Lineare Algebra 1

Skript

Łukasz Grabowski

Universität Leipzig

Inhaltsverzeichnis

Vorwort 4

1 Aussagenlogik 5

1.1 Aussagen . . . 5
1.2 Junktoren . . . 6
1.3 Atome, Formeln und Wahrheitstabellen . . . 8
1.4 Äquivalente Formeln . . . 9

2 Beweise und elementare Arithmetik 12

2.1 Teilbarkeit und größter gemeinsamer Teiler . . . 12
2.2 Beweise und Beweisprinzipien . . . 14
2.3 Modulare Arithmetik . . . 17

3 Prädikatenlogik 20

3.1 Prädikate und freie Variablen . . . 20
3.2 Quantoren . . . 20
3.3 Beweisstrategien für Quantoren . . . 23

4 Mengenlehre 25

4.1 Mengen und Elemente . . . 25
4.2 Gleichheit und Teilmengen . . . 26
4.3 Mengen durch Eigenschaften . . . 27
4.4 Operationen auf Mengen . . . 28
4.5 Mengenoperationen und Logik . . . 29
4.6 Verallgemeinerte Vereinigung und verallgemeinerter Schnitt . . . 32
4.7 Endliche Mengen und Kardinalität . . . 33
4.8 Potenzmenge . . . 33

4.9 Mengen als Bausteine 34

5 Vollständige Induktion **35**

5.1 Summenschreibweise 35
5.2 Die Idee der Induktion 36
5.3 Beispiel: die Summe der ersten n Zahlen 37
5.4 Die Potenzmenge einer endlichen Menge 38
5.5 Induktion mit anderem Startwert 40

6 Relationen **42**

6.1 Geordnete Paare 42
6.2 Kartesische Produkte 43
6.3 Relationen 44
6.4 Darstellungen von Relationen 45
6.5 Eigenschaften von Relationen 46
6.6 Inverse Relation und Komposition 48
6.7 Äquivalenzrelationen 50
6.8 Ordnungsrelationen 52

7 Funktionen **54**

7.1 Funktionen als spezielle Relationen 54
7.2 Injektivität, Surjektivität und Bijektivität 56
7.3 Komposition von Funktionen 57
7.4 Inverse Funktionen 59
7.5 Einseitige Inverse und die Axiome der Mengenlehre 60

8 Kardinalitäten **63**

8.1 Gleichmächtigkeit 63
8.2 Cantors Diagonalargument 65
8.3 Abzählbare Mengen 66
8.4 Vergleich von Kardinalitäten 66
8.5 Cantor-Schröder-Bernstein und Matchings in bipartiten Graphen 68
8.6 Lemma von Zorn 71
8.7 Mehr über unendliche Kardinalitäten 72

8.8 Cantors Satz und die Kontinuumshypothese 74

9 Lineare Gleichungssysteme **77**

9.1 Körper 78

9.1.1 Der Körper der komplexen Zahlen 79

9.1.2 Endliche Körper der Form $\mathbb{Z}/p$ 81

9.2 Gleichungssysteme und die Zeilenstufenform 82

9.3 Gaußsches Eliminationsverfahren 84

10 Vektorräume **89**

10.1 Was jetzt? 89

10.2 Vektorräume 90

10.3 Linearkombinationen und Basen 94

10.4 Lineare Unabhängigkeit; Erzeugendensysteme 97

11 Lineare Abbildungen **101**

11.1 Matrizen als lineare Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$ 104

11.2 Matrix-Beispiele 106

11.3 $M_{m\times n}(\mathbb{K})$ und $\mathrm{Lin}(V,W)$ als Vektorräume 109

11.4 Zusammenhang zwischen linearen Abbildungen... 110

Vorwort

Die ersten Kapitel dieser Notizen behandeln einige Grundlagen der mathematischen Sprache. Dazu gehören Aussagenlogik, Beweistechniken, elementare Arithmetik, Prädikatenlogik und Mengen.

Diese Themen gehören nicht speziell zur linearen Algebra. Vielmehr werden sie in fast allen Bereichen der Mathematik verwendet. Für uns haben sie außerdem eine zweite Funktion: Sie geben einfache Beispiele, an denen wir üben können, wie mathematische Definitionen, Aussagen und Beweise formuliert werden.

Die eigentliche lineare Algebra beginnt in Kapitel 9.

Kapitel 1

Aussagenlogik

Dieses Kapitel ist eine kurze und eher informelle Einführung in die Sprache der Aussagenlogik. Wir behandeln zunächst ganze Aussagen nur danach, ob sie wahr oder falsch sind.

Das Ziel ist nicht, die Logik als eigenes mathematisches Forschungsgebiet vollständig aufzubauen (dafür gibt es andere Module). Das Ziel ist bescheidener: Wir wollen mathematische Sätze lesen, einfache logische Strukturen erkennen und zusammengesetzte Aussagen systematisch auswerten können.

1.1 Aussagen

In der Aussagenlogik interessiert uns zunächst nur, ob ein Satz wahr oder falsch ist. Wir ignorieren dabei sehr viel Inhalt. Das klingt grob, ist aber nützlich: Wenn wir wissen, wie sich die Wahrheitswerte einfacher Aussagen verhalten, können wir die Wahrheitswerte zusammengesetzter Aussagen systematisch berechnen.

Definition 1.1.1. Eine *Aussage* ist eine Äußerung, die genau einen der beiden Wahrheitswerte *wahr* oder *falsch* hat.

Wir schreiben häufig 1 für *wahr* und 0 für *falsch*. Dabei muss der Wahrheitswert nicht sofort bekannt sein. Eine Äußerung kann also eine Aussage sein, auch wenn wir nicht wissen, ob sie wahr oder falsch ist.

Beispiele 1.1.2. *Die folgenden Sätze sind Aussagen:*

(i) 2 *ist eine Primzahl.*

(ii) $2 + 2 = 5$.

(iii) Am 16.11.2022 war in Sachsen ein Feiertag.

> *(iv) Jede gerade natürliche Zahl $n > 2$ ist Summe zweier Primzahlen.*
>
> *Der erste Satz ist wahr, der zweite ist falsch. Beim dritten muss man den Kalender oder das Feiertagsrecht kennen. Der vierte Satz ist die Goldbach-Vermutung; ob er wahr oder falsch ist, ist nicht bekannt. Trotzdem ist es eine Aussage, weil er einen Wahrheitswert hat.*

Nicht jede Äußerung ist eine Aussage. Fragen, Befehle und Ausrufe sind keine Aussagen. Zum Beispiel sind "Hallo!", "Wie heißt du?" und "Bitte nehmen Sie Platz" keine Aussagen. Auch der Satz "Dieser Satz ist falsch" ist problematisch und wird in diesem Kurs nicht als normale Aussage behandelt, weil wir ihm nicht widerspruchsfrei einen Wahrheitswert zuordnen können.

Nehmen wir jetzt einen stark vereinfachten juristischen Satz:

Wenn Anton Mörder ist, dann bekommt Anton lebenslange Freiheitsstrafe.

Dieser Satz verbindet zwei einfachere Aussagen:

$A :=$ Anton ist Mörder,
$B :=$ Anton bekommt lebenslange Freiheitsstrafe.

Das Symbol $:=$ bedeutet, dass die linke Seite durch die rechte Seite definiert wird. In diesem Beispiel ist also A ab diesem Moment der Name für die Aussage "Anton ist Mörder".

Die Verbindung hat die Form "wenn A, dann B". In der Logik schreiben wir dafür $A \implies B$.

Ein anderes Beispiel ist:

Anton tötet heimtückisch oder Anton tötet aus Habgier.

Wenn wir

$C :=$ Anton tötet heimtückisch,
$D :=$ Anton tötet aus Habgier

setzen, dann hat dieser Satz die Form "C oder D". Dafür verwenden wir das Symbol $\vee$ und schreiben kurz $C \vee D$.

Der Punkt ist: Wir zerlegen kompliziertere Sätze in einfachere Aussagen und logische Verknüpfungen.

1.2 Junktoren

Für Aussagen verwenden wir oft Großbuchstaben $A, B, C, \ldots$. Wie wir oben gesehen haben, aus Aussagen können wir neue Aussagen mit logischen Verknüpfungen bauen. Die logischen Verknüpfungen heißen *Junktoren*.

Symbol	Name	Lesart
$\neg A$	Negation	nicht A
$A \wedge B$	Konjunktion	A und B
$A \vee B$	Disjunktion	A oder B
$A \implies B$	Implikation	wenn A, dann B
$A \iff B$	Äquivalenz	A genau dann, wenn B

Bei der Implikation $A \implies B$ heißt A die *Voraussetzung* oder *Vorbedingung*; B heißt die *Folgerung*. Man sagt auch: A impliziert B.

Bemerkung 1.2.1. Das Wort "oder" wird in der Mathematik normalerweise inklusiv verstanden. Die Aussage $A \vee B$ ist also auch dann wahr, wenn A und B beide wahr sind. Wenn man meint, dass genau eine der beiden Aussagen wahr sein soll, muss man dies ausdrücklich sagen.

Wenn die Wahrheitswerte von A und B gegeben sind, dann sind die Wahrheitswerte aller oben genannten Kombinationen durch die folgende Tabelle festgelegt.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \implies B$	$A \iff B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Die Zeile für die Implikation ist für viele am Anfang ungewohnt. Eine Implikation $A \implies B$ ist nur in einem Fall falsch: wenn A wahr und B falsch ist. Wenn A falsch ist, dann gilt $A \implies B$ in der formalen Logik automatisch.

Beispiel 1.2.2. *Betrachten wir den Satz:*

> *Falls es heute um 8 Uhr geregnet hat, dann habe ich einen Regenschirm dabei.*

Setzen wir $A :=$ "Es hat heute um 8 Uhr geregnet" und $B :=$ "Ich habe einen Regenschirm dabei". Wenn es um 8 Uhr nicht geregnet hat, dann ist die Implikation $A \implies B$ formal wahr, egal ob ich einen Regenschirm dabei habe oder nicht. Der Satz verspricht nur etwas für den Fall, dass A eintritt.

Beispiel 1.2.3. *Die Aussage*

> *Falls ich 200 cm groß bin, dann lebe ich auf dem Mars*

ist formal wahr, sofern ich nicht 200 cm groß bin. Das bedeutet nicht, dass es einen

sinnvollen inhaltlichen Zusammenhang zwischen Körpergröße und Wohnort gibt. Die formale Implikation bewertet nur die Wahrheitswerte von Voraussetzung und Folgerung.

1.3 Atome, Formeln und Wahrheitstabellen

Die Aussagen, aus denen wir beginnen, heißen *Atome*. Eine *Formel* ist eine Kombination von Atomen mit Junktoren. Beispiele sind

$$(A \wedge B) \vee C, \qquad (A \implies B) \vee (C \iff (B \wedge A)).$$

Wenn wir eine Formel auswerten wollen, müssen wir den Atomen Wahrheitswerte geben. Eine solche Zuweisung heißt eine *Belegung*. Danach berechnen wir den Wahrheitswert der ganzen Formel Schritt für Schritt.

Die übliche Rangfolge der Junktoren ist:

$$\neg, \quad \wedge, \quad \vee, \quad \implies, \quad \iff .$$

Das heißt: Negationen werden zuerst ausgeführt, danach Konjunktionen, danach Disjunktionen, danach Implikationen, danach Äquivalenzen. Klammern sind aber fast immer die bessere Lösung. Gerade am Anfang sollte man eher zu viele als zu wenige Klammern setzen.

Beispiel 1.3.1. *Wir betrachten*

$$F := ((A \vee B) \implies C) \wedge \neg B.$$

Für die Belegung $A = 0$, $B = 1$, $C = 0$ erhalten wir zuerst $A \vee B = 1$. Also ist $(A \vee B) \implies C$ gleich $1 \implies 0$, also 0. Außerdem ist $\neg B = 0$. Damit ist $F = 0 \wedge 0 = 0$.

