höchstens den Grad n besitzt, gilt

$$g^{(n+1)}(z) \;=\; f^{(n+1)}(z) - \frac{f(x) - T_{f,n}(x, a)}{(x - a)^{n+1}} \cdot (n + 1)! \;\;. \tag{4.8}$$

Wegen Lemma 4.3.22 gilt $g(a) = g'(a) = \cdots = g^{(n)}(a) = 0$; außerdem gilt $g(x) = 0$. Nach Korollar 4.3.14 (Satz von Rolle) gibt es also ein $x_1 \in (a, x)$ mit $g'(x_1) = 0 = g'(a)$. Wendet man den Satz von Rolle ein zweites mal an, so erhält man ein $x_2 \in (a, x_1)$ mit $g''(x_2) = 0 = g''(a)$. Nach weiteren $n-1$ Anwendungen des Satzes erhält man schließlich ein $y = x_{n+1} \in (a, x_n) \subset (a, x)$ mit $g^{(n+1)}(y) = 0$. Wegen (4.8) folgt daraus die Behauptung des Satzes. □

Bemerkung. Der Satz gilt natürlich analog für den Fall, dass wir ein Intervall $[b, a]$ links des Entwicklungspunktes a betrachten.

Beispiel. In Fortsetzung des Beispiels von oben betrachten wir nochmal die Sinusfunktion. Nach dem Satz von Taylor gilt für $n \in \mathbb{N}_0$

$$|\sin(x) - T_{\sin,2n+1}(x, 0)| \;\leq\; \frac{|x|^{2n+2}}{(2n+2)!} \;,$$

da $|\sin^{2n+2}(y)| = |\sin(y)| \leq 1$. Wenn man also $\sin(1/2)$ bis auf 12 Nachkommastellen genau berechnen möchte, kann man dazu das Taylorpolynom $T_{\sin,11}(x, 0)$ auswerten, da

$$|\sin(1/2) - T_{\sin,11}(1/2, 0)| \;\leq\; \frac{1/2^{12}}{12!} \;\leq\; 5.1 \cdot 10^{-13} \;.$$

Definition 4.3.24 (Taylor-Reihen)**.** Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : (a, b) \to \mathbb{R}$ eine unendlich oft differenzierbare Funktion. Dann heißt für $x_0 \in (a, b)$ die Reihe

$$T_f(x, x_0) \;:=\; \sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k$$

die *Taylor-Reihe von f mit Entwicklungspunkt x_0*.

Bemerkung. Wie weiter oben bemerkt, stimmt die Taylor-Reihe der Sinus-Funktion mit Entwicklungspunkt 0 mit der Sinusfunktion überein. Leider verhält sich die Taylor-Reihe nicht immer so gut. Es gibt Funktionen, deren Taylorreihen den Konvergenzradius null haben. Bei anderen Funktionen hat die Taylor-Reihe zwar einen positiven Konvergenzradius, konvergiert jedoch nicht gegen die zu Grunde liegende Funktion.

Definition 4.3.25 (Analytische Funktionen)**.** Es seien $a, b \in \mathbb{R}$ mit $a < b$ und $f : (a, b) \to \mathbb{R}$ eine unendlich oft differenzierbare Funktion. Dann heißt f *analytisch* im Punkt $x_0 \in (a, b)$, falls es ein $\varepsilon > 0$ gibt, so dass sich f auf dem Intervall $(x_0 - \varepsilon, x_0 + \varepsilon)$ als Potenzreihe darstellen lässt; das heißt es gibt eine reelle Folge $(a_n)_{n \in \mathbb{N}_0}$ mit

$$f(x) \;=\; \sum_{k=0}^{\infty} a_k (x - x_0)^k \qquad \text{für } x \in (x_0 - \varepsilon, x_0 + \varepsilon).$$

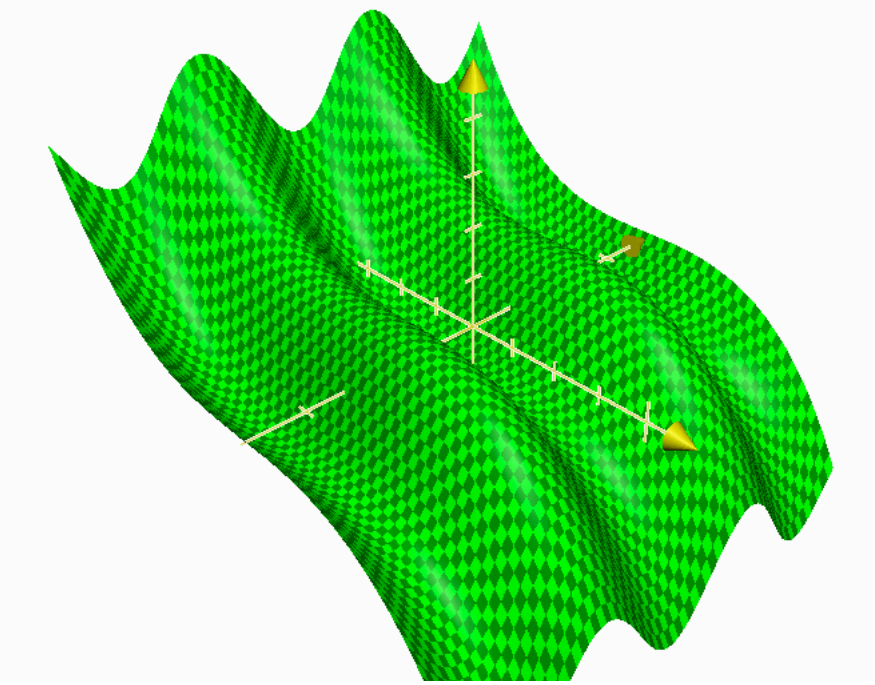


Abbildung 4.3: Der Graph der Funktion $f(x,y) = -\frac{x^3}{300} - \cos(y)$.

Zum Abschluss dieses Abschnitts erwähnen wir noch den folgenden Satz ohne Beweis.

Satz 4.3.26. *Es seien $a, b, x_0 \in \mathbb{R}$ mit $a < x_0 < b$ und $f : (a,b) \to \mathbb{R}$ eine in x_0 analytische Funktion. Dann ist die entsprechende Potenzreihe aus Definition 4.3.25 gleich der Taylor-Reihe von f mit Entwicklungspunkt x_0.*

4.3.5 Funktionen mehrerer Veränderlicher

Wir gehen in diesem Abschnitt kurz auf Funktionen mehrerer reeller Veränderlicher ein und diskutieren insbesondere die Verallgemeinerung des Differenzierbarkeitsbegriffs auf diese Klasse von Funktionen. Ein Beispiel einer solchen Funktion ist die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}$ mit

$$f(x,y) \;:=\; -\frac{x^3}{300} - \cos(y) \;.$$

Der Graph dieser Funktion ist in Abbildung 4.3 dargestellt.

Definition 4.3.27 (Partielle Ableitung)**.** Es sei $n \in \mathbb{N}$, $i \in \{1, \ldots, n\}$ und $f : \mathbb{R}^n \to \mathbb{R}$ eine Funktion. Für fest gewählte $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in \mathbb{R}$ ist die zu f gehörende *i-te partielle Funktion* $f_i : \mathbb{R} \to \mathbb{R}$ gegeben durch

$$f_i(x_i) \;:=\; f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \;.$$

Ist f_i an der Stelle $x_i \in \mathbb{R}$ differenzierbar, so heißt $f_i'(x_i)$ die *partielle Ableitung von f nach x_i an der Stelle* $\mathbf{x} = (x_1, \ldots, x_n)$ oder die *i-te partielle Ableitung von f an der Stelle* $\mathbf{x} = (x_1, \ldots, x_n)$. Man verwendet dann auch die Bezeichnungen

$$f_i'(x_i) \;=\; \frac{\partial f}{\partial x_i}(\mathbf{x}) \;=\; \frac{\partial}{\partial x_i} f(\mathbf{x}) \;\; .$$

Die Funktion f heißt *partiell differenzierbar an der Stelle* $\mathbf{x}$, falls die i-te partielle Ableitung von f an der Stelle $\mathbf{x}$ für alle $i = 1, \ldots, n$ existiert. In diesem Fall heißt der Vektor

$$\operatorname{grad} f(\mathbf{x}) \;:=\; \left(\frac{\partial f}{\partial x_1}(\mathbf{x}), \ldots, \frac{\partial f}{\partial x_n}(\mathbf{x}) \right)$$

der *Gradient* von f an der Stelle $\mathbf{x}$. Ist f an jeder Stelle $\mathbf{x} \in \mathbb{R}^n$ partiell differenzierbar, so nennt man f *partiell differenzierbar*.

Beispiele.

(i) Die Funktion $f : \mathbb{R}^2 \to \mathbb{R}$ mit $f(x, y) = x^2 + y^2$ ist partiell differenzierbar und besitzt die partiellen Ableitungen

$$\frac{\partial f}{\partial x}(x, y) \;=\; 2x \qquad \text{und} \qquad \frac{\partial f}{\partial y}(x, y) \;=\; 2y \;\; .$$

Folglich ist $\operatorname{grad} f(x, y) \;=\; (2x, 2y)$.

(ii) Die Funktion $f : \mathbb{R}^3 \to \mathbb{R}$ mit $f(x, y, z) = x^2 \cdot \sin(y) + x \cdot e^z$ ist partiell differenzierbar und besitzt die partiellen Ableitungen

$$\begin{aligned} \frac{\partial f}{\partial x}(x, y, z) \;&=\; 2x \sin(y) + e^z \;\; , \\ \frac{\partial f}{\partial y}(x, y, z) \;&=\; x^2 \cdot \cos(y) \;\; , \\ \frac{\partial f}{\partial z}(x, y, z) \;&=\; x \cdot e^z \;\; . \end{aligned}$$

Folglich ist $\operatorname{grad} f(x, y, z) \;=\; \big(2x \sin(y) + e^z, x^2 \cdot \cos(y), x \cdot e^z\big)$.

Bemerkung. Der Gradient einer Funktion $f : \mathbb{R}^n \to \mathbb{R}$ gibt die Richtung des steilsten Anstieges der Funktion an.

Beispiele.

(i) Es sei $f(x, y) = (x^2 + y^2)/7 - 1$. Dann gibt $\operatorname{grad} f(x, y) = (2x/7, 2y/7)$ die Richtung des steilsten Anstieges von f im Punkt (x, y) an. Den steilsten Anstieg in (x, y) findet man also immer, wenn man sich vom Ursprung des Koordinatensystems wegbewegt. Siehe auch Abbildung 4.4.

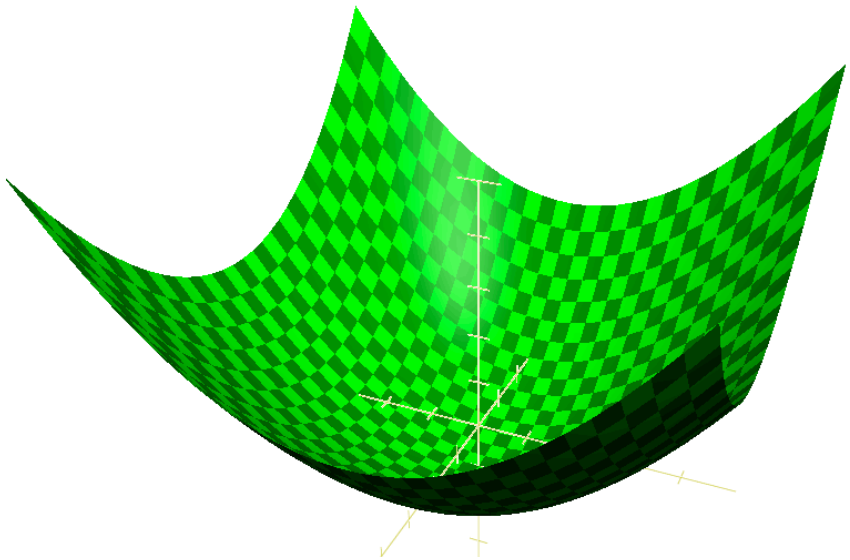


Abbildung 4.4: Der Graph der Funktion $f(x,y) = (x^2 + y^2)/7 - 1$.

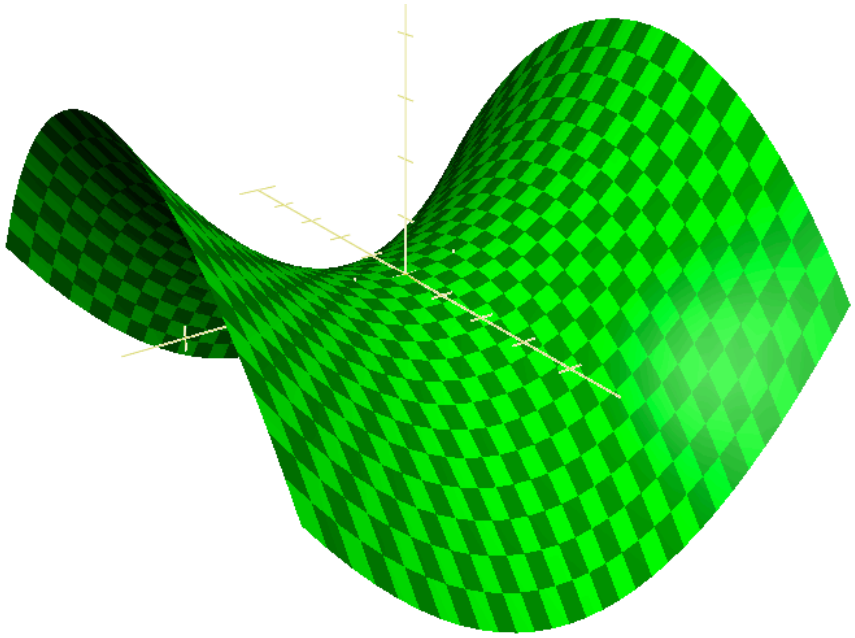


Abbildung 4.5: Der Graph der Funktion $f(x,y) = x^2 - y^2$.

(ii) Es sei $f(x,y) = x^2 - y^2$. Dann ist $\operatorname{grad} f(0,0) = (0,0)$, da die Funktion im Nullpunkt „eben“ ist, also keinen Anstieg besitzt. Siehe auch Abbildung 4.5.

Definition 4.3.28 (Lokale Extrema)**.** Es sei $f : \mathbb{R}^n \to \mathbb{R}$ und $\mathbf{x} \in \mathbb{R}^n$. Dann ist $\mathbf{x}$ ein *lokales Maximum (Minimum)*, falls es ein $\varepsilon > 0$ gibt, so dass $f(\mathbf{x}) \geq f(\mathbf{y})$ ($f(\mathbf{x}) \leq f(\mathbf{y})$) für alle $\mathbf{y} \in \mathbb{R}^n$ mit $|\mathbf{x} - \mathbf{y}| < \varepsilon$. Hierbei bezeichnet $|\mathbf{x} - \mathbf{y}|$ den euklidischen Abstand von $\mathbf{x} = (x_1, \ldots, x_n)$ und $\mathbf{y} = (y_1, \ldots, y_n)$, also

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2} \ .$$

Wir können Lemma 4.3.12 für den Fall von Funktionen mehrerer Veränderlicher wie folgt verallgemeinern.

Lemma 4.3.29. *Es sei $f : \mathbb{R}^n \to \mathbb{R}$ und $\mathbf{x} \in \mathbb{R}^n$. Ist $\mathbf{x}$ ein lokales Extremum von f und ist f an der Stelle $\mathbf{x}$ partiell differenzierbar, so ist* $\operatorname{grad} f(\mathbf{x}) = \mathbf{0}$.

Beweis. Ist $\mathbf{x}$ ein lokales Extremum von f, so ist $\mathbf{x}$ insbesondere ein lokales Extremum der partiellen Funktionen $f_1, \ldots, f_n$. Damit folgt die Behauptung aus Lemma 4.3.12. □

Bemerkung. Das Beispiel der in Abbildung 4.5 dargestellten Funktion zeigt, dass ein Punkt $\mathbf{x}$ (in dem Beispiel der Nullpunkt), der ein lokales Extremum aller partiellen Funktionen $f_1, \ldots, f_n$ ist, nicht notwendigerweise ein lokales Extremum von f sein muss.

Wir benötigen also, wie im eindimensionalen Fall, noch ein hinreichendes Kriterium für die Existenz eines lokalen Extremums.

Bemerkung. Die partiellen Ableitungen $\frac{\partial f}{\partial x_i}$ $(i = 1, ..., n)$ einer Funktion $f : \mathbb{R}^n \to \mathbb{R}$ sind selbst wieder Abbildungen von $\mathbb{R}^n$ nach $\mathbb{R}$ und unter Umständen ebenfalls partiell differenzierbar. Man bezeichnet ihre partiellen Ableitungen $\frac{\partial^2 f}{\partial x_j \partial x_i} = \frac{\partial}{\partial x_j}(\frac{\partial f}{\partial x_i})$ dann als zweite partielle Ableitungen von f.

Ist die zu untersuchende Funktion zweimal stetig partiell differenzierbar, so kann man oft mit den folgenden Hilfsmitteln Aussagen über lokale Extrema treffen.

Definition 4.3.30. Ist $f : \mathbb{R}^n \to \mathbb{R}$ in $\mathbf{x} \in \mathbb{R}^n$ zweimal stetig partiell differenzierbar, so bilden die zweiten partiellen Ableitungen von f die *Hesse-Matrix*

$$H_f(\mathbf{x}) := \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1}(\mathbf{x}) & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(\mathbf{x}) & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n}(\mathbf{x}) \end{pmatrix}$$

von f im Punkt a.

Beispiele.

(i) Die Funktion $f : \mathbb{R}^2 \to \mathbb{R},\ f(x,y) := x^2 + y^2$ hat die partiellen Ableitungen $\frac{\partial f}{\partial x}(x,y) = 2x$ und $\frac{\partial f}{\partial y}(x,y) = 2y$. Die zweiten partiellen Ableitungen lauten also $\frac{\partial^2 f}{\partial x^2}(x,y) = \frac{\partial}{\partial x}(2x) = 2 = \frac{\partial}{\partial y}(2y) = \frac{\partial^2 f}{\partial y^2}(x,y)$ und $\frac{\partial^2 f}{\partial y \partial x}(x,y) = \frac{\partial}{\partial y}(2x) = 0 = \frac{\partial}{\partial x}(2y) = \frac{\partial^2 f}{\partial x \partial y}(x,y)$. Die Hesse-Matrix von f hat somit die Gestalt

$$H_f(x,y) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

(ii) Die Hesse-Matrix der Funktion $f : \mathbb{R}^3 \to \mathbb{R},\ f(x,y,z) := x^2 \cdot \sin(y) + x \cdot e^z$ hat die Gestalt

$$H_f(x,y,z) = \begin{pmatrix} 2\sin(y) & 2x\cos(y) & e^z \\ 2x\cos(y) & -x^2\sin(y) & 0 \\ e^z & 0 & xe^z \end{pmatrix}.$$

Die Hesse-Matrizen in obigen Beispielen sind offenbar symmetrisch. Dies ist kein Zufall, wie der nächste Satz zeigt, den wir ohne Beweis angeben.

Satz 4.3.31 (Satz von Schwarz)**.** *Es sei $f : \mathbb{R}^n \to \mathbb{R}$ eine zweimal stetig partiell differenzierbare Funktion. Dann gilt für alle $i, j = 1, ..., n$:*

$$\frac{\partial^2 f}{\partial x_i \partial x_j} = \frac{\partial^2 f}{\partial x_j \partial x_i}.$$

Es spielt unter den Voraussetzungen des Satzes also keine Rolle, ob man f zuerst nach x_i oder nach x_j ableitet; die Voraussetzung der zweimaligen partiellen Differenzierbarkeit ist dabei wesentlich. Der Satz liefert nun unmittelbar

Korollar 4.3.32. *Es sei $f : \mathbb{R}^n \to \mathbb{R}$ eine zweimal stetig partiell differenzierbare Funktion. Dann ist die Hesse-Matrix H_f von f symmetrisch.*

Mit der Hesse-Matrix kann man eine Funktion nun auf lokale Extrema untersuchen. Dies ist jedoch nicht immer ganz einfach und wir gehen auf den allgemeinen Fall nicht weiter ein. Im zweidimensionalen Fall gibt es aber ein einfaches Kriterium, welches wir ohne Beweis zitieren. Vorweg jedoch noch eine

Definition 4.3.33 (Determinante)**.** Für eine beliebige 2×2-Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{C}^{2\times2}$ definieren wir die *Determinante* von A durch $\det A := a \cdot d - b \cdot c$.

Bemerkung. Man kann die Determinante für quadratische Matrizen beliebiger Größe definieren. Da für uns im Folgenden nur 2×2-Matrizen von Interesse sind, beschränken wir uns auf diesen Fall.

Satz 4.3.34. *Es sei* $f : \mathbb{R}^2 \to \mathbb{R}$ *eine zweimal stetig partiell differenzierbare Funktion. Im Punkt* $\mathbf{x} \in \mathbb{R}^2$ *sei* $\operatorname{grad} f(\mathbf{x}) = 0$. *Dann gilt:*

(i) Ist $\det H_f(\mathbf{x}) > 0$ *und* $\frac{\partial^2 f}{\partial {x_1}^2}(\mathbf{x}) < 0$, *so besitzt* f *im Punkt* $\mathbf{x}$ *ein lokales Maximum.*

(ii) Ist $\det H_f(\mathbf{x}) > 0$ *und* $\frac{\partial^2 f}{\partial {x_1}^2}(\mathbf{x}) > 0$, *so besitzt* f *im Punkt* $\mathbf{x}$ *ein lokales Minimum.*

(iii) Ist $\det H_f(\mathbf{x}) < 0$, *so besitzt* f *im Punkt* $\mathbf{x}$ *kein lokales Extremum.*

(iv) Ist $\det H_f(\mathbf{x}) = 0$, *so macht der Satz keine Aussage.*

4.4 Integralrechnung

Wir motivieren den folgenden Abschnitt klassisch durch den Wunsch, den Flächeninhalt A der Fläche F zu berechnen, die zwischen dem Graphen einer gegebenen Funktion $f : [a, b] \to \mathbb{R}$ und der x-Achse eingeschlossenen wird. Wir betrachten als Beispiel den Halbkreis vom Radius $r > 0$, gegeben durch $f : [-r, r] \to \mathbb{R}$ mit $f(x) := \sqrt{r^2 - x^2}$.

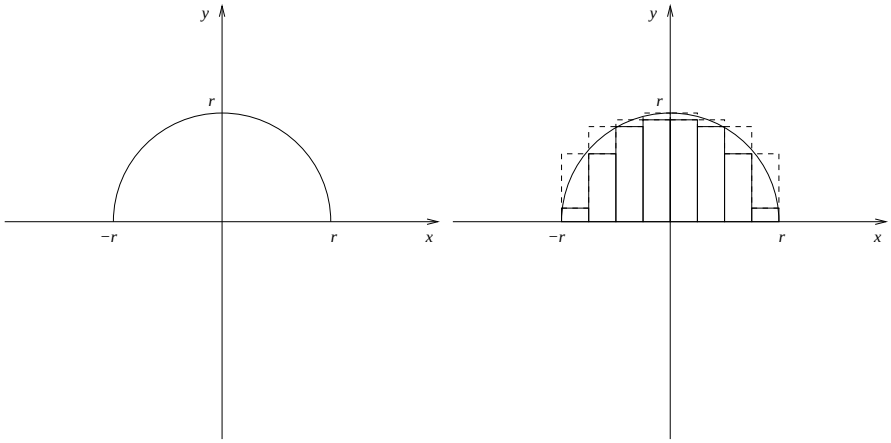


Abbildung 4.6: Approximation der Fläche F für $f(x) = \sqrt{r^2 - x^2}$.

Ein approximativer Ansatz ist nun, wie in Abbildung 4.6, das Intervall $[-r, r]$ zu unterteilen und die Fläche durch Rechtecksflächen anzunähern (von oben oder von unten). Es ist intuitiv klar, dass die Approximation durch die Wahl einer feineren Unterteilung von $[-r, r]$ verbessert werden kann.

Wir formalisieren diese Idee nun und weisen für stetige Funktionen nach, dass der oben heuristisch beschriebene Prozess zum Erfolg führt. Danach stellen wir mit dem Hauptsatz der Differential- und Integralrechnung den Zusammenhang zu den vorigen Abschnitten her.

4.4.1 Das Integral einer Treppenfunktion

Die folgenden Definitionen sind elementargeometrisch motiviert und haben ihren Ursprung in den oben genannten Rechtecksflächen unter dem Graphen einer Funktion.

Definition 4.4.1. Ist $n \in \mathbb{N}^*$, so nennt man eine endliche Folge $x_0, x_1, ..., x_n$ mit $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$ eine *Zerlegung* des Intervalls $[a, b] \subset \mathbb{R}$.

Eine Abbildung $\phi : [a, b] \to \mathbb{R}$ heißt *Treppenfunktion*, falls es eine Zerlegung $x_0, ..., x_n$ des Intervalls $[a, b]$ so gibt, dass ϕ auf allen offenen Teilintervallen (x_i, x_{i+1}), $i = 0, ..., n-1$, konstant ist, das heißt

$$\forall i = 0, ..., n-1 \; \exists c_i \in \mathbb{R} \; \forall y \in (x_i, x_{i+1}) : \phi(y) = c_i \ .$$

Die Menge aller Treppenfunktionen auf $[a, b]$ bezeichnen wir mit $\mathcal{T}_{[a,b]}$.

Bemerkung. Eine Treppenfunktion ϕ ist auch an den Zerlegungspunkten x_i definiert. Wir beachten die Funktionswerte dort aber nicht weiter, weil sie bei der noch folgenden Definition des Integrals keine Rolle spielen.

Beispiel. Die Funktion $\phi : [0, 1] \to \mathbb{R}$ mit $\phi(x) := \begin{cases} 1 & \text{für } x \in [0, \frac{1}{2}] \\ 2 & \text{für } x \in (\frac{1}{2}, \frac{3}{4}] \\ 1 & \text{für } x \in (\frac{3}{4}, 1] \end{cases}$ ist eine Treppenfunktion auf $[0, 1]$.

Lemma 4.4.2. *Die Menge $\mathcal{T}_{[a,b]}$ bildet einen $\mathbb{R}$-Vektorraum.*

Beweis. Die Menge $\mathcal{T}_{[a,b]}$ ist nicht leer, da offenbar jede auf $[a, b]$ konstante Funktion eine Treppenfunktion auf $[a, b]$ ist. Seien nun $\lambda \in \mathbb{R}$ und $\phi, \psi \in \mathcal{T}_{[a,b]}$ beliebig. Da ϕ und ψ Treppenfunktionen sind, gibt es per Definition Zerlegungen $x_0, ..., x_n$ und $y_0, ..., y_m$ von $[a, b]$, so dass ϕ auf den offenen Teilintervallen (x_i, x_{i+1}) und ψ auf den offenen Teilintervallen (y_j, y_{j+1}) konstant ist, für alle $i = 0, ..., n-1$ und $j = 0, ..., m-1$.

Die Funktion $\lambda\phi$ ist auf den offenen Teilintervallen (x_i, x_{i+1}) natürlich ebenfalls konstant, so dass $\lambda\phi \in \mathcal{T}_{[a,b]}$. Für die Funktion $\phi + \psi$ sortiert man die Vereinigung der Zerlegungspunkte $x_0, ..., x_n, y_0, ..., y_m$ der Größe nach und erhält somit eine neue Zerlegung $z_0, ..., z_k$ $(k \leq m + n)$ von $[a, b]$, auf deren Teilintervallen beide Funktionen ϕ und ψ konstant sind. Folglich ist auch $\phi + \psi \in \mathcal{T}_{[a,b]}$. □

Definition 4.4.3 (Integral einer Treppenfunktion)**.** Es sei $\phi \in \mathcal{T}_{[a,b]}$ bzgl. der Zerlegung $x_0, ..., x_n$ und $\xi_i \in (x_i, x_{i+1})$, für alle $i = 0, ..., n-1$. Dann definieren wir das *Integral* $\int_a^b \phi(x)\, dx$ *von* ϕ *über* $[a, b]$ durch die reelle Zahl

$$\int_a^b \phi(x)\, dx \ := \ \sum_{k=0}^{n-1} \phi(\xi_k)(x_{k+1} - x_k) \ .$$

Bemerkung. Die Terme $|\phi(\xi_i)|(x_{i+1} - x_i)$ entsprechen der Fläche des Rechtecks mit Grundseite $[x_i, x_{i+1}]$ und Höhe $|\phi(\xi_i)|$, für alle $i = 0, ..., n-1$. Dies macht deutlich, wieso dies eine Formalisierung der zu Anfang beschriebenen Idee ist. Wir schreiben im Folgenden der Einfachheit halber manchmal $\int_a^b \phi$ anstelle von $\int\limits_a^b \phi(x)\, dx$.

Lemma 4.4.4. *Das Integral für Treppenfunktionen ist wohldefiniert, d.h. es hängt nicht von der gewählten Zerlegung ab.*

Beweisskizze. Zum Beweis startet man mit zwei beliebigen Zerlegungen $x_0, ..., x_n$ und $y_0, ..., y_m$ von $[a, b]$ und Punkten $\xi_i \in (x_i, x_{i+1}),\ \zeta_j \in (y_j, y_{j+1}), i = 0, ..., n,\ j = 0, ..., m$. Wegen $x_0 = a = y_0$ gilt $\phi(\xi_0) = \phi(\zeta_0)$. Ist nun $y_1 = x_1$, so können wir die Argumentation mit x_1 und y_1 fortsetzen. Andernfalls gilt $x_1 > y_1$ oder $x_1 < y_1$. Ohne Einschränkung sei $x_1 > y_1$. Dann ist $(x_0, x_1) \cap (y_1, y_2) \neq \emptyset$ und es folgt $\phi(\zeta_0) = \phi(\xi_0) = \phi(\zeta_1)$. Damit gilt $\phi(\zeta_0)(y_1 - y_0) + \phi(\zeta_1)(y_2 - y_1) = \phi(\zeta_0)(y_2 - y_0)$. Man kann also den Zerlegungspunkt y_1 aus der Zerlegung entfernen und $y_i' := y_{i+1}$ setzen $(i > 0)$. Gilt nun $y_1' = y_2 = x_1$ oder $y_1' < x_1$, so können wir wie oben argumentieren. Ist $x_1 < y_1'$, so erhalten wir analog $\phi(\xi_0) = \phi(\xi_1)$ und wir können den Zerlegungspunkt x_1 aus der Zerlegung entfernen. Da es nur endlich viele Zerlegungspunkte gibt und $x_n = b = y_m$ gilt, erhält man so die Behauptung. □

Das Integral für Treppenfunktionen hat die folgenden Eigenschaften.

Lemma 4.4.5. $\int\limits_a^b : \mathcal{T}_{[a,b]} \to \mathbb{R}$ *ist ein monotones* $\mathbb{R}$*-lineares Funktional auf dem* $\mathbb{R}$*-Vektorraum* $\mathcal{T}_{[a,b]}$*, d.h. für* $\phi, \psi \in \mathcal{T}_{[a,b]}$ *und* $\lambda \in \mathbb{R}$ *gilt:*

(i) $\int\limits_a^b (\phi + \psi) \;=\; \int\limits_a^b \phi + \int\limits_a^b \psi$

(ii) $\int\limits_a^b (\lambda\phi) \;=\; \lambda \int\limits_a^b \phi$

(iii) Ist $\phi(x) \leq \psi(x)$ *für alle* $x \in [a, b]$*, so gilt* $\int\limits_a^b \phi \leq \int\limits_a^b \psi$.

Beweis. Die Aussage ii) folgt sofort aus der Definition des Integrals. Für i) und iii) genügt es, die Abbildungen ϕ und ψ auf einer Zerlegung von $[a, b]$ zu betrachten, bezüglich welcher beide Funktionen Treppenfunktionen sind. □

Wir haben bisher nur erreicht, dass wir den Inhalt der Rechtecksflächen unter einem Graphen berechnen können. Deshalb werden wir nun unser Integral durch den Approximations-Gedanken auf eine größere Klasse von Funktionen ausdehnen.

Definition 4.4.6. Es sei $f : [a, b] \to \mathbb{R}$ eine beschränkte Funktion. Dann ist das *Oberintegral von f über $[a, b]$* definiert durch

$$\mathrm{Int}_a^b(f) \;:=\; \inf \left\{ \int_a^b \phi(x)\, dx \;\middle|\; \phi \in \mathcal{T}_{[a,b]},\ \phi \geq f \right\} .$$

Das *Unterintegral von f über $[a, b]$* definiert durch

$$\mathrm{int}_a^b(f) \;:=\; \sup \left\{ \int_a^b \psi(x)\, dx \;\middle|\; \psi \in \mathcal{T}_{[a,b]},\ \psi \leq f \right\} .$$

Man könnte etwas informell sagen, dass der Graph einer Funktion durch das Ober- und Unterintegral gewissermaßen „eingeschachtelt“ wird. Es stellt sich nun die Frage, ob dieses Konzept überhaupt sinnvoll ist. Das folgende Lemma gibt darauf die Antwort.

Lemma 4.4.7. *Für eine beschränkte Funktion $f : [a, b] \to \mathbb{R}$ existieren stets Ober- und Unterintegral.*

Beweis. Da f beschränkt ist, existieren $m, M \in \mathbb{R}$ mit $m \leq f(x) \leq M$ für alle $x \in [a, b]$. Die konstanten Funktionen $\mathrm{const}(m)$ und $\mathrm{const}(M)$ sind Treppenfunktionen auf $[a, b]$ und es gilt $\mathrm{const}(m) \leq f \leq \mathrm{const}(M)$.

Wegen $\int_a^b \mathrm{const}(m) = m(b-a)$ und $\int_a^b \mathrm{const}(M) = M(b-a)$ sind die Mengen

$$\left\{ \int_a^b \phi \;\middle|\; \phi \in \mathcal{T}_{[a,b]},\ \phi \geq f \right\} \quad \text{und} \quad \left\{ \int_a^b \phi \;\middle|\; \phi \in \mathcal{T}_{[a,b]},\ \phi \leq f \right\}$$

gemäß Lemma 4.4.5 nach unten bzw. oben beschränkt. □

Nachdem wir uns nun von der Existenz der Ober- und Unterintegrale für beschränkte Funktionen überzeugt haben, wollen wir spezifizieren, wann diese auch das gewünschte Ergebnis liefern.

Definition 4.4.8 (Riemann-integrierbare Funktion)**.** Eine beschränkte Funktion $f : [a, b] \to \mathbb{R}$ heißt *Riemann-integrierbar* über $[a, b]$, falls $\mathrm{int}_a^b(f) = \mathrm{Int}_a^b(f)$ gilt. Für eine Riemann-integrierbare Funktion f: $[a, b] \to \mathbb{R}$ heißt $\int_a^b f(x)\, dx := \mathrm{int}_a^b(f)$ das *Riemann-Integral von f über $[a, b]$*.

Stimmen Ober- und Unterintegral nicht überein, so hilft das oben beschriebene Konzept bei der gewünschten Berechnung nicht. Wir sagen dann, dass die besagte Funktion nicht Riemann-integrierbar ist. Der Nachweis der Riemann-Integrierbarkeit einer gegebenen Funktion f ist nicht immer ganz einfach. Das folgende Lemma ist dabei oft sehr hilfreich.

Lemma 4.4.9. *Es sei $f : [a,b] \to \mathbb{R}$ eine beschränkte Funktion. Dann sind die folgenden Aussagen äquivalent:*

(i) f ist Riemann-integrierbar.

(ii) Zu beliebigem $\varepsilon > 0$ gibt es Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ mit $\psi \leq f \leq \phi$ und $\int_a^b \phi - \int_a^b \psi < \varepsilon$.

Beweis. „(i)⇒(ii)“: Sei f Riemann-integrierbar und $\varepsilon > 0$ beliebig. Nach Definition gilt $\int\limits_a^b f = \mathrm{int}_a^b(f) = \mathrm{Int}_a^b(f)$ und zu $\frac{\varepsilon}{2}$ gibt es Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ mit $\psi \leq f \leq \phi$ und $\int\limits_a^b \phi - \int\limits_a^b f < \frac{\varepsilon}{2}$, $\int\limits_a^b f - \int\limits_a^b \psi < \frac{\varepsilon}{2}$. Es folgt $\int\limits_a^b \phi - \int\limits_a^b \psi < \varepsilon$.

„(ii)⇒(i)“: Es sei $\varepsilon > 0$ beliebig. Dann gibt es nach (ii) Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ mit $\psi \leq f \leq \phi$ und $\int\limits_a^b \phi - \int\limits_a^b \psi < \varepsilon$. Per Definition des Ober- und Unterintegrals gilt

$$\int_a^b \psi \leq \mathrm{int}_a^b(f) \leq \mathrm{Int}_a^b(f) \leq \int_a^b \phi$$

und es folgt sofort $\mathrm{Int}_a^b(f) - \mathrm{int}_a^b(f) < \varepsilon$. Da $\varepsilon > 0$ beliebig gewählt war, folgt die Behauptung. □

Wir werden im nächsten Abschnitt zeigen, dass jede stetige Funktion Riemann-integrierbar ist.

4.4.2 Riemann-integrierbare Funktionen

Mit Hilfe der folgenden Definition werden wir die Klasse der Riemann-integrierbaren Funktionen näher klassifizieren.

Definition 4.4.10. Eine Funktion $f : [a,b] \to \mathbb{R}$ heißt *gleichmäßig durch Treppenfunktionen approximierbar*, wenn es zu beliebigem $\varepsilon > 0$ zwei Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ gibt, mit $\psi \leq f \leq \phi$ und $\phi(x) - \psi(x) < \varepsilon$, für alle $x \in [a,b]$.

Bemerkung. Wir hätten auch etwas allgemeiner den Begriff „gleichmäßige Konvergenz“ definieren können. Dabei wird verlangt, dass ab einem geeignetem Index n_0 alle Folgenglieder f_n einer Funktionenfolge $(f_n)_{n\in\mathbb{N}}$ im ε-Schlauch um ihre Grenzfunktion f liegen. Es gilt dann also für alle $x \in [a,b]$ und $n \geq n_0$: $|f(x) - f_n(x)| < \varepsilon$. Die gleichmäßige Konvergenz ist ein sehr viel stärkerer Begriff als die punktweise Konvergenz einer Funktionenfolge. Wir werden diese Allgemeinheit im Folgenden jedoch nicht benötigen und beschränken uns daher auf die obige Definition.

Lemma 4.4.11. *Jede gleichmäßig durch Treppenfunktionen approximierbare Funktion $f : [a, b] \to \mathbb{R}$ ist Riemann-integrierbar auf $[a, b]$.*

Beweis. Es sei $\varepsilon > 0$ beliebig. Dann gibt es zu $\varepsilon' := \frac{\varepsilon}{b-a}$ zwei Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ mit $\psi \leq f \leq \phi$ und $\phi(x) - \psi(x) < \varepsilon'$ für alle $x \in [a, b]$. Es gilt

$$\int_a^b \phi - \int_a^b \psi \;=\; \int_a^b (\phi - \psi) \;\leq\; \int_a^b \varepsilon' \;=\; \varepsilon'(b-a) \;=\; \varepsilon \;.$$

Lemma 4.4.9 liefert somit die Behauptung. □

Wir geben das folgende Lemma ohne Beweis.

Lemma 4.4.12. *Es sei $f : [a, b] \to \mathbb{R}$ eine stetige Funktion auf $[a, b]$. Dann ist f sogar gleichmäßig stetig auf $[a, b]$.*

Damit können wir nun beweisen, dass stetige Funktionen Riemann-integrierbar sind.

Satz 4.4.13 (Riemann-Integrierbarkeit stetiger Funktionen)**.** *Es sei $f : [a, b] \to \mathbb{R}$ eine stetige Funktion. Dann ist f Riemann-integrierbar.*

Beweis. Wir wollen die Behauptung mit Hilfe von Lemma 4.4.11 nachweisen. Dazu sei $\varepsilon > 0$ beliebig. Die Funktion f ist nach Lemma 4.4.12 gleichmäßig stetig. Es gibt daher ein $\delta > 0$, so dass für alle $x, y \in [a, b]$ mit $|x - y| < \delta$ gilt

$$|f(x) - f(y)| \;<\; \frac{\varepsilon}{2} \;=:\; \varepsilon' \;. \tag{4.9}$$

Wir wählen nun ein $n \in \mathbb{N}$ mit $\delta > \frac{b-a}{n} =: \mu$, eine äquidistante Zerlegung $a = x_0 < x_1 < ... < x_n = b$ von $[a, b]$, mit $x_k := a + k\mu$, für alle $k = 0, ..., n$ und definieren zwei Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ durch

$$\phi(x) \;:=\; \begin{cases} f(x_k) + \varepsilon' & \text{für } x \in (x_{k-1}, x_k] \text{ und } k = 1, ..., n, \\ f(a) & x = a, \end{cases}$$

und

$$\psi(x) \;:=\; \begin{cases} f(x_k) - \varepsilon' & \text{für } x \in (x_{k-1}, x_k] \text{ und } k = 1, ..., n, \\ f(a) & x = a. \end{cases}$$

Es gilt somit $\phi(x) - \psi(x) \leq \varepsilon$, für alle $x \in [a, b]$. Wir müssen noch zeigen, dass auf $[a, b]$ die Ungleichungen $\psi \leq f \leq \phi$ erfüllt sind. Für $x = a$ ist nichts zu zeigen. Es sei also $x \in (a, b]$ beliebig. Dann gibt es ein $j \in \{0, ..., n\}$ mit $x \in (x_{j-1}, x_j]$ und es gilt $|x - x_j| < |x_j - x_{j-1}| = \mu < \delta$. Nach (4.9) gilt also $|f(x) - f(x_k)| < \varepsilon'$ und daher

$$\psi(x) \;=\; f(x_k) - \varepsilon' \;<\; f(x) \;<\; f(x_k) + \varepsilon' \;=\; \phi(x) \;.$$

Damit ist der Beweis abgeschlossen. □

Bemerkung. Man kann die Riemann-Integrierbarkeit auch für andere Klassen von Funktionen, wie etwa die stückweise stetigen oder monotonen Funktionen zeigen.

Wir formulieren nun noch einige wichtige Eigenschaften des Riemann-Integrals.

Lemma 4.4.14. *Es seien $f, g : [a, b] \to \mathbb{R}$ Riemann-integrierbare Funktionen und $\lambda \in \mathbb{R}$. Dann gilt*

(i) Die Funktionen λf, $f + g$ sind Riemann-integrierbar und es gilt

$$\int_a^b \lambda f \;=\; \lambda \int_a^b f \quad \textit{und} \quad \int_a^b (f+g) = \int_a^b f + \int_a^b g \;.$$

(ii) Gilt $f(x) \leq g(x)$, für alle $x \in [a, b]$, so ist $\int_a^b f \leq \int_a^b g$.

Beweisskizze. Zu (i): Nach Definition gilt $\mathrm{int}_a^b(f+g) \leq \mathrm{Int}_a^b(f+g)$. Die Rechenregeln für Suprema und Infima liefern

$$\mathrm{Int}_a^b(f+g) \;\leq\; \mathrm{Int}_a^b(f) + \mathrm{Int}_a^b(g) \;\overset{\text{Vor.}}{=}\; \mathrm{int}_a^b(f) + \mathrm{int}_a^b(g) \;\leq\; \mathrm{int}_a^b(f+g) \;.$$

Für $\lambda \geq 0$ gilt $\mathrm{Int}_a^b(\lambda f) = \lambda \mathrm{Int}_a^b(f) \overset{\text{Vor.}}{=} \lambda \mathrm{int}_a^b(f) = \mathrm{int}_a^b(\lambda f)$. Für $\lambda \leq 0$ gilt schließlich $\mathrm{int}_a^b(\lambda f) = \lambda \mathrm{Int}_a^b(f) \overset{\text{Vor.}}{=} \lambda \mathrm{int}_a^b(f) = \mathrm{Int}_a^b(\lambda f)$.

Zu (ii): Die Behauptung folgt unmittelbar aus der Definition des Ober- und Unterintegrals und Lemma 4.4.5. □

Satz 4.4.15. *Es seien $f, g : [a, b] \to \mathbb{R}$ zwei Riemann-integrierbare Funktionen. Dann ist auch die Funktion $f \cdot g$ Riemann-integrierbar.*

Beweis. Wir beweisen zunächst mit Hilfe von Lemma 4.4.9, dass die Funktion f^2 Riemann-integrierbar ist. Da f als Riemann-integrierbare Funktion beschränkt ist, können wir ohne Einschränkung annehmen, dass $0 \leq f \leq 1$ gilt. Andernfalls betrachten wir die nach vorigem Lemma ebenfalls integrierbare Funktion $\lambda f + c$ mit geeigneten $\lambda, c \in \mathbb{R}$.

Es sei nun $\varepsilon > 0$ beliebig. Nach Lemma 4.4.9 gibt es Treppenfunktionen $\phi, \psi \in \mathcal{T}_{[a,b]}$ mit

$$0 \;\leq\; \psi \;\leq\; f \;\leq\; \phi \;\leq\; 1 \qquad \text{und} \qquad \int_a^b (\phi - \psi)(x)\, dx \;<\; \frac{\varepsilon}{2} \;.$$

Es gilt $0 \leq \psi^2 \leq f^2 \leq \phi^2 \leq 1$ und $\phi^2, \psi^2 \in \mathcal{T}_{[a,b]}$. Punktweise gilt zudem $0 \leq \phi + \psi \leq 2$, so dass $\phi^2 - \psi^2 = (\phi + \psi)(\phi - \psi) \leq 2(\phi - \psi)$. Damit erhalten wir schließlich

$$\int_a^b (\phi^2 - \psi^2) \;\leq\; 2 \int_a^b (\phi - \psi) \;<\; \varepsilon \;.$$

Also ist f^2 nach Lemma 4.4.9 integrierbar.

Für eine beliebige Riemann-integrierbare Funktion g folgt die Behauptung deshalb aus der Gleichung $f \cdot g = \frac{1}{4}((f+g)^2 - (f-g)^2)$. □

Satz 4.4.16 (Mittelwertsatz der Integralrechnung)**.** *Es seien $f, g : [a,b] \to \mathbb{R}$ zwei stetige Funktionen mit $g \geq 0$. Dann gibt es ein $\xi \in [a,b]$ mit*

$$\int_a^b (f \cdot g)(x)\, dx \;=\; f(\xi) \int_a^b g(x)\, dx \;.$$

Beweis. Nach Satz 4.4.15 ist die Funktion $f \cdot g$ Riemann-integrierbar. Als stetige Funktion besitzt f im Intervall $[a,b]$ ein globales Maximum und ein globales Minimum. Setze $m := \min\{f(x) \mid x \in [a,b]\}$ und $M := \max\{f(x) \mid x \in [a,b]\}$. Dann gilt $mg \leq fg \leq Mg$ und folglich

$$m \int_a^b g \;=\; \int_a^b (m \cdot g) \;\leq\; \int_a^b (f \cdot g) \;\leq\; \int_a^b (M \cdot g) \;=\; M \int_a^b g \;.$$

Es gibt deshalb ein $\zeta \in [m, M]$ mit $\int_a^b (f \cdot g) = \zeta \int_a^b g$. Da f stetig ist folgt nun mit dem Zwischenwertsatz, dass es ein $\xi \in [a,b]$ gibt mit $f(\xi) = \zeta$. □

Korollar 4.4.17. *Es sei $f : [a,b] \to \mathbb{R}$ eine stetige Funktion. Dann gibt es ein $\xi \in [a,b]$ mit*

$$\int_a^b f(x)\, dx \;=\; f(\xi)(b-a) \;.$$

Beweis. Setze im Mittelwertsatz der Integralrechnung $g \equiv 1$. □

Die Approximation einer Funktion f durch Treppenfunktionen liefert uns die Existenz des Riemann-Integrals von f. Eine tatsächliche Berechnung mittels geeigneter Treppenfunktionen ist zwar oft möglich, aber sehr mühsam. Wir benötigen also noch etwas Werkzeug. Der obige Mittelwertsatz ist nun unser Hilfsmittel, um den Zusammenhang zur Differentialrechnung herzustellen. Dies wird uns auch eine vergleichsweise unkomplizierte Möglichkeit liefern, Integrale tatsächlich zu berechnen.

4.4.3 Integration und Differentiation

Wir bemerken zunächst, dass man das Integral einer auf $[a,b]$ Riemann-integrierbaren Funktion f an einer beliebigen Stelle $t \in (a,b)$ aufteilen kann.

Lemma 4.4.18. *Es sei f auf $[a,b]$ Riemann-integrierbar und $t \in (a,b)$. Dann ist f auch auf den Intervallen $[a,t]$ und $[t,b]$ Riemann-integrierbar und es gilt*

$$\int_a^b f \;=\; \int_a^t f + \int_t^b f \;.$$

Beweisskizze. Man muss lediglich bemerken, dass die Einschränkung einer Treppenfunktion auf ein Teilintervall von $[a,b]$ wieder eine Treppenfunktion ist. Die Integrierbarkeit von f folgt dann wieder mit Lemma 4.4.9 und die Formel für das Integral folgt direkt aus der Definition des Ober- und Unterintegrals. □

Wir haben bisher immer Integrationsgrenzen $a,b \in \mathbb{R}$ mit $a < b$ betrachtet, möchten aber auch andere Fälle zulassen.

Definition 4.4.19. Es sei f eine auf $[a,b]$ Riemann-integrierbare Funktion. Wir setzen $\int_a^a f(x)\,dx := 0$ und $\int_s^t f(x)\,dx := -\int_t^s f(x)\,dx$, für $s,t \in [a,b]$ mit $t \le s$.

Mit diesen Konventionen können wir mit Hilfe des Integrals einer Funktion f eine neue Abbildung definieren.

Definition 4.4.20 (Integralfunktion)**.** Für eine Riemann-integrierbare Funktion f auf $[a,b]$ kann durch $I_f : [a,b] \to \mathbb{R},\ x \mapsto \int_a^x f(t)\,dt$ eine weitere Funktion I_f auf $[a,b]$ definiert werden. Die Funktion I_f heißt die zu f gehörende *Integralfunktion.*

Wir beschäftigen uns im Folgenden nur mit stetigen Funktionen. Für diese ist die Integralfunktion angenehm zu handhaben.

Satz 4.4.21 (Hauptsatz der Differential- und Integralrechnung)**.** *Es sei f eine auf $[a,b]$ stetige Funktion. Dann ist die zu f gehörende Integralfunktion I_f stetig differenzierbar auf $[a,b]$ und es gilt $I_f'(x) = f(x)$.*

Beweis. Wir betracheten den Differenzenquotienten für I_f. Sei dazu $x \in [a,b]$ beliebig und $h \neq 0$. Es ist

$$\frac{I_f(x+h) - I_f(x)}{h} \;=\; \frac{1}{h}\int_x^{x+h} f(t)\,dt \;.$$

Nach dem Mittelwertsatz der Integralrechnung gibt es nun ein $\xi_h \in [x, x+h]$ (bzw. $[x+h, x]$ für $h < 0$) mit

$$\int_x^{x+h} f(t)\ dt \ = \ f(\xi_h)(x+h-x) \ = \ h \cdot f(\xi_h) \ .$$

Wir erhalten damit

$$\frac{I_f(x+h) - I_f(x)}{h} \ = \ f(\xi_h) \ .$$

Für $h \to 0$ konvergiert ξ_h gegen x und mit der Stetigkeit von f erhalten wir somit

$$\lim_{h \to 0} \frac{I_f(x+h) - I_f(x)}{h} \ = \ f(x) \ .$$

Damit ist der Beweis abgeschlossen. □

Definition 4.4.22 (Stammfunktion)**.** Es seien $f, F : [a, b] \to \mathbb{R}$ zwei Funktionen. Ist F differenzierbar mit $F' = f$, so nennt man F eine *Stammfunktion* von f.

Wegen Satz 4.4.21 ist die Integralfunktion einer stetigen Funktion eine Stammfunktion.

Korollar 4.4.23. *Ist $f : [a, b] \to \mathbb{R}$ eine stetige Funktion, so ist die zu f gehörende Integralfunktion I_f eine Stammfunktion von f.*

Wir zeigen als nächstes, dass sich eine beliebige Stammfunktion von f nur um eine Konstante von I_f unterscheiden kann.

Lemma 4.4.24. *Es sei $F : [a, b] \to \mathbb{R}$ eine Stammfunktion von $f : [a, b] \to \mathbb{R}$.*

(i) Ist $G : [a, b] \to \mathbb{R}$ eine weitere Stammfunktion von f, so gibt es ein $\lambda \in \mathbb{R}$ mit $F(x) = G(x) + \lambda$ für alle $x \in [a, b]$.

(ii) Umgekehrt ist für ein beliebiges $\mu \in \mathbb{R}$ die durch $H(x) := F(x) + \mu$ definierte Funktion $H : [a, b] \to \mathbb{R}$ eine Stammfunktion von f.

Die Stammfunktion von f ist also bis auf eine Konstante eindeutig bestimmt.

Beweis. Da $F' = G' = f$, ist $(F - G)'$ die Nullfunktion. Folglich ist $F - G$ konstant. Wegen der Ableitungsregeln gilt $H' = F' = f$. □

Korollar 4.4.25. *Ist $f : [a, b] \to \mathbb{R}$ stetig und $F : [a, b] \to \mathbb{R}$ eine Stammfunktion von f, so gilt*

$$\int_a^b f(x)\ dx \ = \ F(b) - F(a) \ .$$

Beweis. Wegen Korollar 4.4.23 und Lemma 4.4.24 gibt es ein $\lambda \in \mathbb{R}$ mit $F(x) = I_f(x) + \lambda$. Daher gilt

$$\int_a^b f(x)\,dx \;=\; I_f(b) \;=\; I_f(b) - I_f(a) \;=\; F(b) - F(a)\;.$$

Damit ist der Beweis abgeschlossen. □

Wir geben nur einige Beispiele für Stammfunktionen wichtiger Funktionen.

Beispiele.

(i) Die Exponentialfunktion exp ist eine Stammfunktion von sich selbst.

(ii) Die Logarithmus-Funktion ln ist eine Stammfunktion von $x \mapsto 1/x$.

(iii) Die Cosinus-Funktion ist eine Stammfunktion der Sinus-Funktion.

4.4.4 Integrationsregeln

Wir geben einige bekannte Regeln an, die sich bei der Integration von Funktionen als nützlich erweisen.

Satz 4.4.26 (Substitutionsregel)**.** *Es sei $g : [a,b] \to \mathbb{R}$ stetig differenzierbar und $f : g([a,b]) \to \mathbb{R}$ stetig mit Stammfunktion F. Dann ist $F \circ g$ eine Stammfunktion von $(f \circ g) \cdot g'$ und es gilt*

$$\int_a^b (f \circ g)(x) \cdot g'(x)\,dx \;=\; \int_{g(a)}^{g(b)} f(y)\,dy\;.$$

Beweis. Nach der Kettenregel in Satz 4.3.8 (iv) gilt

$$(F \circ g)'(x) \;=\; F'\big(g(x)\big) \cdot g'(x) \;=\; (f \circ g)(x) \cdot g'(x)\;.$$

Damit erhält man mit Hilfe von Korollar 4.4.25

$$\begin{aligned}\int_a^b (f \circ g)(x) \cdot g'(x)\,dx &= (F \circ g)(b) - (F \circ g)(a)\\ &= F\big(g(b)\big) - F\big(g(a)\big)\\ &= \int_{g(a)}^{g(b)} f(y)\,dy\;.\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Korollar 4.4.27. *Es sei $g : [a, b] \to \mathbb{R}$ stetig differenzierbar und streng monoton mit $g(a) = \alpha$ und $g(b) = \beta$. Weiter sei $f : g([a, b]) \to \mathbb{R}$ stetig mit Stammfunktion F. Dann ist*

$$\int_\alpha^\beta f(y)\ dy \ = \ \int_{g^{-1}(\alpha)}^{g^{-1}(\beta)} (f \circ g)(x) \cdot g'(x)\ dx \ .$$

Beispiele.

(i) Wir wollen das Integral

$$\int_{1/\pi}^{2/\pi} -\frac{\sin(1/x)}{x^2}\ dx$$

berechnen. Wir können sofort die Substitutionsregel anwenden: Die Funktion $g : [1/\pi, 2/\pi] \to \mathbb{R}$ mit $g(x) = 1/x$ ist stetig differenzierbar mit Ableitung $g'(x) = -1/x^2$ und die Funktion $f(x) = \sin x$ ist auf $g([1/\pi, 2/\pi]) = [\frac{\pi}{2}, \pi]$ stetig mit Stammfunktion $F(x) = -\cos x$. Nach Substitutionsregel gilt also

$$\begin{aligned}
\int_{1/\pi}^{2/\pi} -\frac{\sin(1/x)}{x^2}\ dx \ &= \ \int_{1/\pi}^{2/\pi} (f \circ g)(x) \cdot g'(x)\ dx \\
&= \ \int_{g(1/\pi)}^{g(2/\pi)} f(y)\ dy \\
&= \ \int_{\pi}^{\pi/2} \sin y\ dy \\
&= \ -\int_{\pi/2}^{\pi} \sin y\ dy \\
&= \ -\left(-\cos(\pi) + \cos(\pi/2)\right) \ = \ -1 \ .
\end{aligned}$$

Wie das nächste Beispiel zeigt, ist man leider nicht immer in der komfortablen Situation, dass der Integrand von der Form $(f \circ g) \cdot g'$ ist.

(ii) Wir zeigen nun

$$\int_{-3/2}^{-1} \sqrt{2x+3}\ dx \ = \ \frac{1}{3} \ .$$

Die Funktion $g(x) := 2x + 3$ ist auf $[-\frac{3}{2}, -1]$ stetig differenzierbar mit Ableitung $g'(x) = 2$. Die Funktion $f(x) := \sqrt{x}$ ist auf $g([-\frac{3}{2}, -1]) = [0, 1]$ stetig mit Stammfunktion $F(x) = \frac{2}{3}x^{\frac{3}{2}}$. Es gilt

$$\sqrt{2x+3} \ = \ (f \circ g)(x) \ = \ \frac{1}{2}(f \circ g)(x) \cdot 2 \ = \ \frac{1}{2}(f \circ g)(x) \cdot g'(x) \ .$$

Die Funktion $\tilde{f}(x) := \frac{1}{2}\sqrt{x}$ ist auf $[0,1]$ ebenfalls stetig mit Stammfunktion $\tilde{F}(x) = \frac{1}{3}x^{\frac{3}{2}}$ und es gilt $\sqrt{2x+3} = (\tilde{f} \circ g)(x) \cdot g'(x)$. Die Substitutionsregel liefert also

$$\begin{aligned}\int_{-3/2}^{-1} \sqrt{2x+3}\; dx &= \int_{-3/2}^{-1} (\tilde{f} \circ g)(x) \cdot g'(x)\; dx \\ &= \int_{g(-3/2)}^{g(-1)} \tilde{f}(y)\; dy \\ &= \int_0^1 \frac{1}{2}\sqrt{y}\; dy \\ &= \tilde{F}(1) - \tilde{F}(0) \;=\; \frac{1}{3}\;.\end{aligned}$$

(iii) Die obigen Beispiele verdeutlichen, wieso die Substitutionsregel nützlich ist. Man kann „störende Anteile“ des Integranden durch Substitution ersetzen. Man benutzt bei Berechnungen oft auch eine etwas heuristisch anmutende Schreibweise, welche wir an

$$\int_{2/4}^{10/4} \frac{1}{\sqrt{4x-1}}\; dx$$

kurz illustrieren. Man setzt $y := g(x) := 4x - 1$. Dann ist „die Ableitung von y nach x“ gegeben durch

$$\frac{dy}{dx} \;:=\; g'(x) \;=\; 4 \quad\Longrightarrow\quad dx = \frac{1}{4}dy\;.$$

Die Funktion $f(y) := \frac{1}{\sqrt{y}}$ ist auf $[g(2/4), g(10/4)]$ stetig mit Stammfunktion $F(y) = 2\sqrt{y}$. Damit „ersetzen“ wir

$$\begin{aligned}\int_{2/4}^{10/4} \frac{1}{\sqrt{4x-1}}\; dx &= \int_{4\cdot\frac{2}{4}-1}^{4\cdot\frac{10}{4}-1} \frac{1}{\sqrt{y}}\frac{1}{4}\; dy \\ &= \frac{1}{2}\int_1^9 \frac{1}{2\sqrt{y}}\; dy \\ &= \frac{1}{2}[\sqrt{y}\;]_1^9 \\ &= \frac{1}{2}(\sqrt{9} - \sqrt{1}) \;=\; 1\;.\end{aligned}$$

Satz 4.4.28 (Partielle Integration)**.** *Es sei $g : [a,b] \to \mathbb{R}$ stetig differenzierbar und $f : g([a,b]) \to \mathbb{R}$ stetig mit Stammfunktion F. Dann ist $F \cdot g$ eine Stammfunktion von $f \cdot g + F \cdot g'$ und es gilt*

$$\int_a^b f(x) \cdot g(x)\; dx \;=\; F(b) \cdot g(b) - F(a) \cdot g(a) - \int_a^b F(x) \cdot g'(x)\; dx\;.$$

Beweis. Nach der Produktregel in Satz 4.3.8 (ii) gilt $(F \cdot g)' = f \cdot g + F \cdot g'$. Folglich ist nach Korollar 4.4.25

$$\begin{aligned} F(b) \cdot g(b) - F(a) \cdot g(a) &= \int_a^b (f \cdot g + F \cdot g')(x)\ dx \\ &= \int_a^b (f \cdot g)(x)\ dx + \int_a^b (F \cdot g')(x)\ dx\ . \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Beispiele.

(i) Es seien $a, b \in \mathbb{R}$ beliebig. Wir betrachten das Integral $\int_a^b x \cdot \cos x\ dx$. Die Funktion $g : [a, b] \to \mathbb{R},\ g(x) := x$ ist stetig differenzierbar mit Ableitung $g'(x) = 1$ und die Funktion $f : [a, b] \to \mathbb{R},\ f(x) := \cos x$ ist stetig auf $[a, b]$ mit Stammfunktion $F(x) = \sin x$. Mittels partieller Integration erhalten wir

$$\begin{aligned} \int_a^b x \cdot \cos x\ dx &= \int_a^b g(x) \cdot f(x)\ dx \\ &= F(b)g(b) - F(a)g(a) - \int_a^b F(x)g'(x)\ dx \\ &= b \cdot \sin b - a \cdot \sin a - \int_a^b \sin x\ dx \\ &= b \cdot \sin b - a \cdot \sin a + \cos b - \cos a\ . \end{aligned}$$

(ii) Es seien $a, b \in \mathbb{R}_{>0}$ beliebig. Wir betrachten das Integral $\int_a^b \frac{\ln x}{x}\ dx$. Die Funktion $g : [a, b] \to \mathbb{R},\ g(x) := \ln x$ ist stetig differenzierbar mit Ableitung $g'(x) = \frac{1}{x}$ und die Funktion $f : [a, b] \to \mathbb{R},\ f(x) := \frac{1}{x}$ ist stetig auf $[a, b]$ mit Stammfunktion $F(x) = \ln x$. Mittels partieller Integration erhalten wir

$$\begin{aligned} \int_a^b \frac{\ln x}{x}\ dx &= \int_a^b f(x) \cdot g(x)\ dx \\ &= F(b)g(b) - F(a)g(a) - \int_a^b F(x)g'(x)\ dx \\ &= \ln b \ln b - \ln a \ln a - \int_a^b \ln x \cdot \frac{1}{x}\ dx\ . \end{aligned}$$

Damit erhält man

$$2 \int_a^b \frac{\ln x}{x}\ dx = (\ln b)^2 - (\ln a)^2$$

und folglich

$$\int_a^b \frac{\ln x}{x}\ dx = \frac{1}{2}((\ln b)^2 - (\ln a)^2)\ .$$

(iii) Es seien $a, b \in \mathbb{R}_{>0}$ beliebig. Wir betrachten das Integral $\int_a^b \ln x \; dx$. Folgender Trick ist oft hilfreich: $\ln x = 1 \cdot \ln x$. Die Funktion $g : [a,b] \to \mathbb{R},\ g(x) := \ln x$ ist stetig differenzierbar mit Ableitung $g'(x) = \frac{1}{x}$ und die Funktion $f : [a,b] \to \mathbb{R},\ f(x) := 1$ ist stetig auf $[a,b]$ mit Stammfunktion $F(x) = x$. Mittels partieller Integration erhalten wir

$$\begin{aligned}
\int_a^b \ln x \; dx &= \int_a^b 1 \cdot \ln x \; dx \\
&= \int_a^b f(x) \cdot g(x) \; dx \\
&= F(b)g(b) - F(a)g(a) - \int_a^b F(x)g'(x) \; dx \\
&= b \ln b - a \ln a - \int_a^b x \cdot \frac{1}{x} \; dx \\
&= b \ln b - a \ln a - \int_a^b 1 \; dx \\
&= b \ln b - a \ln a - b + a \\
&= (b \ln b - b) - (a \ln a - a) \ .
\end{aligned}$$

Wir haben insbesondere eine Stammfunktion G von g gefunden.

4.4.5 Uneigentliche Integrale

Definition 4.4.29 (Uneigentliche Integrale)**.** Es seien $a \in \mathbb{R} \cup \{-\infty\}$, $b \in \mathbb{R} \cup \{\infty\}$ und $c \in (a,b)$. Weiter sei $f : (a,b) \to \mathbb{R}$ eine Funktion.

(i) Ist die Einschränkung von f auf $[c,d]$ für jedes $d > c$ Riemann-integrierbar und existiert der Grenzwert

$$\lim_{d \to b} \int_c^d f(x) \; dx \ ,$$

so bezeichnet man ihn mit

$$\int_c^b f(x) \; dx \ .$$

(ii) Ist die Einschränkung von f auf $[d,c]$ für jedes $d < c$ Riemann-integrierbar und existiert der Grenzwert

$$\lim_{d \to a} \int_d^c f(x) \; dx \ ,$$

so bezeichnet man ihn mit

$$\int_a^c f(x) \; dx \ .$$

(iii) Existieren die Grenzwerte

$$\int_c^b f(x)\ dx \qquad \text{und} \qquad \int_a^c f(x)\ dx\ ,$$

so setzt man

$$\int_a^b f(x)\ dx\ :=\ \int_c^b f(x)\ dx + \int_a^c f(x)\ dx\ .$$

Beispiele.

(i) Es seien $a = -\infty,\ c = 0,\ b = +\infty$ und $f(x) = e^{-x}$. Dann existiert das Integral $\int_0^t f(x)\ dx$ für alle $t \in \mathbb{R}_{\geq 0}$ wegen der Stetigkeit von f und es gilt

$$\int_0^t e^{-x}\ dx\ =\ -e^{-t} + 1\ \stackrel{t\to+\infty}{\longrightarrow}\ 1\ .$$

Somit ist

$$\int_0^{+\infty} e^{-x}\ =\ \lim_{t\to+\infty} \int_0^t e^{-x}\ dx\ =\ 1\ .$$

(ii) Es seien $a = -\infty,\ c = 0,\ b = +\infty$ und $f(x) = e^{-x^2}$. Dann existiert das Integral $\int_0^t f(x)\ dx$ für alle $t \in \mathbb{R}_{\geq 0}$ wegen der Stetigkeit von f.
Es gilt $0 \leq e^{-x^2} \leq 1$, für $0 \leq x \leq 1$ und $0 \leq e^{-x^2} \leq e^{-x}$, für $1 \leq x \leq t$. Wegen der Monotonie des Integrals folgt für $t' < t$ die Ungleichung

$$\begin{aligned}
\int_0^t e^{-x^2}\ dx\ &=\ \int_0^{t'} e^{-x^2}\ dx + \int_{t'}^t e^{-x^2}\ dx \\
&>\ \int_0^{t'} e^{-x^2}\ dx + \int_{t'}^t 0\ dx \\
&=\ \int_0^{t'} e^{-x^2}\ dx\ .
\end{aligned}$$

Die Abbildung $\varphi : (0, +\infty) \to \mathbb{R},\ \varphi(t) := \int_0^t e^{-x^2}\ dx$ ist also streng monoton steigend. Zudem erhalten wir durch

$$\begin{aligned}
\int_0^t e^{-x^2}\ dx\ &=\ \int_0^1 e^{-x^2}\ dx + \int_1^t e^{-x^2}\ dx \\
&\leq\ \int_0^1 1\ dx + \int_1^t e^{-x}\ dx \\
&=\ 1 - e^{-t} + 1\ \leq\ 2\ ,
\end{aligned}$$

dass φ nach oben beschränkt ist. Der Grenzwert $\lim_{t\to+\infty} \int_0^t e^{-x^2}\ dx$ existiert also. Wegen der Symmetrie von f folgt völlig analog, dass auch der Grenzwert $\lim_{t\to-\infty} \int_t^0 e^{-x^2}\ dx$ existiert und es gilt

$$\int_{-\infty}^{+\infty} e^{-x^2}\ dx \ = \ \int_{-\infty}^{0} e^{-x^2}\ dx + \int_0^{+\infty} e^{-x^2}\ dx \ .$$

(iii) Es seien $a = -\infty,\ c = 0,\ b = +\infty$ und $f(x) = \sin x$. Dann existiert das Integral $\int_0^t f(x)\ dx$ für alle $t \in \mathbb{R}_{\geq 0}$ wegen der Stetigkeit von f und es gilt $\int_0^t \sin x\ dx = 1 - \cos t$. Der Grenzwert

$$\lim_{t\to+\infty} \int_0^t \sin x\ dx \ = \ \lim_{t\to+\infty} (1 - \cos t)$$

existiert also nicht.

Bemerkung. Das letzte Beispiel von oben zeigt, dass für eine Funktion $f : (-\infty, \infty) \to \mathbb{R}$ die Existenz des Grenzwertes

$$\lim_{t\to\infty} \int_{-t}^{t} f(x)\ dx$$

nicht hinreichend für die Existenz des uneigentlichen Integrals

$$\int_{-\infty}^{\infty} f(x)\ dx$$

ist. Für $t \geq 0$ gilt nämlich

$$\int_{-t}^{t} \sin x\ dx \ = \ -\cos t + \cos(-t) \ = \ -\cos t + \cos t \ = \ 0 \ ,$$

so dass

$$\lim_{t\to\infty} \int_{-t}^{t} \sin x\ dx \ = \ 0 \ .$$

4.5 Differentialgleichungen

Bei der Beschreibung vieler Phänomene in Technik und Natur spielen Differentialgleichungen eine zentrale Rolle. Darunter fallen beispielsweise Wachstumsprozesse von Populationen, die Entladung eines Kondensators oder Schwingungsprozesse von Pendeln, Federn oder in elektrischen Schaltkreisen. Wir diskutieren zunächst einige Beispiele.