Definition 1.3.2. Eine Formel heißt

(i) *tautologisch*, wenn sie für jede Belegung der Atome wahr ist;

(ii) *unerfüllbar* oder eine *Kontradiktion*, wenn sie für jede Belegung der Atome falsch ist;

(iii) *erfüllbar*, wenn sie für mindestens eine Belegung wahr ist;

(iv) *widerlegbar*, wenn sie für mindestens eine Belegung falsch ist.

Die direkteste Methode zur Untersuchung einer Formel ist die *Wahrheitstabelle*. Wenn eine Formel n verschiedene Atome enthält, dann gibt es 2^n mögliche Belegungen. Man listet alle Belegungen auf und berechnet für jede Belegung den Wahrheitswert der Formel.

Beispiel 1.3.3. *Die Formel* $(A \wedge B) \implies (A \vee B)$ *ist eine Tautologie.*

A	B	$A \wedge B$	$A \vee B$	$(A \wedge B) \implies (A \vee B)$
0	*0*	*0*	*0*	*1*
0	*1*	*0*	*1*	*1*
1	*0*	*0*	*1*	*1*
1	*1*	*1*	*1*	*1*

In der letzten Spalte steht nur der Wahrheitswert 1*. Also ist die Formel unabhängig von der Belegung wahr.*

1.4 Äquivalente Formeln

Definition 1.4.1. Zwei Formeln F und G heißen *äquivalent*, wenn sie für jede Belegung der Atome denselben Wahrheitswert haben.

Äquivalente Formeln drücken logisch dasselbe aus, auch wenn sie syntaktisch anders aussehen. Wenn Formeln F und G äquivalent sind, schreiben wir auch $F \equiv G$.

Beispiel 1.4.2. *Es gilt* $A \implies B \equiv \neg A \vee B$*. Wir vergleichen die Wahrheitstabellen:*

A	B	$A \implies B$	$\neg A \vee B$
0	*0*	*1*	*1*
0	*1*	*1*	*1*
1	*0*	*0*	*0*
1	*1*	*1*	*1*

Die beiden letzten Spalten stimmen überein. Diese Äquivalenz nennt man oft die Elimination der Implikation.

Für Formeln F und G gilt $F \equiv G$ genau dann, wenn $F \iff G$ eine Tautologie ist.

Einige Äquivalenzen werden ständig benutzt:

Äquivalenz	Name
$A \wedge B \equiv B \wedge A$	Kommutativität von $\wedge$
$A \vee B \equiv B \vee A$	Kommutativität von $\vee$
$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	Assoziativität von $\wedge$
$(A \vee B) \vee C \equiv A \vee (B \vee C)$	Assoziativität von $\vee$
$A \wedge (A \vee B) \equiv A$	Absorption
$A \vee (A \wedge B) \equiv A$	Absorption
$A \vee \neg A \equiv 1$	ausgeschlossenes Drittes
$A \wedge \neg A \equiv 0$	Widerspruch
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	De Morgan
$\neg(A \vee B) \equiv \neg A \wedge \neg B$	De Morgan
$A \implies B \equiv \neg A \vee B$	Elimination von $\implies$
$A \iff B \equiv (A \implies B) \wedge (B \implies A)$	Elimination von $\iff$
$A \wedge A \equiv A$	Idempotenz von $\wedge$
$A \vee A \equiv A$	Idempotenz von $\vee$
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	Distributivität
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$	Distributivität

Bemerkung 1.4.3. Die Formeln $(A \implies B) \implies C$ und $A \implies (B \implies C)$ sind nicht äquivalent. Zum Beispiel für $A = 0$, $B = 0$, $C = 0$ ist die erste Formel falsch, die zweite wahr. Bei Implikationen müssen Klammern also verwendet werden.

Substitutionsprinzip und Äquivalenzketten

Wenn $U \equiv U'$, dann darf man in einer größeren Formel eine Unterformel U durch U' ersetzen. Die neue Formel ist zur alten äquivalent. Dieses Prinzip nennt man das *Substitutionsprinzip*.

Beispiel 1.4.4. *Wir zeigen mit einer Äquivalenzkette, dass*

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

äquivalent zu $A \wedge (B \vee C)$ *ist:*

$$\begin{aligned}
((A \wedge B) \vee (A \wedge C)) \wedge A &\equiv (A \wedge (B \vee C)) \wedge A && \textit{Distributivität} \\
&\equiv A \wedge (A \wedge (B \vee C)) && \textit{Kommutativität von } \wedge \\
&\equiv (A \wedge A) \wedge (B \vee C) && \textit{Assoziativität von } \wedge \\
&\equiv A \wedge (B \vee C) && \textit{Idempotenz von } \wedge .
\end{aligned}$$

Beispiel 1.4.5. *Die Formel* $F := (A \implies B) \vee \neg B$ *ist eine Tautologie. Tatsächlich gilt*

$$\begin{aligned}
(A \implies B) \vee \neg B &\equiv (\neg A \vee B) \vee \neg B && \textit{Elimination von } \implies \\
&\equiv \neg A \vee (B \vee \neg B) && \textit{Assoziativität von } \vee \\
&\equiv \neg A \vee 1 && \textit{ausgeschlossenes Drittes} \\
&\equiv 1.
\end{aligned}$$

Kapitel 2

Beweise und elementare Arithmetik

In diesem Kapitel verwenden wir elementare Arithmetik als Übungsfeld für Beweise. Die Begriffe sind einfach genug, dass man die Rechnungen direkt sehen kann, aber sie reichen aus, um wichtige Beweisformen kennenzulernen: direkte Beweise, Kontraposition, Widerspruchsbeweise, Äquivalenzbeweise und Fallunterscheidungen.

Wir beginnen mit einer kurzen Einführung in die elementare Arithmetik. Danach besprechen wir die Beweisprinzipien ausdrücklich und veranschaulichen sie durch Beweise einiger arithmetischer Sätze.

2.1 Teilbarkeit und größter gemeinsamer Teiler

Diese Begriffe sind auch in der Informatik wichtig, insbesondere in der Kryptographie. Hier dienen sie vor allem als gutes Übungsfeld für Beweise.

Wir benutzen folgende Zahlenmengen:

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

Definition 2.1.1. Seien $a, b \in \mathbb{Z}$. Wir sagen, dass a die Zahl b *teilt*, und schreiben $a \mid b$, wenn es ein $k \in \mathbb{Z}$ mit $ak = b$ gibt.

Beispiel 2.1.2. *Es gilt* $3 \mid 12$*, denn* $12 = 3 * 4$*. Es gilt aber* $5 \nmid 12$*, denn es gibt keine ganze Zahl* k *mit* $5k = 12$*.*

Zwei einfache Eigenschaften der Teilbarkeit werden ständig benutzt.

Proposition 2.1.3. *Seien* $d, a, b \in \mathbb{Z}$*.*

(i) Falls $d \mid a$ *und* $d \mid b$*, dann* $d \mid a + b$*.*

(ii) Falls $d \mid a$, dann $d \mid ab$.

Beweis. (i) Aus $d \mid a$ und $d \mid b$ folgt, dass es $k, l \in \mathbb{Z}$ mit $a = dk$ und $b = dl$ gibt. Dann ist

$$a + b = dk + dl = d(k + l).$$

Da $k + l \in \mathbb{Z}$ gilt, folgt $d \mid a + b$.

(ii) Aus $d \mid a$ folgt, dass es $k \in \mathbb{Z}$ mit $a = dk$ gibt. Dann ist $ab = dkb = d(kb)$, und $kb \in \mathbb{Z}$. Also gilt $d \mid ab$. □

Division mit Rest und größter gemeinsamer Teiler

Für $a, b \in \mathbb{N}_+$ können wir b durch a mit Rest teilen:

$$b = qa + r,$$

wobei $q, r \in \mathbb{N}$ und $0 \leqslant r < a$ gilt. Die Zahl q heißt der Ganzzahlquotient, die Zahl r heißt der Rest. Zum Beispiel gilt

$$45 = 6 * 7 + 3.$$

Für ganze Zahlen kann man ebenfalls eine Division mit Rest formulieren. Wenn $a, b \in \mathbb{Z}$ und $a \neq 0$, dann schreiben wir $b = qa + r$ mit $q \in \mathbb{Z}$, $r \in \mathbb{N}$ und $0 \leqslant r < |a|$.

Definition 2.1.4. Seien $a, b \in \mathbb{N}_+$. Der *größte gemeinsame Teiler* von a und b ist die größte natürliche Zahl d mit $d \mid a$ und $d \mid b$. Wir bezeichnen ihn mit $\mathrm{ggT}(a, b)$.

Zum Beispiel gilt $\mathrm{ggT}(10, 17) = 1$ und $\mathrm{ggT}(49, 14) = 7$. Außerdem definieren wir $\mathrm{ggT}(0, a) = \mathrm{ggT}(a, 0) = a$ für $a \in \mathbb{N}$, insbesondere $\mathrm{ggT}(0, 0) = 0$. Für $a, b \in \mathbb{Z}$ setzen wir

$$\mathrm{ggT}(a, b) := \mathrm{ggT}(|a|, |b|).$$

Der Euklidische Algorithmus

Der größte gemeinsame Teiler wird mit dem Euklidischen Algorithmus berechnet. Man führt wiederholt Divisionen mit Rest durch, bis der Rest 0 auftritt. Der letzte von 0 verschiedene Rest ist der gesuchte größte gemeinsame Teiler.

Beispiel 2.1.5. *Wir berechnen* $\mathrm{ggT}(161, 119)$*:*

$$\begin{aligned} 161 &= 1 * 119 + 42, \\ 119 &= 2 * 42 + 35, \\ 42 &= 1 * 35 + 7, \\ 35 &= 5 * 7 + 0. \end{aligned}$$

Der letzte von 0 *verschiedene Rest ist* 7. *Also ist* $\mathrm{ggT}(161, 119) = 7$.

Der Algorithmus erklärt auch, warum dieser Rest wirklich der größte gemeinsame Teiler ist.

Wenn eine Zahl d sowohl 161 als auch 119 teilt, dann teilt sie auch $42 = 161 - 119$. Hier benutzen wir Proposition 2.1.3: Aus $d \mid 161$ und $d \mid 119$ folgt auch $d \mid (161 - 119)$.

Dann teilt d auch $35 = 119 - 2 * 42$.

Danach teilt sie $7 = 42 - 35$.

Also teilt jeder gemeinsame Teiler von 161 und 119 auch den letzten nichtverschwindenden Rest.

Diese Argumentation funktioniert genauso im Allgemeinen und liefert die folgende Eigenschaft.

Proposition 2.1.6. *Seien* $a, b \in \mathbb{Z}$. *Falls* $d \mid a$ *und* $d \mid b$, *dann gilt* $d \mid \mathrm{ggT}(a, b)$.

Satz 2.1.7 (Lemma von Bézout)**.** *Seien* $a, b \in \mathbb{Z}$. *Dann gibt es ganze Zahlen* $x, y \in \mathbb{Z}$ *mit*

$$ax + by = \mathrm{ggT}(a, b).$$

Beweis. Die Idee ist, im Euklidischen Algorithmus von unten nach oben zu gehen. Im Beispiel $a = 161$, $b = 119$ gilt

$$\begin{aligned} 7 &= 42 - 1 * 35 \\ &= 42 - 1 * (119 - 2 * 42) \\ &= 3 * 42 - 1 * 119 \\ &= 3 * (161 - 1 * 119) - 1 * 119 \\ &= 3 * 161 - 4 * 119. \end{aligned}$$

Damit haben wir eine Darstellung $7 = 161 * 3 + 119 * (-4)$ gefunden. Der allgemeine Fall funktioniert genauso: Jede Restgleichung kann nach dem Rest aufgelöst und dann rückwärts eingesetzt werden. □

2.2 Beweise und Beweisprinzipien

Viele mathematische Aussagen haben die Form $A \implies B$: Wenn die Voraussetzung A gilt, dann gilt die Folgerung B. Ein Beweis muss erklären, warum man aus A tatsächlich B schließen darf.