Beispiele.

(i) Wir betrachten eine Population (Seerosen, Kaninchen, Bakterien etc.), die zum Anfangszeitpunkt 0 die Größe y_0 besitzt. Das Wachstum der Population hängt immer von der aktuellen Größe der Population ab. Bezeichnet man die Größe der Population zum Zeitpunkt t mit $y(t)$, so wird dadurch eine Funktion $y : [0, \infty) \to \mathbb{R}$ definiert. Das Wachstum der Population zum Zeitpunkt t wird durch die Ableitung $y'(t)$ beschrieben. Unter gewissen Umständen ist das Wachstum proportional zur Populationsgröße, das heißt

$$y'(t) \;=\; \alpha \cdot y(t) \tag{4.10}$$

für ein $\alpha > 0$.

Die Gleichung (4.10) heißt *Differentialgleichung*. Zusammen mit der *Anfangsbedingung* $y(0) = y_0$ spricht man von einem *Anfangswertproblem*.

(ii) Wir betrachten den Abkühlungsprozess einer heißen Tasse Kaffee, die zum Zeitpunkt $t = 0$ die Anfangstemperatur y_0 hat. Die Temperatur des Kaffees zum Zeitpunkt t bezeichnen wir mit $y(t)$. Die Ableitung $y'(t)$ der dadurch definierten Funktion $y : [0, \infty) \to \mathbb{R}$ gibt die Änderung der Temperatur des Kaffees zum Zeitpunkt t an. Diese Änderung ist proportional zur Differenz der Temperatur $y(t)$ des Kaffees und der (konstanten) Umgebungstemperatur T, das heißt es gilt

$$y'(t) \;=\; \alpha \cdot \big(y(t) - T\big)$$

für ein $\alpha \in \mathbb{R}$. Da sich der anfangs heiße Kaffee abkühlt, sollte $y'(t) < 0$ gelten, so dass $\alpha < 0$.

(iii) Die Schwingung eines Pendels kann wie folgt beschrieben werden. Die Auslenkung des Pendels aus der Gleichgewichtslage zum Zeitpunkt t wird mit $y(t)$ bezeichnet. Dann bezeichnet $y'(t)$ die Geschwindigkeit und $y''(t)$ die Beschleunigung zum Zeitpunkt t. Das Pendel strebt immer in seine Gleichgewichtslage zurück und erfährt dabei eine Beschleunigung, die proportional zu seiner Auslenkung ist, das heißt

$$y''(t) = -\omega^2 \cdot y(t)$$

für ein $\omega \in \mathbb{R}$.

Definition 4.5.1 (Gewöhnliche Differentialgleichung)**.** Es sei $F : \mathbb{R}^{n+2} \to \mathbb{R}$. Die Gleichung

$$F\big(t, y(t), y'(t), y''(t), \ldots, y^{(n)}(t)\big) \;=\; 0 \;, \tag{4.11}$$

in der neben der unabhängigen Variablen t und einer gesuchten Funktion $y = y(t)$ auch deren Ableitungen bis zur Ordnung n auftreten, heißt *gewöhnliche Differentialgleichung n-ter Ordnung*. Ist t_0 aus dem Definitionsbereich von y, so heißen gegebene Werte $y(t_0), y'(t_0), \ldots, y^{(n-1)}(t_0)$ *Anfangsbedingungen*. Die Differentialgleichung (4.11) zusammen mit ihren Anfangsbedingungen wird *Anfangswertproblem* genannt.

Bei den oben diskutierten Beispielen handelt es sich also um gewöhnliche Differentialgleichungen erster und zweiter Ordnung.

4.5.1 Lineare Differentialgleichungen

Definition 4.5.2 (Lineare homogene Differentialgleichung)**.** Für $\alpha \in \mathbb{R} \setminus \{0\}$ nennen wir die gewöhnliche Differentialgleichung

$$y'(t) \;=\; \alpha \cdot y(t)$$

linear und *homogen*.

Satz 4.5.3. *Es sei $\alpha \in \mathbb{R}$. Zu gegebenen Werten $t_0, y_0 \in \mathbb{R}$ gibt es genau eine Funktion $y : \mathbb{R} \to \mathbb{R}$, die die lineare homogene Differentialgleichung*

$$y'(t) \;=\; \alpha \cdot y(t)$$

löst und den Anfangswert $y(t_0) = y_0$ hat, nämlich

$$y(t) \;=\; \exp\big(\alpha(t - t_0)\big) \cdot y_0 \;. \tag{4.12}$$

Beweis. Man rechnet leicht nach, dass die in (4.12) gegebene Funktion y die Differentialgleichung und die Anfangswertbedingungen erfüllt. Wir nehmen an, dass $\bar{y}$ eine weitere Funktion mit diesen Eigenschaften ist. Wir betrachten die Funktion $f(t) := \exp(-\alpha(t - t_0)) \cdot \bar{y}(t)$. Dann gilt nach Produktregel

$$\begin{aligned} f'(t) \;&=\; -\alpha \cdot \exp(-\alpha(t - t_0)) \cdot \bar{y}(t) + \exp(-\alpha(t - t_0)) \cdot \bar{y}'(t) \\ &=\; -\alpha \cdot \exp(-\alpha(t - t_0)) \cdot \bar{y}(t) + \exp(-\alpha(t - t_0)) \cdot \alpha \cdot \bar{y}(t) \\ &=\; 0 \;. \end{aligned}$$

Folglich ist f konstant, also $f(t) = f(t_0) = y_0$. Damit erhält man

$$\bar{y}(t) \;=\; \exp(\alpha(t - t_0)) \cdot f(t) \;=\; \exp(\alpha(t - t_0)) \cdot y_0 \;=\; y(t)$$

für alle t. □

Definition 4.5.4 (Lineare inhomogene Differentialgleichung)**.** Es sei $g : \mathbb{R} \to \mathbb{R}$ stetig und $\alpha \in \mathbb{R}$. Dann nennen wir die gewöhnliche Differentialgleichung

$$y'(t) \;=\; \alpha \cdot y(t) + g(t)$$

linear und *inhomogen*.

Satz 4.5.5. *Es sei $g : \mathbb{R} \to \mathbb{R}$ stetig und $\alpha \in \mathbb{R}$. Zu gegebenen Werten $t_0, y_0 \in \mathbb{R}$ gibt es genau eine Funktion $y : \mathbb{R} \to \mathbb{R}$, die die lineare inhomogene Differentialgleichung*

$$y'(t) \;=\; \alpha \cdot y(t) + g(t)$$

löst und den Anfangswert $y(t_0) = y_0$ hat, nämlich

$$y(t) \;=\; \exp\bigl(\alpha(t-t_0)\bigr) \cdot y_0 + \exp\bigl(\alpha(t-t_0)\bigr) \int_{t_0}^{t} \exp\bigl(-\alpha(s-t_0)\bigr) \cdot g(s)\; ds \;\; .$$

Beweis. Man rechnet leicht nach, dass die gegebene Funktion y die Differentialgleichung und die Anfangswertbedingungen erfüllt. Wir nehmen an, dass $\bar{y}$ eine weitere Funktion mit diesen Eigenschaften ist. Wir betrachten die Funktion $\hat{y}(t) := y(t) - \bar{y}(t)$, für die gilt

$$\hat{y}'(t) \;=\; y'(t) - \bar{y}'(t) \;=\; 0$$

und $\hat{y}(t_0) = y'(t_0) - \bar{y}'(t_0) = 0$. Folglich ist $\hat{y}$ die eindeutige Lösung der linearen homogenen Differentialgleichung mit $\alpha = 0$ und Anfangswert 0 und damit nach Satz 4.5.3 die Nullfunktion. Folglich ist $\bar{y} = y$. □

4.5.2 Eine nichtlineare Differentialgleichung

Wir betrachten in diesem Abschnitt beispielhaft die folgende nichtlineare Differentialgleichung:

$$y'(t) \;=\; \alpha \cdot y^2 - \beta \cdot y$$

mit $\alpha, \beta \in \mathbb{R} \setminus \{0\}$. Dadurch wird ein etwas komplexerer Wachstumsprozess einer Population beschrieben, den wir im Folgenden studieren werden.

Zur Lösung der Differentialgleichung definieren wir die Funktion $u := 1/y$, für die gilt

$$u' \;=\; -\frac{y'}{y^2} \;=\; -\frac{\alpha \cdot y^2 - \beta \cdot y}{y^2} \;=\; \beta \cdot u - \alpha \;\; .$$

Die Funktion u erfüllt also eine einfache lineare inhomogene Differentialgleichung. Damit erhält man (wir setzen $t_0 := 0$)

$$u(t) \;=\; \exp(\beta \cdot t) \cdot u_0 + \frac{\alpha}{\beta}\bigl(1 - \exp(\beta \cdot t)\bigr) \;\; .$$

Daraus ergibt sich

$$y(t) \;=\; \frac{\beta \cdot y_0}{(\beta - \alpha \cdot y_0) \cdot \exp(\beta \cdot t) + \alpha \cdot y_0} \;\; .$$

Wir diskutieren nun das Verhalten von y für bestimmte Werte der Parameter α und β.

- Ist $\alpha < 0$ und $\beta < 0$, so gilt für jeden beliebigen Startwert y_0, dass

$$\lim_{t\to\infty} y(t) \;=\; \frac{\beta}{\alpha} \;.$$

  Das bedeutet also, dass sich die Population auf Dauer stabilisiert.

- Ist $\alpha > 0$ und $\beta > 0$ mit $\beta > \alpha \cdot y_0$, so gilt

$$\lim_{t\to\infty} y(t) \;=\; 0$$

  und die Population stirbt aus.

- Ist $\alpha > 0$ und $\beta > 0$ mit $\beta = \alpha \cdot y_0$, so gilt

$$y(t) \;=\; \frac{\beta}{\alpha} \qquad \text{für alle } t.$$

  Das heißt, die Population bleibt konstant.

- Ist schließlich $\alpha > 0$ und $\beta > 0$ mit $\beta < \alpha \cdot y_0$, so gilt

$$\lim_{t\to t_1} y(t) \;=\; \infty \qquad \text{für} \quad t_1 \;:=\; \frac{1}{\beta} \ln\left(\frac{\alpha \cdot y_0}{\alpha \cdot y_0 - \beta}\right) \;.$$

  Das heißt, die Population explodiert nach konstanter Zeit.

4.5.3 Lineare Schwingungsgleichung

Wir studieren in diesem Abschnitt die schon weiter oben betrachtete Schwingungsgleichung, die durch

$$y''(t) \;=\; -\,\omega^2 \cdot y(t)$$

gegeben ist. Man spricht hier auch von einer *freien* und *homogenen* Schwingungsgleichung. Eine Verallgemeinerung dieser Differentialgleichung spielt bei der Beschreibung von Schwingungen in elektrischen Stromkreisen, wie sie in jedem Computer auftauchen (beispielsweise bei der Taktung des Prozessors), eine wichtige Rolle.

Satz 4.5.6 (Lösung der freien homogenen Schwingungsgleichung)**.** *Es sei* $\omega \in \mathbb{R}\backslash\{0\}$. *Zu gegebenen Werten* $t_0, y_0, v_0 \in \mathbb{R}$ *gibt es genau eine Funktion* $y : \mathbb{R} \to \mathbb{R}$, *die die Differentialgleichung zweiter Ordnung*

$$y''(t) \;=\; -\,\omega^2 \cdot y(t)$$

löst und die Anfangswerte $y(t_0) = y_0$ *und* $y'(t_0) = v_0$ *hat, nämlich*

$$y(t) \;=\; y_0 \cos\big(\omega(t - t_0)\big) + \frac{v_0}{\omega} \sin\big(\omega(t - t_0)\big) \;.$$

Beweis. Man rechnet leicht nach, dass die gegebene Funktion y die Differentialgleichung und die Anfangswertbedingungen erfüllt. Wir nehmen an, dass $\bar{y}$ eine weitere Funktion mit diesen Eigenschaften ist. Wir betrachten die Funktion $\hat{y}(t) := y(t) - \bar{y}(t)$, für die gilt

$$\hat{y}'' + \omega^2 \cdot \hat{y} \;=\; 0 \;.$$

Multipliziert man diese Gleichung mit $2\hat{y}'$, so erhält man

$$0 \;=\; 2 \cdot \hat{y}'' \cdot \hat{y}' + 2\omega^2 \cdot \hat{y} \cdot \hat{y}' \;=\; \big((\hat{y}')^2\big)' + \omega^2(\hat{y}^2)' \;.$$

Folglich ist die Funktion $(\hat{y}')^2 + \hat{y}^2$ konstant und zwar mit Wert

$$\big(\hat{y}'(t_0)\big)^2 + \big(\hat{y}(t_0)\big)^2 \;=\; 0 \;.$$

Daraus folgt sofort, dass $\hat{y}^2 = 0$, und damit $y = \bar{y}$. □

Kapitel 5

Kombinatorik und Graphentheorie

Die ersten beiden Abschnitte dieses Kapitels über Kombinatorik basieren ursprünglich auf §12 *Abzählende Kombinatorik* und §13 *Rekursion und erzeugende Funktionen* des Skriptes *Lineare Algebra für Informatiker (Version 1996/2000)* von Gerd Wegner. Es wurde seither von Herrn Möller und Herrn Scharlau überarbeitet. Ich danke den Genannten für das zur Verfügung Stellen des Materials.

Im ersten Abschnitt geht es um abzählende Kombinatorik. Zunächst werden einige elementare Techniken wie das Prinzip des doppelten Abzählens besprochen. Nach einer ausführlichen Behandlung der Binomialkoeffizienten werden dann die auch in der (endlichen) Stochastik benutzten Zählkoeffizienten für geordnete und ungeordnete Auswahlen ohne und mit Wiederholung aus einer endlichen Menge hergeleitet. Weiter wird das Prinzip der Inklusion und Exklusion behandelt. Schließlich werden rekursive Anzahlformeln für Partitionen hergeleitet, vorrangig für Mengenpartitionen (Stirlingzahlen zweiter und erster Art), kurz auch für Zahlpartitionen.

Im zweiten Teil werden rekursiv definierte Folgen behandelt. Es wird die Methode der erzeugenden Funktionen eingeführt und verschiedene Techniken für die Lösung von Rekursionsgleichungen werden besprochen. Der Schwerpunkt liegt auf linearen Rekursionen. Die Lösungen hängen von den Startwerten der Rekursion ab; im linearen Fall führt das auf eine entsprechende lineare Struktur auf der Lösungsmenge, die im Fall konstanter Koeffizienten zu einem vollständigen Lösungsverfahren führt. Als Folgerung ergeben sich auch Aussagen über das Wachstum solcher rekursiver Folgen.

Im dritten Teil geben wir schließlich eine kurze Einführung in die Graphentheorie.

5.1 Abzählende Kombinatorik

5.1.1 Einige elementare Zählprinzipien

Wir haben im Laufe der bisherigen Vorlesung schon mehrfach Dinge abgezählt, etwa bei Teilmengen. Bei allen Abzählverfahren werden die folgenden Grundaussagen häufig stillschweigend verwendet. Wir haben diese Aussagen teilweise bereits in Kapitel 1, Lemma 1.2.12 und Lemma 1.2.16 erwähnt.

Lemma 5.1.1. *Es seien $M_1, \ldots, M_r$ endliche Mengen. Dann gilt*

(i) $|\bigcup_{k=1}^{r} M_k| = \sum_{k=0}^{r} |M_k|$*, falls die Mengen paarweise disjunkt sind;*

(ii) $|\prod_{k=1}^{r} M_k| = \prod_{k=1}^{r} |M_k|$.

Dabei bezeichnet $\prod_{k=1}^{r} M_k$ das r-fache kartesische Produkt $M_1 \times M_2 \times \cdots \times M_r$.

Beweis. Aussage (i) ist trivial, und (ii) erhält man mit Induktion über r, wobei man $(x_1, \ldots, x_r)$ mit $((x_1, \ldots, x_{r-1}), x_r)$ identifiziert. □

Als nächstes besprechen wir das sogenannte Prinzip des *doppelten Abzählens*; es ist sehr einfach zu begründen, liefert aber oft überraschende Vereinfachungen.

Satz 5.1.2 (Doppeltes Abzählen)**.** *Es sei eine Relation R zwischen zwei endlichen Mengen M und N gegeben, also $R \subseteq M \times N$. Für $x \in M$ bezeichne $r(x)$ die Anzahl der mit x in Relation stehenden $y \in N$, und entsprechend $s(y)$ für $y \in N$ die Anzahl der mit y in Relation stehenden $x \in M$. Dann gilt*

$$\sum_{x \in M} r(x) \;=\; \sum_{y \in N} s(y) \;.$$

Beweis. Für $(x, y) \in M \times N$ setzen wir $a(x, y) := 1$, falls $(x, y) \in R$ und $a(x, y) := 0$, falls $(x, y) \notin R$. (Wenn man so will, betrachten wir die *charakteristische Funktion* $a : M \times N \to \{0, 1\}$ der Teilmenge $R \subseteq M \times N$.) Dann gilt für $x_0 \in M$ und $y_0 \in N$ nach Definition

$$r(x_0) \;=\; \sum_{y \in N} a(x_0, y) \qquad \text{und} \qquad s(y_0) \;=\; \sum_{x \in M} a(x, y_0) \;.$$

Es folgt

$$\sum_{x \in M} r(x) \;=\; \sum_{(x,y) \in M \times N} a(x, y) \;=\; \sum_{y \in N} s(y) \;.$$

Beide in Frage stehenden Zahlen sind also gleich der Anzahl aller in Relation stehenden Paare (x, y) (also $|R|$) und deshalb gleich. □

Wenn die beiden Mengen jeweils in einer konkreten Aufzählung ihrer Elemente gegeben sind als $M = \{x_1, x_2, \ldots, x_m\}$ und $N = \{y_1, y_2, \ldots, y_n\}$, dann entspricht die charakteristische Funktion a einer (booleschen) $m \times n$-Matrix über $\{0, 1\}$, die auch *Inzidenzmatrix* der Relation R genannt wird. Der Beweis von Satz 5.1.2 läuft dann darauf hinuas, dass man diese Matrix einmal spaltenweise und einmal zeilenweise durchläuft.

Abzählargumente werden auch benutzt, um (nicht-konstruktive) Existenzbeweise zu führen. Das Grundprinzip steckt dabei oft im sogenannten *Dirichletschen Schubfachprinzip*: Wenn man n Objekte auf k Fächer verteilt und $n > k$ ist, dann landen in einem Fach mindestens zwei Objekte. Eine mathematisch präzise Form dieser Aussage ist die folgende:

Satz 5.1.3 (Schubfachprinzip, "pigeonhole principle"). *Es sei $f : X \to Y$ eine Abbildung zwischen endlichen Mengen und $|X| > |Y|$. Dann gibt es ein $y \in Y$ mit $|f^{-1}(y)| \geq 2$.*

Beispiele.

(i) Eine Bibliothek habe mehr als 4000 Bücher. Keines der Bücher habe mehr als 4000 Seiten. Dann gibt es (mindestens) zwei Bücher mit der gleichen Seitenzahl.

(ii) Es sei X eine endliche Menge von Personen. Wir betrachten auf X die Relation "x kennt y" und nehmen an, diese Relation sei symmetrisch. Dann gibt es in X gibt zwei Personen, die die gleiche Anzahl von anderen Personen aus X kennen.

Denn: Es sei $n = |X|$. Wir betrachten die Funktion $f : X \to \{0, \ldots, n-1\}$, wobei $f(x) = m$ bedeutet, dass $x \in X$ genau m andere Personen in X kennt. Das Schubfachprinzip ist nicht direkt anwendbar weil

$$|X| \;=\; n \;=\; |\{0, \ldots, n-1\}| \;.$$

Wir verwenden einen kleinen Trick und ersetzen $\{0, \ldots, n-1\}$ durch das Bild $Y := f(X) \subseteq \{0, \ldots, n-1\}$. Wir behaupten, dass Y eine echte Teilmenge von $\{0, \ldots, n-1\}$ ist; dann ist $|X| > |Y|$ und das Schubfachprinzip anwendbar.

Erster Fall: Es gibt ein $a \in X$ mit $f(a) = 0$, also einen Einsiedler, der niemanden kennt. Dann kennen die anderen ihn auch nicht; das heißt, keiner kennt alle anderen. Somit ist $n - 1 \notin Y$.

Zweiter Fall: Es gibt kein $a \in X$ mit $f(a) = 0$. Dann ist $0 \notin Y$, und die Behauptung $Y \neq \{0, \ldots, n-1\}$ gilt ebenfalls.

5.1.2 Binomialkoeffizienten

Wir definieren zunächst die sogenannten Binomialkoeffizienten, die uns schon einmal in Kapitel 4, Abschnitt 4.1.5 begegnet sind.

Definition 5.1.4 (Binomialkoeffizienten)**.** Für $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$ wird der *Binomialkoeffizient* als

$$\binom{n}{k} := \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k}$$

(lies: „n über k“) definiert. Für $k = 0$ setzt man

$$\binom{n}{0} := 1 \qquad \text{für alle } n \in \mathbb{N}_0.$$

Der Zähler des definierenden Bruchs von $\binom{n}{k}$ wird *fallende Faktorielle von n der Länge k* genannt und mit $(n)_k$ bezeichnet, also

$$(n)_k := n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) \ .$$

Bemerkung. Wir fassen im Folgenden einige Eigenschaften von Binomialkoeffizienten zusammen.

(i) Für $n, k \in \mathbb{N}_0$ mit $n \geq k$ ist

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

(ii) Für $n < k$ gilt $\binom{n}{k} = 0$.

(iii) Für $n \in \mathbb{N}_0$ gilt $\binom{n}{0} = \binom{n}{n} = 1$.

(iv) Für $0 \leq k \leq n$ gilt wegen (i) die Symmetrieeigenschaft

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

(v) Die Definition von $\binom{x}{k}$ ergibt auch für beliebiges $x \in \mathbb{R}$ Sinn. Wenn x keine ganze Zahl ist, ergibt sich auch für $x < k$ ein von Null verschiedener Wert.

Satz 5.1.5 (Rekursionsformel für Binomialkoeffizienten)**.** *Für $k, n \in \mathbb{N}_0$ gilt*

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

Beweis. Für $k = 0$ überprüft man die Behauptung direkt anhand der Definition. Für $k > 0$ gilt

$$\binom{n}{k} = \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k}$$

und entsprechend

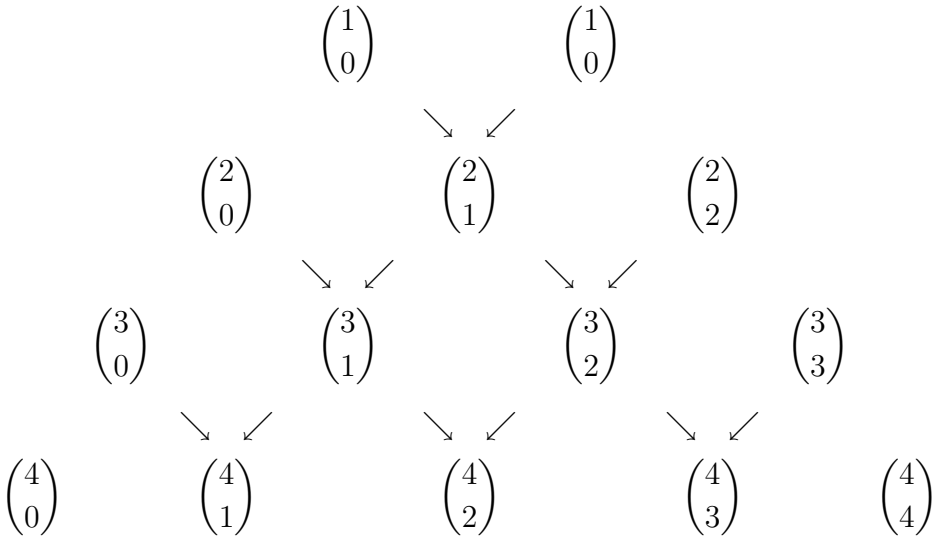
$$\binom{n}{k+1} = \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k} \cdot \frac{n-k}{k+1} \ .$$

Erweitert man im Bruch von $\binom{n}{k}$ Zähler und Nenner mit $k+1$, dann lässt sich bei der Addition von $\binom{n}{k}$ und $\binom{n}{k+1}$ einiges ausklammern, und man erhält die Behauptung:

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k} \cdot \frac{1}{k+1} \cdot \big((k+1) + (n-k)\big) \\
&= \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k} \cdot \frac{1}{k+1} \cdot (n+1) \\
&= \frac{n+1}{1} \cdot \frac{n}{2} \cdot \ldots \cdot \frac{n-k+2}{k} \cdot \frac{n-k+1}{k+1} \\
&= \binom{n+1}{k+1} \ .
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Wir erläutern noch die rekursive Berechnung der Binomialkoeffizienten gemäß Satz 5.1.5. Sie wird oft in Form des sogenannten *Pascal'schen Dreiecks* notiert:



u.s.w.

Mit konkreten Zahlen also

$$
\begin{array}{ccccccccccccc}
 & & & & 1 & & 1 & & & & & & \\
 & & & 1 & & 2 & & 1 & & & & & \\
 & & 1 & & 3 & & 3 & & 1 & & & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 & &
\end{array}
$$

u.s.w.

Von Lemma 5.1.1 (i) macht man bei Abzählung mit Hilfe von Fallunterscheidungen Gebrauch, wobei darauf zu achten ist, dass die Fälle disjunkt sind (und natürlich andererseits alle Möglichkeiten erschöpfen). Ein einfaches Beispiel hierfür ist der Beweis zu folgendem bekannten Resultat, das wir schon in Kapiel 1 erwähnt haben (siehe Lemma 1.2.14).

Lemma 5.1.6. *Eine n-elementige Menge besitzt 2^n Teilmengen, das heißt also $|\mathcal{P}(M)| = 2^n$ für $|M| = n$.*

Beweis. Wir verwenden Induktion über n: Für $|M| = 0$, das heißt $M = \emptyset$, ist $\mathcal{P}(M) = \{\emptyset\}$ und damit $|\mathcal{P}(M)| = 1 = 2^0$. Es sei nun $n > 0$ und $|M| = n$, also $M \neq \emptyset$. Wir zeichnen ein Element a in M aus und zerlegen $\mathcal{P}(M)$ in zwei disjunkte Klassen $\mathcal{P}(M) = \mathcal{G}_1 \cup \mathcal{G}_2$, nämlich in

$$\mathcal{G}_1 \;:=\; \{A \mid A \subset M \wedge a \notin A\} \quad \text{und in} \quad \mathcal{G}_2 \;:=\; \{A \mid A \subset M \wedge a \in A\} \;.$$

Die Klasse $\mathcal{G}_1$ ist nichts anderes als $\mathcal{P}(M \setminus \{a\})$. Daher ist nach Induktionsannahme $|\mathcal{G}_1| = 2^{n-1}$. Die Menge $\mathcal{G}_2$ wird durch die Zuordnung $A \mapsto A \setminus \{a\}$ bijektiv auf $\mathcal{P}(M \setminus \{a\})$ abgebildet, also ist auch $|\mathcal{G}_2| = 2^{n-1}$. Nun folgt mit Lemma 5.1.1 (i) die Behauptung. □

Die Idee dieses Beweises, durch geeignete Fallunterscheidung zu einer Rekursionsformel für die gesuchte Anzahl a_n zu kommen (die hier einfach $a_n = 2a_{n-1}$ lautet), ist typisch für viele Anzahlbestimmungen und wird uns im Folgenden noch öfter begegnen. Ebenso die Idee, durch Auszeichnung eines Elementes zu dieser Rekursion zu gelangen.

Wir wollen nun Lemma 5.1.6 dahingehend verschärfen, dass wir die Anzahl der Teilmengen mit genau k Elementen, kurz als *k-Teilmengen* bezeichnet, bestimmen. Dieses führt wieder auf die oben eingeführten Binomialkoeffizienten, denn es gilt:

Satz 5.1.7. *Es seien $k, n \in \mathbb{N}_0$. Die Anzahl der k-Teilmengen einer n-elementigen Menge ist $\binom{n}{k}$.*

Beweis. Es sei $a(n,k)$ die gesuchte Anzahl. Natürlich ist $a(0,k) = 0$ für alle $k > 0$ und $a(n,0) = 1$ für alle $n \in \mathbb{N}_0$. Für $n \geq 1$ und $k \geq 1$ verwenden wir dasselbe Argument wie im Beweis zu Lemma 5.1.6: Ist $|M| = n+1$ und x ein fest gewähltes Element von M, so gilt für eine beliebige $(k+1)$-Teilmenge von M:

- Entweder enthält sie x nicht und ist damit eine $(k+1)$-Teilmenge der n-elementigen Menge $M \setminus \{x\}$.
- Oder sie enthält x; solche $(k+1)$-Teilmengen von M entsprechen umkehrbar eindeutig den k-Teilmengen von $M \setminus \{x\}$.

Daher gilt $a(n+1,k+1) = a(n,k+1) + a(n,k)$. Die Zahlen $a(n,k)$ genügen also derselben Rekursionsformel wie die Binomialkoeffizienten nach Satz 5.1.5:

$$\binom{n+1}{k+1} \;=\; \binom{n}{k+1} + \binom{n}{k}$$

und auch denselben Anfangsbedingungen

$$a(n,0) \;=\; 1 \;=\; \binom{n}{0} \quad \text{und} \quad a(0,k) \;=\; 0 \;=\; \binom{0}{k} \qquad \text{für } n \in \mathbb{N}_0 \text{ und } k \in \mathbb{N}.$$

Da durch die Rekursion und die Anfangsbedingungen die Zahlen für alle $n, k \in \mathbb{N}_0$ eindeutig bestimmt sind, folgt $a(n,k) = \binom{n}{k}$ für alle $k, n \in \mathbb{N}_0$. □

Auch dies ist eine mehrfach wiederkehrende Idee in der Kombinatorik: Nachweis der Gleichheit zweier Zahlenfolgen durch den Beweis, dass sie derselben Rekursion und denselben Anfangsbedingungen genügen.

Die Binomialkoeffizienten treten in der Kombinatorik vielfach auf. Ein Beispiel ist die uns bereits aus Kapitel 4, Lemma 4.1.42 bekannte Binomialformel.

Satz 5.1.8 (Binomischer Lehrsatz)**.** *Es seien a und b aus einem kommutativen Ring R mit Eins und $n \in \mathbb{N}_0$. Dann gilt*

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

Beweis. Beim Ausmultiplizieren von

$$(a+b)^n \;=\; (a+b) \cdot (a+b) \cdot \ldots \cdot (a+b)$$

müssen wir uns bei jedem Faktor $(a+b)$ für a oder b entscheiden. Wenn wir uns bei den Faktoren mit den Nummern $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ für a entscheiden, so entspricht jede solche Wahl eindeutig einer k-Teilmenge von $\{1, 2, \ldots, n\}$. Hierfür gibt es nach Satz 5.1.7 genau $\binom{n}{k}$ Möglichkeiten. Wenn wir uns k mal

für a entscheiden, tritt b genau $n-k$ mal auf. Daher haben wir genau $\binom{n}{k}$ Summanden $a^k b^{n-k}$. Für die Summe bedeutet das

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

Damit ist der Beweis abgeschlossen. □

Für die Binomialkoeffizienten und für verwandte Zahlen gibt es eine Fülle von Identitäten. Zwei einfache Beispiele hierfür sind

$$\sum_{k=0}^{n} \binom{n}{k} \;=\; 2^n \qquad \text{für alle } n \in \mathbb{N}_0$$

und

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k \;=\; 0 \qquad \text{für alle } n > 0.$$

Beides lässt sich sehr einfach sowohl mit Satz 5.1.8 wie auch mit Satz 5.1.7 und Lemma 5.1.6 begründen.

Der folgende Satz gibt ein etwas komplizierteres Beispiel einer Identität für Binomialkoeffizienten.

Satz 5.1.9. *Für $m, n \in \mathbb{N}_0$ gilt*

$$\binom{m+n}{m} \;=\; \sum_{k=0}^{m} \binom{m}{k} \cdot \binom{n}{k} \;.$$

Beweis. Man beachte zunächst, dass beide Seiten symmetrisch in m und n sind, da die auf der rechten Seite stehende Summe stets bei der kleineren der beiden Zahlen abgebrochen werden kann; die übrigen Summanden verschwinden. Es sei daher ohne Beschränkung der Allgemeinheit $m \leq n$. Zum Beweis der Gleichung zählt man in dem in Abbildung 5.1 dargestellten Rechteckgitter die Gesamtheit $\mathcal{W}$ aller kürzesten Wege vom Punkt $(0,0)$ zum Punkt (n,m) auf zwei Weisen ab. Jeder solche Weg besteht aus m senkrechten Einheitswegstrecken und n waagerechten Einheitswegstrecken in beliebiger Reihenfolge. Wenn wir in der Reihenfolge des Weges jede senkrechte Strecke durch „0“ und jede waagerechte Strecke durch „1“ symbolisieren, so wird jeder kürzeste Weg umkehrbar eindeutig dargestellt durch eine 0-1-Sequenz der Länge $m+n$ mit genau m Einsen. Die gesuchte Anzahl ist also gleich der Anzahl dieser 0-1-Sequenzen und damit gleich $\binom{m+n}{m}$.

Zum anderen benutzt jeder Weg aus $\mathcal{W}$ genau einen der Punkte $x_k = (m-k, k)$ und es gibt (nach der ersten Überlegung) genau $\binom{m}{k}$ kürzeste Wege von $(0,0)$

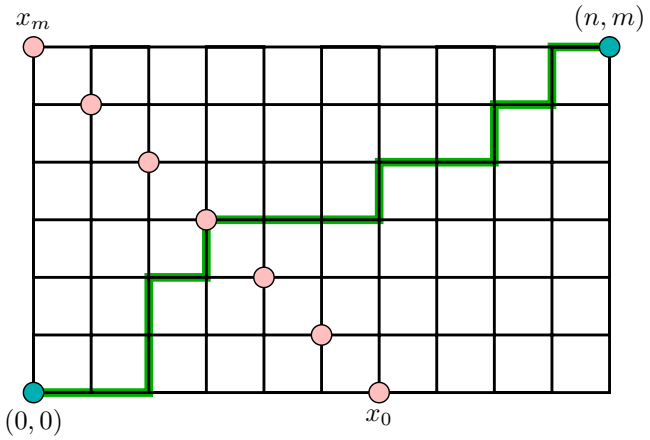


Abbildung 5.1: Jeder kürzeste Weg von $(0,0)$ nach (n,m) muss durch einen der Punkte x_k, $k = 0,\ldots,m$ gehen.

nach x_k und genau $\binom{n}{m-k}$ kürzeste Wege von x_k nach (n,m). Das ergibt die zweite Anzahl:

$$\sum_{k=0}^{m} \binom{m}{k} \cdot \binom{n}{m-k} \;=\; \sum_{j=0}^{m} \binom{m}{m-j} \cdot \binom{n}{j} \;=\; \sum_{k=0}^{m} \binom{m}{k} \cdot \binom{n}{k} \;.$$

Damit ist der Beweis abgeschlossen. □

Einen zweiten Beweis für Satz 5.1.9 erhält man durch Anwendung von Satz 5.1.8 auf beide Seiten der Gleichung

$$(1+t)^{m+n} \;=\; (1+t)^m \cdot (1+t)^n$$

und Vergleich der Koeffizienten von t^m.

5.1.3 Auswahlen aus einer Menge

Viele einfache kombinatorischen Fragestellungen lassen sich zurückführen auf gewisse Grundaufgaben, aus einer gegebenen endlichen Menge bestimmte Auswahlen zu treffen. Je nachdem, ob wir es zulassen, dass dabei ein und dasselbe Element mehrfach ausgewählt wird (ohne oder mit Wiederholungen), und ob wir die Auswahl als geordnet betrachten (1. Element, 2. Element, ...) oder als ungeordnet, ergeben sich vier verschiedene Anzahlen.

Satz 5.1.10. *Es seien $k,n \in \mathbb{N}_0$ und M eine endliche Menge mit $|M| = n$ Elementen. Dann wird die Anzahl der Möglichkeiten für die Auswahl von k Elementen aus dieser n-elementigen Menge M gegeben durch*

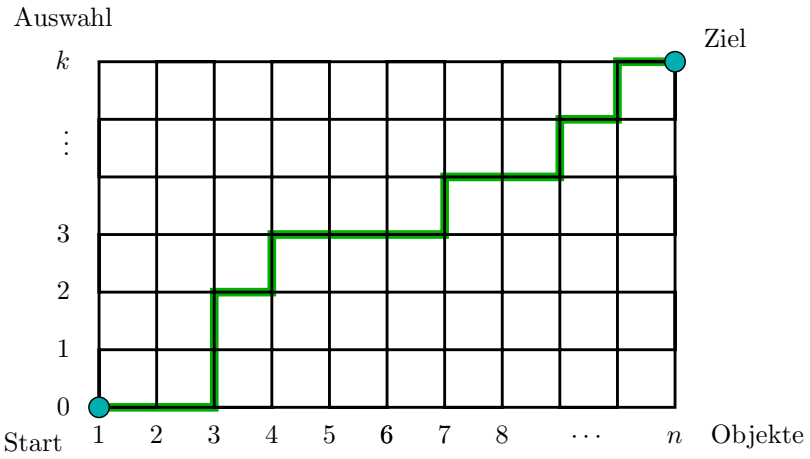


Abbildung 5.2: Jeder kürzeste Weg von $(0,0)$ nach (n,k) induziert genau eine ungeordnete Auswahl mit Wiederholungen und umgekehrt.

	geordnet	*ungeordnet*
ohne Wiederholungen	$(n)_k$	$\binom{n}{k}$
mit Wiederholungen	n^k	$\binom{n+k-1}{k}$

Die geordneten Auswahlen ohne Wiederholungen heißen *k-Permutationen* und auch die übrigen Auswahlen haben Namen, auf deren Nennung wir hier aber verzichten.

Beweis. Bei der geordneten Auswahl ohne Wiederholungen haben wir es mit k-Tupeln aus der Menge M zu tun. Zur Besetzung der ersten Stelle des k-Tupels hat man freie Auswahl unter allen n Elementen von M, also n Möglichkeiten. Für den zweiten Eintrag des k-Tupels bleiben noch $n-1$ Möglichkeiten, da wir keine Wiederholungen zulassen. Sind schließlich $k-1$ Stellen schon besetzt, so hat man zur Besetzung der k-ten Stelle nur noch die Auswahl unter $n-k+1$ Elementen. Aufmultiplizieren der unabhängigen Möglichkeiten ergibt die gewünschte Zahl.

Den Fall der geordneten Auswahl mit Wiederholungen behandelt man analog, wobei jetzt bei jeder Stelle die volle Auswahl aus allen n Elementen von M besteht.

Ungeordnete Auswahlen ohne Wiederholung können einfach als Teilmengen aufgefasst werden. Somit folgt die Behauptung aus Satz 5.1.7.

Der Fall der ungeordneten Auswahl mit Wiederholungen ist etwas schwieriger zu behandeln. Die Formel lässt sich wieder mit einem Gitterweg-Argument (vgl. Abbildung 5.1 im Beweis zu Satz 5.1.9) beweisen. Wir betrachten die ganzzahligen Gitterpunkte (x,y) mit den Koordinaten $x \in \{1,\ldots,n\}$ und $y \in \{0,\ldots,k\}$ (siehe Abbildung 5.2). Die x-Koordinate entspreche einer Durchnummerierung der Elemente von M bzw. o.B.d.A. sei $M = \{1,2,\ldots,n\}$; da es bei einer ungeordneten

Auswahl auf die Reihenfolge nicht ankommt, können wir sie gemäß dieser Nummerierung von M anordnen. Jede Auswahl entspricht dann einem kürzesten Weg im Gitter vom Start $(0,0)$ zum Ziel (n,k), indem wir die Benutzung einer senkrechten Strecke von (i,j) nach $(i,j+1)$ als Wahl des Elementes i interpretieren. In der Abbildung (hier ist $n=11$ und $k=6$) entspricht also der markierte Weg der Auswahl 3|3|4|7|9|10. Nach der Überlegung im Beweis zu Satz 5.1.9 ist die Anzahl also gleich $\binom{n+k-1}{k}$ (beachte, dass die Nummerierung in der Horizontalen hier mit 1 beginnt). □

Die in Satz 5.1.10 auftretenden Anzahlen lassen auch andere Interpretationen zu. So ist zum Beispiel die Anzahl n^k aller geordneten Auswahlen mit Wiederholungen von k Elementen aus n Elementen auch die Anzahl aller Abbildungen einer k-Menge in eine n-elementige Menge, oder die Anzahl der Einordnungsmöglichkeiten von k unterscheidbaren Objekten in n unterscheidbare Fächer. Auch die Anzahl der Einordnungsmöglichkeiten von k nicht unterscheidbaren Objekten in n unterscheidbare Fächer tritt in Satz 5.1.10 auf (welche ist das?).

Die Binomialzahlen besitzen eine sowohl kombinatorisch wie auch (in Analogie zu Satz 5.1.8) algebraisch motivierte Verallgemeinerung.

Definition 5.1.11. Für $n = n_1 + \ldots + n_k$ mit $n_1, \ldots, n_k \in \mathbb{N}_0, k \in \mathbb{N}$ heißt

$$\binom{n}{n_1, \ldots, n_k} := \frac{n!}{n_1! \cdot \ldots \cdot n_k!}$$

ein *Multinomialkoeffizient.*

Bemerkung.

(i) Speziell für $k=2$, $n = n_1 + n_2$ ist

$$\binom{n}{n_1, n_2} = \binom{n}{n_1} = \binom{n}{n_2} .$$

(ii) Wenn man im Fall $k=n$ alle $n_i = 1$ wählt, so erhält man

$$\binom{n}{1, \ldots, 1} = n! .$$

Die kombinatorische Bedeutung der Multinomialkoeffizienten liegt in der folgenden Anzahlbestimmung:

Satz 5.1.12. *Es seien n Objekte von k Sorten gegeben, wobei n_i (nicht unterscheidbare) Objekte der i-ten Sorte vorhanden seien (für $i = 1, \ldots, k$); das Tupel $(n_1, \ldots, n_k)$ heißt die* Spezifikation *der Objekte. Dann ist $\binom{n}{n_1, \ldots, n_k}$ die Anzahl der möglichen Anordnungen dieser Objekte als Folge der Länge n.*

Beweis. Es sei a die gesuchte Anzahl bei fester Spezifikation $(n_1, \ldots, n_k)$. Ersetzen wir die n_1 Objekte der ersten Sorte durch n_1 unterscheidbare Objekte, so erhöht dies die Anzahl der möglichen Anordnungen um den Faktor $n_1!$, die Anzahl der Permutationsmöglichkeiten dieser n_1 Elemente. Gleiches bei allen Sorten durchgeführt ergibt schließlich $a \cdot n_1! \cdot \ldots \cdot n_k!$ Möglichkeiten. Da nun aber alle Elemente voneinander verschieden sind, ist diese Anzahl gleich $n!$, woraus die Behauptung folgt. □

Beispiel. Für vier Objekte der Spezifikation $(1, 1, 2)$, die wir uns durch die Buchstaben a, b, c, c gegeben denken, hat man die folgenden zwölf Anordnungsmöglichkeiten:

abcc	*bacc*	*cabc*	*cbca*
acbc	*bcac*	*cacb*	*ccab*
accb	*bcca*	*cbac*	*ccba*

Die algebraische Bedeutung der Multinomialkoeffizienten liegt in der folgenden Verallgemeinerung von Satz 5.1.8.

Satz 5.1.13. *Es seien $x_1, \ldots, x_k$ Elemente eines kommutativen Ringes und $n \in \mathbb{N}_0$. Dann gilt*

$$(x_1 + \cdots + x_k)^n = \sum_{\substack{n_1,\ldots,n_k \geq 0 \\ n_1+\cdots+n_k=n}} \binom{n}{n_1, \ldots, n_k} \cdot x_1^{n_1} \cdot \ldots \cdot x_k^{n_k} \ .$$

Beweis. Beim Ausmultiplizieren des Produktes auf der linken Seite der behaupteten Gleichung, bestehend aus den n Faktoren $(x_1 + \ldots + x_k)$, tritt $x_1^{n_1} \cdot \ldots \cdot x_k^{n_k}$ als Summand genau so oft auf, wie es Anordnungsmöglichkeiten von x_1 (n_1-mal),…,x_k (n_k-mal) gibt. □

5.1.4 Ein- und Ausschließen

Wir wollen jetzt eine häufig benötigte Variante von Lemma 5.1.1 (i) betrachten. Wie bestimmt man die Kardinalität einer als Vereinigung von Teilmengen gegebenen Menge, wenn diese Teilmengen nicht paarweise disjunkt sind? Dazu ein Beispiel: Wieviele natürlichen Zahlen ≤ 100 sind durch 2, 3 oder 5 teilbar? Bezeichnen wir mit M_k die Menge der durch k teilbaren Zahlen ≤ 100, so wird also nach $|M_2 \cup M_3 \cup M_5|$ gefragt. Für eine einzelne Teilmenge gilt $|M_k| = \lfloor \frac{100}{k} \rfloor$, wenn wir für $x \in \mathbb{R}$ mit $\lfloor x \rfloor$ wieder die größte ganze Zahl $\leq x$ bezeichnen (Gaußklammer). Die Summe dieser Einzelkardinalitäten ergibt eine zu große Zahl, da hier die in den Durchschnitten liegenden Elemente mehrfach gezählt werden. Das Abziehen der Kardinalitäten aller zweifachen Durchschnitte, also von $|M_2 \cap M_3|$, $|M_2 \cap M_5|$ und $|M_3 \cap M_5|$, erbringt ein zu kleines Resultat, da jetzt die Zahlen des dreifachen Durchschnitts $M_2 \cap M_3 \cap M_5$ (also die durch 30

teilbaren Zahlen) zunächst dreifach gezählt, dann aber auch wieder dreifach abgezogen wurden. Das richtige Ergebnis ist also

$$\begin{aligned}|M_2 \cup M_3 \cup M_5| &= |M_2| + |M_3| + |M_5| \\ &\quad - |M_2 \cap M_3| - |M_2 \cap M_5| - |M_3 \cap M_5| \\ &\quad + |M_2 \cap M_3 \cap M_5| \\ &= \frac{100}{2} + \left\lfloor \frac{100}{3} \right\rfloor + \frac{100}{5} - \left\lfloor \frac{100}{6} \right\rfloor - \frac{100}{10} - \left\lfloor \frac{100}{15} \right\rfloor + \left\lfloor \frac{100}{30} \right\rfloor \\ &= 74 \ .\end{aligned}$$

Diese hier am Beispiel dreier Mengen vorgeführte Berechnungsmethode lässt sich verallgemeinern auf eine beliebige (endliche) Anzahl von Mengen, wobei wir außerdem noch, statt einfach die Elemente zu zählen, eine Gewichtung der Elemente mit Werten aus einer additiven Gruppe (z.B. $(K, +)$, K Körper) zulassen können.

Satz 5.1.14 (Ein- und Ausschließen, Inklusion-Exklusion)**.** *Es sei M eine nichtleere Menge, $(G, +)$ eine abelsche Gruppe und $w : M \to G$ eine Abbildung (Gewichtsfunktion). Dann gilt für endliche Teilmengen $M_1, \ldots, M_r$ von M*

$$w(M_1 \cup \cdots \cup M_r) \ = \ \sum_{k=1}^{r} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le r} w(M_{i_1} \cap \cdots \cap M_{i_k}) \ ,$$

wobei $w(A) := \sum_{x \in A} w(x)$ ist für endliche Teilmengen $A \subset M$.

Beweis. Wir verwenden Induktion über r. Für $r = 1$ ist nichts zu zeigen (die Formel liefert $w(M_1) = w(M_1)$) und im Falle $r = 2$ erhält man $w(M_1 \cup M_2) = w(M_1) + w(M_2) - w(M_1 \cap M_2)$, was man wie beim vorausgehenden Beispiel mit drei Mengen direkt bestätigt. Es sei nun $r > 2$. Durch Klammerung und Anwendung der Formel für zwei Mengen folgt zunächst

$$\begin{aligned}w\big((M_1 \cup \cdots \cup M_{r-1}) \cup M_r\big) &= w(M_1 \cup \cdots \cup M_{r-1}) + w(M_r) \\ &\quad - w\big((M_1 \cup \cdots \cup M_{r-1}) \cap M_r\big) \ .\end{aligned}$$

Der letzte Term kann mit Hilfe des Distributivgesetzes umgeformt werden in

$$w\big((M_1 \cup \cdots \cup M_{r-1}) \cap M_r\big) \ = \ w\big((M_1 \cap M_r) \cup \cdots \cup (M_{r-1} \cap M_r)\big) \ .$$

Nun kann man auf den ersten und letzten Term die Induktionsannahme anwenden und erhält damit (nach Umordnung) die Behauptung, wobei der letzte Term diejenigen Summanden der Behauptung liefert, bei denen M_r beteiligt und $k \ge 2$ ist. □

Die Formulierung von Satz 5.1.14 in der allgemeinen Form mit der Gewichtsfunktion spielt vor allem bei wahrscheinlichkeitstheoretischen Anwendungen (x ein Elementarereignis und $w(x)$ seine Wahrscheinlichkeit) eine Rolle. Für den Spezialfall $G := \mathbb{Z}$ und $w(x) := 1$ für alle $x \in M$ liefert Satz 5.1.14 die folgende Anzahlformel.

Korollar 5.1.15. *Es sei M eine nicht-leere Menge. Dann gilt für endliche Teilmengen $M_1, \ldots, M_r$ von M*

$$|M_1 \cup \cdots \cup M_r| \;=\; \sum_{k=1}^{r} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le r} |M_{i_1} \cap \cdots \cap M_{i_k}| \;.$$

Bemerkung. Die Formel vom Ein- und Ausschließen wird häufig auch in einer komplementären Form verwendet: Man fragt nach der Anzahl (oder dem Gewicht) aller Elemente einer Menge M, die gewisse gegebene Eigenschaften $E_1, \ldots, E_r$ *nicht* haben, also nach der Kardinalität (oder dem Gewicht) von $M \setminus (M_1 \cup \cdots \cup M_r)$, wenn wir $M_k := \{x \mid x \in M \;\wedge\; x \text{ hat die Eigenschaft } E_k\}$ setzen. Mit Satz 5.1.14 erhält man dafür

$$w\big(M \setminus (M_1 \cup \cdots \cup M_r)\big) \;=\; w(M) + \sum_{k=1}^{r} (-1)^{k} \sum_{1 \le i_1 < \cdots < i_k \le r} w(M_{i_1} \cap \cdots \cap M_{i_k}) \;.$$

Ein klassisches Anwendungsbeispiel für die Formel vom Ein- und Ausschließen ist etwa das Problem von Montmort, das man (ursprünglich ein Lotterieproblem) in folgende Fragestellung einkleiden kann: n Ehepaare treffen sich zu einem Tanzabend; wieviele Möglichkeiten gibt es, n Tanzpaare so zu bilden, dass keine Ehepaare zusammen tanzen? Dies ist äquivalent zur Frage nach der Anzahl aller fixpunktfreien Permutationen von n Elementen.

Definition 5.1.16 (Permutation, Fixpunkt)**.**

(i) Es sei M eine Menge und $f : M \to M$ eine bijektive Abbildung. Dann heißt f eine *Permutation von M*.

(ii) Ein Element $x \in M$ mit $f(x) = x$ heißt *Fixpunkt* von $f : M \to M$.

(iii) Eine Permutation f von M heißt *fixpunktfrei*, falls kein Element aus M ein Fixpunkt von f ist, das heißt $f(x) \neq x$ für alle $x \in M$.

(iv) Die Gesamtheit aller Permutationen der Menge $\{1, 2, \ldots, n\}$ bezeichnet man mit S_n. Die Menge S_n bildet zusammen mit der Verknüpfung von Abbildungen $\circ : S_n \times S_n \to S_n$ eine Gruppe, die *symmetrische Gruppe*.

Die Antwort auf die oben gestellte Frage gibt nun der folgende Satz:

Satz 5.1.17. *Die Anzahl der fixpunktfreien Permutationen in S_n ist*

$$D_n \;:=\; n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad .$$

Die Zahlen D_n heißen Rencontre-Zahlen *(nach dem "Problème des Rencontres" von Montmort) oder* Derangement-Zahlen.

Beweis. Für $k = 1, \ldots, n$ bezeichne P_k die Menge aller Permutationen aus S_n mit Fixpunkt k. Mit Korollar 5.1.15 in der komplementären Form erhält man

$$\begin{aligned} D_n &= |S_n \setminus (P_1 \cup \ldots \cup P_n)| \\ &= n! + \sum_{k=1}^{n} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} |P_{i_1} \cap \cdots \cap P_{i_k}| \quad . \end{aligned}$$

Da $P_{i_1} \cap \cdots \cap P_{i_k}$ die Menge aller Permutationen ist, die die k Elemente $i_1, \ldots, i_k$ als Fixpunkte haben, gibt es eine Bijektion zwischen $P_{i_1} \cap \cdots \cap P_{i_k}$ und der Menge der Permutationen von $n-k$ Elementen S_{n-k}. Folglich ist $|P_{i_1} \cap \cdots \cap P_{i_k}| = (n-k)!$, so dass

$$\begin{aligned} D_n &= n! + \sum_{k=1}^{n} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} (n-k)! \\ &= n! + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= n! + n! \cdot \sum_{k=1}^{n} (-1)^k \frac{1}{k!} \\ &= n! \cdot \sum_{k=0}^{n} (-1)^k \frac{1}{k!} \quad . \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Eine andere Einkleidung des Problems ist folgende: Wenn jemand n Briefe und die zugehörigen Umschläge schreibt und dann die Briefe willkürlich in die Umschläge steckt, wie groß ist die Wahrscheinlichkeit (berechnet als Bruchteil von 1 aus dem Verhältnis der Anzahl der hier zu betrachtenden Möglichkeiten zur Anzahl aller Möglichkeiten), dass keiner der Adressaten den ihm zugedachten Brief erhält? Diese Wahrscheinlichkeit wird gegeben durch

$$p_n \;:=\; \frac{D_n}{n!} \;=\; \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$$

und da dies die mit dem n-ten Glied abgebrochene Reihe für e^{-1} ist, folgt

$$\left| p_n - \frac{1}{e} \right| \;<\; \frac{1}{(n+1)!} \;.$$

Die Wahrscheinlichkeit p_n konvergiert also für $n \to \infty$ gegen $1/e$ und zwar sehr rasch. Der Anteil der fixpunktfreien unter allen Permutationen einer n-elementigen Menge ist also von n beinahe unabhängig und $\frac{n!}{e}$ ist eine gute Näherung für D_n.

5.1.5 Partitionen und Stirlingzahlen zweiter Art

Eine Anzahl, die ebenfalls als Bestandteil vieler komplexerer Abzählprobleme auftritt, ist die Anzahl der Möglichkeiten, eine gegebene Menge in eine vorgegebene Anzahl von Teilmengen zu zerlegen. Im Folgenden verallgemeinern wir den Begriff *Partition* aus Definition 1.2.15.

Definition 5.1.18. Es sei $k \in \mathbb{N}$ und M eine nicht-leere Menge. Eine *k-Partition* von M ist eine Partition, die aus genau k nicht-leeren Teilmengen von M besteht, das heißt

$$M \;=\; \bigcup_{i=1}^{k} M_i \;, \quad \text{mit} \quad M_i \neq \emptyset, \quad \text{und} \quad M_i \cap M_j \;=\; \emptyset \quad \text{für } i \neq j.$$

Wir bezeichnen mit $S(n,k)$ die Anzahl der verschiedenen k-Partitionen einer n-elementigen Menge. Ferner setzen wir $S(0,0) := 1$, $S(n,0) := 0$ für $n > 0$ und $S(0,k) := 0$ für $k > 0$. Diese Zahlen heißen *Stirlingzahlen zweiter Art*.

Da nach Satz 1.5.5 die Partitionen einer Menge M umkehrbar eindeutig den Äquivalenzrelationen auf dieser Menge entsprechen, erhalten wir das folgende Korollar.

Korollar 5.1.19. *Es sei M eine nicht-leere endliche Menge und $n = |M|$. Die Anzahl der Äquivalenzrelationen mit genau k Äquivalenzklassen auf M ist $S(n,k)$.*

Beispiel. Die k-Partitionen für $k = 1, 2, 3, 4$ einer 4-elementigen Menge $\{a, b, c, d\}$ werden (in naheliegender Notation) in Tabelle 5.1 gegeben. Daran kann man die in der letzten Zeile angegebenen Werte der Stirlingzahlen $S(4,k)$ für $k = 1, 2, 3, 4$ ablesen.

Satz 5.1.20 (Rekursionsformel für die Stirlingzahlen zweiter Art)**.** *Für $n, k \in \mathbb{N}$ gilt*

$$S(n,k) \;=\; S(n-1,k-1) + k \cdot S(n-1,k) \;.$$

$k=$	1	2	3	4
	$abcd$	$a\|bcd$	$a\|b\|cd$	$a\|b\|c\|d$
		$b\|acd$	$a\|c\|bd$	
		$c\|abd$	$a\|d\|bc$	
		$d\|abc$	$b\|c\|ad$	
		$ab\|cd$	$b\|d\|ac$	
		$ac\|bd$	$c\|d\|ab$	
		$ad\|bc$		
$S(4,k)=$	1	7	6	1

Tabelle 5.1: Alle k-Partitionen der Menge $\{a,b,c,d\}$ für $k=1,2,3,4$.

Beweis. Für $k=1$ oder $k>n$ verifiziert man leicht die Richtigkeit der Formel. Es sei also $|M|=n\geq 2$. Wir wählen wieder ein Element $a\in M$ fest und teilen (in Analogie zum Beweis von Satz 5.1.7) die k-Partitionen von M in zwei Typen ein:

- Die Teilmenge $\{a\}$ ist selbst eine Klasse. Dann bilden die übrigen Klassen eine $(k-1)$-Partition von $M\setminus\{a\}$. Folglich gehören genau $S(n-1,k-1)$ k-Partitionen zu diesem Typ.
- Das Element a gehört zu einer Klasse A mit $|A|\geq 2$. Diese k-Partitionen von M werden durch Wegnahme von a wieder auf k-Partitionen von $M\setminus\{a\}$ abgebildet. Genauer gesagt haben jeweils k dieser k-Partitionen von M dasselbe Bild, nämlich diejenigen, die man aus einer k-Partition von $M\setminus\{a\}$ erhält, indem man jeweils eine der k Klassen um das Element a erweitert. Daher gibt es $k\cdot S(n-1,k)$ k-Partitionen des zweiten Typs.

Damit ist der Beweis abgeschlossen. □

Diese Rekursionsformel erlaubt wie bei den Binomialkoeffizienten die sukzessive Berechnung der $S(n,k)$ aus ihren in Definition 5.1.18 angegebenen Anfangswerten. In Tabelle 5.2 sind die Stirlingzahlen zweiter Art $S(n,k)$ für kleine Werte von n und k angegeben. Auch für die Stirlingzahlen gibt es viele Summenidentitäten, wofür wir hier ein Beispiel angeben.

Satz 5.1.21. *Für $n,k\in\mathbb{N}$ gilt*

$$S(n,k) \;=\; \sum_{i=0}^{n-1}\binom{n-1}{i}\cdot S(i,k-1)\;.$$

Beweis. Wir beweisen dies kombinatorisch, indem wir die k-Partitionen einer n-elementigen Menge M auf andere Weise abzählen. Es sei $a\in M$ fest gewählt. Für

$n\backslash k$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	0	1	1	0	0	0	0
3	0	1	3	1	0	0	0
4	0	1	7	6	1	0	0
5	0	1	15	25	10	1	0
6	0	1	31	90	65	15	1

Tabelle 5.2: Tabelle der Stirlingzahlen zweiter Art $S(n,k)$.

jedes $i \in \{0,\ldots,n-1\}$ gibt es $\binom{n-1}{n-1-i} = \binom{n-1}{i}$ Möglichkeiten, eine Teilmenge A von M mit $a \in A$ und $|A| = n-i$ zu wählen. Zu jeder dieser Teilmengen ist die Anzahl der $(k-1)$-Partitionen von $M \setminus A$ gleich $S(i,k-1)$. Hieraus folgt die Behauptung. □

5.1.6 Stirlingzahlen erster Art

Es gibt noch andere Stirlingzahlen, die man „von erster Art“ nennt. Vor der Definition erinnern wir an die symmetrische Gruppe S_n, die aus allen Permutationen σ der Menge $\{1,\ldots,n\}$ besteht.

Definition 5.1.22 (Zyklus)**.** Eine Permutation σ der Menge $\{a_1,\ldots,a_m\}$ heißt *Zyklus*, falls es zu jedem $j \in \{1,\ldots,m\}$ ein $k \in \mathbb{N}_0$ gibt, so dass $\sigma^k(a_1) = a_j$. (Hier bezeichnet σ^k die k-fache Hintereinanderausführung von σ.)

Beispiel. Die Permutation σ von $\{2,4,5,6,7\}$, die gegeben ist durch

i	2	4	5	6	7
$\sigma(i)$	5	7	4	2	6

ist ein Zyklus. Denn es gilt

$$2 = \sigma^0(2)\,, \quad 5 = \sigma^1(2)\,, \quad 4 = \sigma^2(2)\,, \quad 7 = \sigma^3(2) \quad \text{und} \quad 6 = \sigma^4(2)\,.$$

Man schreibt dann auch kurz $\sigma = (2,5,4,7,6)$ oder $\sigma = (5,4,7,6,2)$ oder $\sigma = (4,7,6,2,5)$ etc.

Lemma 5.1.23. *Jede Permutation $\sigma \in S_n$ kann als Produkt von Zyklen geschrieben werden.*

Wir erläutern diese Einsicht nur kurz an einem Beispiel. Daraus sollte auch klar werden, wie man das Lemma allgemein beweist.

Beispiel. Die Permutation $\sigma \in S_8$ sei gegeben durch

i	1	2	3	4	5	6	7	8
$\sigma(i)$	3	5	1	2	4	8	7	6

Offenbar ist $\sigma(1) = 3$ und $\sigma^2(1) = \sigma(3) = 1$. Die Permutation σ „enthält“ also den Zyklus $(1, 3)$. Auch 2 ist kein Fixpunkt und es gilt $\sigma(2) = 5$, $\sigma(5) = 4$ und $\sigma(4) = 2$. Das ergibt den Zyklus $(2, 5, 4)$. Weiter erhält man den Zyklus $(6, 8)$ und den trivialen Zyklus (7). Zusammenfassend gilt daher

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

Damit können wir jetzt die Stirlingzahlen erster Ordnung definieren.

Definition 5.1.24. Die Anzahl der Permutationen aus S_n, die aus k Zyklen bestehen, heißt *Stirlingzahl erster Art* und wird mit $s(n, k)$ bezeichnet.

Bemerkung.

(i) Weil die Anzahl aller Permutationen $n!$ ist, gilt

$$\sum_{k=1}^{n} s(n,k) \;=\; n! \;.$$

(ii) Es gibt keine Permutation mit $k = 0$ Zyklen und nur eine Permutation in S_n mit $k = n$ Zyklen. In diesem Fall haben alle Zyklen die Länge 1, also gibt es n Fixpunkte und wir haben die identische Abbildung.

(iii) Zusätzlich definiert man noch $s(0, 0) := 1$. Es gilt also

$$s(n,k) \;=\; \begin{cases} 0 & \text{für } k = 0,\ n \in \mathbb{N}, \\ 1 & \text{für } k = n \in \mathbb{N}_0. \end{cases}$$

Satz 5.1.25 (Rekursion für die Stirlingzahlen erster Art)**.** *Für $n, k \in \mathbb{N}$ gilt*

$$s(n,k) \;=\; s(n-1,k-1) + (n-1) \cdot s(n-1,k) \;.$$

Beweis. Wir betrachten eine Permutation aus S_n mit k Zyklen und unterscheiden zwei Fälle. Erster Fall: Die Zahl n ist Fixpunkt. Dann bilden die restlichen $k - 1$ Zyklen eine Permutation von $\{1, \ldots, n-1\}$. Es gibt $s(n-1, k-1)$ solche Permutationen. Dies ist folglich auch die Anzahl der Permutationen aus S_n mit k Zyklen und Fixpunkt n.

Zweiter Fall: Die Zahl n ist kein Fixpunkt, also in einem Zyklus der Länge ≥ 2 enthalten. Entfernt man n aus diesem Zyklus, so erhält man eine Permutation aus S_{n-1} mit k Zyklen. Umgekehrt sei eine solche Permutation

$$(a_{1,1}, a_{1,2}, \ldots, a_{1,\ell_1})(a_{2,1}, a_{2,2}, \ldots, a_{2,\ell_2}) \ldots (a_{k,1}, a_{k,2}, \ldots, a_{k,\ell_k})$$

gegeben. Dann gilt zunächst einmal $\ell_1 + \ell_2 + \cdots + \ell_k = n-1$. Aus solchen Permutationen kann man durch Einfügen von n in einen der Zyklen jede Permutation aus S_n mit k Zyklen bekommen, bei der n nicht Fixpunkt ist.

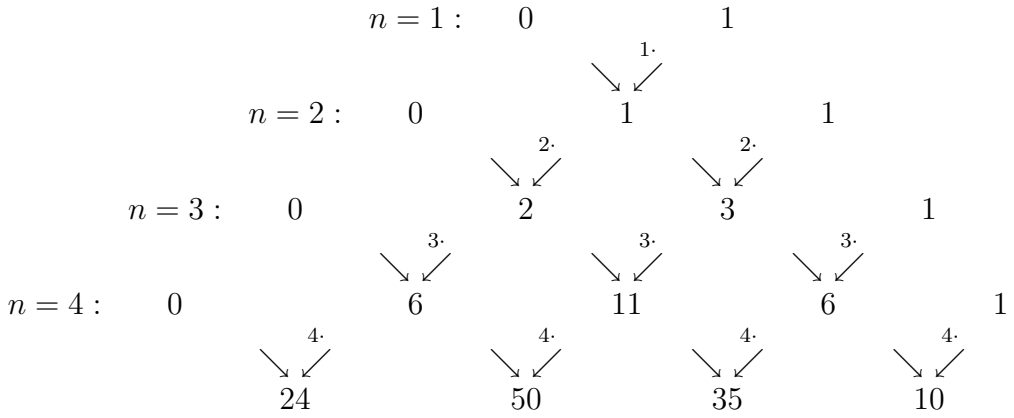
Im ersten Zyklus kann man n nach jedem $a_{1,j}$ einfügen, $j = 1, \ldots, \ell_1$. Jedesmal erhält man einen anderen $(\ell_1 + 1)$-Zyklus. (Einfügen vor a_{11} ist gleichwertig mit Einfügen nach a_{1,ℓ_1}, also kein neuer Zyklus). Allgemein bekommt man durch Einfügen von n im Zyklus der Länge ℓ genau ℓ verschiedene Zyklen der Länge $\ell+1$. Man kann n in jeden Zyklus einfügen. Daher ergeben sich genau

$$\ell_1 + \ell_2 + \cdots + \ell_k \;=\; n-1$$

verschiedene Möglichkeiten.

Dieses Verfahren ist anwendbar auf jede Permutation von S_{n-1} mit k Zyklen, also auf $s(n-1,k)$ Permutationen. Folglich gibt es $(n-1)\cdot s(n-1,k)$ Permutationen in S_n aus k Zyklen, die n nicht als Fixpunkt haben. Damit ist der Beweis abgeschlossen. □

Die Rekursion aus Satz 5.1.25 kann wie folgt veranschaulicht werden:



usw.

5.1.7 Zerlegungen einer natürlichen Zahl

Bis jetzt haben wir Zerlegungen von Mengen betrachtet. In diesem Abschnitt wenden wir uns den Zerlegungen einer natürlichen Zahl $N \in \mathbb{N}$ als Summe natürlicher Zahlen zu:

$$N \;=\; n_1 + n_2 + \cdots + n_k \;, \quad n_1, n_2, \ldots, n_k \in \mathbb{N}.$$

Diese Zerlegungen heißen *Zahlpartitionen* oder *arithmetische Partitionen*.

Definition 5.1.26. Es sei $1 \le k \le n$. Die Anzahl der Zerlegungen von n in genau k natürliche Summanden ohne Berücksichtigung der Reihenfolge wird mit $P(n,k)$ bezeichnet. Ferner sei $P(0,0) := 1$ und $P(n,k) := 0$ für $k = 0$ und $n > 0$ sowie für $k > n$. Die $P(n,k)$ heißen *(arithmetische) Partitionszahlen*.

Beispiele.

(i) Die möglichen Zerlegungen der Zahl 4 in zwei Summanden sind 3+1 und 2+2; also ist $P(4,2) = 2$.

(ii) Die Zerlegung der Zahl 7 in drei Summanden sind $5+1+1$, $4+2+1$, $3+3+1$ und $3+2+2$; also ist $P(7,3) = 4$.

Jede k-Partition einer n-elementigen Menge $M = M_1 \cup M_2 \cup \cdots \cup M_k$ bewirkt eine Zerlegung von n in k natürliche Summanden, nämlich $n = |M_1| + |M_2| + \cdots + |M_k|$, jedoch gehören zu einer solchen Summenzerlegung im allgemeinen mehrere k-Partitionen der Menge. Daher fallen die arithmetischen Partitionszahlen für großes n wesentlich kleiner aus als die mengentheoretischen Partitionszahlen $S(n,k)$.

Auch für diese Partitionszahlen gibt es eine einfache Rekursionsformel.