Direkter Beweis

Beim direkten Beweis nimmt man die Voraussetzung an und leitet daraus die Folgerung ab.

Beispiel 2.2.1. *Der Satz "Falls $d \mid a$ und $d \mid b$, dann $d \mid a + b$" wurde oben direkt bewiesen. Wir nahmen $d \mid a$ und $d \mid b$ an, schrieben $a = dk$ und $b = dl$, und erhielten daraus $a + b = d(k + l)$.*

Kontraposition

Die Formeln $A \implies B$ und $\neg B \implies \neg A$ sind äquivalent. Die zweite Formel heißt die *Kontraposition* der ersten.

Warum ist das richtig? Die Implikation $A \implies B$ ist genau dann falsch, wenn $A = 1$ und $B = 0$ gilt. Die Implikation $\neg B \implies \neg A$ ist genau dann falsch, wenn $\neg B = 1$ und $\neg A = 0$ gilt, also ebenfalls genau dann, wenn $B = 0$ und $A = 1$ gilt. Die beiden Formeln haben also in jeder Belegung denselben Wahrheitswert.

Beispiel 2.2.2. *Wir zeigen: Ist $n \in \mathbb{Z}$ und ist n^2 gerade, dann ist n gerade.*

Direkt wäre dieser Satz etwas unhandlich. Per Kontraposition zeigen wir stattdessen: Wenn n ungerade ist, dann ist n^2 ungerade.

Beweis. Sei n ungerade. Dann gibt es ein $k \in \mathbb{Z}$ mit $n = 2k + 1$. Also gilt

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Dies ist ungerade. Also ist die Kontraposition bewiesen, und damit auch der ursprüngliche Satz. □

Beweis durch Widerspruch

Beim *Beweis durch Widerspruch* wollen wir eine Aussage A zeigen. Wir nehmen stattdessen $\neg A$ an und leiten daraus einen Widerspruch her. Ein Widerspruch kann zum Beispiel eine Aussage der Form $B \wedge \neg B$ sein. Wenn $\neg A$ unmöglich ist, muss A gelten.

Satz 2.2.3. *Es gibt keine rationale Zahl x mit $x^2 = 2$.*

Beweis. Wir nehmen zum Widerspruch an, dass es eine rationale Zahl x mit $x^2 = 2$ gibt. Dann können wir $x = \frac{m}{n}$ mit teilerfremden ganzen Zahlen m, n und $n \neq 0$ schreiben. Aus $x^2 = 2$ folgt

$$\frac{m^2}{n^2} = 2,$$

also $m^2 = 2n^2$. Damit ist m^2 gerade. Nach dem oben bewiesenen Satz ist dann auch m gerade. Also gibt es ein $k \in \mathbb{Z}$ mit $m = 2k$.

Dann gilt

$$2n^2 = m^2 = (2k)^2 = 4k^2,$$

also $n^2 = 2k^2$. Damit ist auch n^2 gerade, und wieder folgt, dass n gerade ist.

Nun sind m und n beide gerade. Das widerspricht der Wahl von m und n als teilerfremde Zahlen. Also war die Annahme falsch, und es gibt keine rationale Zahl x mit $x^2 = 2$. □

In diesem Beweis war die Aussage A: "Es gibt keine rationale Zahl x mit $x^2 = 2$." Aus der Annahme $\neg A$ haben wir eine teilerfremde Darstellung $x = \frac{m}{n}$ erhalten. Der Widerspruch bestand darin, dass dieselben Zahlen m, n am Ende beide gerade sein mussten und also doch nicht teilerfremd sein konnten.

In echten Beweisen ist genau dies oft der schwierige Schritt: Man muss eine passende zusätzliche Aussage finden, an der der Widerspruch sichtbar wird.

Äquivalenzen beweisen

Um $A \iff B$ zu beweisen, beweist man meistens zwei Implikationen:

$$A \implies B \qquad \text{und} \qquad B \implies A.$$

Die Schreibweise $F \equiv G$ verwenden wir vor allem, wenn wir über die Äquivalenz von Formeln sprechen. In ausgeschriebenen mathematischen Sätzen verwenden wir dafür oft die Formulierung "genau dann, wenn", abgekürzt "gdw.". Zum Beispiel bedeutet der Satz "Eine ganze Zahl n ist gerade genau dann, wenn n^2 gerade ist" dasselbe wie:

$$n \text{ ist gerade} \implies n^2 \text{ ist gerade} \qquad \text{und} \qquad n^2 \text{ ist gerade} \implies n \text{ ist gerade}.$$

Beispiel 2.2.4. *Eine ganze Zahl n ist gerade genau dann, wenn n^2 gerade ist.*

Beweis. Die Richtung "wenn n^2 gerade ist, dann ist n gerade" wurde bereits per Kontraposition bewiesen.

Für die andere Richtung nehmen wir an, dass n gerade ist. Dann gibt es $k \in \mathbb{Z}$ mit $n = 2k$. Also gilt $n^2 = 4k^2 = 2(2k^2)$. Damit ist n^2 gerade. □

Fallunterscheidung

Bei einer *Fallunterscheidung* zerlegt man die Situation in mehrere mögliche Fälle. Wichtig sind zwei Punkte: Die Fälle müssen alle Möglichkeiten abdecken, und in jedem Fall muss die Behauptung wirklich bewiesen werden.

Beispiel 2.2.5. *Wir wollen zeigen: Für jedes $n \in \mathbb{Z}$ ist n^2 durch 3 teilbar oder lässt beim Teilen durch 3 den Rest 1. Jede ganze Zahl n hat eine der drei Formen $n = 3k$, $n = 3k+1$ oder $n = 3k+2$ mit $k \in \mathbb{Z}$. Ist $n = 3k$, dann ist $n^2 = 9k^2 = 3(3k^2)$ durch 3 teilbar. Ist $n = 3k+1$, dann ist $n^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$. Ist $n = 3k+2$, dann ist $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$. Damit sind alle Fälle abgedeckt.*

2.3 Modulare Arithmetik

Definition 2.3.1. Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}_+$. Wir sagen, dass a und b *kongruent modulo n* sind, und schreiben

$$a \equiv b \mod n,$$

wenn a und b beim Teilen durch n denselben Rest haben.

Zum Beispiel gilt

$$27 \equiv 7 \equiv 2 \mod 5, \qquad 113 \equiv 15 \mod 7, \qquad 2 \equiv -3 \mod 5.$$

Eine äquivalente Charakterisierung ist besonders nützlich:

$$a \equiv b \mod n \qquad \text{genau dann, wenn} \qquad n \mid a - b.$$

Die Begründung ist einfach: Wenn a und b beim Teilen durch n denselben Rest haben, dann ist ihre Differenz ein Vielfaches von n. Umgekehrt folgt aus $n \mid a - b$, dass a und b beim Teilen durch n denselben Rest haben.

Satz 2.3.2. *Seien $a, b, c, d \in \mathbb{Z}$ und $n \in \mathbb{N}_+$. Falls $a \equiv b \mod n$ und $c \equiv d \mod n$, dann gilt*

$$a + c \equiv b + d \mod n \qquad \textit{und} \qquad ac \equiv bd \mod n.$$

Beweis. Aus $a \equiv b \mod n$ und $c \equiv d \mod n$ folgt $n \mid a - b$ und $n \mid c - d$.

Für die Summe gilt

$$(a + c) - (b + d) = (a - b) + (c - d).$$

Nach Proposition 2.1.3 teilt n daher auch diese Summe. Also gilt $a + c \equiv b + d \mod n$.

Für das Produkt schreiben wir

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d).$$

Wieder teilt n beide Summanden auf der rechten Seite. Also gilt $n \mid ac - bd$ und damit $ac \equiv bd \mod n$. □

Beispiel 2.3.3. *Wir berechnen* $7^5 + 13^{20}$ *modulo* 5 *mit Hilfe von Satz 2.3.2. Nach Satz 2.3.2 dürfen wir dabei mit kongruenten Zahlen rechnen. Es gilt* $7 \equiv 2$ *und* $13 \equiv 3 \equiv -2 \mod 5$. *Also*

$$7^5 + 13^{20} \equiv 2^5 + 3^{20} \equiv 2^5 + (-2)^{20} \mod 5.$$

Nun ist $2^2 = 4 \equiv -1 \mod 5$. *Daher ist* $2^4 \equiv 1 \mod 5$, *also* $2^5 \equiv 2 \mod 5$. *Außerdem ist* $(-2)^{20} = 2^{20} = (2^4)^5 \equiv 1 \mod 5$. *Insgesamt erhalten wir*

$$7^5 + 13^{20} \equiv 2 + 1 \equiv 3 \mod 5.$$

Wir betrachten Beispiel 2.2.5 noch einmal, nun mit unserer neuen Kongruenznotation.

Satz 2.3.4. *Für jedes* $n \in \mathbb{Z}$ *gilt* $n^2 \equiv 0 \mod 3$ *oder* $n^2 \equiv 1 \mod 3$.

Beweis. Jede ganze Zahl ist modulo 3 kongruent zu genau einer der Zahlen 0, 1, 2. Wir betrachten diese drei Fälle.

Falls $n \equiv 0 \mod 3$, dann ist nach Satz 2.3.2 $n^2 \equiv 0^2 \equiv 0 \mod 3$.

Falls $n \equiv 1 \mod 3$, dann ist $n^2 \equiv 1^2 \equiv 1 \mod 3$.

Falls $n \equiv 2 \mod 3$, dann ist $n^2 \equiv 2^2 = 4 \equiv 1 \mod 3$.

Damit ist die Behauptung in allen Fällen bewiesen. □

Wir betrachten nun noch einige weitere Aussagen aus der Arithmetik, um zu sehen, wie die oben eingeführten Beweistechniken in der Praxis funktionieren.

Satz 2.3.5. *Sei* $n \in \mathbb{N}$, *und seien* $d_k \dots d_0$ *die Dezimalstellen von* n. *Dann gilt*

$$3 \mid n \quad \textit{genau dann, wenn} \quad 3 \mid d_0 + d_1 + \ldots + d_k.$$

Beweis. Wir können n als

$$n = d_0 + 10d_1 + 10^2 d_2 + \ldots + 10^k d_k = \sum_{i=0}^{k} d_i 10^i$$

schreiben. Da $10 \equiv 1 \mod 3$ gilt, folgt $10^i \equiv 1 \mod 3$ für jedes i. Also gilt

$$n \equiv d_0 + d_1 + \ldots + d_k \mod 3.$$

Daher ist n genau dann durch 3 teilbar, wenn die Summe $d_0 + d_1 + \ldots + d_k$ durch 3 teilbar ist. □

Satz 2.3.6. *Sei $n \in \mathbb{N}$. Falls $2^n - 1$ prim ist, dann ist n prim.*

Beweis. Wir beweisen die Kontraposition. Nehmen wir also an, dass n nicht prim ist. Dann können wir $n = ab$ mit $a, b > 1$ schreiben. Es gilt

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1.$$

Mit der Formel

$$x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \ldots + x + 1)$$

erhalten wir

$$2^n - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^a + 1).$$

Da $a > 1$ gilt, ist $2^a - 1 > 1$. Außerdem ist $2^a - 1 < 2^{ab} - 1 = 2^n - 1$. Somit hat $2^n - 1$ einen echten Teiler und ist nicht prim. Das beweist die Kontraposition. □

Satz 2.3.7. *Es gibt keine größte Primzahl.*

Beweis. Wir führen einen Beweis durch Widerspruch. Angenommen, es gäbe eine größte Primzahl. Dann könnten wir alle Primzahlen als

$$p_1, p_2, \ldots, p_k$$

auflisten. Betrachten wir nun

$$N := p_1 * p_2 * \ldots * p_k + 1.$$

Die Zahl N ist größer als 1, also besitzt sie einen Primteiler. Dieser Primteiler müsste einer der aufgelisteten Primzahlen sein, sagen wir p_i.