Satz 5.1.27 (Rekursionsformel für die arithmetischen Partitionszahlen)**.** *Für* $1 \leq k \leq n$ *gilt*

$$P(n,k) \;=\; P(n-1,k-1) + P(n-k,k) \;.$$

Beweis. Die Zerlegungen von n in genau k Summanden zerfallen in zwei Klassen, nämlich in solche, bei denen 1 als Summand auftritt und in solche, bei denen sämtliche Summanden größer als 1 sind. Lassen wir bei den Zerlegungen des ersten Typs einen Summanden 1 weg, so bleibt eine Zerlegung von $n-1$ in genau $k-1$ Summanden und dafür gibt es $P(n-1,k-1)$ Möglichkeiten. Bei den Zerlegungen des zweiten Typs können wir von jedem Summanden 1 abziehen und erhalten so eine Zerlegung von $n-k$ in genau k Summanden, wofür es $P(n-k,k)$ Möglichkeiten gibt. □

5.2 Rekursion und erzeugende Funktionen

Hat man ein von einem ganzzahligen Parameter n abhängendes Anzahlproblem, so erhält man für die Anzahlen eine Zahlenfolge $a_0, a_1, a_2, \ldots$ und diese Folge kann man (wie jede Zahlenfolge) als Koeffizientenfolge einer Potenzreihe

$$\sum_{n=0}^{\infty} a_n t^n$$

ansehen. Die Idee, auf diese Weise Potenzreihen bei der Lösung kombinatorischer Aufgaben einzusetzen, geht auf Laplace zurück. Falls außerdem die Potenzreihe eine Funktion darstellt, die man in geschlossener Form angeben kann, so hat man damit die Möglichkeit, die Information über die Zahlenfolge $a_0, a_1, a_2, \ldots$ in Form eines geschlossenen Funktionsausdrucks zu „speichern“. Nicht selten kann man auf dem Umweg über die Potenzreihen aus einer rekursiven Darstellung einer Folge eine explizite Darstellung gewinnen.

Im Folgenden werden wir zunächst formale Potenzreihen und erzeugende Funktionen definieren. Es werden einige Eigenschaften des Rings der formalen Potenzreihen besprochen. Dann wird als Beispiel die Rekursionsgleichung für die sogenannten Catalan'schen Zahlen gelöst. Im zweiten Teil dieses Abschnitts werden, ausgehend vom Beispiel der Fibonacci-Zahlen, allgemein lineare Rekursionsgleichungen besprochen und unter gewissen Voraussetzungen vollständig gelöst.

Im Folgenden bezeichne $\mathbb{K}$ immer den Körper der reellen oder komplexen Zahlen, also $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

5.2.1 Formale Potenzreihen und erzeugende Funktionen

Die in der Einleitung angesprochene Methode der Potenzreihen scheint zunächst einmal Analysiskenntnisse vorauszusetzen. Man kann jedoch Potenzreihen auch als rein algebraischen Begriff einführen, entsprechend der Einführung des Polynomringes $R[t]$ in Kapitel 2, Abschnitt 2.2.2. Allerdings können wir nicht einfach t als ein neu hinzukommendes Element mit „verträglichen" Recheneigenschaften ansehen, denn unendliche Summen sind nicht definiert. Ein Polynom

$$\sum_{k=0}^{n} a_k t^k$$

aus $\mathbb{K}[t]$ kann man als eine Abbildung $\varphi \in \mathbb{K}^{(\mathbb{N}_0)}$ auffassen (mit $\varphi(k) = a_k$ für $k = 0, \ldots, n$), also als eine Abbildung von $\mathbb{N}_0$ nach $\mathbb{K}$ mit $\varphi(k) = 0$ für fast alle $k \in \mathbb{N}_0$. Das heißt, dass nur für endlich viele k gilt $\varphi(k) \neq 0$. Lässt man diese Zusatzforderung an die Abbildung φ weg, so erhält man die Menge $\mathbb{K}^{\mathbb{N}_0}$ aller Abbildungen von $\mathbb{N}_0$ nach $\mathbb{K}$, die entsprechend eineindeutig mit Potenzreihen identifiziert werden können. Wir wissen bereits aus Kapitel 3, Abschnitt 3.2.1, dass $\mathbb{K}^{\mathbb{N}_0}$ einen $\mathbb{K}$-Vektorraum bildet. Die folgende Definition besagt, dass man $\mathbb{K}^{\mathbb{N}_0}$ sogar als Ring auffassen kann.

Definition 5.2.1 (Ring der formalen Potenzreihen)**.** Die Menge $\mathbb{K}^{\mathbb{N}_0}$ aller Abbildungen $\varphi : \mathbb{N}_0 \to \mathbb{K}$ bildet mit den Verknüpfungen

$$\begin{aligned} (\lambda\varphi)(k) &:= \lambda \cdot \varphi(k) && \text{für } \lambda \in \mathbb{K},\ k \in \mathbb{N}_0, \\ (\varphi + \psi)(k) &:= \varphi(k) + \psi(k) && \text{für } \lambda \in \mathbb{K},\ k \in \mathbb{N}_0, \end{aligned}$$

einen $\mathbb{K}$-Vektorraum und mit der Multiplikation

$$(\varphi \cdot \psi)(k) := \sum_{i+j=k} \varphi(i) \cdot \psi(j)$$

einen Ring mit Einselement, den *Ring* $\mathbb{K}[[t]]$ *der formalen Potenzreihen* über dem Körper $\mathbb{K}$.

Die Überprüfung der Ringeigenschaften bereitet überhaupt keine Schwierigkeiten. Wir ersparen uns daher die Einzelheiten.

Bemerkung.

(i) Eine formale Potenzreihe, als Abbildung $\varphi : \mathbb{N}_0 \to \mathbb{K}$ durch $n \mapsto a_n$ definiert, ist nichts anderes als eine (unendliche) Zahlenfolge $a_0, a_1, a_2, \ldots$ und wird analog zu den Polynomen geschrieben als

$$\sum_{n=0}^{\infty} a_n t^n \ ,$$

unabhängig von jeder Konvergenzforderung. Das Symbol t ist dann ein Rechensymbol und die Schreibweise dadurch begründet, dass das formale Rechnen mit solchen Potenzreihen genau dem Rechnen mit Reihen entspricht. Die Multiplikation entspricht genau dem Cauchyprodukt von Reihen (siehe auch Satz 4.1.34):

$$\left(\sum_{n=0}^{\infty} a_n t^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n t^n\right) \ = \ \sum_{n=0}^{\infty} c_n t^n \quad \text{mit} \quad c_n \ = \ \sum_{i+j=n} a_i b_j \ .$$

Diese Koeffizienten ergeben sich beim formalen sukzessiven Ausmultiplizieren der beiden Reihen und dem anschließenden Neuordnen der Glieder nach Potenzen von t. Das bei Polynomen gewohnte Einsetzen von Körperelementen x an Stelle von t (der Einsetzungshomomorphismus, siehe Kapitel 2, Abschnitt 2.2.4) hat dann allerdings im Allgemeinen keinen Sinn, da das Einsetzen von Null verschiedener Elemente Konvergenzbetrachtungen erforderlich macht.

(ii) Der Polynomring $\mathbb{K}[t]$ ist ein Unterring von $\mathbb{K}[[t]]$.

Definition 5.2.2 (Erzeugende Funktion)**.** Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge aus $\mathbb{K}^{\mathbb{N}_0}$. Dann heißt die formale Potenzreihe

(i) $a(t) := \sum\limits_{n=0}^{\infty} a_n t^n$ die *(gewöhnliche) erzeugende Funktion* und

(ii) $A(t) := \sum\limits_{n=0}^{\infty} \frac{a_n}{n!} t^n$ die *exponentielle erzeugende Funktion*

der Zahlenfolge $(a_n)_{n\in\mathbb{N}_0}$.

Im Falle der Konvergenz können wir also $a(t)$ bzw. $A(t)$ als Funktion von $t \in \mathbb{K}$ auffassen und dann auch Sätze der Analysis zu Hilfe nehmen, z.B. das gliedweise Differenzieren (siehe Satz 4.3.7). Insbesondere wird die exponentielle erzeugende Funktion mit dem Hintergedanken definiert, auch bei einer schnell wachsenden Zahlenfolge (a_n) eine nicht nur für $t = 0$ konvergente Reihe zu erhalten.

Tatsächlich kann man aber etwa die Differentiation auch als rein algebraische Operation betrachten. Wir kommen darauf an Hand von Beispielen gleich noch zurück.

Beispiel. Es sei $a_n := 1$ für alle $n \in \mathbb{N}_0$. Dann ist die erzeugende Funktion die bekannte geometrische Reihe mit dem Konvergenzradius 1:

$$a(t) \;=\; \sum_{n=0}^{\infty} t^n \;=\; \frac{1}{1-t} \;.$$

Diese Gleichung ist aber auch rein algebraisch sinnvoll; sie kann so gelesen werden, dass $\sum_{n=0}^{\infty} t^n$ und $1-t$ im Ring $\mathbb{K}[[t]]$ invertierbare Elemente und zueinander invers sind. Die entsprechende Gleichung

$$\left(\sum_{n=0}^{\infty} t^n\right) \cdot (1-t) \;=\; 1$$

bestätigt man durch Ausmultiplizieren gemäß Definition 5.2.1 (Cauchyprodukt).

In Verallgemeinerung des Beispiels gilt:

Lemma 5.2.3 (Invertierbare Potenzreihen)**.** *Für die Menge $\mathbb{K}[[t]]^*$ der invertierbaren Potenzreihen (also der Einheiten im Ring aller Potenzreihen) gilt*

$$\mathbb{K}[[t]]^* \;=\; \left\{ \sum_{n=0}^{\infty} a_n t^n \in \mathbb{K}[[t]] \;\middle|\; a_0 \neq 0 \right\} \;.$$

Beweis. Zu „$\subseteq$“: Ist $\sum_{n=0}^{\infty} a_n t^n$ invertierbar, so existiert $\sum_{n=0}^{\infty} b_n t^n$ mit

$$\left(\sum_{n=0}^{\infty} a_n t^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n t^n\right) \;=\; 1 \;.$$

Dann gilt nach Definition des Produktes in $\mathbb{K}[[t]]$, dass $a_0 b_0 = 1$ und daher $a_0 \neq 0$.

Zu „$\supseteq$“: Man setzt $b_0 := a_0^{-1}$ und definiert dann iterativ

$$b_n \;:=\; -\frac{1}{a_0} \cdot \sum_{k=1}^{n} a_k b_{n-k} \;.$$

Mit der dadurch definierten formalen Potenzreihe $\sum_{n=0}^{\infty} b_n t^n$ gilt dann

$$\left(\sum_{n=0}^{\infty} a_n t^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n t^n\right) \;=\; 1 \;.$$

Damit ist der Beweis abgeschlossen. □

Wir diskutieren einige weitere Beispiele erzeugender Funktionen.

Beispiele.

(i) Für die Folge $a_n := n!$ hat die gewöhnliche erzeugende Funktion $a(t) := \sum_{n=0}^{\infty} n! t^n$ keinen positiven Konvergenzradius (d.h. sie konvergiert für kein $t \neq 0$). Dagegen ist die exponentielle erzeugende Funktion

$$A(t) \;:=\; \sum_{n=0}^{\infty} \frac{n!}{n!} t^n \;=\; \sum_{n=0}^{\infty} t^n \;=\; \frac{1}{1-t} \;,$$

also wieder die geometrische Reihe. Dies demonstriert die Wirkung der Faktoren $\frac{1}{n!}$ in der exponentiellen erzeugenden Funktion als „Konvergenz erzeugende Faktoren“ und macht deutlich, dass die exponentielle erzeugende Funktion vor allem in Zusammenhang mit analytischen Betrachtungen von Interesse ist.

(ii) Die erzeugende Funktion von $a_n := n$ erhält man mittels gliedweiser Differentiation aus dem Beispiel oben:

$$\begin{aligned} a(t) \;:=\; \sum_{n=0}^{\infty} n t^n \;&=\; t \cdot \sum_{n=1}^{\infty} n t^{n-1} \;=\; t \cdot \left(\sum_{n=0}^{\infty} t^n \right)' \\ &=\; t \cdot \left(\frac{1}{1-t} \right)' \;=\; \frac{t}{(1-t)^2} \;. \end{aligned}$$

Diese Differentiation kann auch als rein algebraische Operation wie folgt definiert werden:

Definition 5.2.4 (Formale Derivation)**.** Die *formale Derivation* oder *formale Ableitung* wird definiert als Abbildung

$$\begin{array}{rcl} D : \mathbb{K}[[t]] & \longrightarrow & \mathbb{K}[[t]] \\ \sum\limits_{n=0}^{\infty} a_n t^n & \longmapsto & \sum\limits_{n=0}^{\infty} (n+1) a_{n+1} t^n \end{array} \;.$$

Bemerkung. Man rechnet leicht nach, dass die üblichen wohlbekannten Differentiationsregeln gelten, d.h. es gilt für alle $a(t), b(t) \in \mathbb{K}[[t]]$ und alle $\lambda, \mu \in \mathbb{K}$ insbesondere

$$\begin{array}{ll} D\big(\lambda \cdot a(t) + \mu \cdot b(t)\big) \;=\; \lambda \cdot D\big(a(t)\big) + \mu \cdot D\big(b(t)\big) & \text{(Linearität),} \\ D\big(a(t) \cdot b(t)\big) \;=\; b(t) \cdot D\big(a(t)\big) + a(t) \cdot D\big(b(t)\big) & \text{(Produktregel).} \end{array}$$

Die Gleichung $a(t) = t/(1-t)^2$ aus dem letzten Beispiel können wir in $\mathbb{K}[[t]]$ auch lesen als $a(t) \cdot (1-t)^2 = t$ und in dieser Form auch einfach durch Ausmultiplizieren von $\big(\sum_{n=0}^{\infty} n t^n\big) \cdot (1-t)^2$ bestätigen.

Beispiel. Es sei $m \in \mathbb{N}$ fest. Für $a_n := \binom{m}{n}$ (beachte, dass $a_n = 0$ für $n > m$) haben wir gemäß Satz 5.1.8 als erzeugende Funktion

$$a(t) \;:=\; \sum_{n=0}^{\infty} a_n t^n \;=\; \sum_{n=0}^{m} \binom{m}{n} t^n \;=\; (1+t)^m \;.$$

Hier besteht offenbar eine besonders enge Verwandtschaft zwischen der kombinatorischen Fragestellung, die die Zahlenfolge definiert, und der erzeugenden Funktion dieser Folge. Wir werden dies noch analysieren und für Verallgemeinerungen nutzen.

Zunächst wollen wir an einem Beispiel skizzieren, wie man die erzeugende Funktion einsetzen kann, um für eine kombinatorisch definierte Zahlenfolge zu einer expliziten Formel zu kommen.

Definition 5.2.5 (Catalan'sche Zahlen)**.** Die Anzahl c_n der Möglichkeiten, ein n-faches Produkt einer Menge $(M, \cdot)$ mit einer Verknüpfung, die weder kommutativ noch assoziativ zu sein braucht, durch Klammerung auf die Produktbildung von Paaren zurückzuführen (ohne diese Klammerung ist das n-fache Produkt für $n > 2$ in einer nichtassoziativen Struktur gar nicht erklärt), wird die *n-te Catalan'sche Zahl* genannt. Dabei ist $c_0 := 0$ und $c_1 := 1$.

Zur Illustration seien die Klammerungsmöglichkeiten für $2 \le n \le 4$ explizit aufgelistet:

$$\begin{array}{lll}
n = 2: & (x_1 x_2) & c_2 = 1 \\
n = 3: & ((x_1 x_2) x_3), (x_1 (x_2 x_3)) & c_3 = 2 \\
n = 4: & \begin{array}{l}(((x_1 x_2) x_3) x_4), ((x_1 x_2)(x_3 x_4)), ((x_1 (x_2 x_3)) x_4), \\ (x_1 ((x_2 x_3) x_4)), (x_1 (x_2 (x_3 x_4)))\end{array} & c_4 = 5
\end{array}$$

Eine andere Interpretation dieser Anzahl c_n ist die Anzahl verschiedener „binärer Wurzelbäume“ mit n Enden (Blättern). Abbildung 5.3 zeigt diese verschiedenen Wurzelbäume für $n = 4$ in der Reihenfolge, wie sie den eben aufgelisteten Klammerungen entsprechen.

Satz 5.2.6.

(i) Die Catalan'schen Zahlen c_n genügen der Rekursion

$$c_n \;=\; \sum_{k=0}^{n} c_k \cdot c_{n-k} \qquad \text{für } n \ge 2.$$

(ii) Ihre erzeugende Funktion genügt der Funktionalgleichung

$$c(t)^2 - c(t) + t \;=\; 0$$

und wird als reelle Funktion für $x \le 1/4$ gegeben durch

$$c(x) \;=\; \tfrac{1}{2}(1 - \sqrt{1-4x}) \;.$$

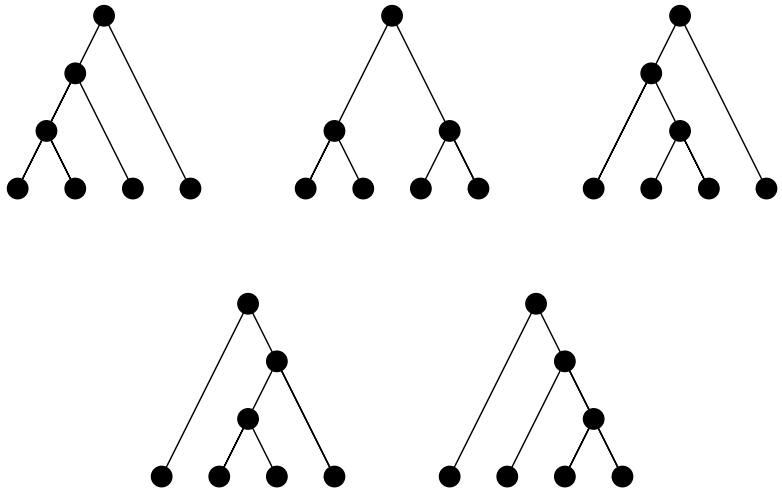


Abbildung 5.3: Die fünf binären Wurzelbäume mit 4 Blättern.

(iii) Für $n \geq 1$ werden die Catalan'schen Zahlen gegeben durch

$$c_n \;=\; \frac{1}{n}\binom{2n-2}{n-1} \;.$$

Beweis. Zu (i): Die äußerste Klammer eines n-fachen, mit Klammern versehenen Produktes verklammert ein k-faches Produkt mit einem $(n-k)$-fachen, wobei $k \in \{1, \ldots, n-1\}$ ist. Für diese Teilprodukte gibt es c_k bzw. c_{n-k} Möglichkeiten und damit für das gesamte Produkt $\sum_{k=1}^{n-1} c_k \cdot c_{n-k}$ Möglichkeiten. Wegen $c_0 = 0$ kann man das auch in der Form $\sum_{k=0}^{n} c_k \cdot c_{n-k}$ schreiben.

Zu (ii): Diese Rekursionsformel setzt man nun in die formale Potenzreihe ein, wozu man, da die Formel ja nur für $n \geq 2$ gilt, die ersten beiden Summanden abtrennt:

$$c(t) \;=\; \sum_{n=0}^{\infty} c_n t^n \;=\; c_0 + c_1 t + \sum_{n=2}^{\infty} c_n t^n \;=\; t + \sum_{n=2}^{\infty} \left(\sum_{k=0}^{n} c_k c_{n-k} \right) t^n \;.$$

Man erkennt, dass die rechts stehende Reihe gerade das Produkt der erzeugenden Funktion mit sich selbst ist, also gilt

$$c(t) \;=\; t + c(t)^2 \;.$$

Nun greift die reelle Analysis ein. Für solche $x \in \mathbb{R}$, für die $c(x)$ definiert ist (d.h., für die die Reihe konvergiert), hat man jetzt eine quadratische Gleichung für $c(x)$, deren Auflösung $c(x) = (1 - \sqrt{1-4x})/2$ liefert (da $c(0) = 0$).

Zu (iii): Man kann die Funktion $c(x) = (1 - \sqrt{1-4x})/2$ als Potenzreihe darstellen, deren Koeffizienten dann die angegebene explizite Gestalt der c_n liefert. Wir verzichten auf weitere Details des Beweises. □

Nicht immer erhält man die erzeugende Funktion so einfach wie hier. Das Verfahren, eine Rekursion (falls vorhanden) in die formale Potenzreihe einzusetzen, um damit eine Funktionalgleichung für die erzeugende Funktion zu gewinnen, lässt sich jedoch stets anwenden. Bei manchen kombinatorischen Problemen kann man jedoch die erzeugende Funktion direkt aus der Problemstellung heraus gewinnen. Wir greifen dazu das obige Beispiel der Binomialkoeffizienten noch einmal auf.

Beispiel. Nach Satz 5.1.10 oder Satz 5.1.7 ist $\binom{n}{k}$ die Anzahl der Möglichkeiten, k (verschiedene) Elemente aus einer n-elementigen Menge auszuwählen. Es seien $u_1, \ldots, u_n$ beliebige reelle Zahlen und t eine Unbestimmte. Dann ist

$$(1 + u_1 t) \cdot (1 + u_2 t) \cdot \ldots \cdot (1 + u_n t)$$

ein Polynom aus $\mathbb{R}[t]$ und Ausmultiplizieren führt zu

$$\begin{aligned} &1 + (u_1 + \cdots + u_n) \cdot t \\ &\quad + (u_1 u_2 + u_1 u_3 + \cdots + u_1 u_n + u_2 u_3 + \cdots + u_{n-1} u_n) \cdot t^2 \\ &\quad + \cdots + (u_1 u_2 \ldots u_n) \cdot t^n \ . \end{aligned}$$

Der Term t^k hat also als Koeffizienten die Summe aller Auswahlen (als Produkte geschrieben) von k verschiedenen Elementen aus der Zahlenmenge $\{u_1, u_2, \ldots, u_n\}$. Setzen wir alle u_k gleich 1, so gibt daher dieser Koeffizient die Anzahl der k-Auswahlen an, nämlich $\binom{n}{k}$.

Diese Idee wird in dem folgenden Satz verallgemeinert.

Satz 5.2.7 (Erzeugende Funktion für Auswahlen)**.** *Die erzeugende Funktion für die Anzahl derjenigen Auswahlen mit Wiederholung aus n verschiedenen Elementen, bei denen die Vielfachheit des k-ten Elementes (für $k \in \{1, \ldots, n\}$) aus einer gegebenen Zahlenmenge $N_k \subseteq \mathbb{N}_0$ stammt, wird gegeben durch*

$$\prod_{k=1}^{n} \left(\sum_{j \in N_k} t^j \right) \ .$$

Beweis. Es seien wieder $u_1, \ldots, u_n$ beliebige reelle Zahlen. Beim Ausmultiplizieren von

$$\left(\sum_{j \in N_1} {u_1}^j t^j \right) \cdot \left(\sum_{j \in N_2} {u_2}^j t^j \right) \cdot \ldots \cdot \left(\sum_{j \in N_n} {u_n}^j t^j \right)$$

erhält man eine Summe oder (falls wenigstens eine der Zahlenmengen N_j unendlich ist) eine Reihe, in welcher der Koeffizient von t^k die Summe all derjenigen k-Auswahlen mit Wiederholung (wie oben als Produkt geschrieben) von $u_1, \ldots, u_n$ ist, bei denen die Häufigkeit von u_j ($j \in \{1, \ldots, n\}$) durch eine Zahl aus der Menge N_j gegeben wird. Setzen wir wieder alle u_j gleich 1, so gibt der so entstehende Koeffizient von t^k gerade die Anzahl dieser k-Auswahlen an. □

Beispiel. Was ist die Anzahl der 4-Auswahlen von a, b, c, d, wenn die Häufigkeit des Auftretens von a genau 0 oder 3, von b 0, 1 oder 2, von c beliebig und von d kongruent 1 modulo 3 ist? Nach Satz 5.2.7 ist die erzeugende Funktion für die Anzahl solcher k-Auswahlen mit Wiederholung

$$\begin{aligned}&(1+t^3)\cdot(1+t+t^2)\cdot(1+t+t^2+t^3+\dots)\cdot(t+t^4+t^7+t^{10}+\dots)\\ &\quad = \ t+2t^2+3t^3+5t^4+\dots \ .\end{aligned}$$

Die Anzahl der Auswahlen der gesuchten Art ist also 5, was man hier auch leicht durch explizite Angabe dieser Auswahlen überprüfen kann. In geschlossener Form schreibt sich diese erzeugende Funktion übrigens als

$$\frac{t+t^4}{1-2t+t^2} \ .$$

Korollar 5.2.8. *Die erzeugende Funktion für die Anzahl a_k aller k-Auswahlen mit Wiederholung aus einer Menge mit n Elementen ist*

$$\left(\sum_{j=0}^{\infty} t^j\right)^n \ = \ \frac{1}{(1-t)^n} \ = \ \sum_{k=0}^{\infty} \binom{n+k-1}{k} t^k \ .$$

Beweis. Die Behauptung folgt mit Satz 5.1.10, wonach wir diese Anzahl ja schon kennen. Man kann diese Potenzreihenentwicklung für $(1-t)^{-n}$ aber auch direkt beweisen (zum Beispiel mit Induktion nach n unter Benutzung der Rekursionsformel für die Binomialkoeffizienten), was dann einen neuen Beweis für diese Anzahl liefert. □

Für weitere Beispiele dieser Art, bei denen man die erzeugende Funktion direkt aus der Fragestellung heraus konstruieren kann, sei auf die Literatur über Kombinatorik verwiesen.

5.2.2 Lineare Rekursionsgleichungen

Wir wollen die bei der Behandlung der Catalan'schen Zahlen aufgetretenen rekursiv definierten Zahlenfolgen aufgreifen und hierzu zunächst ein weiteres Beispiel einer besonders wichtigen Zahlenfolge, die Fibonacci-Zahlen betrachten. Wir haben diese Zahlenfolge bereits in Kapitel 2, Abschnitt 2.1.3 betrachtet, führen sie jetzt jedoch mittels einer kombinatorischen Definition ein.

Definition 5.2.9 (Fibonacci-Zahlen)**.** Die n-te *Fibonacci-Zahl* f_n ($n \geq 2$) ist die Anzahl aller 0/1-Sequenzen der Länge $n-2$, die keine benachbarten Einsen enthalten. Ferner setzen wir $f_0 := 0$ und $f_1 := 1$.

Bemerkung. Es ist also $f_2 = 1$ (die leere Sequenz), $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$ etc.

Satz 5.2.10 (Fibonacci-Zahlen)**.** *Für die Fibonacci-Zahlen gilt:*

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

(ii) Die erzeugende Funktion ist $f(t) = \dfrac{t}{1-t-t^2}$.

(iii) Eine explizite Darstellung ist $f_n = \left\lfloor \frac{1}{2} + \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \right\rfloor$.

Beweis. Zu (i): Es sei M_n die Menge aller 0/1-Sequenzen der Länge $n-2$, die der angegebenen Bedingung genügen, und davon $M_n^{(\varepsilon)}$ die Menge derjenigen, die an der letzten Stelle die Ziffer ε haben, für $\varepsilon \in \{0,1\}$. Es ist demnach

$$M_n \;=\; M_n^{(0)} \dot\cup M_n^{(1)} \quad \text{und somit} \quad f_n \;=\; |M_n| \;=\; |M_n^{(0)}| + |M_n^{(1)}| \;.$$

Nun ist $|M_n^{(0)}| = |M_{n-1}|$, da Anhängen einer 0 an eine Sequenz der Länge $n-3$ eine bijektive Abbildung $M_{n-1} \to M_n^{(0)}$ liefert. Ist die letzte Stelle einer Sequenz der Länge $n-2$ mit einer 1 besetzt, so ist der Vorgänger notwendigerweise eine 0 und das liefert $|M_n^{(1)}| = |M_{n-1}^{(0)}| = |M_{n-2}|$. Aus beidem folgt die Behauptung.

Zu (ii): Es sei $f(t) = \sum_{n=0}^{\infty} f_n t^n$ die erzeugende Funktion der Fibonacci-Zahlen. Wie bei den Catalan'schen Zahlen erhalten wir durch Umformen und Einsetzen der Rekursion eine Funktionalgleichung für $f(t)$, die hier linear ist und damit durch Auflösung ohne weiteres die geschlossene Form von $f(t)$ liefert:

$$\begin{aligned} f(t) \;&=\; \sum_{n=0}^{\infty} f_n t^n \;=\; t + \sum_{n=2}^{\infty} f_{n-1} t^n + \sum_{n=2}^{\infty} f_{n-2} t^n \\ &=\; t + t \cdot f(t) + t^2 \cdot f(t) \;. \end{aligned}$$

Damit erhält man

$$f(t) \;=\; \frac{t}{1-t-t^2} \;.$$

Zu (iii): Die Nullstellen des Nenners sind $(-1 \pm \sqrt{5})/2$ und damit erhalten wir durch Partialbruchzerlegung

$$f(t) \;=\; \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \frac{1+\sqrt{5}}{2} t} - \frac{1}{1 - \frac{1-\sqrt{5}}{2} t} \right) \;.$$

Nun ist $\frac{1}{1-at} = \sum_{n=0}^{\infty} a^n t^n$ und dies können wir auf beide Brüche in der Klammer anwenden. Damit folgt

$$f_n \;=\; \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) \;.$$

Da außerdem $\left| \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \right| < \frac{1}{2}$ für alle $n \in \mathbb{N}$ und f_n eine ganze Zahl ist, folgt die Behauptung. □

Dass die Auswertung der Rekursion hier bei den Fibonaccizahlen so problemlos funktioniert, liegt an der besonders einfachen Bauart dieser Rekursion: Sie ist linear und homogen und hat konstante Koeffizienten (Näheres siehe folgende Definition). Für solche Fälle besprechen wir gleich noch ein vereinfachtes Auswertungsverfahren. Zur Demonstration der Zugkraft obiger Methode wollen wir sie jedoch noch auf ein einfaches inhomogenes Beispiel anwenden.

Beispiel. Die Folge (a_n) sei rekursiv definiert durch $a_n = 2a_{n-1} + 1$ mit dem Startwert $a_0 = 0$. Durch Einsetzen dieser Rekursion in die erzeugende Funktion erhalten wir

$$\begin{aligned} a(t) &= \sum_{n=0}^{\infty} a_n t^n = \sum_{n=1}^{\infty} (2a_{n-1} + 1)t^n = t \cdot \sum_{n=0}^{\infty} (2a_n + 1)t^n \\ &= 2t \cdot a(t) + \frac{t}{1-t} \ . \end{aligned}$$

Daher gilt

$$\begin{aligned} a(t) &= \frac{t}{(1-t)(1-2t)} = -\frac{1}{1-t} + \frac{1}{1-2t} \\ &= -\sum_{n=0}^{\infty} t^n + \sum_{n=0}^{\infty} 2^n t^n = \sum_{n=0}^{\infty} (2^n - 1)t^n \ . \end{aligned}$$

Also ist $a_n = 2^n - 1$.

Definition 5.2.11 (Lineare Rekursion)**.** Eine *lineare Rekursion* r-ten Grades mit konstanten Koeffizienten ist eine Gleichung

$$(R) \qquad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r} + c_0 \qquad \text{für } n \geq r,$$

mit $c_0, \ldots, c_r \in \mathbb{K}$ und $c_r \neq 0$. Im Fall $c_0 = 0$ heißt sie homogen, sonst inhomogen. Ersetzen wir c_0 durch 0, so nennen wir das die zugehörige *homogene Rekursion* und bezeichnen sie mit (R_0). Das Polynom

$$\chi(t) := t^r - c_1 t^{r-1} - \cdots - c_r$$

heißt *charakteristisches Polynom* der Rekursion.

Bemerkung. Zunächst haben wir hier absichtlich keine Startwerte vorgegeben. Demgemäß ist die Lösung nicht eindeutig und (R_0) hat jedenfalls $a_n = 0$ für alle $n \in \mathbb{N}_0$ als Lösung. Neben dem charakteristischen Polynom betrachten wir noch

$$\psi(t) := 1 - c_1 t - \cdots - c_r t^r \ .$$

Dieses Polynom erhält man formal aus $\chi(t)$ in der Form $\psi(t) = t^r \chi(1/t)$.

Satz 5.2.12 (Lösung homogener linearer Rekursionen)**.** *Die Lösungsmenge der homogenen Rekursion, aufgefasst als Menge formaler Potenzreihen,*

$$L(R_0) \;:=\; \left\{ \sum_{n=0}^{\infty} a_n t^n \;\mid\; (a_n)_{n\in\mathbb{N}_0} \text{ genügt } (R_0) \right\}$$

ist ein r-dimensionaler Unterraum von $\mathbb{K}[[t]]$. Es gilt

$$L(R_0) \;=\; \psi(t)^{-1} \cdot \mathbb{K}[t]_r \;\;,$$

wobei $\mathbb{K}[t]_r$ die Menge aller Polynome aus $\mathbb{K}[t]$ vom Grade kleiner gleich $r-1$ einschließlich dem Nullpolynom bezeichnet.

Beweis. Wegen $c_r \neq 0$ ist $\psi(t) \in \mathbb{K}[[t]]^*$, das heißt $\psi(t)^{-1}$ existiert. Es sei nun $\sum_{k=0}^{\infty} b_k t^k \in \psi(t) \cdot \mathbb{K}[[t]]$, also

$$\sum_{k=0}^{\infty} b_k t^k \;=\; (1 - c_1 t - \cdots - c_r t^r) \cdot \sum_{n=0}^{\infty} a_n t^n \;\;,$$

wobei $a(t) \in \mathbb{K}[[t]]$ beliebig ist. Dann ist $\sum_{n=0}^{\infty} a_n t^n \in L(R_0)$ äquivalent zu

$$b_k \;=\; a_k - c_1 a_{k-1} - \cdots - c_r a_{k-r} \;=\; 0 \qquad \text{für } k \geq r$$

und das ist die Behauptung. □

Bemerkung. Man sieht nun auch, wie man zu gegebenen Startbedingungen $a_0, \ldots, a_{r-1}$ sofort die erzeugende Funktion in geschlossener Darstellung bekommt. Sie wird gegeben durch

$$a(t) \;=\; \frac{b_0 + b_1 t + \cdots + b_{r-1} t^{r-1}}{1 - c_1 t - \cdots - c_r t^r}$$

mit

$$\begin{aligned} b_0 &= a_0 \\ b_1 &= a_1 - c_1 a_0 \\ &\vdots \\ b_{r-1} &= a_{r-1} - c_1 a_{r-2} - \cdots - c_{r-1} a_0 \;\;. \end{aligned}$$

Aus dieser geschlossenen Form die explizite Darstellung der a_n zu gewinnen, erfordert dann Partialbruchzerlegung. Im Falle der Fibonacci-Zahlen hatten wir insofern Glück, als der Nenner $\psi(t) = 1 - t - t^2$ zwei verschiedene (und sogar reelle) Nullstellen hatte. Dies ist der einfachste Fall.

Satz 5.2.13 (Lösung inhomogener linearer Rekursionen)**.**

(i) $a_n = q^n$ *ist eine Lösung von* (R_0) *genau dann, wenn* $\chi(q) = 0$.

(ii) Hat $\chi(t)$ r *paarweise verschiedene, reelle Nullstellen* $q_1, \ldots, q_r$, *so ist*

$$a_n \;=\; \lambda_1 q_1^n + \cdots + \lambda_r q_r^n \qquad \textit{mit } \lambda_1, \ldots, \lambda_r \in K$$

die allgemeine Lösung von (R_0).

Bemerkung. Man kann bei Satz 5.2.13 (ii) natürlich auch mit komplexen Nullstellen von $\chi(t)$ arbeiten, bekommt damit aber auch komplexe Werte für die a_n.

Beweisskizze. Zu (i): Diese Äquivalenz ergibt sich unmittelbar durch Einsetzen.

Zu (ii): Nach (i) sind dies jedenfalls Lösungen, da die Linearkombination von Lösungen ja wieder eine Lösung ist. In Frage steht also nur, ob man auf diese Weise alle Lösungen bekommt. Dazu ist nur zu zeigen (wenn wir wieder zur Potenzreihenschreibweise übergehen), dass die Potenzreihen

$$\sum_{n=0}^{\infty} {q_i}^n t^n \qquad \text{mit } i \in \{1, \ldots, r\}$$

den ganzen Raum $L(R_0)$ aufspannen. Da wir schon wissen (vgl. Satz 5.2.12), dass dieser Raum $L(R_0)$ die Dimension r hat, genügt hierfür die lineare Unabhängigkeit der Vektoren

$$\begin{pmatrix} 1 \\ q_i \\ q_i^2 \\ \vdots \\ q_i^{r-1} \end{pmatrix} \qquad \text{für } i \in \{1, \ldots, r\}.$$

Wir gehen nicht auf weitere Details ein. □

Bemerkung.

(i) Bei einem Rekursionsproblem mit vorgegebenen Startwerten nimmt man die Anpassung der allgemeinen Lösung durch geeignete Wahl der Parameter $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$. Bei der Fibonacci-Rekursion etwa haben wir

$$q_1 \;=\; -\frac{1+\sqrt{5}}{2} \qquad \text{und} \qquad q_2 \;=\; \frac{-1+\sqrt{5}}{2}$$

als allgemeine Lösung, also $a_n = \lambda_1 {q_1}^n + \lambda_2 {q_2}^n$. Um die Startwerte $a_0 = 0$ und $a_1 = 1$ zu realisieren, wählt man

$$\lambda_1 \;=\; \frac{1}{\sqrt{5}} \qquad \text{und} \qquad \lambda_2 \;=\; -\frac{1}{\sqrt{5}} \;.$$

(ii) Wir erwähnen noch ohne Beweis, dass man beim Auftreten einer k-fachen Nullstelle q_j von $\chi(t)$ neben q_j^n auch noch $nq_j{}^n, \ldots, n^{k-1}q_j{}^n$ als Lösungen der homogenen Rekursion hat. Die allgemeine Lösung ist dann also Linearkombination von solchen Termen.

Bei inhomogenen Rekursionen wird die Sache schwieriger. Ähnlich zum Fall linearer Gleichungssysteme gilt der folgende Satz.

Satz 5.2.14 (Lösung inhomogener linearer Rekursionen)**.** *Der Lösungsraum $L(R)$ (als Unterraum von $\mathbb{K}[[t]]$) einer inhomogenen Rekursion ist ein Translat des Lösungsraumes $L(R_0)$ der zugehörigen homogenen Rekursion. Das heißt, gilt $\sum_{n=0}^{\infty} a_n t^n \in L(R)$, so ist*

$$L(R) \;=\; \sum_{n=0}^{\infty} a_n t^n + L(R_0) \;\; .$$

Dies verifiziert man wie bei linearen Gleichungssystemen.

$L(R_0)$ kann man nach den vorgenannten Methoden allgemein bestimmen und das Problem der Bestimmung von $L(R)$ reduziert sich damit auf die Aufgabe, irgendeine Lösung zu finden. Dafür gibt es keine in jedem Fall zugkräftige Methode, man verwendet spezielle Lösungsansätze in Abhängigkeit vom Aussehen des Störgliedes c_0. Ein häufiger Fall ist etwa der, dass c_0 ein Polynom in n ist (was insbesondere den Fall einschließt, dass c_0 eine Konstante ist). Ein hierfür bewährter Lösungsansatz ist, für a_n ebenfalls ein Polynom vom gleichen Grade mit zunächst unbestimmten Koeffizienten anzusetzen und dann die Koeffizienten durch Einsetzen zu bestimmen. Statt allgemeiner Formulierung rechnen wir nur ein Beispiel.

Beispiel. Es sei $a_n = 2a_{n-1} + n^2 - 2n + 2$ und wir suchen die Lösung zum Startwert $a_0 = 1$. Die homogene Rekursion $a_n = 2a_{n-1}$ hat die allgemeine Lösung $a_n = \lambda 2^n$ und zur Bestimmung einer Lösung der inhomogenen Rekursion machen wir den Ansatz $a_n = xn^2 + yn + z$. Dies in die Rekursion eingesetzt führt zur Gleichung

$$xn^2 + yn + z \;=\; 2\left(x(n-1)^2 + y(n-1) + z\right) + y(n-1) + z + n^2 - 2n + 2 \;\; .$$

Nach Potenzen in n ergibt das

$$(x+1)n^2 + (y - 4x - 2)n + (2x - 2y + z + 2) \;=\; 0 \;\; .$$

Dies kann nur dann für alle $n \in \mathbb{N}$ gelten, wenn die Koeffizienten der Potenzen von n einzeln verschwinden:

$$\left\{ \begin{array}{rcl} x + 1 & = & 0 \\ y - 4x - 2 & = & 0 \\ 2x - 2y + z + 2 & = & 0 \end{array} \right.$$

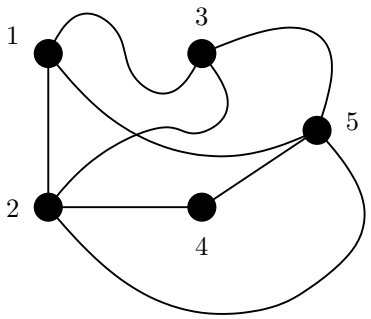


Abbildung 5.4: Ein Graph mit Knotenmenge $V = \{1, 2, 3, 4, 5\}$ und Kantenmenge $E = \{e_1, \ldots, e_8\}$, mit $e_1 = \{1, 2\}$, $e_2 = \{1, 3\}$, $e_3 = \{1, 5\}$, $e_4 = \{2, 3\}$, $e_5 = \{2, 4\}$, $e_6 = \{2, 5\}$, $e_7 = \{3, 5\}$ und $e_8 = \{4, 5\}$.

Dieses Gleichungssystem hat die eindeutige Lösung $x = -1$, $y = -2$ und $z = -4$. Somit ist $a_n = \lambda 2^n - n^2 - 2n - 4$ die allgemeine Lösung und die gewünschte Anfangsbedingung wird mit $\lambda = 5$ befriedigt.

5.3 Graphentheorie

Graphen spielen in sehr vielen Bereichen eine wichtige Rolle. Sie dienen unter anderem zur Modellierung von Netzen, wie etwa Computernetzen, Verkehrsnetze, Telekommunikationsnetze etc.

5.3.1 Grundlegende Begriffe der Graphentheorie

Definition 5.3.1 (Endliche Graphen)**.** Es sei V eine endliche Menge und $E \subseteq \big\{\{u, v\} \mid u, v \in V \text{ und } u \neq v\big\}$. Dann heißt das Tupel $G = (V, E)$ ein *(endlicher) Graph* mit *Knotenmenge* V und *Kantenmenge* E. Ist $e = \{u, v\} \in E$, so sagt man, dass die Kante e die beiden Knoten u und v *verbindet*; u und v heißen auch *Endknoten* von e. Die Knoten u und v heißen in diesem Fall *adjazent* und man sagt, dass die Kante $e = \{u, v\}$ *inzident* zu u und v ist.

Beispiel. Ein Beispiel eines Graphen ist in Abbildung 5.4 abgebildet.

Bemerkung. Ein Graph ist nach Definition also nichts anderes als eine endliche Menge V zusammen mit einer symmetrischen Relation auf V: Zwei Knoten aus V stehen in Relation zueinander, falls sie durch eine Kante verbunden sind.

Bemerkung. Man kann die Definition von Graphen in verschiedene Richtungen verallgemeinern, um unterschiedlichen Ansprüchen bei der Modellierung von Netzwerken gerecht zu werden.

(i) So kann man beispielsweise Kanten zulassen, die einen Knoten mit sich selbst verbinden (sogenannte *Schleifen*) oder man kann erlauben, dass mehrere Kanten dasselbe Knotenpaar verbinden (sogenannte *parallele* Kanten).

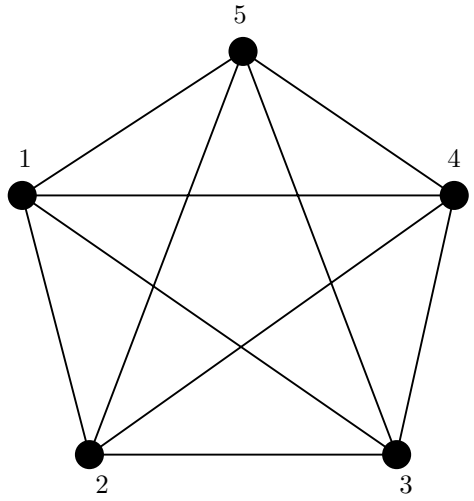


Abbildung 5.5: Der vollständige Graph auf fünf Knoten K_5.

(ii) Man kann an Stelle der ungerichteten Kanten auch gerichtete Kanten (oder *Bögen*) betrachten. In diesem Fall spricht man von *gerichteten Graphen* oder *Digraphen* $D = (V, A)$ mit Knotenmenge V und Bogenmenge $A \subseteq V \times V$. Eine Kante $a = (u, v) \in A$ ist dann von Knoten $u \in V$ nach Knoten $v \in V$ gerichtet.

Der Einfachheit halber beschränken wir uns hier auf den in Definition 5.3.1 beschriebenen Fall *einfacher* Graphen.

Die Anzahl der Kanten eines Graphen auf n Knoten ist offenbar durch $\binom{n}{2}$ nach oben beschränkt. Graphen, die diese obere Schranke erreichen, heißen vollständig.

Definition 5.3.2 (Vollständige Graphen)**.** Ein Graph $G = (V, E)$ heißt *vollständig*, falls jedes Knotenpaar durch eine Kante verbunden wird, das heißt, falls für die Anzahl der Kanten $|E| = \binom{|V|}{2}$ gilt. Den vollständigen Graphen auf n Knoten bezeichnet man mit K_n.

Beispiel. In Abbildung 5.5 ist der vollständige Graph mit fünf Knoten dargestellt.

Wir führen als nächstes den Begriff des Grads eines Knoten ein.

Definition 5.3.3 (Knotengrad)**.** Es sei $G = (V, E)$ ein Graph. Der *Grad* $d(u)$ eines Knotens $u \in V$ ist die Anzahl der zu diesem Knoten inzidenten Kanten, also

$$d(u) \ := \ |\{e \in E \mid u \in e\}| \ .$$

Beispiel. Wir betrachten noch mal den Graphen aus Abbildung 5.4. Der Knoten 1 hat Grad 3, Knoten 2 hat Grad 4, Knoten 3 hat Grad 3, Knoten 4 hat Grad 2 und Knoten 5 hat Grad 4. Im K_5 aus Abbildung 5.5 hat jeder Knoten Grad 4. Ganz allgemein hat im K_n jeder Knoten den Grad $n - 1$.

Satz 5.3.4. *Es sei $G = (V, E)$ ein Graph. Dann gilt*

$$\sum_{u \in V} d(u) \;=\; 2|E| \;\; .$$

Beweis. Man überzeugt sich leicht davon, dass jede Kante aus E in der Summe $\sum_{u \in V} d(u)$ genau zweimal gezählt wird, nämlich einmal für jeden der beiden Endknoten der Kante. □

Alternativ kann man Satz 5.3.4 auch mit Hilfe von Satz 5.1.2 (doppeltes Abzählen) beweisen.

Beispiel. Der Graph $G = (V, E)$ in Abbildung 5.4 besteht aus $|V| = 5$ Knoten und $|E| = 8$ Kanten. Wenn wir die Knotengrade addieren, erhalten wir

$$\sum_{i=1}^{5} d(i) = 3 + 4 + 3 + 2 + 4 = 16 = 2|E|.$$

Als nächstes beschäftigen wir uns mit Kantenfolgen und Wegen in Graphen.

Definition 5.3.5 (Kantenfolgen, Wege, Kreise)**.** Es sei $G = (V, E)$ ein Graph und $v_0, \ldots, v_n \in V$ mit $e_i := \{v_{i-1}, v_i\} \in E$ für $i = 1, \ldots, n$.

(i) Dann heißt $e_1, \ldots, e_n$ eine *Kantenfolge von v_0 zu v_n*. Ist $v_0 = v_n$, so heißt die Kantenfolge *geschlossen*.

(ii) Sind die Knoten $v_0, \ldots, v_n$ paarweise verschieden, so nennt man die Kantenfolge $e_1, \ldots, e_n$ auch *Weg* oder *Pfad* (von v_0 nach v_n).

(iii) Ist die Kantenfolge $e_1, \ldots, e_n$ geschlossen und sind die Knoten $v_1, \ldots, v_n$ paarweise verschieden, so handelt es sich um einen *Kreis*.

Beispiel. In dem in Abbildung 5.5 dargestellten K_5 ist

$$\{1,2\}, \{2,4\}, \{4,5\}, \{5,1\}, \{1,4\}, \{4,3\}$$

eine Kantenfolge von Knoten 1 zu Knoten 3. Diese Kantenfolge ist jedoch kein Weg, da Knoten mehrfach besucht werden. Die Kantenfolge

$$\{1,2\}, \{2,4\}, \{4,5\}, \{5,3\}$$

ist ein Weg von Knoten 1 zu Knoten 3. Hängt man noch die Kante $\{3,1\}$ an, so erhält man den Kreis

$$\{1,2\}, \{2,4\}, \{4,5\}, \{5,3\}, \{3,1\} \;\; .$$

Siehe dazu auch Abbildung 5.6.

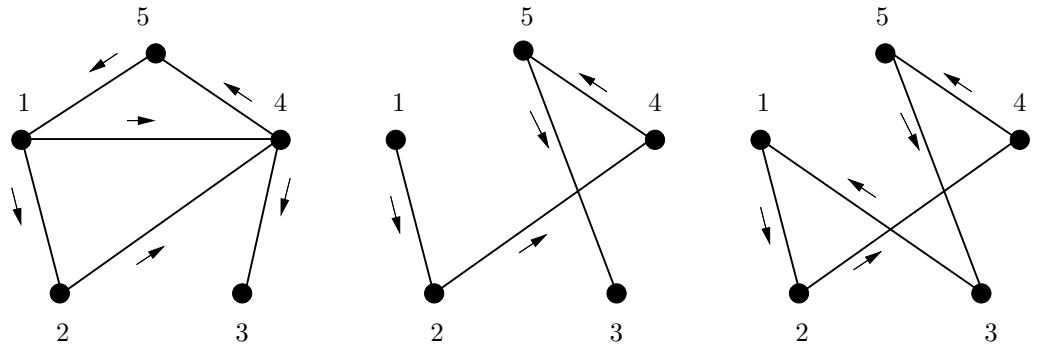


Abbildung 5.6: Eine Kantenfolge, ein Weg und ein Kreis im K_5.

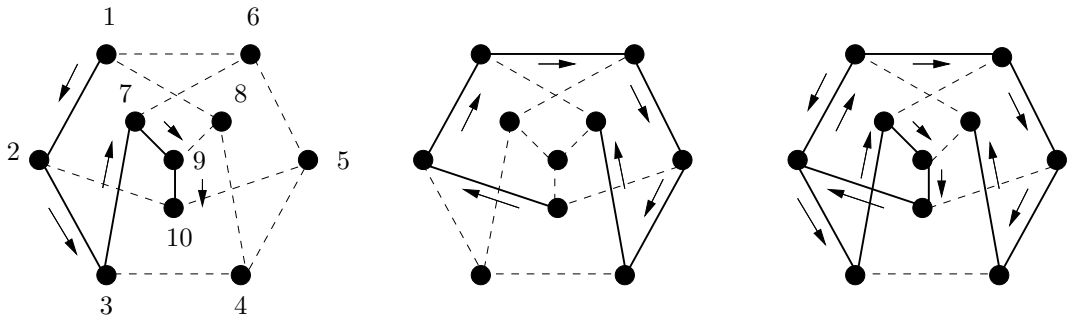


Abbildung 5.7: Eine Kantenfolge von 1 nach 10 und eine von 10 nach 8 liefert eine Kantenfolge von 1 nach 8.

Lemma 5.3.6. *Es sei $G = (V, E)$ ein Graph und $u, v, w \in V$. Ist $e_1, \ldots, e_n$ eine Kantenfolge von u nach v und $f_1, \ldots, f_m$ eine Kantenfolge von v nach w, so ist $e_1, \ldots, e_n, f_1, \ldots, f_m$ eine Kantenfolge von u nach w.*

Beweis. Folgt sofort aus Definition 5.3.5. □

Beispiel. In dem in Abbildung 5.7 dargestellten Graphen sind

$$\{1,2\},\{2,3\},\{3,7\},\{7,9\},\{9,10\},$$

und

$$\{10,2\},\{2,1\},\{1,6\},\{6,5\},\{5,4\},\{4,8\},$$

zwei Wege von 1 nach 10 bzw. von 10 nach 8, also insbesondere Kantenfolgen. Zusammen liefern Sie eine Kantenfolge von 1 nach 8, welche aber kein Weg mehr ist.

Satz 5.3.7. *Es sei $G = (V, E)$ ein Graph und $u, v \in V$ zwei Knoten. Gibt es eine Kantenfolge von u nach v, so gibt es auch einen Weg von u nach v.*

Beweis. Wir betrachten eine Kantenfolge von u nach w, die aus der minimalen Anzahl Kanten besteht. Diese kürzeste Kantenfolge sei

$$\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{n-1}, v_n\} \ ,$$

mit $v_0 = u$ und $v_n = w$. Diese Kantenfolge ist ein Weg von u nach w. Denn andernfalls gibt es $i, j \in \{0, 1, \ldots, n\}$ mit $i < j$ und $v_i = v_j$. Dann erhält man jedoch durch „Abkürzen“ eine kürzere Kantenfolge von u nach w, nämlich

$$\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{i-1}, v_i\}, \{v_j, v_{j+1}\}, \ldots, \{v_{n-1}, v_n\} \ .$$

Dies ist ein Widerspruch zur Wahl der ursprünglichen Kantenfolge. □

Definition 5.3.8 (Teilgraph)**.** Es sei $G = (V, E)$ ein Graph. Der Graph $G' = (V', E')$ heißt *Teilgraph* von G, falls $V' \subseteq V$ und $E' \subseteq E$ gilt. Der Teilgraph G' heißt *aufspannend*, falls $V' = V$ gilt.

Bemerkung. Man beachte, dass (V', E') nicht für jede mögliche Wahl von Teilmengen $V' \subseteq V$ und $E' \subseteq E$ einen Teilgraphen von $G = (V, E)$ darstellt. Damit (V', E') ein Graph ist, muss nämlich gelten, dass $e \subseteq V'$ für alle $e \in E'$.

Beispiele.

(i) Die Abbildung 5.8 zeigt drei Teilgraphen $G_1 = (V_1, E_1)$ mit

$$V_1 = \{1, 2, 3, 4, 5\}, \ E_1 = \{\{5, 1\}, \{5, 2\}, \{5, 3\}, \{5, 4\}\},$$

$G_2 = (V_2, E_2)$ mit

$$V_2 = \{1, 2, 4, 5\}, \ E_2 = \{\{5, 1\}, \{1, 4\}\}$$

und $G_3 = (V_3, E_3)$ mit

$$V_3 = \{1, 2, 3, 4, 5\}, \ E_3 = \emptyset$$

von K_5.

(ii) Die Abbildung 5.9 zeigt keinen Graphen, also insbesondere keinen Teilgraphen von K_5. Die untere mit Knoten 3 inzidente Kante $\{2, 3\}$ ist unzulässig, weil Knoten 2 nicht in der Knotenmenge des vermeintlichen Teilgraphen enthalten ist.

5.3.2 Zusammenhängende Graphen und Euler-Touren

Definition 5.3.9 (Zusammenhängende Graphen)**.** Ein Graph $G = (V, E)$ heißt *zusammenhängend*, falls es zu jedem Knotenpaar $u, v \in V$ einen Weg von u nach v gibt.

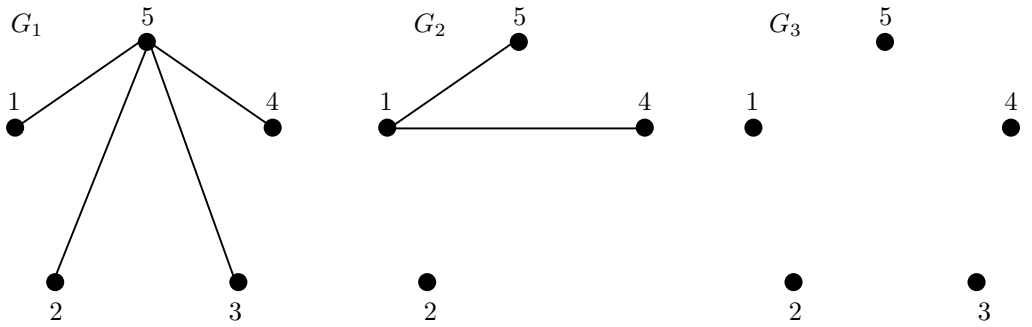


Abbildung 5.8: Drei Teilgraphen von K_5

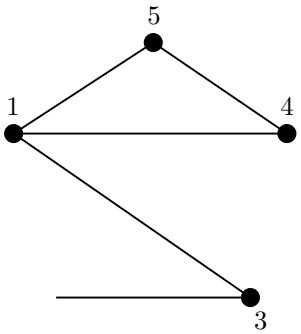


Abbildung 5.9: Kein Teilgraph von K_5, Knoten 2 fehlt.

Satz 5.3.10 (Zusammenhangskomponenten)**.** *Es sei $G = (V, E)$ ein Graph. Dann gibt es eine Partition der Knotenmenge V in Teilmengen $V_1, \ldots, V_k$ und eine Partition der Kantenmenge E in Teilmengen $E_1, \ldots, E_k$, so dass $G_i = (V_i, E_i)$ ein zusammenhängender Teilgraph von G ist, für $i = 1, \ldots, k$. Die Teilgraphen $G_1, \ldots, G_k$ sind bis auf ihre Reihenfolge eindeutig und heißen* Zusammenhangskomponenten *von G. Ist G zusammenhängend, so ist $k = 1$.*

Beispiel. Der Graph $G = (V, E)$ in Abbildung 5.10 besteht aus drei Zusammenhangskomponenten $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ und $G_3 = (V_3, E_3)$ mit $V_1 = \{5, 6, 7\}, V_2 = \{2, 3, 4\}, V_3 = \{1\}, E_1 = \{e_5, e_6, e_7\}, E_2 = \{e_2, e_3, e_4\}$ und $E_3 = \emptyset$.

Beweis von Satz 5.3.10. Wir betrachten die folgende Äquivalenzrelation auf der Knotenmenge V: Zwei Knoten u und v stehen in Relation zueinander, falls es einen Weg von u nach v gibt. Man überprüft leicht, dass es sich dabei tatsächlich um eine Äquivalenzrelation handelt.

Es seien $V_1, \ldots, V_k$ die Äquivalenzklassen dieser Äquivalenzrelation und $E_i := \{e \in E \mid e \subseteq V_i\}$ für $i = 1, \ldots, k$. Dann bilden $V_1, \ldots, V_k$ eine Partition von V und wir müssen noch zeigen, dass auch $E_1, \ldots, E_k$ eine Partition von E bilden. Da diese Kantenteilmengen nach Definition paarweise disjunkt sind, bleibt zu

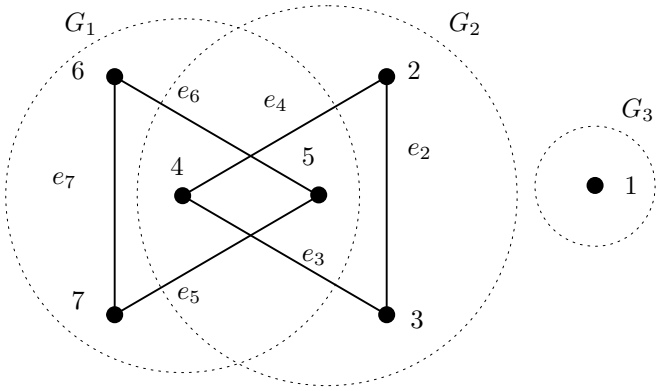


Abbildung 5.10: Ein Graph G mit drei Zusammenhangskomponenten G_1, G_2, G_3.

zeigen, dass ihre Vereinigung die gesamte Kantenmenge E ist. Wir nehmen an, dass es eine Kante $e = \{u, v\} \in E \setminus (E_1 \cup \cdots \cup E_k)$ gibt. Dann müssen die beiden Endknoten u und v in unterschiedlichen Knotenteilmengen liegen, also $u \in V_i$ und $v \in V_j$ mit $i \neq j$. Das führt aber zu einem Widerspruch, da zwei durch eine Kante verbundene Knoten nach Definition in Relation zueinander stehen und deshalb nicht unterschiedlichen Äquivalenzklassen angehören können.

Wir zeigen als nächstes, dass die so definierten Teilgraphen $G_i = (V_i, E_i)$ zusammenhängend sind, für $i = 1, \ldots, k$. Nach Definition gibt es zu jedem Knotenpaar $u, v \in V_i$ einen Weg von u nach v in G. Man sieht leicht, dass dieser Weg nur Knoten aus V_i besuchen kann und daher alle seine Kanten aus E_i sind. Folglich handelt es sich dabei auch um einen Weg von u nach v in G_i.

Die Eindeutigkeit der Teilgraphen $G_1, \ldots, G_k$ kann man wie folgt zeigen. Wir nehmen an, dass $G_i' = (V_i', E_i')$, $i = 1, \ldots, k'$, auch den Bedingungen des Satzes genügen. Da G_i' zusammenhängend ist, gibt es zwischen je zwei Knoten aus V_i' einen Weg in G_i' und damit auch in G. Folglich muss V_i' eine Teilmenge einer Äquivalenzklasse V_j sein. Um zu zeigen, dass $V_i' = V_j$ gilt, nehmen wir im Widerspruch dazu an, dass es ein $\ell \neq i$ gibt, so dass auch $V_\ell' \subset V_j$ gilt. Es sei $u \in V_i'$ und $v \in V_\ell'$. Da $u, v \in V_j$, gibt es einen Weg von u nach v in G. Dieser Weg muss offenbar eine Kante e enthalten, die aus V_i' hinausführt, das heißt, genau einer der beiden Endknoten von e ist in V_i'. Dann kann aber die Kante e nicht in E_i' und auch in keiner anderen Kantenteilmenge E_m', $m \neq i$, liegen. Dies ist ein Widerspruch.

Wir haben also gezeigt, dass $V_i' = V_j$ gelten muss. Genauso kann man jetzt zeigen, dass dann $E_i' = E_j$ gilt. Damit ist der Beweis abgeschlossen. □

Definition 5.3.11 (Euler'sche Graphen, Euler-Touren)**.** Ein zusammenhängender Graph $G = (V, E)$ heißt *Euler'sch*, falls es eine geschlossene Kantenfolge gibt, die jede Kante aus E genau einmal enthält. Eine solche geschlossene Kantenfolge heißt *Euler-Tour*.

Beispiel. Der Graph G aus Abbildung 5.11 ist Euler'sch. Eine Euler-Tour ist

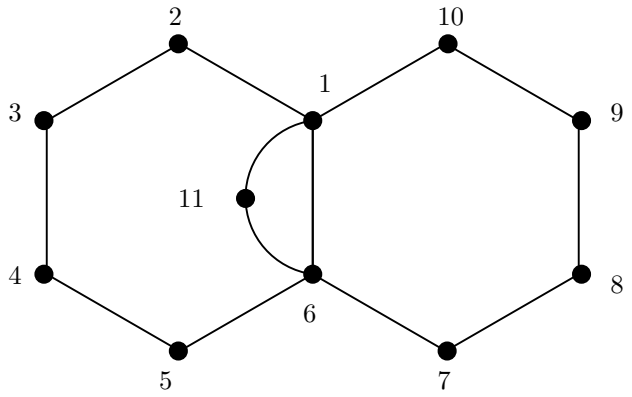


Abbildung 5.11: Ein Euler'scher Graph G.

z.B. durch die Kantenfolge

$$\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\},\{6,7\},\{7,8\},\{8,9\},\{9,10\},$$

$$\{10,1\},\{1,6\},\{6,11\},\{11,1\}$$

gegeben. Wenn wir aus G die Kante $\{6,12\}$ oder die Kante $\{11,12\}$ entfernen, ist G nicht mehr Euler'sch. Man kann zwar Kantenfolgen finden, die keine Kante zweimal enthalten, aber keine geschlossene Kantenfolge mit dieser Eigenschaft.

Satz 5.3.12 (Satz von Euler)**.** *Ein zusammenhängender Graph $G = (V, E)$ ist genau dann Euler'sch, wenn der Grad jedes Knotens aus V gerade ist.*

Beispiel. Der Graph G aus Abbildung 5.11 illustriert den obigen Satz. In G hat jeder Knoten geraden Grad. Der Knoten 1 hat Grad null, die Knoten 11 und 6 haben Grad vier und alle übrigen Knoten haben Grad zwei. Wenn wir aus G etwa die Kante $\{11,12\}$ entfernen, verringert sich der Grad von Knoten 11 um eins und G verliert die Euler-Eigenschaft.

Der folgende Beweis von Satz 5.3.12 liefert nicht nur die Existenz einer Euler-Tour in G, sondern gleichzeitig auch einen Algorithmus zur Berechnung einer Euler-Tour.

Beweis von Satz 5.3.12. Ist G Euler'sch, so muss der Grad jedes Knotens gerade sein, da die Eulertour bei jedem Besuch eines Knotens $v \in V$ genau zwei zu v inzidente Kanten verwendet.

Wir nehmen im Folgenden an, dass G zusammenhängend ist und der Grad jedes Knotens gerade ist. Ausgehend von einem beliebigen Knoten $v \in V$ konstruieren wir eine Kantenfolge, die keine Kante aus E mehr als einmal benutzt. Sind wir mit der Kantenfolge von v ausgehend an einem Knoten u angekommen, wählen wir, wenn möglich, eine zu u inzidente Kante, die noch nicht benutzt wurde. Gibt es keine solche Kante mehr, so muss $u = v$ sein. Denn andernfalls

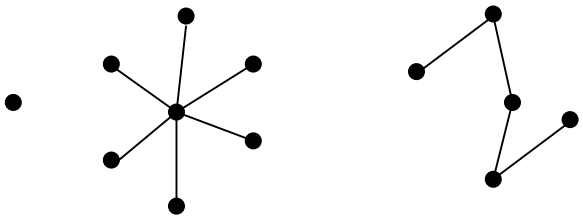


Abbildung 5.12: Ein Wald.

enthält unsere Kantenfolge bislang eine ungerade Zahl von Kanten, die zu u inzident sind. Da der Grad von u gerade ist, muss es also eine weitere Kante geben, die noch nicht benutzt wurde. Auf diese Weise erhalten wir also eine geschlossene Kantenfolge $e_1, \ldots, e_k$, in der keine Kante zweimal vorkommt. Sind das bereits alle Kanten aus E, so sind wir fertig.

Es sei also im Folgenden $e' \in E \setminus \{e_1, \ldots, e_k\}$. Wir zeigen zunächst, dass es einen Knoten $v \in (e_1 \cup \cdots \cup e_k)$ gibt und eine zu v inzidente Kante e, die nicht in der geschlossenen Kantenfolge enthalten ist. Ist einer der beiden Endknoten u von e' in $e_1 \cup \cdots \cup e_k$ enthalten, so können wir $v = u$ und $e = e'$ setzen. Andernfalls gibt es einen Weg von u zu einem Knoten $w \in (e_1 \cup \cdots \cup e_k)$. Dann sei v der erste Knoten aus $e_1 \cup \cdots \cup e_k$ auf diesem Weg und e die Kante des Weges, auf der v erreicht wird.

Löschen wir die Kanten der geschlossenen Kantenfolge $e_1, \ldots, e_k$ aus E, so besitzt der dadurch entstandene Teilgraph G' von G noch immer die Eigenschaft, dass alle Knoten in G' geraden Grad haben. Folglich können wir wie oben ausgehend von v eine geschlossene Kantenfolge in G' konstruieren und an geeigneter Stelle in die zuvor konstruierte geschlossene Kantenfolge $e_1, \ldots, e_k$ einsetzen, so dass eine längere geschlossene Kantenfolge entsteht.

Das beschriebene Vorgehen wiederholt man so lange, bis die geschlossene Kantenfolge alle Kanten von G enthält. Da sich die Länge der geschlossenen Kantenfolge bei jeder Iteration vergrößert, ist man nach endlich vielen Schritten am Ziel angelangt. □

5.3.3 Bäume und Wälder

Definition 5.3.13 (Bäume, Wälder)**.** Ein Graph $G = (V, E)$ heißt *Wald*, falls G keinen Kreis enthält. Ein zusammenhängender Wald heißt *Baum*.

Beispiele.

(i) Die Abbildung 5.12 zeigt einen unzusammenhängenden, kreisfreien Graphen, also einen Wald. Die Zusammenhangskomponenten sind natürlich ebenfalls kreisfrei und somit Bäume.

(ii) Die Abbildung 5.13 zeigt einen zusammenhängenden, kreisfreien Graphen, also einen Baum.

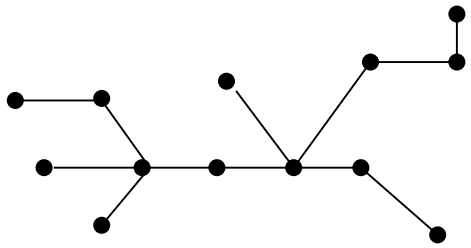


Abbildung 5.13: Ein Baum.

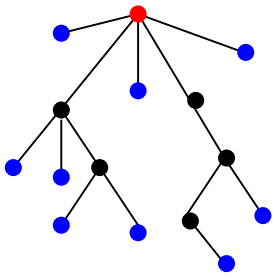


Abbildung 5.14: Klassische Darstellung eines Baumes.

(iii) Bäume werden klassisch wie in Abbildung 5.14 dargestellt und dann als *Wurzelbäume* bezeichnet. Ein Wurzelbaum ist ein Baum $T = (V, E)$ zusammen mit einem ausgezeichneten Knoten $w \in V$, welchen man als *Wurzel* bezeichnet. Dieser wird in Darstellungen dann meist als höchster Knoten eingezeichnet und ist in Abbildung 5.14 rot dargestellt. Alle Wege von der Wurzel zu einem anderen Knoten verlaufen die ganze Zeit abwärts. Die Knoten, die unterhalb eines bestimmten Knotens liegen und von diesem aus über eine Kante erreicht werden können, heißen *Nachfolger* dieses Knotens.

(iv) In Abbildung 5.15 haben alle Knoten des Wurzelbaumes höchstens zwei Nachfolger. Ein solcher Baum wird als *binärer Baum* oder als *binärer Wurzelbaum* bezeichnet.