Aber N hat beim Teilen durch p_i den Rest 1, denn das Produkt $p_1 * \ldots * p_k$ ist durch p_i teilbar. Also kann p_i die Zahl N nicht teilen. Das ist ein Widerspruch. Folglich gibt es keine größte Primzahl. □

Kapitel 3

Prädikatenlogik

3.1 Prädikate und freie Variablen

Die Aussagenlogik behandelt ganze Aussagen als unteilbare Atome. Das reicht für viele mathematische Sätze nicht. Betrachten wir noch einmal den Satz:

> Für jede ganze Zahl n gilt: Falls n^2 gerade ist, dann ist n gerade.

Dieser Satz spricht über eine Variable n. Der Ausdruck "n^2 ist gerade" ist noch keine Aussage, solange n nicht festgelegt ist. Wenn wir aber $n = 5$ einsetzen, erhalten wir eine Aussage; ebenso für $n = 58$ oder $n = -3$.

Definition 3.1.1. Ein *Prädikat* ist eine Aussagenschablone mit Variablen. Sobald man konkrete Werte für die Variablen einsetzt, entsteht eine Aussage.

Beispiel 3.1.2. *Sei* Gerade(n) *das Prädikat "n ist gerade". Dann ist* Gerade(5) *eine falsche Aussage und* Gerade(8) *eine wahre Aussage.*

Sei QuadratGerade(n) *das Prädikat "n^2 ist gerade". Dann ist* QuadratGerade(5) *falsch und* QuadratGerade(8) *wahr.*

Meistens schreiben wir Prädikate nicht mit eigenen Namen wie QuadratGerade(n). Wir müssen aber erkennen, dass zum Beispiel der Ausdruck "$x^2 = 2$" ein Prädikat mit der freien Variable x ist. Insbesondere das Prädikat QuadratGerade(n) würden wir eher als "$2 \mid n^2$" schreiben.

3.2 Quantoren

Um aus Prädikaten Aussagen zu machen, können wir Quantoren benutzen.

Definition 3.2.1. Der *Allquantor* $\forall$ bedeutet "für alle". Der *Existenzquantor* $\exists$ bedeutet "es gibt mindestens ein".

Der *Grundbereich* gibt an, über welche Objekte die Variable laufen darf. In der Formel $\forall_{n\in\mathbb{Z}} F(n)$ ist der Grundbereich zum Beispiel die Menge $\mathbb{Z}$ der ganzen Zahlen. Die Aussage behauptet dann, dass $F(n)$ für jede ganze Zahl n gilt.

Wenn der Grundbereich nicht ausdrücklich angegeben ist, muss aus dem Kontext klar sein, über welche Objekte gesprochen wird.

Wir können zum Beispiel schreiben

$$\forall n \in \mathbb{Z}\,\big(\text{QuadratGerade}(n) \implies \text{Gerade}(n)\big).$$

Die Klammern sind hier wichtig: Der Allquantor bezieht sich auf die ganze Implikation. Im mathematischen Alltag würden wir dieselbe Aussage meist direkt mit Teilbarkeit schreiben:

$$\forall_{n\in\mathbb{Z}}\,\big(2 \mid n^2 \implies 2 \mid n\big).$$

Manchmal schreibt man den Grundbereich auch als eigenes Prädikat:

$$\forall n\,\big(n \in \mathbb{Z} \implies (\text{QuadratGerade}(n) \implies \text{Gerade}(n))\big).$$

In diesem Modul werden wir meistens den Grundbereich der Variablen direkt nach dem Quantor schreiben. Häufig schreiben wir die Variablen unter den Quantor, also zum Beispiel $\forall_{n\in\mathbb{Z}}$.

Häufig schreibt man in solchen Formeln ein Komma als Abkürzung für "und". Zum Beispiel

$$\exists_{x\in\mathbb{R}}\,(x > 0,\ x^2 = 2)$$

Beispiel 3.2.2. *Die Aussage "Es gibt keine rationale Zahl x mit $x^2 = 2$" kann man schreiben als*

$$\neg\big(\exists_{x\in\mathbb{Q}}\,(x^2 = 2)\big).$$

Äquivalent dazu ist

$$\forall_{x\in\mathbb{Q}}\,(x^2 \neq 2).$$

Negation von Quantoren

Die Negation von Quantoren folgt zwei einfachen Regeln:

$$\neg\forall_x F(x) \equiv \exists_x \neg F(x), \qquad \neg\exists_x F(x) \equiv \forall_x \neg F(x).$$

In Worten: "Nicht alle haben die Eigenschaft" heißt "mindestens eines hat die Eigenschaft nicht". Und "Es gibt keines mit der Eigenschaft" heißt "alle haben die Eigenschaft nicht".

Beispiel 3.2.3. *Die Negation von*

$$\forall_{n\in\mathbb{Z}} \big(\text{QuadratGerade}(n) \implies \text{Gerade}(n)\big)$$

ist

$$\exists_{n\in\mathbb{Z}} \neg\big(\text{QuadratGerade}(n) \implies \text{Gerade}(n)\big).$$

Da $P \implies Q$ genau dann falsch ist, wenn P wahr und Q falsch ist, ist dies äquivalent zu

$$\exists_{n\in\mathbb{Z}} \big(\text{QuadratGerade}(n) \wedge \neg\, \text{Gerade}(n)\big).$$

In Worten: Es gibt eine ganze Zahl n, deren Quadrat gerade ist, die selbst aber ungerade ist.

Mehrere Quantoren

Bei mehreren Quantoren ist die Reihenfolge wichtig. Zum Beispiel bedeutet

$$\forall_{n\in\mathbb{N}} \exists_{m\in\mathbb{N}} (m > n)$$

für jede natürliche Zahl gibt es eine größere natürliche Zahl. Dagegen bedeutet

$$\exists_{m\in\mathbb{N}} \forall_{n\in\mathbb{N}} (m > n),$$

dass es eine natürliche Zahl gibt, die größer als alle natürlichen Zahlen ist. Diese zweite Aussage ist falsch.

Wir können auch kompliziertere Sätze formalisieren. Zum Beispiel:

$$\forall_{n\in\mathbb{N}\setminus\{0,1\}} \exists_{p\in\mathbb{N}} \big(\text{Prim}(p) \wedge p \mid n\big).$$

Dies liest man als: Jede natürliche Zahl größer als 1 hat einen Primteiler.

Bemerkung 3.2.4. Man darf Variablennamen in getrennten Teilen einer Formel wiederverwenden, aber am Anfang ist das oft verwirrend. Statt

$$(\exists_x A(x)) \wedge (\forall_x (A(x) \implies B(x)))$$

kann man genauso gut

$$(\exists_x A(x)) \wedge (\forall_y (A(y) \implies B(y)))$$

schreiben. Inhaltlich ist das hier dasselbe, aber die zweite Version ist für Anfänger oft leichter zu lesen.

Aufeinanderfolgende Quantoren mit demselben Variablennamen, etwa $\forall_x \exists_x A(x, x)$, sollen in diesem Modul nicht verwendet werden.

Der Grund ist nicht, dass solche Ausdrücke formal völlig sinnlos wären, sondern dass sie sehr verwirrend sein können. Formal bindet der innere Quantor den Namen x

neu. Die beiden x in $A(x, x)$ gehören also zum inneren Quantor, nicht zum äußeren. Die Formel $\forall_x \exists_x A(x, x)$ ist also mit der Formel

$$\forall_x \exists_y A(y, y)$$

äquivalent. Der äußere Quantor hat dann in der eigentlichen Aussage keine sichtbare Variable mehr.

3.3 Beweisstrategien für Quantoren

Allquantor

Um eine Aussage der Form $\forall_{x \in X} F(x)$ zu beweisen, nimmt man ein beliebiges Element u des Grundbereichs X und zeigt $F(u)$. Das Wort *beliebig* ist wichtig: Man darf keine zusätzliche Eigenschaft von u annehmen, die nicht für alle Elemente des Grundbereichs gilt.

Existenzquantor

Um eine Aussage der Form $\exists_{x \in X} F(x)$ zu beweisen, muss man ein geeignetes Beispiel angeben oder konstruieren. Dann prüft man, dass dieses Beispiel die gewünschte Eigenschaft hat.

Beispiel 3.3.1. *Wir beweisen: Für jede natürliche Zahl existiert eine echt größere gerade natürliche Zahl.*

Formal:

$$\forall_{n \in \mathbb{N}} \exists_{m \in \mathbb{N}} (2 \mid m \wedge m > n).$$

Beweis. Sei $n \in \mathbb{N}$ beliebig. Wir definieren

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

Dann ist m durch 2 teilbar. Außerdem gilt

$$m - n = 2(n + 1) - n = n + 2 > 0.$$

Also ist $m > n$. Damit haben wir für ein beliebiges n ein passendes m konstruiert. □

Ein häufiger falscher Versuch wäre, $m := 2n$ zu setzen. Für $n = 0$ wäre dann $m = 0$ und nicht $m > n$. Der Fehler besteht darin, unbemerkt anzunehmen, dass $n > 0$ ist. Bei einem Beweis für alle $n \in \mathbb{N}$ ist das nicht zulässig, wenn $0 \in \mathbb{N}$ gilt.

Beispiel 3.3.2. *Betrachten wir für natürliche Zahlen x, y das Prädikat $A(x, y)$ mit der Bedeutung $x + y = 2x$. Dann gilt*

$$\forall_{x\in\mathbb{N}}\, \exists_{y\in\mathbb{N}}\, A(x, y).$$

Denn sei x beliebig. Wir wählen $y := x$. Dann ist $x + y = x + x = 2x$, also gilt $A(x, y)$.

Beispiel 3.3.3. *Für jedes $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, sodass für alle natürlichen Zahlen $n > N$ gilt: $\frac{1}{n} < \varepsilon$.*

Formal:

$$\forall_{\varepsilon>0}\, \exists_{N\in\mathbb{N}}\, \forall_{n\in\mathbb{N}}\, \big(n > N \implies \tfrac{1}{n} < \varepsilon\big).$$

Beweis. Sei $\varepsilon > 0$ beliebig. Wir wählen

$$N := \left\lceil \frac{1}{\varepsilon} \right\rceil.$$

Sei nun $n \in \mathbb{N}$ mit $n > N$. Dann gilt

$$\frac{1}{n} < \frac{1}{N} \leqslant \frac{1}{1/\varepsilon} = \varepsilon,$$

sofern $N > 0$ ist. Da $\varepsilon > 0$ gilt, ist $\lceil 1/\varepsilon \rceil \geqslant 1$, also ist dies erfüllt. Damit ist die Behauptung gezeigt. □

Kapitel 4

Mengenlehre

In diesem Kapitel führen wir die Sprache der Mengen ein. Diese Sprache ist eine der wichtigsten Grundsprachen der Mathematik. Alle mathematischen Objekte, die später in diesem Modul vorkommen, werden mit Hilfe von Mengen aufgebaut.

Der Schwerpunkt liegt hier nicht auf axiomatischer Mengenlehre. Wir wollen vor allem sicher mit der Notation und den Grundbegriffen umgehen können. Zum Beispiel: Was bedeutet $x \in M$? Was ist eine Teilmenge? Wie liest man Ausdrücke wie $M \cup N$ oder $M \cap N$?