Satz 5.3.14. *Jeder zusammenhängende Graph enthält einen Baum als aufspannenden Teilgraphen. So ein Teilgraph wird auch* spannender Baum *oder* aufspannender Baum *genannt.*

Beweis. Es sei $G = (V, E)$ ein zusammenhängender Graph. Ist G kreisfrei, so ist G selbst ein aufspannender Baum und wir sind fertig. Anderfalls sei $e_1, \ldots, e_k$ ein Kreis in G. Wir betrachten den aufspannenden Teilgraphen G' von G der durch Löschen der Kante e_k entsteht.

Wir behaupten, dass G' zusammenhängend ist. Es seien $u, v \in V$ beliebig. Dann gibt es einen Weg $f_1, \ldots, f_\ell$ von u nach v in G. Ist $f_i \neq e_k$ für $i = 1, \ldots, \ell$,

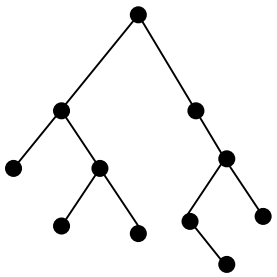


Abbildung 5.15: Ein binärer Wurzelaum.

so ist dies auch ein Weg in G'. Andernfalls sei $f_i = e_k$ für ein $i \in \{1, \ldots, \ell\}$. Dann ist

$$f_1, \ldots, f_{i-1}, e_1, \ldots, e_{k-1}, f_{i+1}, \ldots, f_\ell$$

oder

$$f_1, \ldots, f_{i-1}, e_{k-1}, \ldots, e_1, f_{i+1}, \ldots, f_\ell$$

eine Kantenfolge von u nach v in G'. Wegen Satz 5.3.7 gibt es dann auch einen Weg von u nach v in G'. Folglich ist G' zusammenhängend.

Durch das Löschen von e_k hat man den Kreis $e_1, \ldots, e_k$ zerstört. Ist G' kreisfrei, so sind wir fertig. Andernfalls wiederholt man das beschriebene Vorgehen so lange, bis alle Kreise zerstört sind. Da G nur endlich viele Kanten enthält, endet das Verfahren nach endlich vielen Schritten. □

Definition 5.3.15 (Blätter in Bäumen)**.** Ein Knoten eines Baumes mit Knotengrad 1 heißt *Blatt*.

Beispiel. In Abbildung 5.14 sind die Blätter des Wurzelbaumes blau eingefärbt.

Satz 5.3.16. *Es sei $G = (V, E)$ ein Baum mit mindestens zwei Knoten, das heißt $|V| \geq 2$. Dann besitzt G mindestens zwei Blätter.*

Beweis. Es sei $e_1, \ldots, e_k$ ein längster Weg in G. Dieser Weg führt von einem Knoten $u \in V$ zu einem anderen Knoten $v \in V$. Wir behaupten, dass u und v Blätter sind. Denn angenommen $d(u) \geq 2$, so gibt es außer e_1 eine weitere zu u inzidente Kante e_0. Der andere Endknoten von e kann kein Knoten des Weges $e_1, \ldots, e_k$ sein, da dadurch ein Kreis in G geschlossen würde. Folglich ist $e_0, e_1, \ldots, e_k$ ein Weg, der länger ist als $e_1, \ldots, e_k$. Dies ist ein Widerspruch. Für den Knoten v argumentiert man analog. □

Satz 5.3.17. *Ein Baum $G = (V, E)$ besitzt genau eine Kante weniger als Knoten, das heißt $|E| = |V| - 1$.*

Beweis. Wir beweisen die Behauptung durch vollständige Induktion über die Anzahl der Knoten $|V|$. Die Behauptung ist offenbar wahr für den eindeutigen Baum mit einem Knoten $(\{v\}, \emptyset)$. Es sei jetzt $G = (V, E)$ ein Baum mit $|V| \geq 2$. Wegen Satz 5.3.16 besitzt G ein Blatt $v \in V$ mit inzidenter Kante $e \in E$. Der Teilgraph G' von G, der durch Löschen von v und e entsteht ist offenbar zusammenhängend und kreisfrei, also ein Baum. Damit besitzt G' nach Induktionsvoraussetzung genau einen Knoten mehr als Kanten. Folglich gilt dieselbe Eigenschaft für G. □

Bemerkung. Die Satzaussage ist sehr intuitiv und lässt sich an Abbildung 5.14 gut veranschaulichen. Wir starten mit dem Wurzelknoten (rot markiert). Für jede Kante, die wir an die Wurzel anhängen möchten, müssen wir auch einen zusätzlichen Knoten, den Endknoten der jeweiligen Kante, zur Knotenmenge hinzufügen. Diese Knoten sind dann entweder Blätter (blau markiert) oder es werden weitere Kanten und ebensoviele Knoten angefügt. Dies geschieht solange, bis nur noch Blätter angefügt werden. Es müssen also zur Wurzel ebensoviele Knoten wie Kanten angefügt werden und es gibt stets einen Knoten mehr, als es Kanten gibt.

Korollar 5.3.18. *Ist $G = (V, E)$ ein zusammenhängender Graph, so gilt $|E| \geq |V| - 1$.*

Beweis. Die Behauptung folgt unmittelbar aus Satz 5.3.17 und Satz 5.3.14. □

Definition 5.3.19 (Zyklomatische Zahl)**.** Es sei $G = (V, E)$ ein Graph. Dann heißt

$$\nu(G) \ := \ |E| - |V| + 1$$

die *zyklomatische Zahl* von G.

Korollar 5.3.20. *Es sei $G = (V, E)$ ein zusammenhängender Graph. Dann gilt $\nu(G) \geq 0$. Ist $\nu(G) = 0$, so ist G ein Baum.*

Beweis. Folgt unmitelbar aus Korollar 5.3.18 und Satz 5.3.17. □

Korollar 5.3.21. *Ist $G = (V, E)$ ein Graph und $\nu(G) < 0$, so ist G nicht zusammenhängend.*

Kapitel 6

Algebra

Wir setzen in diesem Kapitel die in Kapitel 2, Abschnitt 2.2 begonnene Behandlung grundlegender algebraischer Strukturen fort. Wir knüpfen dabei nahtlos an den genannten Abschnitt an. Es empfiehlt sich daher, vor der Lektüre dieses Kapitels noch einmal die in Abschnitt 2.2 gelegten Grundlagen zu wiederholen.

6.1 Gruppentheorie

6.1.1 Untergruppen und erzeugte Untergruppen

Wir geben zunächst die folgende äquivalente Charakterisierung von Untergruppen an.

Lemma 6.1.1. *Es sei $(G, \circ)$ eine Gruppe. Eine nichtleere Teilmenge $H \subseteq G$ bildet genau dann eine Untergruppe von G, wenn für alle $x, y \in H$ gilt, dass $x \circ y^{-1} \in H$.*

Beweis. Die Notwendigkeit der gegebenen Bedingung folgt sofort aus der Tatsache, dass eine Untergruppe selbst wieder eine Gruppe ist (siehe Lemma 2.2.7). Um zu zeigen, dass die Bedingung auch hinreichend ist, müssen wir die drei Eigenschaften aus Definition 2.2.6 überprüfen.

Zu (i): Da H nicht leer ist, gibt es ein $x \in H$, so dass auch $e = x \circ x^{-1} \in H$. Zu (iii): Für $x \in H$ gilt $x^{-1} = e \circ x^{-1} \in H$. Zu (ii): Es seien $x, y \in H$. Nach dem eben gezeigten gilt $y^{-1} \in H$, so dass $x \circ y = x \circ (y^{-1})^{-1} \in H$. □

Bemerkung. Wir verwenden wie bei Zahlen die folgende Notation. Für ein Element $x \in G$ der Gruppe $(G, \circ)$ und eine natürliche Zahl $n \in \mathbb{N}$ sei x^n die n-fache Verknüpfung von x mit sich selbst. Weiter sei $x^0 := e$ und $x^{-n} := (x^{-1})^n = (x^n)^{-1}$. Dann gilt für $q, r \in \mathbb{Z}$, dass $x^q \circ x^r = x^{q+r}$.

Lemma 6.1.2. *Es sei $(G, \circ)$ eine Gruppe und $x \in G$. Dann ist $H := \{x^q \mid q \in \mathbb{Z}\}$ die kleinste Untergruppe von G, die x enthält. Wir schreiben auch $H = \langle x \rangle$ und nennen $\langle x \rangle$ die* von x erzeugte Untergruppe von G.

Beweis. Mit Hilfe von Lemma 6.1.1 zeigt man leicht, dass H eine Untergruppe von G ist. Offenbar enthält jede Untergruppe U von G mit $x \in U$ auch alle Elemente aus H. □

Bemerkung. Alternativ kann man Lemma 6.1.2 beweisen, indem man feststellt, dass $\langle x \rangle$ das Bild des durch $\varphi(q) := x^q$ definierten Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(G, \circ)$ ist. Nach Lemma 2.2.15 ist das Bild eines Gruppenhomomorphismus nach G eine Untergruppe von G.

Lemma 6.1.3. *Es sei $(G, \circ)$ eine endliche Gruppe mit neutralem Element e und $x \in G$. Dann gilt für $k := |\langle x \rangle|$, dass $x^k = e$ und*

$$\langle x \rangle \;=\; \{x^0, x^1, x^2, x^3, \ldots, x^{k-1}\} \;.$$

Man nennt $\langle x \rangle$ auch zyklische Untergruppe *von G oder* zyklische Gruppe.

Beweis. Da G endlich ist, gibt es $0 \leq i < j$ mit $x^i = x^j$. Durch Multiplikation dieser Gleichung mit x^{-i} erhält man $x^{j-i} = e$. Wir wählen jetzt $k' \in \mathbb{N}$ minimal mit $x^{k'} = e$. Insbesondere gilt dann $x^{-1} = x^{k'-1}$. Aus der obigen Betrachtung folgt für $0 \leq i < j < k'$, dass $x^i \neq x^j$. Es genügt also zu zeigen, dass

$$\langle x \rangle \;=\; \{x^0, x^1, x^2, x^3, \ldots, x^{k'-1}\} \;.$$

Dies folgt aus der Tatsache, dass $x^q = x^{(q \mod k')}$ für alle $q \in \mathbb{Z}$. □

In Verallgemeinerung der in Lemma 6.1.2 eingeführten Sprechweise definieren wir jetzt allgemeiner die von einigen Elementen aus G erzeugte Untergruppe von G.

Satz 6.1.4. *Es sei $(G, \circ)$ eine Gruppe und X eine nichtleere Teilmenge von G. Dann ist*

$$H \;:=\; \left\{ {x_1}^{q_1} \circ \cdots \circ {x_k}^{q_k} \mid k \in \mathbb{N},\, x_1, \ldots, x_k \in X \text{ und } q_1, \ldots, q_k \in \{1, -1\} \right\}$$

die kleinste Untergruppe von G, die X enthält. Wir schreiben auch $H = \langle X \rangle$ und nennen $\langle X \rangle$ die von X erzeugte Untergruppe von G.

Beweis. Man rechnet leicht nach, dass H eine Untergruppe von G ist. Es ist auch klar, dass jede Untergruppe von G, die X enthält, auch alle Elemente aus H enthalten muss. □

Beispiele. In den Übungen haben wir bereits eine *Diedergruppe*, die Symmetriegruppe des Quadrats $D_4 \subset S_4$, kennengelernt.

(i) Die von der Drehung $\sigma_1 = (1, 2, 3, 4)$ erzeugte zyklische Untergruppe $\langle \sigma_1 \rangle$ enthält auch alle anderen Drehungen aus D_4, das heißt

$$\langle (1, 2, 3, 4) \rangle \;=\; \{\mathrm{id}, (1, 2, 3, 4), (1, 3) \circ (2, 4), (1, 4, 3, 2)\} \;.$$

(ii) Die von der Spiegelung $\pi_1 = (2,4)$ erzeugte zyklische Untergruppe $\langle \pi_1 \rangle$ enthält hingegen nur die Identität und π_1.

(iii) Nehmen wir zu π_1 noch die Spiegelung $\pi_2 = (1,3)$ hinzu, so erhalten wir $\langle \pi_1, \pi_2 \rangle = \{\mathrm{id}, \pi_1, \pi_2, \sigma_2\}$, wobei $\sigma_2 = (1,3) \circ (2,4)$ die Drehung des Vierecks um den Winkel π ist.

(iv) Wenn wir aber zu π_1 die Drehung σ_1 hinzufügen, erhalten wir neben allen Drehungen auch alle Spiegelungen. Es gilt also $\langle \pi_1, \sigma_1 \rangle = D_4$.

Die Gruppe D_4 ist nicht die einzige Diedergruppe. Wir präzisieren dies im nächsten Abschnitt.

Untergruppen von Permutationsgruppen

Da wir uns bisher hauptsächlich mit der symmetrischen Gruppe S_n beschäftigt haben, diskutieren wir kurz noch einige konkrete Permutationsgruppen und wichtige Untergruppen von Permutationsgruppen.

(i) Die Gruppe $(S_2, \circ)$ enthält zwei Elemente und ist isomorph zu $(\mathbb{Z}_2, +)$.

(ii) Die Gruppe $(S_3, \circ)$ enthält sechs Elemente und kann als Diedergruppe D_3, der Gruppe der Spiegelungen und Drehungen eines gleichseitigen Dreiecks, interpretiert werden. Diese ist nicht abelsch und daher von $(\mathbb{Z}_6, +)$ verschieden.

(iii) Für $n \geq 3$ erklärt man die Diedergruppe D_n als Symmetriegruppe eines regelmäßigen n-Ecks. Nummeriert man dessen Eckpunkte fortlaufend mit $1, ..., n$, so wird D_n als Untergruppe non S_n von den Permutationen

$$\sigma = (1, ..., n) \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n-1 & \dots & 2 \end{pmatrix}$$

erzeugt. Hierbei entspricht σ einer Drehung des regelmäßigen n-Ecks um den Winkel $\frac{2\pi}{n}$ und τ einer Spiegelung an der Symmetrieachse durch den Punkt 1. Die Gruppe D_n enthält $2n$ Elemente.

Wir wollen nun noch die *alternierende Gruppe* A_n definieren. Dafür benötigen wir zunächst den Begriff des *Signums* einer Permutation.

Definition 6.1.5. Für eine Permutation $\pi \in S_n$ definiert man das *Signum* durch

$$\mathrm{sgn}(\pi) \;:=\; \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}.$$

Bemerkung. Das Signum kann die Werte 1 und -1 annehmen und gibt an, ob sich die Permutation π als Produkt einer geraden oder ungeraden Anzahl von Transpositionen schreiben lässt (eine Transposition ist ein Zykel der Länge zwei, also etwa (i,j)). Ist $\mathrm{sgn}(\pi) = 1$, so heißt π *gerade*, sonst *ungerade*.

Beispiel. Es sei $\pi = (1,2) \circ (3,4) \in S_4$. Dann ist

$$\begin{aligned}
\mathrm{sgn}(\pi) &= \tfrac{(\pi(1)-\pi(2))(\pi(1)-\pi(3))(\pi(1)-\pi(4))(\pi(2)-\pi(3))(\pi(2)-\pi(4))(\pi(3)-\pi(4))}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} \\
&= \frac{(2-1)(2-4)(2-3)(1-4)(1-3)(4-3)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} \\
&= (-1)\cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \;=\; 1 \;.
\end{aligned}$$

Lemma 6.1.6. *Die Abbildung* $\mathrm{sgn} : S_n \to \{-1,1\}$ *von der Gruppe* $(S_n, \circ)$ *in die multiplikative Gruppe* $(\{-1,1\}, \cdot\,)$ *ist ein Gruppenhomomorphismus.*

Beweis. Es seien $\pi, \pi' \in S_n$ beliebig. Dann gilt

$$\begin{aligned}
\mathrm{sgn}(\pi \circ \pi') &= \prod_{i<j} \frac{(\pi\circ\pi')(i) - (\pi\circ\pi')(j)}{i-j} \\
&= \prod_{i<j} \left(\frac{(\pi\circ\pi')(i) - (\pi\circ\pi')(j)}{\pi'(i)-\pi'(j)} \cdot \frac{\pi'(i)-\pi'(j)}{i-j} \right) \\
&= \prod_{i<j} \frac{(\pi\circ\pi')(i) - (\pi\circ\pi')(j)}{\pi'(i)-\pi'(j)} \cdot \prod_{i<j} \frac{\pi'(i)-\pi'(j)}{i-j} \\
&= \mathrm{sgn}(\pi) \cdot \mathrm{sgn}(\pi') \;,
\end{aligned}$$

da die Menge $\{(\pi'(i), \pi'(j)) \mid 1 \le i < j \le n\}$ in Bijektion zu den 2-elementigen Teilmengen von $\{1, ..., n\}$ steht. □

(iv) Man definiert die *alternierende Gruppe* $A_n \subset S_n$ durch

$$A_n \;:=\; \mathrm{Kern}(\mathrm{sgn}) = \{\pi \in S_n \mid \mathrm{sgn}(\pi) = 1\} \;.$$

Die alternierenden Gruppen spielen in der Gruppentheorie eine wichtige Rolle und sind deshalb eine Erwähnung wert. Wir gehen aber nicht weiter ins Detail.

(v) Die *Klein'sche Vierergruppe* $V_4 \subset S_4$ ist gegeben durch

$$V_4 \;=\; \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\} \;.$$

Es gilt $V_4 \subset D_4$ und $V_4 \subset A_4$. Das heißt, V_4 ist Untergruppe von D_4 und von A_4.

6.1.2 Gruppenordnungen und der Satz von Lagrange

Wir definieren als nächstes die Ordnung einer Gruppe und die Ordnung eines Elements einer Gruppe.

Definition 6.1.7 (Gruppenordnung, Ordnung eines Gruppenelements)**.** Es sei $(G, \circ)$ eine Gruppe.

(i) Enthält G unendlich viele Elemente, so ist die *Ordnung von* G unendlich. Andernfalls ist die *Ordnung von* G die Kardinalität der Menge G.

(ii) Die *Ordnung eines Elements* $x \in G$ ist die Ordnung der von x erzeugten Untergruppe $\langle x \rangle$.

Beispiel. Die zyklischen Untergruppen $\langle \sigma_1 \rangle$ und $\langle \pi_1 \rangle$ aus Beispiel 6.1.1 haben Ordnung 4 bzw. 2. Also hat σ_1 die Ordnung 4 und π_1 die Ordnung 2. Allgemeiner ist die Ordnung einer Drehung aus der Diedergruppe D_n stets ein Teiler von n, wogegen jede Spiegelung aus D_n die Ordnung 2 hat. Die Gruppe D_n hat die Ordnung $2n$.

Bemerkung. Nach Lemma 6.1.3 ist die Ordnung eines Gruppenelements x die kleinste natürliche Zahl k mit $x^k = e$.

Ziel dieses Abschnitts ist es zu zeigen, dass für den Fall endlicher Gruppen die Ordnung einer Untergruppe ein Teiler der Gruppenordnung ist. Dazu benötigen wir den Begriff der Nebenklasse.

Definition 6.1.8 (Nebenklassen)**.** Es sei $(G, \circ)$ eine Gruppe und H eine Untergruppe von G. Für $x \in G$ nennen wir die Menge

$$x \circ H \;:=\; \{x \circ y \mid y \in H\}$$

die *zu* x *gehörende Linksnebenklasse von* H. Analog heißt

$$H \circ x \;:=\; \{y \circ x \mid y \in H\}$$

die *zu* x *gehörende Rechtsnebenklasse von* H.

Beispiel. Die symmetrische Gruppe S_3 ist gegeben durch

$$S_3 \;=\; \{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$

und die alternierende Gruppe $A_3 \subset S_3$ ist gegeben durch

$$A_3 \;=\; \{\mathrm{id}, (1,2,3), (1,3,2)\} \;.$$

Die zu $(1,2)$ gehörende Linksnebenklasse von A_3 stimmt mit der zugehörigen Rechtsnebenklasse überein.

$$\begin{aligned}(1,2)\circ A_3 &= \{(1,2)\circ\mathrm{id},(1,2)\circ(1,2,3),(1,2)\circ(1,3,2)\}\\ &= \{(1,2),(2,3),(1,3)\}\\ &= \{\mathrm{id}\circ(1,2),(1,3,2)\circ(1,2),(1,2,3)\circ(1,2)\}\\ &= A_3\circ(1,2)\ .\end{aligned}$$

Die zu $(1,2,3)$ gehörenden Links- und Rechtsnebenklassen der zyklischen Untergruppe $\langle(1,2)\rangle$ sind hingegen verschieden.

$$\begin{aligned}(1,2,3)\circ\langle(1,2)\rangle &= \{(1,2,3)\circ\mathrm{id},(1,2,3)\circ(1,2)\}\\ &= \{(1,2,3),(1,3)\}\\ \langle(1,2)\rangle\circ(1,2,3) &= \{\mathrm{id}\circ(1,2,3),(1,2)\circ(1,2,3)\}\\ &= \{(1,2,3),(2,3)\} \neq (1,2,3)\circ\langle(1,2)\rangle\ .\end{aligned}$$

Die Nebenklassen einer Untergruppe können insbesondere als Urbilder unter Gruppenhomomorphismen auftauchen.

Satz 6.1.9. *Es seien $(G,\circ)$ und $(G',\bullet)$ Gruppen und $\varphi: G\to G'$ ein Gruppenhomomorphismus. Ist $y\in\mathrm{Bild}(\varphi)$ und $x\in G$ mit $\varphi(x)=y$, so ist*

$$\varphi^{-1}(y) \;=\; x\circ\mathrm{Kern}(\varphi) \;=\; \mathrm{Kern}(\varphi)\circ x\ .$$

Beweis. Im Folgenden bezeichnen wir das neutrale Element von G mit e und das neutrale Element von G' mit f. Wir zeigen, dass $\varphi^{-1}(y)=x\circ\mathrm{Kern}(\varphi)$. Der Beweis, dass $\varphi^{-1}(y)=\mathrm{Kern}(\varphi)\circ x$ funktioniert völlig analog.

Zunächst einmal gilt $\varphi^{-1}(y)\supseteq x\circ\mathrm{Kern}(\varphi)$, da für $x'\in\mathrm{Kern}(\varphi)$ gilt, dass

$$\varphi(x\circ x') \;=\; \varphi(x)\bullet\varphi(x') \;=\; y\bullet f \;=\; y\ .$$

Es bleibt also zu zeigen, dass $\varphi^{-1}(y)\subseteq x\circ\mathrm{Kern}(\varphi)$. Es sei also $z\in\varphi^{-1}(y)$, das heißt $\varphi(z)=y$. Wir müssen zeigen, dass es ein $x'\in\mathrm{Kern}(\varphi)$ gibt mit $z=x\circ x'$. Setzen wir $x':=x^{-1}\circ z$, dann gilt $x'\in\mathrm{Kern}(\varphi)$, da

$$\varphi(x') \;=\; \varphi(x^{-1})\bullet\varphi(z) \;=\; \varphi(x)^{-1}\bullet\varphi(z) \;=\; y^{-1}\bullet y \;=\; f\ .$$

Außerdem ist

$$x\circ x' \;=\; x\circ x^{-1}\circ z \;=\; e\circ z \;=\; z\ .$$

Damit ist der Beweis abgeschlossen. □

Als Folgerung aus Satz 6.1.9 können wir jetzt ein einfaches Kriterium für die Injektivität eines Gruppenhomomorphismus notieren.

Korollar 6.1.10. *Es seien $(G, \circ)$ und $(G', \bullet)$ Gruppen und $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann ist φ genau dann ein Gruppenmonomorphismus (d.h. injektiv), wenn* $\mathrm{Kern}(\varphi)$ *nur das neutrale Element e von G enthält.*

Beweis. Die Notwendigkeit des genannten Kriteriums für die Injektivität von φ ist klar, da nach Lemma 2.2.14 das neutrale Element e von G immer im Kern von φ enthalten ist.

Wir müssen noch zeigen, dass die Bedingung hinreichend ist. Wir nehmen also an, dass $\mathrm{Kern}(\varphi) = \{e\}$. Es seien also $x, x' \in G$ mit $\varphi(x) = \varphi(x')$. Wegen Satz 6.1.9 gilt dann

$$\{x\} \;=\; x \circ \{e\} \;=\; x \circ \mathrm{Kern}(\varphi) \;=\; x' \circ \mathrm{Kern}(\varphi) \;=\; x' \circ \{e\} \;=\; \{x'\} \;.$$

Folglich ist also $x = x'$ und der Beweis ist abgeschlossen. □

Beispiel. Es sei $\sigma \in S_n$ beliebig. Die Abbildung

$$\varphi_\sigma : S_n \to S_n \;, \qquad \pi \mapsto \sigma \circ \pi \circ \sigma^{-1}$$

heißt *Konjugation (mit σ)*. Für $\pi_1, \pi_2 \in S_n$ gilt:

$$\begin{aligned} \varphi_\sigma(\pi_1 \circ \pi_2) &= \sigma \circ (\pi_1 \circ \pi_2) \circ \sigma^{-1} \\ &= \sigma \circ (\pi_1 \circ \mathrm{id} \circ \pi_2) \circ \sigma^{-1} \\ &= \sigma \circ (\pi_1 \circ (\sigma^{-1} \circ \sigma) \circ \pi_2) \circ \sigma^{-1} \\ &= (\sigma \circ \pi_1 \circ \sigma^{-1}) \circ (\sigma \circ \pi_2 \circ \sigma^{-1}) \\ &= \varphi_\sigma(\pi_1) \circ \varphi_\sigma(\pi_2) \;. \end{aligned}$$

Folglich ist φ_σ ein Gruppenhomomorphismus. Ist $\varphi_\sigma(\pi_1) = \mathrm{id}$, so gilt $\sigma \circ \pi_1 = \sigma$ und wegen der Eindeutigkeit des neutralen Elements folgt $\pi_1 = \mathrm{id}$. Der Kern von φ_σ besteht also nur aus der Identität und Korollar 6.1.10 liefert, dass φ_σ ein injektiver Gruppenhomomorphismus ist. Da φ_σ die endliche Menge S_n in sich selbst abbildet, ist φ_σ also auch bijektiv und damit ein Gruppenisomorphismus.

Es sei noch bemerkt, dass für einen r-Zyklus $\pi = (x_1, ..., x_r) \in S_n$ die Gleichung

$$\varphi_\sigma(\pi) = (\sigma(x_1), ..., \sigma(x_r)) \tag{6.1}$$

gilt.

Wir können jetzt den wichtigen Satz von Lagrange beweisen.

Satz 6.1.11 (Satz von Lagrange)**.** *Es sei $(G, \circ)$ eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann teilt die Ordnung von H die Ordnung von G. Den Quotienten $|G|/|H|$ nennt man auch den* Index *der Untergruppe H in G.*

Beweis. Wir definieren auf G eine Relation $\sim$ durch

$$x \sim y \ :\Longleftrightarrow \ x^{-1} \circ y \in H \ .$$

Man rechnet leicht nach, dass es sich hier um eine Äquivalenzrelation handelt, deren Äquivalenzklassen den Linksnebenklassen von H entsprechen. Es gilt nämlich

$$x \sim y \iff y \in x \circ H \ .$$

Die Linksnebenklassen von H bilden also eine Partition der Menge G. Wir zeigen noch, dass die Kardinalität einer beliebigen Linksnebenklasse $x \circ H$ von H gleich der Kardinalität von H ist. Daraus folgt dann die Behauptung und der Index von H in G entspricht der Anzahl der verschiedenen Linksnebenklassen von H.

Um zu zeigen, dass $|H| = |x \circ H|$, konstruieren wir eine bijektive Abbildung von H nach $x \circ H$. Diese Abbildung ist gegeben durch $y \mapsto x \circ y$. Die Surjektivität folgt sofort aus der Definition. Auch die Injektivität sieht man leicht, da aus $x \circ y = x \circ y'$ folgt, dass

$$y \ = \ x^{-1} \circ (x \circ y) \ = \ x^{-1} \circ (x \circ y') \ = \ y' \ .$$

Damit ist der Beweis abgeschlossen. □

Korollar 6.1.12. *Es sei $(G, \circ)$ eine endliche Gruppe mit neutralem Element e und $x \in G$. Dann ist die Ordnung von x ein Teiler der Gruppenordnung $|G|$ und es gilt $g^{|G|} = e$.*

Beweis. Die Ordnung k von x ist nach Definition die Ordnung der von x erzeugten Untergruppe $\langle x \rangle$ von G und damit nach Satz 6.1.11 ein Teiler der Ordnung von G. Es sei also $\ell \in \mathbb{N}$ mit $|G| = k \cdot \ell$. Dann ist

$$x^{|G|} \ = \ x^{k \cdot \ell} \ = \ (x^k)^\ell \ = \ e^\ell \ = \ e \ .$$

Damit ist der Beweis abgeschlossen. □

Beispiel. Die Ordnung der Drehung $\sigma = (1, 2, \ldots, n) \in D_n$ ist n, die einer Spiegelung $\pi \in D_n$ ist 2 und D_n hat die Ordnung $2n$. Die Diedergruppe D_n ist Untergruppe von S_n und S_n hat die Ordnung $n!$. Die Ordnung eines beliebigen Zykels der Länge k in S_n ist k.

6.1.3 Der Homomorphiesatz für Gruppen

In diesem Abschnitt beweisen wir einen wichtigen Satz über Gruppen und Gruppenhomomorphismen — den Homomorphiesatz. Wir beginnen mit der Definition spezieller Untergruppen, die Normalteiler genannt werden.

Definition 6.1.13 (Normalteiler)**.** Es sei $(G, \circ)$ eine Gruppe und $N \subseteq G$ eine Untergruppe. Dann ist N ein *Normalteiler*, falls $x \circ N = N \circ x$ für alle $x \in G$.

Beispiele.

(i) Ist G eine abelsche Gruppe, so ist jede Untergruppe H von G ein Normalteiler in G.

(ii) Wir haben schon gesehen, dass die zu $(1,2)$ gehörenden Links- und Rechtsnebenklassen von A_3 übereinstimmen. Da $|S_3|/|A_3| = 6/3 = 2$ ist, gibt es nach dem Satz von Lagrange nur zwei verschiedene Links- und Rechtsnebenklassen von A_3. Die zweite Links- bzw. Rechtsnebenklasse ist gegeben durch $\mathrm{id} \circ A_3 = A_3 = A_3 \circ \mathrm{id}$. Die alternierende Gruppe A_3 ist also ein Normalteiler vom Index 2 in S_3. Dies gilt entsprechend für alle alternierenden Gruppen A_n $(n > 1)$.

(iii) Die Klein'sche Vierergruppe V_4 ist ein Normalteiler in S_4. Dies verifiziert man direkt durch Nachrechnen, oder elegant mit Hilfe von Gleichung (6.1).

Bemerkung. Um nachzuweisen, dass eine Untergruppe H einer Gruppe G ein Normalteiler ist, genügt es zu zeigen, dass für alle $x \in G$ gilt:

$$H \subset xHx^{-1} \quad \text{oder alternativ} \quad xHx^{-1} \subset H \ .$$

Das wichtigste Beispiel für Normalteiler wird durch den Kern eines Gruppenhomomorphismus gegeben.

Lemma 6.1.14. *Es seien $(G, \circ)$ und $(G', \bullet)$ zwei Gruppen und $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann ist* $\mathrm{Kern}(\varphi)$ *ein Normalteiler von G.*

Beweis. Die Aussage folgt sofort aus Satz 6.1.9. □

Unser Ziel ist es zu zeigen, dass die Nebenklassen eines Normalteilers mit einer natürlich definierten Verknüpfung wieder eine Gruppe bilden.

Satz 6.1.15 (Faktorgruppe, Quotientengruppe)**.** *Es sei $(G, \circ)$ eine Gruppe und $N \subseteq G$ ein Normalteiler. Wir bezeichnen die Menge der Nebenklassen von N mit G/N. Dann bildet G/N zusammen mit der durch*

$$(x \circ N) \bullet (y \circ N) \ := \ (x \circ y) \circ N$$

definierten Verknüpfung $\bullet$ eine Gruppe, die sogenannte Faktor- *oder* Quotientengruppe *von G modulo N. Die* kanonische Projektion $\pi : G \to G/N,\ x \mapsto x \circ N$ *ist ein surjektiver Homomorphismus mit* $\mathrm{Kern}(\pi) = N$.

Beweis. Wir müssen zunächst zeigen, dass die oben angegebene Verknüpfung $\bullet$ wohldefiniert ist. Ist $x \circ N = x' \circ N$ und $y \circ N = y' \circ N$, so muss gelten, dass

$$(x \circ y) \circ N \ = \ (x' \circ y') \circ N \ .$$

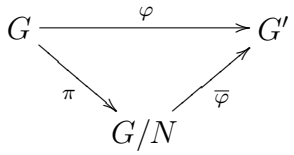
Da $x \circ N = x' \circ N$, gibt es ein $x'' \in N$ mit $x = x' \circ x''$. Analog gibt es ein $y'' \in N$ mit $y = y' \circ y''$. Da N ein Normalteiler ist, gilt

$$\begin{aligned}(x \circ y) \circ N &= (x' \circ x'' \circ y' \circ y'') \circ N = (x' \circ x'' \circ y') \circ (y'' \circ N) \\ &= (x' \circ x'' \circ y') \circ N = x' \circ \big((x'' \circ y') \circ N\big) \\ &= x' \circ \big(N \circ (x'' \circ y')\big) = x' \circ \big((N \circ x'') \circ y'\big) \\ &= x' \circ (N \circ y') = x' \circ (y' \circ N) \\ &= (x' \circ y') \circ N \ .\end{aligned}$$

Jetzt überprüft man leicht, dass $(G/N, \bullet)$ eine Gruppe ist. Die Verknüpfung $\bullet$ ist assoziativ, da $\circ$ assoziativ ist. Das neutrale Element von G/N ist $e \circ N = N$, wobei e das neutrale Element von G bezeichnet. Das zu $x \circ N$ inverse Element in G/N ist $x^{-1} \circ N$. Man erhält nun unmittelbar durch Nachrechnen, dass die Projektion π ein Gruppenhomomorphismus ist. Die Surjektivität von π und die Aussage $\mathrm{Kern}(\pi) = N$ folgen ebenfalls sofort. □

Der Gruppenhomomorphismus $\pi : G \to G/N$ erfüllt eine sogenannte *universelle Eigenschaft*, die G/N bis auf Isomorphie eindeutig charakterisiert:

Satz 6.1.16 (Universelle Eigenschaft)**.** *Es seien $(G, \bullet)$ und $(G', \cdot)$ zwei Gruppen, $\varphi : G \to G'$ ein Gruppenhomomorphismus und $N \subseteq G$ ein Normalteiler mit $N \subseteq \mathrm{Kern}(\varphi)$. Dann existiert ein eindeutig bestimmter Gruppenhomomorphismus $\overline{\varphi} : G/N \to G'$, mit $\varphi = \overline{\varphi} \circ \pi$. Man sagt dann auch, dass das Diagramm*



„kommutiert“. Es gilt $\mathrm{Bild}(\overline{\varphi}) = \mathrm{Bild}(\varphi)$, $\mathrm{Kern}(\overline{\varphi}) = \pi\big(\mathrm{Kern}(\varphi)\big)$ *und* $\mathrm{Kern}(\varphi) = \pi^{-1}(\mathrm{Kern}(\overline{\varphi}))$.

Beweis. Wenn $\overline{\varphi}$ existiert, so muss

$$\overline{\varphi}(x \bullet N) = \overline{\varphi}(\pi(x)) = \varphi(x)$$

für alle $x \in G$ gelten, also ist $\overline{\varphi}$ eindeutig bestimmt.