4.1 Mengen und Elemente

Der Begriff einer Menge ist ein Grundbegriff. Das bedeutet: Wir definieren ihn in diesem Kurs nicht aus noch einfacheren Begriffen. Informell kann man an eine Menge als eine *Zusammenfassung von unterscheidbaren Objekten* denken.

Die Objekte, die in M enthalten sind, heißen *Elemente* von M. Wenn x ein Element von M ist, schreiben wir $x \in M$. Wenn x kein Element von M ist, schreiben wir $x \notin M$.

Beispiele 4.1.1. *Die folgenden Mengen werden in diesem Modul häufig vorkommen:*

(i) $\mathbb{N}$ *ist die Menge der natürlichen Zahlen. In diesem Modul gilt* $0 \in \mathbb{N}$.

(ii) $\mathbb{Z}$ *ist die Menge der ganzen Zahlen.*

(iii) $\mathbb{Q}$ *ist die Menge der rationalen Zahlen.*

(iv) $\mathbb{R}$ *ist die Menge der reellen Zahlen.*

Mengen können durch Aufzählung angegeben werden. Zum Beispiel ist $\{1, 2, 3\}$ die Menge, deren Elemente genau 1, 2 und 3 sind. Unvollständige Aufzählungen sind ebenfalls üblich, wenn das Muster klar ist, etwa

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}, \qquad \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Die *leere Menge* wird mit $\emptyset$ bezeichnet. Sie enthält keine Elemente. Die Menge $\{\emptyset\}$ ist dagegen nicht leer: Sie hat genau ein Element, nämlich die leere Menge.

Bemerkung 4.1.2. (i) Ein Element kann nicht mehrfach in einer Menge enthalten sein. Daher gilt $\{1, 1, 2\} = \{1, 2\}$.

(ii) Die Reihenfolge der Elemente spielt keine Rolle. Daher gilt $\{1, 2, 3\} = \{2, 3, 1\}$.

(iii) Eine Menge ist von ihren Elementen zu unterscheiden. Insbesondere gilt $\{3\} \neq 3$ und $\{\emptyset\} \neq \emptyset$.

Mengen können Elemente verschiedener Art enthalten. Zum Beispiel ist $\{\mathbb{R}, 2, \emptyset\}$ eine Menge mit drei Elementen: der Menge $\mathbb{R}$, der Zahl 2 und der leeren Menge.

Beispiel 4.1.3. *Sei*

$$M := \{\emptyset, \{\emptyset\}\}.$$

Dann gilt $\emptyset \in M$ und $\{\emptyset\} \in M$. Dagegen gilt $\{\{\emptyset\}\} \notin M$. Die Menge M hat genau zwei Elemente: eines davon ist $\emptyset$, das andere ist $\{\emptyset\}$.

Wenn wir $x, y, z \in M$ schreiben, bedeutet das nur, dass x, y und z Elemente von M sind. Es bedeutet nicht, dass x, y und z verschieden sein müssen. Es kann also durchaus $x = y = z$ gelten.

4.2 Gleichheit und Teilmengen

Zwei Mengen sind gleich, wenn sie dieselben Elemente enthalten.

Definition 4.2.1. Seien M und N Mengen. Dann gilt $M = N$, wenn für jedes Objekt x gilt:

$$x \in M \quad \text{genau dann, wenn} \quad x \in N.$$

Anders gesagt: Eine Menge ist vollständig durch ihre Elemente bestimmt. Es gibt z.B. genau eine leere Menge: Wenn zwei Mengen keine Elemente enthalten, dann enthalten sie genau dieselben Elemente, und sind daher gleich.

Definition 4.2.2. Seien M und N Mengen. Wir sagen, dass M eine *Teilmenge* von N ist, und schreiben $M \subseteq N$, wenn jedes Element von M auch ein Element von N ist. Formal:

$$M \subseteq N \quad \iff \quad \forall x\,(x \in M \implies x \in N).$$

Manchmal schreibt man auch $N \supseteq M$ und sagt, dass N eine Obermenge von M ist. Falls $M \subseteq N$ und $M \neq N$ gilt, heißt M eine *echte Teilmenge* von N. Dafür schreiben wir $M \subsetneq N$.

In diesem Modul bedeutet die Notation $\subset$ dasselbe wie $\subseteq$.

Für jede Menge M gilt $\emptyset \subseteq M$ und $M \subseteq M$. Die erste Aussage ist am Anfang ungewohnt: Sie ist wahr, weil es kein Element der leeren Menge gibt, das die Bedingung verletzen könnte.

Satz 4.2.3. *Für alle Mengen M und N gilt*

$$M = N \quad \Longleftrightarrow \quad M \subseteq N \text{ und } N \subseteq M.$$

Beweis. Angenommen zunächst $M = N$. Dann hat jedes Element von M auch die Eigenschaft, Element von N zu sein, also gilt $M \subseteq N$. Umgekehrt gilt genauso $N \subseteq M$.

Angenommen nun $M \subseteq N$ und $N \subseteq M$. Sei x ein beliebiges Objekt. Aus $x \in M$ folgt wegen $M \subseteq N$, dass $x \in N$. Aus $x \in N$ folgt wegen $N \subseteq M$, dass $x \in M$. Also gilt für jedes x: $x \in M$ genau dann, wenn $x \in N$. Daher gilt $M = N$. □

Dieser einfache Satz ist sehr wichtig: Um die Gleichheit zweier Mengen zu zeigen, zeigt man häufig beide Inklusionen.

4.3 Mengen durch Eigenschaften

Mengen hängen eng mit einstelligen Prädikaten zusammen. Ein einstelliges Prädikat ist eine Aussageform $P(x)$ mit einer Variablen. Sobald wir ein konkretes Objekt für x einsetzen, entsteht eine Aussage.

Wenn wir ein Prädikat $P(x)$ haben, können wir die Objekte, für die $P(x)$ wahr ist, zu einer Menge zusammenfassen. Man schreibt

$$\{x \colon P(x)\}$$

Das liest man als: die Menge aller x, für die $P(x)$ gilt. Eine andere Notation, die wir in diesem Modul nicht benutzen, lautet $\{x \mid P(x)\}$.

Oft geben wir zusätzlich einen Grundbereich an:

$$\{x \in \mathbb{Z} \colon P(x)\}\,.$$

Das bedeutet: Wir betrachten nur ganze Zahlen x, und nehmen genau diejenigen auf, für die $P(x)$ gilt.

Beispiele 4.3.1. *Es gilt*

$$\{n \in \mathbb{N} \colon 2 \mid n\} = \{n \in \mathbb{N} \colon \exists_{k \in \mathbb{N}}\, n = 2k\}\,.$$

Beide Mengen sind die Menge der geraden natürlichen Zahlen. Für jedes $n \in \mathbb{N}$ sind die Aussagen "$2 \mid n$" und "$\exists_{k \in \mathbb{N}}\, n = 2k$" äquivalent.

Ein weiteres Beispiel ist

$$\{a \in \mathbb{Z} \colon 3 \mid a,\ 7 \nmid a\}\,.$$

Das Komma in der Mengenbeschreibung bedeutet immer "und". Die Menge enthält also die ganzen Zahlen, die durch 3 *teilbar sind, aber nicht durch* 7*.*

Informell kann man sagen: Eine Teilmenge eines Grundbereichs U und ein einstelliges Prädikat auf U enthalten dieselbe Information. Zu einem Prädikat $P(x)$ gehört die Menge $\{x \in U \colon P(x)\}$. Umgekehrt gehört zu einer Menge $M \subseteq U$ das Prädikat $x \in M$.

Manchmal verwenden wir eine etwas freiere Notation. Zum Beispiel schreiben wir

$$\left\{a + b \in \mathbb{R} \colon a \in \mathbb{Q},\ b \in \left\{\sqrt{2}, \sqrt{3}\right\}\right\}.$$

Beispiele für Elemente dieser Menge sind $1 + \sqrt{2}$ und $\frac{2}{3} + \sqrt{3}$. Wenn wir dieselbe Menge sehr formal schreiben wollen, lautet sie

$$\left\{x \in \mathbb{R} \colon \exists a \in \mathbb{Q}\, \exists b \in \left\{\sqrt{2}, \sqrt{3}\right\}\ (x = a + b)\right\}.$$

4.4 Operationen auf Mengen

Seien M und N Mengen. Aus ihnen können wir neue Mengen bilden.

Definition 4.4.1. Die *Vereinigung* von M und N ist

$$M \cup N := \{x \colon x \in M \text{ oder } x \in N\}\,.$$

Der *Schnitt* von M und N ist

$$M \cap N := \{x \colon x \in M \text{ und } x \in N\}\,.$$

Die *Differenz* von M und N ist

$$M \setminus N := \{x \colon x \in M \text{ und } x \notin N\}\,.$$

Das Wort "oder" ist hier wieder inklusiv zu verstehen. Ein Element von $M \cup N$ darf also in M, in N oder in beiden Mengen liegen.

Wenn $M \cap N = \emptyset$ gilt, dann heißen M und N *disjunkt*. Sie haben dann kein gemeinsames Element.

Im Kontext von Mengenoperationen gibt es oft eine feste Grundmenge U, in der alle betrachteten Mengen enthalten sind. Wenn $M \subseteq U$ gilt, definieren wir das *Komplement* von M in U durch

$$M^{\mathrm{c}} := \{u \in U \colon u \notin M\} = U \setminus M.$$

Das Komplement hängt von der Grundmenge U ab. Wenn U nicht klar ist, muss man sie angeben.

Beispiel 4.4.2. *Sei* $U = \{1, 2, 3, 4, 5\}$ *und* $M = \{1, 3, 5\}$. *Dann gilt*

$$M^{\mathrm{c}} = \{2, 4\}.$$

Wenn wir stattdessen $U' = \{1, 2, 3, 4, 5, 6, 7\}$ *als Grundmenge nehmen, dann ist das Komplement von* M *gleich* $\{2, 4, 6, 7\}$.

4.5 Mengenoperationen und Logik

Die Operationen auf Mengen verhalten sich ähnlich wie die logischen Junktoren. Der Grund ist, dass Aussagen über Elemente von Mengen direkt in logische Aussagen übersetzt werden können:

$$\begin{aligned} x \in M \cup N &\iff (x \in M) \vee (x \in N), \\ x \in M \cap N &\iff (x \in M) \wedge (x \in N), \\ x \in M \setminus N &\iff (x \in M) \wedge \neg(x \in N). \end{aligned}$$

Die so entstehenden logischen Formeln können wir mit den logischen Äquivalenzen aus dem ersten Kapitel umformen. Auf diese Weise erhalten wir entsprechende Eigenschaften von Mengen. Das folgende Beispiel zeigt dieses Prinzip.

Satz 4.5.1 (Distributivität)**.** *Für alle Mengen* M, N *und* P *gilt*

$$M \cup (N \cap P) = (M \cup N) \cap (M \cup P).$$

Beweis. Wir zeigen die Gleichheit durch Vergleich der Elemente. Sei x beliebig. Dann gilt

$$\begin{aligned} x \in M \cup (N \cap P) &\iff (x \in M) \vee (x \in N \cap P) \\ &\iff (x \in M) \vee ((x \in N) \wedge (x \in P)) \\ &\iff ((x \in M) \vee (x \in N)) \wedge ((x \in M) \vee (x \in P)) \\ &\iff (x \in M \cup N) \wedge (x \in M \cup P) \\ &\iff x \in (M \cup N) \cap (M \cup P). \end{aligned}$$

Da dies für jedes x gilt, sind die beiden Mengen gleich. □

Die dritte Äquivalenz im obigen Beweis ist genau das Distributivgesetz aus der Aussagenlogik:

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

Mit derselben Technik erhält man viele grundlegende Rechenregeln für Mengen. Die folgende Tabelle fasst einige davon zusammen. Dabei seien M, N und P Teilmengen einer festen Grundmenge U.

Regel	Name
$M \cup N = N \cup M$	Kommutativität von $\cup$
$M \cap N = N \cap M$	Kommutativität von $\cap$
$(M \cup N) \cup P = M \cup (N \cup P)$	Assoziativität von $\cup$
$(M \cap N) \cap P = M \cap (N \cap P)$	Assoziativität von $\cap$
$M \cup M = M$	Idempotenz von $\cup$
$M \cap M = M$	Idempotenz von $\cap$
$M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$	Distributivität
$M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$	Distributivität
$M \cup \emptyset = M$	neutrales Element für $\cup$
$M \cap U = M$	neutrales Element für $\cap$
$M \cup M^{\mathrm{c}} = U$	Komplement
$M \cap M^{\mathrm{c}} = \emptyset$	Komplement
$(M^{\mathrm{c}})^{\mathrm{c}} = M$	doppeltes Komplement
$(M \cup N)^{\mathrm{c}} = M^{\mathrm{c}} \cap N^{\mathrm{c}}$	De Morgan
$(M \cap N)^{\mathrm{c}} = M^{\mathrm{c}} \cup N^{\mathrm{c}}$	De Morgan

Wie bei den Äquivalenzketten im ersten Kapitel können wir auch andere Eigenschaften von Mengen mit Hilfe dieser Grundregeln beweisen.

Satz 4.5.2. *Seien $M, N \subseteq U$. Dann gilt*

$$M \setminus N = (M^{\mathrm{c}} \cup N)^{\mathrm{c}}.$$

Beweis. Wir rechnen die rechte Seite schrittweise um. Zuerst benutzen wir die De-Morgan-Regel für das Komplement einer Vereinigung:

$$(M^{\mathrm{c}} \cup N)^{\mathrm{c}} = (M^{\mathrm{c}})^{\mathrm{c}} \cap N^{\mathrm{c}}.$$

Jetzt benutzen wir die Regel für das doppelte Komplement:

$$(M^{\mathrm{c}})^{\mathrm{c}} \cap N^{\mathrm{c}} = M \cap N^{\mathrm{c}}.$$

Schließlich verwenden wir die Definition des Komplements und die Definition der Mengendifferenz:

$$M \cap N^{\mathrm{c}} = \{x \colon x \in M \text{ und } x \notin N\} = M \setminus N.$$

Insgesamt erhalten wir also

$$(M^{\mathrm{c}} \cup N)^{\mathrm{c}} = M \setminus N.$$

Damit folgt die Behauptung. □

Für die spätere Verwendung geben wir auch der folgenden Eigenschaft einen Namen.

Satz 4.5.3 (Monotonie)**.** *Seien $M \subseteq M'$ und $N \subseteq N'$. Dann gilt*

$$M \cap N \subseteq M' \cap N'$$

und

$$M \cup N \subseteq M' \cup N'.$$

Beweis. Für die erste Inklusion sei $x \in M \cap N$. Dann gilt $x \in M$ und $x \in N$. Wegen $M \subseteq M'$ und $N \subseteq N'$ folgt $x \in M'$ und $x \in N'$. Also gilt $x \in M' \cap N'$.

Für die zweite Inklusion sei $x \in M \cup N$. Dann gilt $x \in M$ oder $x \in N$. Im ersten Fall folgt $x \in M'$; im zweiten Fall folgt $x \in N'$. Also gilt in jedem Fall $x \in M' \cup N'$. □

Zum Schluss benutzen wir den folgenden Satz, um eine weitere Beweistechnik zu besprechen. Wenn wir zeigen wollen, dass drei oder mehr Aussagen äquivalent sind, müssen wir nicht jede Aussage direkt mit jeder anderen vergleichen. Für Aussagen A, B und C genügt es zum Beispiel,

$$A \implies B, \qquad B \implies C, \qquad C \implies A$$

zu zeigen. Dann folgt aus jeder der drei Aussagen auch jede andere. Diese Beweisform nennt man einen *Ringschluss*.

Satz 4.5.4. *Für alle Mengen M und N sind die folgenden Aussagen äquivalent:*

(1) $M \subseteq N$.

(2) $M \cap N = M$.

(3) $M \cup N = N$.

Beweis. (1) $\implies$ (2): Angenommen $M \subseteq N$. Wenn $x \in M$, dann gilt auch $x \in N$, also $x \in M \cap N$. Daher gilt $M \subseteq M \cap N$. Umgekehrt gilt immer $M \cap N \subseteq M$ direkt nach der Definition des Schnittes. Zusammen folgt $M \cap N = M$.

(2) $\implies$ (3): Angenommen $M \cap N = M$. Wegen $M \cap N = M$ und $M \cap N \subseteq N$ folgt also $M \subseteq N$. Wegen $M \subseteq N$ und $N \subseteq N$ folgt aus Monotonie $M \cup N \subseteq N \cup N$. Mit Idempotenz erhalten wir $N \cup N = N$, also $M \cup N \subseteq N$. Die andere Inklusion $N \subseteq M \cup N$ gilt direkt nach der Definition der Vereinigung. Also ist $M \cup N = N$.

(3) $\implies$ (1): Angenommen $M \cup N = N$. Da immer $M \subseteq M \cup N$ gilt, folgt $M \subseteq N$. □

4.6 Verallgemeinerte Vereinigung und verallgemeinerter Schnitt

Bisher haben wir Vereinigung und Schnitt für zwei Mengen definiert. Oft wollen wir aber viele Mengen gleichzeitig vereinigen oder schneiden.

Sei I eine Menge, und sei für jedes $i \in I$ eine Menge M_i gegeben. Dann definieren wir

$$\bigcup_{i \in I} M_i := \{x \colon \exists i \in I \, (x \in M_i)\}$$

und

$$\bigcap_{i \in I} M_i := \{x \colon \forall i \in I \, (x \in M_i)\} \, .$$

Die Menge I heißt *Indexmenge*.

Beispiel 4.6.1. *Für jede Menge M gilt*

$$M = \bigcup_{m \in M} \{m\} \, .$$

Jedes Element von M liegt in seiner Einermenge $\{m\}$, und die Vereinigung all dieser Einermengen gibt genau M zurück.

Beispiel 4.6.2. *Es gilt*

$$\mathbb{R}_+ = \bigcup_{n \in \mathbb{N}_+} \left[\frac{1}{n}, n\right] ,$$

wobei $\mathbb{R}_+$ die Menge der positiven reellen Zahlen bezeichnet, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ gilt, und $[a, b] = \{x \in \mathbb{R} \colon a \leqslant x \leqslant b\}$. Jede positive reelle Zahl liegt in einem Intervall dieser Form: Für ein hinreichend großes n gilt zugleich $\frac{1}{n} \leqslant x$ und $x \leqslant n$.

Wenn $I = \{u, u+1, \ldots, o\} \subseteq \mathbb{N}$ ist, schreibt man häufig

$$\bigcup_{i=u}^{o} M_i \quad \text{und} \quad \bigcap_{i=u}^{o} M_i.$$

Das ist nur eine Notationsvariante für die Vereinigung oder den Schnitt über alle Indizes i von u bis o.

Bemerkung 4.6.3. Für eine Menge $\mathcal{F}$, deren Elemente selbst Mengen sind, schreiben wir auch

$$\bigcup \mathcal{F} := \bigcup_{A \in \mathcal{F}} A.$$

Entsprechend schreibt man

$$\bigcap \mathcal{F} := \bigcap_{A \in \mathcal{F}} A.$$

Ein Beispiel ist

$$\bigcap \{\{1,3,5\},\{1,2,3\},\{2,3,5\}\} = \{3\}.$$

Bemerkung 4.6.4. Die leere Vereinigung ist unproblematisch:

$$\bigcup_{i\in\emptyset} M_i = \emptyset.$$

Der leere Schnitt braucht dagegen eine feste Grundmenge U. Innerhalb einer solchen festen Grundmenge U setzt man

$$\bigcap_{i\in\emptyset} M_i = U.$$

Ohne Grundmenge ist dieser Ausdruck nicht definiert.

4.7 Endliche Mengen und Kardinalität

Eine Menge ist entweder endlich oder unendlich. Für eine endliche Menge M schreiben wir $|M|$ für die Anzahl ihrer Elemente. Diese Zahl heißt die *Kardinalität* von M. Für unendliche Mengen schreiben wir manchmal informell $|M| = \infty$.

Für endliche Mengen gilt stets

$$|M \cup N| \leqslant |M| + |N|.$$

Wenn M und N disjunkt sind, dann gilt sogar

$$|M \cup N| = |M| + |N|.$$

Beispiele 4.7.1. *Es gilt*

$$|\{1,2,3\} \cup \{2,4,6\}| = 5 < 6 = 3 + 3.$$

Hier überlappen die Mengen, denn 2 *liegt in beiden Mengen.*

Dagegen gilt

$$|\{1,2,3\} \cup \{4,5,6\}| = 6 = 3 + 3,$$

weil die beiden Mengen disjunkt sind.

4.8 Potenzmenge

Definition 4.8.1. Für eine Menge M ist die *Potenzmenge* $\mathcal{P}(M)$ die Menge aller Teilmengen von M:

$$\mathcal{P}(M) := \{N \colon N \subseteq M\}\,.$$

Beispiele 4.8.2. *Es gilt*

$$\mathcal{P}(\emptyset) = \{\emptyset\}\,.$$

Die leere Menge hat genau eine Teilmenge, nämlich sich selbst.

Für $M = \{1, 2, 3\}$ *gilt*

$$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}\,.$$

Außerdem gilt

$$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}\,.$$

Wenn M endlich ist, dann gilt

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

Der intuitive Grund ist einfach: Um eine Teilmenge $S \subseteq M$ festzulegen, treffen wir für jedes Element $x \in M$ genau eine von zwei Entscheidungen: $x \in S$ oder $x \notin S$. Wenn M genau n Elemente hat, gibt es daher 2^n Möglichkeiten. Im nächsten Kapitel beweisen wir diese Aussage genau mit vollständiger Induktion.

4.9 Mengen als Bausteine

Alles in der modernen Mathematik kann mit Hilfe von Mengen aufgebaut werden. Ein klassisches Beispiel ist die mengentheoretische Konstruktion der natürlichen Zahlen:

$$0 := \emptyset, \qquad 1 := \{0\}\,, \qquad 2 := \{0, 1\}\,, \qquad 3 := \{0, 1, 2\}\,, \quad \ldots$$

Diese Konstruktion ist konzeptionell interessant, aber in diesem Modul - und fast überall in Mathematik - werden wir mit natürlichen Zahlen wie gewohnt rechnen.

Eine Analogie aus der Informatik kann hier hilfreich sein. Ein Computer arbeitet auf sehr niedriger Ebene mit Bits und einfachen Operationen. Trotzdem müssen wir nicht bei jedem Programm darüber nachdenken, wie die Bits im Inneren manipuliert werden. Ähnlich kann man in der Mathematik alles aus Mengen konstruieren, ohne diese Konstruktionen ständig auszupacken.

Kapitel 5

Vollständige Induktion

5.1 Summenschreibweise

Im vorherigen Kapitel haben wir verallgemeinerte Vereinigungen kennengelernt. Statt viele Mengen einzeln zu schreiben, konnten wir zum Beispiel

$$\bigcup_{i=1}^{4} M_i$$

schreiben. Das steht für

$$M_1 \cup M_2 \cup M_3 \cup M_4.$$

Für Summen gibt es eine ganz ähnliche Notation. Statt viele Summanden einzeln zu schreiben, verwenden wir das Summenzeichen $\sum$.

Für Zahlen $a_1, a_2, \ldots, a_n$ bedeutet

$$\sum_{i=1}^{n} a_i$$

die Summe

$$a_1 + a_2 + \ldots + a_n.$$

Die Variable i heißt dabei der *Index* der Summe. Sie läuft von der unteren Grenze 1 bis zur oberen Grenze n.