Umgekehrt können wir $\overline{\varphi}$ durch die Gleichung $\overline{\varphi}(x \bullet N) = \varphi(x)$ definieren, wenn wir zeigen, dass $\varphi(x)$ unabhängig von der Wahl des Repräsentanten $x' \in x \bullet N$ ist. Das heißt, wenn $x \bullet N = x' \bullet N$ ist, so muss $\varphi(x) = \overline{\varphi}(x \bullet N) = \overline{\varphi}(x' \bullet N) = \varphi(x')$ gelten.

Es sei also $x \bullet N = x' \bullet N$, für zwei Elemente $x, x' \in G$. Dann gilt $x^{-1} \bullet x' \in N \subseteq \mathrm{Kern}(\varphi)$ und somit $f = \varphi(x^{-1} \bullet x') = \varphi(x)^{-1} \cdot \varphi(x')$, wobei f das neutrale Element in G' bezeichnet. Damit ist $\varphi(x) = \varphi(x')$. Dass $\overline{\varphi}$ ein Gruppenhomomorphismus ist, ergibt sich sofort aus der Gruppenstruktur von G/N oder, anders ausgedrückt, aus der Tatsache, dass π ein Epimorphismus von Gruppen ist.

Die Gleichung $\text{Kern}(\varphi) = \pi^{-1}(\text{Kern}(\overline{\varphi}))$ folgt aus der Tatsache, dass φ die Komposition von $\overline{\varphi}$ mit π ist. Weiter gelten $\text{Bild}(\overline{\varphi}) = \text{Bild}(\varphi)$ und $\text{Kern}(\overline{\varphi}) = \pi(\text{Kern}(\varphi))$ aufgrund der Surjektivität von π. □

Damit können wir nun den Homomorphiesatz für Gruppen beweisen.

Korollar 6.1.17 (Homomorphiesatz)**.** *Ist $\varphi : G \to G'$ ein surjektiver Gruppenhomomorphismus, so ist G' isomorph zu $G/\operatorname{Kern}(\varphi)$.*

Beweis. Der Kern von φ ist nach Lemma 6.1.14 ein Normalteiler in G. Nach der universellen Eigenschaft der kanonische Projektion existiert also ein Gruppenhomomorphismus $\overline{\varphi} : G/\operatorname{Kern}(\varphi) \to G'$. Wegen der Surjektivität von φ und $\text{Bild}(\varphi) = \text{Bild}(\overline{\varphi})$ ist auch $\overline{\varphi}$ surjektiv. Die Injektivität von $\overline{\varphi}$ folgt sofort aus $\text{Kern}(\overline{\varphi}) = \pi(\text{Kern}(\varphi))) = e \circ \text{Kern}(\varphi)$ zusammen mit Korollar 6.1.10, denn $e \circ \text{Kern}(\varphi)$ ist das neutrale Element in G/N. □

Korollar 6.1.18. *Es sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann ist $G/\operatorname{Kern}(\varphi)$ isomorph zu $\text{Bild}(\varphi)$.*

Beweis. $\text{Bild}(\varphi)$ ist als Untergruppe von G' selbst eine Gruppe und somit ist $\varphi : G \to \text{Bild}(\varphi)$ ein surjektiver Gruppenhomomorphismus. Der Homomorphiesatz liefert also die Behauptung. □

Beispiel. Es sei X eine Menge, $Y \subseteq X$ eine Teilmenge, $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$ und $(G^X, \circ)$ die Gruppe der G-wertigen Funktionen auf X. Dann ist $N := \{f \in G^X \mid f(y) = e \text{ für alle } y \in Y\}$ ein Normalteiler in G^X und G/N ist isomorph zu G^Y, denn die Einschränkungsabbildung $\varphi : G^X \to G^Y,\ f \mapsto f|_Y$ ist ein surjektiver Gruppenhomomorphismus.

6.2 Ringtheorie

In diesem Abschnitt werden wir die Resultate über Gruppen aus Abschnitt 6.1 sinngemäß auf Ringe zu übertragen versuchen. Dazu empfiehlt es sich zunächst, sich die Definitionen und elementaren Einsichten über Ringe, Unterringe und Ringhomomorphismen aus Kapitel 2, Abschnitt 2.2 in Erinnerung zu rufen.

Bemerkung. Es seien $(R, +, \cdot)$ und $(R', \oplus, \odot)$ Ringe mit Nullelementen $0 \in R$ und $0' \in R'$. Dann ist der Ringhomomorphismus $\varphi : R \to R'$ genau dann injektiv, wenn $\text{Kern}(\varphi) := \{x \in R \mid \varphi(x) = 0'\}$ nur aus dem Nullelement $0 \in R$ besteht. Dies folgt unmittelbar aus Korollar 6.1.10, da φ nach Definition auch ein Gruppenhomomorphismus von $(R, +)$ nach $(R', \oplus)$ ist.

Wir geben in dem folgenden Lemma eine Charakterisierung von Unterringen an, die unmittelbar aus der entsprechenden Charakterisierung von Untergruppen in Lemma 6.1.1 folgt.

Lemma 6.2.1. *Es sei $(R,+,\cdot)$ ein Ring und $\emptyset \neq S \subseteq R$. Dann bildet S einen Unterring von R, falls für alle $x,y \in S$ gilt, dass $x-y \in S$ und $x \cdot y \in S$.*

Beweis. Die Behauptung folgt unmittelbar aus der Definition von Unterringen (Definition 2.2.10) und Lemma 6.1.1. □

Damit können wir jetzt leicht den folgenden Satz beweisen.

Satz 6.2.2. *Es seien $(R,+,\cdot)$ und $(R',\oplus,\odot)$ Ringe und $\varphi : R \to R'$ ein Ringhomomorphismus. Ist S ein Unterring von R, so ist das Bild $\varphi(S)$ ein Unterring von R'. Ist umgekehrt S' ein Unterring von R', so ist das Urbild $\varphi^{-1}(S')$ ein Unterring von R.*

Beweis. Der Beweis folgt unmittelbar aus Lemma 6.2.1 □

6.2.1 Faktorringe und Ideale

Da die additive Gruppe $(R,+)$ eines jeden Rings $(R,+,\cdot)$ kommutativ ist, ist jede Untergruppe ein Normalteiler. Insbesondere ist jeder Unterring $S \subseteq R$ ein Normalteiler von $(R,+)$. Folglich kann man die Faktorgruppe $(R/S,\oplus)$ betrachten und fragen, unter welchen Umständen $R/S = \{x+S \mid x \in R\}$ als Ring aufgefasst werden kann. Wir wissen bereits, dass die Addition $\oplus$ auf R/S definiert wird durch

$$(x+S) \oplus (y+S) \;:=\; (x+y)+S \;.$$

Daher wäre es naheliegend, auch eine Multiplikation $\odot$ auf R/S zu definieren durch

$$(x+S) \odot (y+S) \;:=\; (x \cdot y)+S \;.$$

Damit diese Multiplikation wohldefiniert ist, muss für $x,x',y,y' \in R$ mit $x+S = x'+S$ und $y+S = y'+S$ gelten, dass

$$(x \cdot y)+S \;=\; (x' \cdot y')+S \;.$$

Im Folgenden sei $x \cdot S$ und $S \cdot x$ für $x \in R$ und $S \subseteq R$ definiert als

$$x \cdot S \;:=\; \{x \cdot s \mid s \in S\} \qquad \text{und} \qquad S \cdot x \;:=\; \{s \cdot x \mid s \in S\} \;.$$

Lemma 6.2.3. *Es sei $(R,+,\cdot)$ ein Ring und $S \subseteq R$ ein Unterring von R. Die beiden folgenden Aussagen sind äquivalent:*

(i) Für alle $x,x',y,y' \in R$ mit $x+S = x'+S$ und $y+S = y'+S$ gilt, dass $(x \cdot y)+S = (x' \cdot y')+S$.

(ii) Für alle $x \in R$ gilt $x \cdot S \subseteq S$ und $S \cdot x \subseteq S$.

Beweis. „(i)⇒(ii)“: Es sei $x \in R$ und $s \in S$. Dann ist $s + S = 0 + S$ und folglich wegen (i) $(x \cdot s) + S = (x \cdot 0) + S = S$. Daraus folgt $x \cdot s \in S$ und daher $x \cdot S \subseteq S$. Analog zeigt man $S \cdot x \subseteq S$.

„(ii)⇒(i)“: Es seien $x, x', y, y' \in R$ mit $x+S = x'+S$ und $y+S = y'+S$. Dann gilt $x-x' \in S$ und $y-y' \in S$. Wegen (ii) folgt daraus $x \cdot y - x' \cdot y = (x-x') \cdot y \in S$ und $x' \cdot y - x' \cdot y' = x' \cdot (y-y') \in S$. Da S ein Unterring von R ist, ist $(S, +)$ erst recht Untergruppe von $(R, +)$. Folglich ist

$$x \cdot y - x' \cdot y' \;=\; (x \cdot y - x' \cdot y) + (x' \cdot y - x' \cdot y') \;\in\; S \;.$$

Also ist $x \cdot y + S = x' \cdot y' + S$. □

Man überzeugt sich leicht davon, dass die Bedingung (ii) aus Lemma 6.2.3 nicht für beliebige Unterringe erfüllt ist:

Beispiel. Der Körper der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ ist ein Unterring des Körpers der reellen Zahlen $(\mathbb{R}, +, \cdot)$. Es gilt jedoch nicht, dass $q \cdot r \in \mathbb{Q}$ für alle $q \in \mathbb{Q}$ und $r \in \mathbb{R}$. Wähle beispielsweise $q = 1$ und $r = \sqrt{2}$.

Definition 6.2.4 (Ideale)**.** Es sei $(R, +, \cdot)$ ein Ring. Ein Unterring $S \subseteq R$ heißt *Ideal*, wenn $x \cdot S \subseteq S$ und $S \cdot x \subseteq S$ für alle $x \in R$.

Lemma 6.2.5. *Es sei $(R, +, \cdot)$ ein Ring und $\emptyset \neq S \subseteq R$. Die Teilmenge S ist genau dann ein Ideal in R, wenn $s - s' \in S$, $x \cdot s \in S$ und $s \cdot x \in S$ für alle $s, s' \in S$ und $x \in R$.*

Beweis. Die Behauptung folgt direkt aus Lemma 6.2.1 und Definition 6.2.4. □

Beispiele.

(i) Für einen beliebigen Ring $(R, +, \cdot)$ sind die Teilringe $\{0\}$ und R Ideale. Sie heißen *triviale Ideale*. Jedes andere Ideal heißt *nicht trivial*. Ein Ideal $S \neq R$ heißt *echtes Ideal*.

(ii) Ist K ein Körper, so sind die trivialen Ideale die einzigen Ideale in K. Denn ist $S \neq \{0\}$ ein Ideal, dann gibt es ein $0 \neq s \in S$. Dieses Element s besitzt ein Inverses s^{-1}, so dass für beliebige $x \in K$ gilt, dass $x = x \cdot s^{-1} \cdot s \in (x \cdot s^{-1}) \cdot S \subseteq S$. Folglich ist $S = K$.

(iii) Wir betrachten den Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot)$. Für beliebige $q \in \mathbb{Z}$ ist $q \cdot \mathbb{Z}$ ein Ideal.

(iv) Ist R ein kommutativer Ring und $R[X]$ der zugehörige Polynomring, so ist $q \cdot R[X]$ für $q \in R[X]$ offenbar ein Unterring von $R[X]$ und sogar ein Ideal.

Wegen Lemma 6.2.3 können wir für einen Ring R und ein Ideal $S \subseteq R$ den Faktorring R/S definieren.

Satz 6.2.6 (Faktorring, Restklassenring)**.** *Es sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ ein Ideal. Dann bildet die Menge $R/S := \{x + S \mid x \in R\}$ zusammen mit der Addition*

$$(x + S) \oplus (y + S) \;:=\; (x + y) + S$$

und der Multiplikation

$$(x + S) \odot (y + S) \;:=\; (x \cdot y) + S$$

einen Ring $(R/S, \oplus, \odot)$, den zu R und S gehörenden Faktor- *oder* Restklassenring*.*

Beweis. Aus Lemma 6.2.3 folgt, dass nicht nur die uns bereits bekannte Addition $\oplus$ sondern auch die Multiplikation $\odot$ wohldefiniert sind. Die Eigenschaften eines Rings überprüft man nun leicht. Sie folgen direkt aus der Tatsache, dass $(R, +, \cdot)$ ein Ring ist. □

Beispiel. Es sei $m \geq 2$. Wie schon weiter oben erwähnt, ist $m\mathbb{Z}$ ein Ideal des Rings $\mathbb{Z}$. Den Faktorring $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus Kapitel 2. Man kann nämlich leicht zeigen, dass $\mathbb{Z}/m\mathbb{Z}$ isomorph ist zu dem Ring $(\mathbb{Z}_m, +_m, \cdot_m)$. Zunächst überzeugt man sich leicht davon, dass

$$\mathbb{Z}/m\mathbb{Z} \;=\; \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\} \;.$$

Mit diesen Nebenklassen rechnet man so wie mit den Elementen von $\mathbb{Z}_m$.

Satz 6.2.7 (Erzeugte Ideale)**.** *Es sei $(R, +, \cdot)$ ein Ring mit Eins und $\emptyset \neq S \subseteq R$. Dann ist*

$$\langle S \rangle_I \;=\; \left\{ \sum_{k=1}^{n} (x_k \cdot s_k \cdot y_k) \;\middle|\; x_k, y_k \in R, s_k \in S, n \in \mathbb{N} \right\}$$

ein Ideal. Wir nennen $\langle S \rangle_I$ das von S erzeugte Ideal*.*

Beweis. Nachrechnen! □

Bemerkung. Man kann sich leicht davon überzeugen, dass $\langle S \rangle_I$ das bezüglich Inklusion kleinste Ideal ist, das S enthält.

Wir halten im Folgenden noch den Spezialfall von Satz 6.2.7 fest, in dem die Menge S nur aus einem Element besteht.

Korollar 6.2.8 (Hauptideale)**.** *Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $s \in R$. Dann ist $s \cdot R = R \cdot S$ das von s erzeugte Ideal. Man nennt dieses ideal auch* Hauptideal*.*

Damit können wir jetzt eine einfache Charakterisierung von Körpern angeben.

Satz 6.2.9. *Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.*

(i) Ein Element $x \in R$ ist genau dann eine Einheit, wenn das von x erzeugte Hauptideal $x \cdot R$ der ganze Ring R ist, also $x \cdot R = R$.

(ii) Der Ring R ist genau dann ein Körper, wenn R nur die beiden trivialen Ideale $\{0\}$ und R enthält.

Beweis. Wir beweisen zunächst die Aussage (i). Sei $x \in R$ eine Einheit. Dann existiert ein $y \in R$ mit $1 = x \cdot y \in x \cdot R$. Da $x \cdot R$ ein Ideal in R ist, gilt nun per Definition $r = r \cdot 1 \in x \cdot R$, für alle $r \in R$. Damit haben wir $R \subseteq x \cdot R$ und die andere Inklusion ist klar. Ist umgekehrt das von $x \in R$ erzeugte Ideal $x \cdot R$ schon der ganze Ring R, so gilt $1 \in R = x \cdot R$. Es folgt, dass ein $y \in R$ existiert, mit $1 = x \cdot y$ und x ist folglich eine Einheit.

Die Aussage (ii) folgt nun unmittelbar. Wir haben weiter oben schon gesehen, dass ein Körper R nur die trivialen Ideale $\{0\}$ und R enthält. Es ist also nur noch die Umkehrung zu beweisen. Es sei dazu $x \in R \setminus \{0\}$ beliebig. Dann ist das von x erzeugte Ideal $x \cdot R$ nicht das Nullideal $\{0\}$ und folglich gilt $x \cdot R = R$. Nach Aussage (i) ist x damit eine Einheit in R. Da x beliebig gewählt war, folgt, dass in R jedes Element außer dem Nullelement 0 eine Einheit ist und R ist damit ein Körper. □

Lemma 6.2.10. *Es seien $(R, +, \cdot)$ und $(R', \oplus, \odot)$ zwei Ringe und $\varphi : R \to R'$ ein Ringhomomorphismus. Dann ist* $\mathrm{Kern}(\varphi)$ *ein Ideal in R.*

Beweis. Wir rechnen die Behauptung einfach nach. Es seien $0' \in R'$ das Nullelement in R', $r \in R$ und $a, b \in \mathrm{Kern}(\varphi)$ beliebig. Dann gilt:

$$\varphi(a - b) \;=\; \varphi(a) \ominus \varphi(b) \;=\; 0' \ominus 0' \;=\; 0'$$

und

$$\varphi(r \cdot a) \;=\; \varphi(r) \odot \varphi(a) \;=\; \varphi(r) \odot 0' \;=\; 0' \;,$$

also $a - b,\ r \cdot a \in \mathrm{Kern}(\varphi)$. □

Bemerkung. Das Bild $\mathrm{Bild}(\varphi)$ eines Ringhomomorphismus $\varphi : R \to R'$ ist i.A. nur ein Unterring und kein Ideal in R. Man betrachte etwa die Inklusionsabbildung $\iota : K \to K[X]$.

Wir beenden diesen Abschnitt mit dem Homomorphiesatz für Ringe. Die universelle Eigenschaft der Projektionsabbildung $\pi : G \to G/N,\ x \mapsto x \circ N$ von einer Gruppe $(G, \circ)$ in die Faktorgruppe $(G/N, \bullet)$, wobei $N \subseteq G$ ein Normalteiler in G ist, überträgt sich in direkter Weise auf die Situation in Ringen. Ideale nehmen hier die Position der Normalteiler ein. Wir formulieren anstelle der universellen Eigenschaft diesmal direkt das Analogon des Homomorphiesatzes.

Satz 6.2.11. *Es seien $(R, +, \cdot)$ und $(R', \oplus, \odot)$ zwei Ringe und $\varphi : R \to R'$ ein surjektiver Ringhomomorphismus. Dann ist $R/\operatorname{Kern}(\varphi)$ isomorph zu R' und ein Isomorphismus ist gegeben durch*

$$\tilde{\varphi} : R/\operatorname{Kern}(\varphi) \to R' \ , \qquad x + \operatorname{Kern}(\varphi) \mapsto \varphi(x) \ .$$

Beweis. Die Mengen R und R' bilden zusammen mit den Verknüpfungen $+$ und $\oplus$ kommutative Gruppen $(R, +)$ und $(R', \oplus)$. Wir können den Ringhomomorphismus $\varphi : R \to R'$ entsprechend als Gruppenhomomorphismus auffassen und den Homomorphiesatz für Gruppen anwenden. (Als Ideal in $(R, +, \cdot)$ ist $\operatorname{Kern}(\varphi)$ ein Normalteiler in $(R, +)$.)

Dieser liefert nun die kanonische Existenz eines Gruppenisomorphismus $\overline{\varphi} : R/\operatorname{Kern}(\varphi) \to R'$. Dabei ist $\overline{\varphi}$ durch die Gleichung $\overline{\varphi}(x + \operatorname{Kern}(\varphi)) = \varphi(x)$ charakterisiert und dank der Struktur des Faktorrings liefert eine einfache Rechnung, dass sich $\overline{\varphi}$ zu einem Isomorphismus $\tilde{\varphi} : R/\operatorname{Kern}(\varphi) \to R'$ von Ringen fortsetzt. □

Korollar 6.2.12. *Ist $(K, +, \cdot)$ ein Körper, $(R, \oplus, \odot)$ ein Ring mit mindestens zwei Elementen und $\varphi : K \to R$ ein surjektiver Ringhomomorphismus. Dann ist R isomorph zu K.*

Beweis. Da φ ein Ringhomomorphismus ist, gilt $\varphi(1_K) = 1_R \neq 0_R$ und deshalb $\operatorname{Kern}(\varphi) \neq K$. Da $\operatorname{Kern}(\varphi)$ aber ein Ideal in K ist, folgt $\operatorname{Kern}(\varphi) = \{0\}$. Der Homomorphiesatz liefert die Behauptung. □

Bemerkung. Der Beweis zeigt insbesondere, dass jeder Homomorphismus von einem Körper K in einen Ring $R \neq 0$ injektiv ist.

6.2.2 Polynomringe

Wir haben in Kapitel 2 bereits Teilbarkeitstheorie für ganze Zahlen betrieben und den euklidischen Algorithmus kennen gelernt. In Polynomringen über einem Körper K finden wir eine völlig analoge Situation vor.

Definition 6.2.13 (Teilbarkeit)**.** Es sei $(R, +, \cdot)$ ein kommutativer Ring und $a, b \in R$. Man sagt, *a teilt b*, oder *b ist durch a teilbar*, wenn ein $x \in R$ mit $b = x \cdot a$ existiert. Notation: $a \mid b$.

Die obige Definition spiegelt also ebenfalls die Situation in $\mathbb{Z}$ wieder. Das folgende Lemma ist oft nützlich. Den Beweis überlassen wir als einfache Übungsaufgabe.

Lemma 6.2.14. *Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $a, b \in R$.*

(i) $a \mid b$ genau dann, wenn $b \cdot R \subseteq a \cdot R$,

(ii) Es sei R nullteilerfrei. Dann gilt $a \cdot R = b \cdot R$ genau dann, wenn $a = be$ gilt, für eine Einheit $e \in R^*$.

Wir beschäftigen uns nun mit dem Polynomring $K[X]$ über einem Körper K und wiederholen zunächst kurz einige Fakten ohne Beweis.

Satz 6.2.15. *Es sei $(R, +, \cdot)$ ein Integritätsbereich und $p, q \in R[X] \setminus \{0\}$. Dann gilt*

$$\operatorname{grad}(p \cdot q) \;=\; \operatorname{grad}(p) + \operatorname{grad}(q) \;.$$

Korollar 6.2.16. *Es sei K ein Körper, dann ist $K[X]$ nullteilerfrei und ein Polynom $p \in K[X]$ ist genau dann eine Einheit, wenn $\operatorname{grad}(p) = 0$ gilt.*

Bemerkung. Wenn wir jedem Polynom $p \in K[X]$ seinen Grad $\operatorname{grad}(p)$ zuweisen, erhalten wir eine Abbildung $\operatorname{grad} : K[X] \to \mathbb{N}_0 \cup \{-1\},\ p \mapsto \operatorname{grad}(p)$, die sogenannte *Gradabbildung*.

Wir können, ähnlich wie in $\mathbb{Z}$, Division mit Rest in $K[X]$ durchführen. Hierbei nimmt die Gradabbildung eine tragende Rolle ein.

Satz 6.2.17 (Division mit Rest)**.** *Es sei K ein Körper und $0 \neq f \in K[X]$. Dann gibt es zu jedem $g \in K[X]$ eindeutig bestimmte Polynome q und r in $K[X]$ mit $g = q \cdot f + r$ und $\operatorname{grad}(r) < \operatorname{grad}(f)$.*

Beweis. Wir beweisen zunächst die Existenz der Zerlegung. Ist $\operatorname{grad}(g) < \operatorname{grad}(f)$, so können wir $q = 0$ und $r = g$ wählen. Sei also $\operatorname{grad}(g) \geq \operatorname{grad}(f)$. Wir führen nun eine Induktion über $\operatorname{grad}(g)$ durch.

Es sei $\operatorname{grad}(g) = 0$. Wegen $\operatorname{grad}(f) \leq \operatorname{grad}(g)$ und $f \neq 0$ gilt dann $\operatorname{grad}(f) = 0$ und f ist demnach eine Einheit in $K[X]$. Wir wählen also $q = g \cdot f^{-1}$ und $r = 0$.

Es sei die Existenz schon für alle Polynome $g \in K[X]$ mit $\operatorname{grad}(g) \leq m - 1$ bewiesen. Es sei nun

$$g(X) \;=\; \sum_{k=0}^{m} a_k X^k \quad \text{und} \quad f(X) \;=\; \sum_{k=0}^{n} b_k X^k \;, \quad \text{mit } n \leq m \text{ und } a_m, b_n \neq 0.$$

Eine kurze Rechnung liefert für $g_1(X) := g(X) - a_m b_n^{-1} X^{m-n} f(X)$, dass $\operatorname{grad}(g_1) \leq \operatorname{grad}(g) - 1$ gilt. Nach Induktionsvoraussetzung ist $g_1 = q_1 \cdot f + r_1$, mit $\operatorname{grad}(r_1) < \operatorname{grad}(f)$. Dann ist

$$g \;=\; (a_m b_n^{-1} x^{m-n} + q_1) f + r_1$$

die gesuchte Zerlegung.

Wir beweisen nun die Eindeutigkeit der Zerlegung. Es sei $g = q_1 \cdot f + r_1 = q_2 \cdot f + r_2$, mit $\operatorname{grad}(r_1), \operatorname{grad}(r_2) < \operatorname{grad}(f)$. Dann ist $(q_2 - q_1)f = r_1 - r_2$ und es gilt

$$\begin{aligned} \operatorname{grad}(r_1 - r_2) \;&=\; \operatorname{grad}\big((q_2 - q_1)f\big) \\ &=\; \operatorname{grad}(q_2 - q_1) + \operatorname{grad}(f) \\ &>\; \operatorname{grad}(q_2 - q_1) + \max\{\operatorname{grad}(r_1), \operatorname{grad}(r_2)\} \\ &\geq\; \operatorname{grad}(q_2 - q_1) + \operatorname{grad}(r_1 - r_2) \;. \end{aligned}$$

Es folgt nun $\text{grad}(q_2 - q_1) < 0$ und deshalb $q_1 = q_2$. Damit muss aber auch $r_1 = r_2$ gelten. □

Beispiel. Es seien $g(X) = X^5 + 3X^4 + X^3 - 6X^2 - X + 1$, $f(X) = X^3 + 2X^2 + X - 1 \in \mathbb{Q}[X]$.

$$
\begin{array}{l}
(X^5 + 3X^4 + X^3 - 6X^2 - X + 1) : (X^3 + 2X^2 + X - 1) = X^2 + X - 2 \\
\underline{-X^5 - 2X^4 - X^3 + X^2} \\
\qquad X^4 \qquad\quad - 5X^2 - X + 1 \\
\qquad \underline{-X^4 - 2X^3 - X^2 + X} \\
\qquad\quad - 2X^3 - 6X^2 \qquad + 1 \\
\qquad\quad \underline{2X^3 + 4X^2 + 2X - 2} \\
\qquad\qquad - 2X^2 + 2X - 1
\end{array}
$$

Es gilt also $g = (X^2 + X - 2) \cdot f + (-2X^2 + 2X - 1)$.

Dank der Division mit Rest können wir den euklidischen Algorithmus also, genau wie für ganze Zahlen, auch für Polynome nutzen, etwa um den größten gemeinsamen Teiler zweier Polynome zu bestimmen. Bevor wir uns damit im nächsten Abschnitt befassen, formulieren wir noch zwei einfache Folgerungen aus dem Satz.

Korollar 6.2.18. *Es sei K ein Körper und $a \in K$. Im Polynomring $K[X]$ ist das Polynom $f \in K[X]$ genau dann durch $(X - a)$ teilbar, wenn die durch f gegebene Polynomfunktion in a eine Nullstelle hat.*

Beweis. Ist $f(X) = (X - a) \cdot g(X)$, so ist offenbar $f(a) = 0$. Es sei nun umgekehrt $f(a) = 0$. Division mit Rest liefert $f(X) = (X - a) \cdot q(X) + r(X)$, mit $\text{grad}(r) < \text{grad}\big((X - a)\big) = 1$. Damit ist r konstant und wegen $0 = f(a) = r(a)$ gilt $r = 0$. □

Korollar 6.2.19. *Es sei K ein Körper. Dann ist jedes Ideal $J \subseteq K[X]$ ein Hauptideal.*

Beweis. Es sei $J \subseteq K[X]$ ein Ideal. Ist $J = \{0\}$, so sind wir fertig. Andernfalls existiert ein $h \in J,\ h \neq 0$. Dann ist $A := \{m \in \mathbb{N}_0 \mid \exists h \in J : \text{grad}(h) = m\} \neq \emptyset$ und A besitzt ein kleinstes Element n. Es sei nun $f \in J$ mit $\text{grad}(f) = n$ und $g \in J$ beliebig. Dann ist $g = q \cdot f + r$, mit $\text{grad}(r) < \text{grad}(f)$. Da alle Elemente $\neq 0$ in J mindestens den Grad $n = \text{grad}(f)$ haben, folgt aus $r = g - q \cdot f \in J$, dass $r = 0$ ist. Es gilt also $J = \langle f \rangle_I$. □

6.2.3 Größter gemeinsamer Teiler in Polynomringen

Wir beginnen mit der Definition von normierten Polynomen.

Definition 6.2.20 (Normierte Polynome)**.** Ein Polynom $f = \sum_{k=0}^{n} a_k X^k \in K[X]$ heißt *normiert*, falls $a_n = 1$ gilt.

Bemerkung. Man kann ein beliebiges Polynom $f \in K[X]$ *normieren*, indem man f mit dem Inversen des Leitkoeffizienten multipliziert. Dies geht auch in Polynomringen über einem Ring R, solange der Leitkoeffizient des Polynoms eine Einheit in R ist.

Den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache definiert man in Polynomringen analog zum Fall der ganzen Zahlen.

Definition 6.2.21 (ggT in Polynomringen)**.** Es sei K ein Körper und $g, h \in K[X]\backslash\{0\}$. Ein Polynom $f \in K[X]$ heißt *größter gemeinsamer Teiler* von g und h, falls f ein normiertes Polynom von maximalem Grad ist, welches g und h teilt. Notation: $f = \mathrm{ggT}(g, h)$. Die Polynome g und h heißen *teilerfremd*, falls $\mathrm{ggT}(g, h) = 1$ gilt.

Definition 6.2.22 (kgV in Polynomringen)**.** Es sei K ein Körper und $g, h \in K[X] \setminus \{0\}$. Ein Polynom $f \in K[X]$ heißt *kleinstes gemeinsames Vielfaches* von g und h, falls f ein normiertes Polynom von minimalem Grad ist, welches von g und h geteilt wird. Notation: $f = \mathrm{kgV}(g, h)$.

Der folgende Satz ist eine Übertragung des Lemmas von Bezout (siehe Korollar 2.4.4) auf Polynomringe.

Satz 6.2.23. *Es sei K ein Körper, $g, h \in K[X]$, wobei g oder h ungleich 0 seien. Dann ist* $\mathrm{ggT}(g, h)$ *eindeutig bestimmt und es existieren Polynome $s, t \in K[X]$ mit*

$$\mathrm{ggT}(g, h) \;=\; g \cdot s + h \cdot t \;\; .$$

Beweis. Wir bilden

$$J \;:=\; g \cdot K[X] + h \cdot K[X] \;=\; \{g \cdot v + h \cdot w \mid v, w \in K[X]\} \;\; .$$

Es ist leicht zu sehen, dass J ein Ideal $\neq 0$ ist. Nach Korollar 6.2.19 existiert also ein normiertes Polynom $f \in J$, so dass $J = f \cdot K[X] = \langle f \rangle_I$ ist. Wegen $f \in J = g \cdot K[X] + h \cdot K[X]$ existieren Polynome $s, t \in K[X]$ mit $f = g \cdot s + h \cdot t$.

Wir zeigen nun, dass f der eindeutig bestimmte größte gemeinsame Teiler von g und h ist. Es gilt $g = g \cdot 1 + h \cdot 0 \in J$, also $g = f \cdot u$, für ein $u \in K[X]$ und f teilt folglich g. Analog folgt, dass f auch ein Teiler von h ist. Es sei nun f' ein weiterer gemeinsamer Teiler von g und h. Dann teilt f' auch $g \cdot s + h \cdot t = f$. Demnach gilt $\mathrm{grad}(f') \leq \mathrm{grad}(f)$ und f ist ein größter gemeinsamer Teiler von g und h. Es bleibt der Nachweis der Eindeutigkeit.

Angenommen, f' ist normiert und $\mathrm{grad}(f') = \mathrm{grad}(f)$. Da f' ein Teiler von f ist gilt $f' = qf$ und es folgt, dass $\mathrm{grad}(q) = 0$ gilt. Also ist $q \in K \setminus \{0\}$. Da f und f' normiert sind, ist $q = 1$ und folglich $f = f'$. $\square$

Korollar 6.2.24. *Es sei K ein Körper und $g, h \in K[X]$, nicht beide gleich 0.*

(i) Ist $f \in K[X]$ ein Teiler von g und h, so ist f ein Teiler von $\mathrm{ggT}(g,h)$.

(ii) Sind $g, h \in K[X]$ normiert, so ist $g \cdot h = \mathrm{kgV}(g,h) \cdot \mathrm{ggT}(g,h)$.

(iii) Sind $g, h \neq 0$ und ist $f \in K[X]$ ein Vielfaches von g und h, so ist $\mathrm{kgV}(g,h)$ *ein Teiler von f.*

Beweis. Die Aussage (i) haben wir schon im Beweis des obigen Satzes gesehen.

Zu Aussage (ii): Es gilt $g = q_1 \,\mathrm{ggT}(g,h)$ und $h = q_2 \,\mathrm{ggT}(g,h)$ für geeignete Polynome $q_1, q_2 \in K[X]$; also $g \cdot h = q_1 \cdot q_2 \cdot \mathrm{ggT}(g,h)^2$. Wir zeigen nun, dass

$$u \;:=\; q_1 \cdot q_2 \cdot \mathrm{ggT}(g,h) \;=\; \mathrm{kgV}(g,h) \;.$$

Offensichtlich gilt $g \mid u$ und $h \mid u$. Es sei nun $p \in K[X]$ gegeben mit $g \mid p$ und $h \mid p$. Wir zeigen, dass u ein Teiler von p ist. Es gibt $r, v \in K[X]$ mit $p = g \cdot r = h \cdot v$. Weiter gibt es nach Satz 6.2.23 Polynome $s, t \in K[X]$ mit $\mathrm{ggT}(g,h) = g \cdot s + h \cdot t$. Also ist

$$\begin{aligned} \mathrm{ggT}(g,h)p &= (g \cdot s + h \cdot t) \cdot p \\ &= s \cdot g \cdot p + t \cdot h \cdot p \\ &= s \cdot g \cdot h \cdot v + t \cdot h \cdot g \cdot r \\ &= g \cdot h \cdot (s \cdot v + t \cdot r) \\ &= \mathrm{ggT}(g,h) \cdot u \cdot (s \cdot v + t \cdot r) \;. \end{aligned}$$

Kürzen mit $\mathrm{ggT}(g,h)$ liefert $p = u \cdot (s \cdot v + t \cdot r)$, also $u \mid p$. Daraus folgt $u = kgV(g,h)$ und damit die Behauptung.

Aussage (iii) zeigt man ähnlich. □

Zur Berechnung des größten gemeinsamen Teilers von zwei Polynomen kann man, wie im Falle von ganzen Zahlen, den euklidischen Algorithmus verwenden. Damit erhält man auch die in Satz 6.2.23 gegebene Darstellung des ggTs (durch Rückwärtseinsetzen). Da es hier eine unmittelbare Analogie zum in Kapitel 2 besprochenen Fall des Rings der ganzen Zahlen gibt, verzichten wir auf eine erneute detailierte Darstellung und verweisen stattdessen auf die entsprechenden Abschnitte in Kapitel 2.