Beispiele 5.1.1. *Es gilt*

$$\sum_{i=1}^{4} i = 1 + 2 + 3 + 4 = 10.$$

Außerdem gilt

$$\sum_{i=0}^{3} i^2 = 0^2 + 1^2 + 2^2 + 3^2 = 14.$$

Auch gilt

$$\sum_{k=1}^{4}(2k-1) = 1+3+5+7 = 16.$$

Für eine konstante Folge gilt zum Beispiel

$$\sum_{i=1}^{5} 7 = 7+7+7+7+7 = 35.$$

Die untere Grenze muss nicht 0 oder 1 sein. Zum Beispiel gilt

$$\sum_{i=3}^{6} i = 3+4+5+6 = 18.$$

Der Indexname ist nur ein Platzhalter. Zum Beispiel gilt

$$\sum_{i=1}^{4} i^2 = \sum_{k=1}^{4} k^2 = 1^2+2^2+3^2+4^2.$$

Eine Summe, bei der die obere Grenze kleiner als die untere Grenze ist, heißt eine leere Summe. In diesem Modul setzen wir eine leere Summe gleich 0.

5.2 Die Idee der Induktion

Viele mathematische Aussagen betreffen alle natürlichen Zahlen. Ein typisches Beispiel ist

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \qquad \text{für alle } n \in \mathbb{N}.$$

Man kann diese Aussage für $n = 0$, $n = 1$, $n = 2$ und viele weitere Werte überprüfen. Das reicht aber nicht als Beweis, denn es bleiben immer noch unendlich viele natürliche Zahlen übrig.

Die vollständige Induktion ist eine Beweismethode, mit der man Aussagen über alle natürlichen Zahlen beweisen kann. Die Idee ist wie bei einer unendlichen Reihe von Dominosteinen: Wenn der erste Stein fällt und jeder Stein den nächsten umstößt, dann fallen alle Steine.

Prinzip der vollständigen Induktion. Sei $F(n)$ ein Prädikat über natürliche Zahlen. Angenommen, es gelten die folgenden beiden Aussagen:

(i) $F(0)$ ist wahr.

(ii) Für jedes $n \in \mathbb{N}$ gilt $F(n) \implies F(n+1)$.

Dann gilt $F(n)$ für alle $n \in \mathbb{N}$.

In der Praxis funktioniert ein solcher Beweis folgendermaßen. Zuerst beweisen wir die gewünschte Aussage für $n = 0$. Dieser Teil heißt *Induktionsanfang*. Dann wählen wir eine feste natürliche Zahl n und nehmen an, dass die gewünschte Aussage für dieses n gilt. Diese Annahme heißt *Induktionshypothese*. Danach formulieren wir, was wir für $n + 1$ zeigen wollen. Diese Aussage heißt *Induktionsbehauptung*. Zum Schluss beweisen wir die Induktionsbehauptung *mit Hilfe der Induktionshypothese*.

In diesem Modul müssen Induktionsbeweise diese Teile klar markieren, so wie in den Beispielen unten. Wenn diese Markierungen in einer Klausur fehlen, kostet das Punkte.

Bemerkung 5.2.1. Der letzte Teil, also der Beweis der Induktionsbehauptung aus der Induktionshypothese, heißt *Induktionsschritt*. Dieses Wort muss aber in diesem Modul nicht ausdrücklich verwendet werden; wichtig sind vor allem die klare Markierung von Induktionsanfang, Induktionshypothese und Induktionsbehauptung sowie die Stelle im Beweis, an der die Induktionshypothese verwendet wurde.

Normalerweise schreibt man in einem Induktionsbeweis nicht ausdrücklich hin, was das Prädikat $F(n)$ ist. Das ist meistens aus dem Kontext klar. In den folgenden Beispielen machen wir es trotzdem gelegentlich, damit man leichter erkennt, wie das abstrakte Prinzip der vollständigen Induktion mit dem konkreten Beweis zusammenhängt.

5.3 Beispiel: die Summe der ersten n Zahlen

Satz 5.3.1. *Für alle $n \in \mathbb{N}$ gilt*

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

Beweis. Wir beweisen die Aussage durch vollständige Induktion über n. Genauer betrachten wir das Prädikat

$$F(n): \quad \sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Induktionsanfang. Für $n = 0$ gilt

$$\sum_{i=0}^{0} i = 0 = \frac{0 * 1}{2}.$$

Also gilt die Behauptung für $n = 0$.

Sei $n \in \mathbb{N}$. Wir nehmen an, dass die folgende *Induktionshypothese* gilt:

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

Wir möchten jetzt die folgende *Induktionsbehauptung* zeigen:

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

Beweis der Induktionsbehauptung. Wir rechnen

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^{n} i + (n+1) \\ &\overset{\text{IH}}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

Dabei wurde in der zweiten Zeile die Induktionshypothese verwendet. Nach dem Prinzip der vollständigen Induktion gilt die Behauptung für alle $n \in \mathbb{N}$. □

5.4 Die Potenzmenge einer endlichen Menge

Wir beweisen nun die Formel über Potenzmengen aus dem vorherigen Kapitel.

Satz 5.4.1. *Wenn M eine endliche Menge ist, dann gilt*

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

Beweis. Wir führen vollständige Induktion über $n = |M|$. Genauer beweisen wir für jedes $n \in \mathbb{N}$ die Aussage:

$$F(n): \quad \text{Für jede Menge } M \text{ mit } |M| = n \text{ gilt } |\mathcal{P}(M)| = 2^n.$$

Induktionsanfang. Sei M eine Menge mit $|M| = 0$. Dann ist $M = \emptyset$. Es gilt $\mathcal{P}(\emptyset) = \{\emptyset\}$, also

$$|\mathcal{P}(M)| = 1 = 2^0.$$

Sei $n \in \mathbb{N}$. Wir nehmen an, dass die folgende *Induktionshypothese* gilt: Für jede Menge N mit $|N| = n$ gilt

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

Wir möchten jetzt die folgende *Induktionsbehauptung* zeigen: Für jede Menge M mit $|M| = n + 1$ gilt

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

Beweis der Induktionsbehauptung. Sei also M eine Menge mit $|M| = n + 1$. Dann ist M nicht leer. Wir wählen ein Element $x \in M$ und setzen

$$N := M \setminus \{x\}.$$

Dann gilt $|N| = n$.

Wir teilen nun alle Teilmengen von M in zwei Klassen ein:

(a) Teilmengen, die x nicht enthalten,

(b) Teilmengen, die x enthalten.

Die Teilmengen aus (a) sind genau die Teilmengen von N, also die Elemente von $\mathcal{P}(N)$.

Um die zweite Klasse zu verstehen, betrachten wir kurz ein konkretes Beispiel. Für $M = \{1, 2, 3\}$ und $x = 3$ ist $N = \{1, 2\}$. Die Teilmengen von M, die 3 nicht enthalten, sind

$$\emptyset, \quad \{1\}, \quad \{2\}, \quad \{1, 2\}.$$

Die Teilmengen, die 3 enthalten, sind

$$\{3\}, \quad \{1, 3\}, \quad \{2, 3\}, \quad \{1, 2, 3\}.$$

Die zweite Liste entsteht aus der ersten, indem man überall das Element 3 hinzufügt.

Im Allgemeinen entstehen die Teilmengen aus (b) genauso: Wir nehmen eine Teilmenge $S \subseteq N$ und fügen das Element x hinzu. Sie haben also die Form $S \cup \{x\}$ mit $S \in \mathcal{P}(N)$.

Daher ist

$$\mathcal{P}(M) = \mathcal{P}(N) \cup \{S \cup \{x\} : S \in \mathcal{P}(N)\}.$$

Diese beiden Mengen sind disjunkt. Außerdem haben sie gleich viele Elemente: Aus jeder Teilmenge S von N entsteht genau eine Teilmenge $S \cup \{x\}$ der zweiten Klasse. Umgekehrt erhält man aus jeder Teilmenge der zweiten Klasse wieder genau eine Teilmenge von N, indem man das Element x entfernt. Also folgt

$$|\mathcal{P}(M)| = |\mathcal{P}(N)| + |\mathcal{P}(N)| = 2\,|\mathcal{P}(N)|.$$

Mit der Induktionshypothese erhalten wir

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

Nach dem Prinzip der vollständigen Induktion gilt die Behauptung für alle endlichen Mengen. □

5.5 Induktion mit anderem Startwert

Der Induktionsanfang muss nicht immer bei 0 liegen. Manchmal möchten wir eine Aussage nur für alle natürlichen Zahlen ab einem bestimmten Startwert beweisen.

Induktion ab einem Startwert. Sei $m \in \mathbb{N}$, und sei $F(n)$ ein Prädikat über natürliche Zahlen $n \geqslant m$. Angenommen, es gelten:

(i) $F(m)$ ist wahr.

(ii) Für jedes $n \geqslant m$ gilt $F(n) \implies F(n+1)$.

Dann gilt $F(n)$ für alle $n \in \mathbb{N}$ mit $n \geqslant m$.

Satz 5.5.1. *Für alle $n \in \mathbb{N}$ mit $n \geqslant 16$ gilt*

$$n^3 < 2^n.$$

Beweis. Wir beweisen die Aussage durch vollständige Induktion ab 16. Genauer betrachten wir für $n \geqslant 16$ das Prädikat

$$F(n): \quad n^3 < 2^n.$$

Zunächst benötigen wir eine kleine Abschätzung. Für alle $n \geqslant 16$ gilt

$$\left(\frac{n+1}{n}\right)^3 < 2.$$

Für $n \geqslant 16$ gilt nämlich $\frac{1}{n} \leqslant \frac{1}{16}$, also

$$\frac{n+1}{n} = 1 + \frac{1}{n} \leqslant 1 + \frac{1}{16} = \frac{17}{16}.$$

Damit genügt es, die rechte Seite abzuschätzen:

$$\left(\frac{17}{16}\right)^3 < \left(\frac{6}{5}\right)^3 = \frac{216}{125} < 2.$$

Induktionsanfang. Für $n = 16$ gilt

$$16^3 = 2^{12} < 2^{16}.$$

Sei $n \in \mathbb{N}$ mit $n \geqslant 16$. Wir nehmen an, dass die folgende *Induktionshypothese* gilt:

$$n^3 < 2^n.$$

Wir möchten jetzt die folgende *Induktionsbehauptung* zeigen:

$$(n+1)^3 < 2^{n+1}.$$

Beweis der Induktionsbehauptung. Wir schreiben

$$(n+1)^3 = n^3 \left(\frac{n+1}{n}\right)^3.$$

Mit der Induktionshypothese erhalten wir

$$(n+1)^3 < 2^n \left(\frac{n+1}{n}\right)^3.$$

Wegen der Abschätzung oben ist der zweite Faktor kleiner als 2. Also folgt

$$(n+1)^3 < 2^n * 2 = 2^{n+1}.$$

Damit ist die Induktionsbehauptung bewiesen, und die Behauptung folgt. □

Kapitel 6

Relationen

In den ersten Kapiteln haben wir Aussagen, Beweise, Mengen und Induktion eingeführt. In diesem Kapitel benutzen wir diese Sprache, um mathematische Strukturen aus Mengen aufzubauen.

Alle mathematischen Strukturen können in der modernen Mathematik letztlich mit Hilfe von Mengen beschrieben werden. Zum Beispiel kann man auch die natürlichen Zahlen selbst mengentheoretisch definieren, etwa durch $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$ und so weiter. Im mathematischen Alltag verwendet man aber meistens nicht diese interne Konstruktion, sondern arbeitet mit den dadurch bereitgestellten Begriffen.

Der wichtigste neue Begriff ist der Begriff einer Relation. Relationen sind sehr flexibel. Sie können ausdrücken, dass eine Zahl kleiner als eine andere ist, dass zwei Menschen befreundet sind, dass zwei Wörter gleich lang sind, dass eine Zahl eine andere teilt, oder dass zwei Mengen dieselbe Anzahl von Elementen haben. Auch Funktionen sind, aus mengentheoretischer Sicht, spezielle Relationen.

Um Relationen definieren zu können, beginnen wir zuerst mit geordneten Paaren und kartesischen Produkten.

6.1 Geordnete Paare

Bei Mengen spielt die Reihenfolge keine Rolle: Es gilt zum Beispiel $\{1, 2\} = \{2, 1\}$. Für viele mathematische Konstruktionen brauchen wir aber Objekte, bei denen die Reihenfolge eine Rolle spielt.

Definition 6.1.1. Ein *geordnetes Paar* besteht aus zwei Objekten in einer bestimmten Reihenfolge. Wir schreiben es als (a, b).

Die entscheidende Eigenschaft geordneter Paare ist:

$$(a, b) = (c, d) \quad \Longleftrightarrow \quad a = c \text{ und } b = d.$$

Diese Eigenschaft ist der Grund, warum die Klammern rund sind und warum die Reihenfolge wichtig ist. Im Allgemeinen ist (a, b) dasselbe wie (b, a) genau dann wenn $a = b$. Z.B. gilt es $(2, 5) \neq (5, 2)$.

Man kann geordnete Paare in der Mengenlehre selbst durch Mengen definieren, zum Beispiel durch die Kuratowski-Definition

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Bemerkung 6.1.2. Man kann die Kuratowski-Definition als eine Art *Implementierung* des geordneten Paares verstehen. Sie ist wichtig, wenn man wissen möchte, wie geordnete Paare vollständig aus Mengen aufgebaut werden können. Im normalen mathematischen Alltag interessiert uns aber meistens nicht diese interne Konstruktion, sondern nur die Schnittstelle:

$$(a, b) = (c, d) \quad \Longleftrightarrow \quad a = c \text{ und } b = d.$$

In diesem Modul werden wir geordnete Paare daher über diese Gleichheitsregel verwenden.

6.2 Kartesische Produkte

Definition 6.2.1. Seien M und N Mengen. Das *kartesische Produkt* von M und N ist

$$M \times N := \{(m, n) \colon m \in M,\ n \in N\}.$$

Das kartesische Produkt ist also die Menge aller geordneten Paare, bei denen das erste Element aus M kommt und das zweite Element aus N kommt.

Beispiel 6.2.2. *Sei $M = \{1, 2, 3\}$ und $N = \{1, 3\}$. Dann ist*

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

Dagegen ist

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

Diese beiden Mengen sind nicht gleich.

Es gilt also $M \times N \neq N \times M$, außer wenn $M = N$ oder wenn eine der Mengen leer ist.

Beispiel 6.2.3. *Wir können $\mathbb{R} \times \mathbb{R}$ als die Menge aller Punkte in der Ebene auffassen. Das Paar (x, y) beschreibt dann den Punkt mit entsprechenden Koordinaten.*

Kartesische Produkte können auch mit mehr als zwei Faktoren gebildet werden. Man schreibt dann zum Beispiel

$$M \times N \times P = \{(m, n, p) \colon m \in M,\ n \in N,\ p \in P\}\,.$$

Ein Element davon ist ein geordnetes Tripel.

6.3 Relationen

Definition 6.3.1. Seien M und N Mengen. Eine *Relation* R von M nach N ist eine Teilmenge

$$R \subseteq M \times N.$$

Wenn $M = N$ gilt, nennen wir R auch eine Relation auf M.

Eine Relation entscheidet also, welche Paare (m, n) aus $M \times N$ in einer bestimmten Beziehung stehen.

Statt $(m, n) \in R$ schreiben wir häufig

$$m\ R\ n.$$

Wenn aus dem Kontext klar ist, welche Relation gemeint ist, schreiben wir auch $m \sim n$. Wenn das Paar nicht in der Relation liegt, schreiben wir $(m, n) \notin R$ oder sagen, dass nicht $m\ R\ n$ gilt.

Ein Relationszeichen bindet stärker als die logischen Junktoren. Die Aussage

$$x \sim y \vee y \sim x$$

bedeutet also

$$(x \sim y) \vee (y \sim x).$$

Beispiele 6.3.2. *(i) Die leere Relation $\emptyset \subseteq M \times N$ ist eine Relation von M nach N.*

(ii) Die volle Relation $M \times N$ ist ebenfalls eine Relation von M nach N.

(iii) Auf jeder Menge M gibt es die Identitätsrelation

$$\mathrm{id}_M := \{(m, m) \colon m \in M\}\,.$$

(iv) Die Relation $\leq$ auf $\mathbb{N}$ ist die Menge

$$\{(m, n) \in \mathbb{N} \times \mathbb{N} \colon m \leq n\}\,.$$

(v) Die Teilmengenrelation $\subseteq$ ist eine Relation auf $\mathcal{P}(M)$.

(vi) Die Teilbarkeitsrelation auf $\mathbb{N}$ *ist gegeben durch*

$$m \mid n \quad \Longleftrightarrow \quad \exists_{k\in\mathbb{N}}\, n = mk.$$

Bemerkung 6.3.3. Relationen müssen nicht symmetrisch sein. Aus $m \leq n$ folgt im Allgemeinen nicht $n \leq m$. Bei der Freundschaftsrelation auf Facebook würde man dagegen erwarten, dass aus "x ist befreundet mit y" auch "y ist befreundet mit x" folgt. Solche Unterschiede werden durch Eigenschaften von Relationen beschrieben.

Beispiel 6.3.4. *Sei* $M = \{1, 2, 3\}$ *und sei* R *die Relation auf* M *mit*

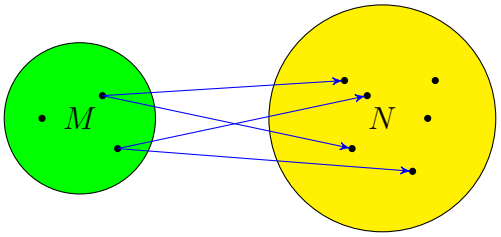
$$R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}.$$

Dann gilt zum Beispiel $1\ R\ 2$ *und* $3\ R\ 1$*, aber nicht* $2\ R\ 1$*. Diese Relation kann man als gerichteten Graphen darstellen: Die Elemente von* M *sind die Knoten, und für jedes Paar* $(x, y) \in R$ *zeichnen wir einen Pfeil von* x *nach* y*.*

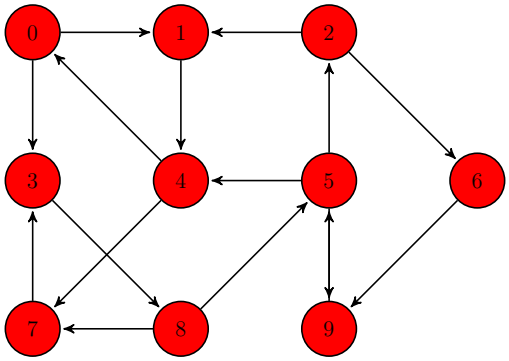
6.4 Darstellungen von Relationen

Relationen werden häufig als gerichtete Graphen dargestellt. Die Knoten sind die Elemente der beteiligten Mengen, und gerichtete Pfeile repräsentieren die Relation.

Wenn R eine Relation von M nach N ist, zeichnen wir die Elemente von M und die Elemente von N oft getrennt. Ein Pfeil von $m \in M$ nach $n \in N$ bedeutet dann, dass $m\ R\ n$ gilt.



Wenn R eine Relation auf einer Menge M ist, dann sind Start- und Zielmenge dieselbe Menge. Dann zeichnet man nur eine Knotenmenge und Pfeile zwischen diesen Knoten.



6.5 Eigenschaften von Relationen

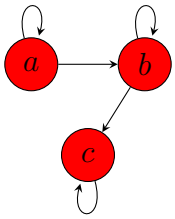
Viele wichtige Klassen von Relationen werden durch allgemeine Eigenschaften beschrieben. In diesem Abschnitt sei immer $R \subseteq M \times M$ eine Relation auf einer Menge M. Die folgenden Begriffe beschreiben, wie die Pfeile im zugehörigen gerichteten Graphen aussehen.

Reflexivität

Die Relation R heißt *reflexiv*, wenn jedes Element von M in Relation zu sich selbst steht:

$$\forall_{x \in M}\, x\ R\ x.$$

Im Graphen bedeutet das: Jeder Knoten hat eine Schleife.



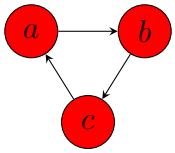
Beispiele: Die Gleichheitsrelation $=$ auf jeder Menge ist reflexiv. Die Relation $\leq$ auf $\mathbb{R}$ ist reflexiv. Die Relation $<$ auf $\mathbb{R}$ ist nicht reflexiv, denn nie gilt $x < x$.

Irreflexivität

Die Relation R heißt *irreflexiv*, wenn kein Element von M in Relation zu sich selbst steht:

$$\forall_{x \in M}\, \neg(x\ R\ x).$$

Im Graphen bedeutet das: Kein Knoten hat eine Schleife.



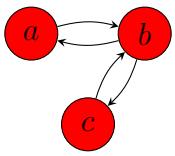
Beispiele: Die Relation $<$ auf $\mathbb{R}$ ist irreflexiv. Die Relation $\subsetneq$ auf $\mathcal{P}(M)$ ist irreflexiv. Die Relation $\leq$ ist nicht irreflexiv.

Symmetrie

Die Relation R heißt *symmetrisch*, wenn aus $x\ R\ y$ immer $y\ R\ x$ folgt:

$$\forall_{x,y\in M}\,(x\ R\ y\implies y\ R\ x).$$

Im Graphen bedeutet das: Jeder Pfeil zwischen zwei verschiedenen Knoten kommt in beide Richtungen vor.



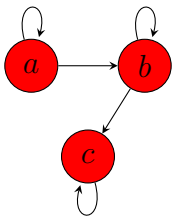
Beispiele: Die Gleichheitsrelation $=$ auf jeder Menge ist symmetrisch. Die Freundschaftsrelation auf Facebook ist symmetrisch. Die Relation $\leq$ auf $\mathbb{R}$ ist nicht symmetrisch.

Antisymmetrie

Die Relation R heißt *antisymmetrisch*, wenn zwei verschiedene Elemente nicht in beide Richtungen in Relation stehen können:

$$\forall_{x,y\in M}\,\big((x\ R\ y\wedge y\ R\ x)\implies x=y\big).$$

Im Graphen bedeutet das: Zwischen zwei verschiedenen Knoten gibt es keine Pfeile in beide Richtungen. Schleifen sind dabei erlaubt.



Beispiele: Die Relationen $<$ und $\leq$ auf $\mathbb{R}$ sind antisymmetrisch. Die Teilmengenrelation $\subseteq$ auf $\mathcal{P}(M)$ ist antisymmetrisch: Wenn $A\subseteq B$ und $B\subseteq A$ gelten, dann gilt $A=B$. Die Freundschaftsrelation auf Facebook ist nicht antisymmetrisch.

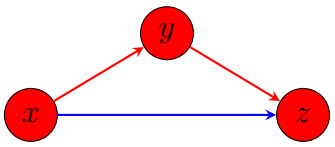
> **Bemerkung 6.5.1.** Symmetrisch und antisymmetrisch bedeuten nicht das Gegenteil voneinander. Die Gleichheitsrelation ist sowohl symmetrisch als auch antisymmetrisch. Symmetrisch heißt: Jeder Pfeil darf zurückgehen. Antisymmetrisch heißt: Ein Pfeil darf nur dann zurückgehen, wenn er eigentlich eine Schleife ist.

Transitivität

Die Relation R heißt *transitiv*, wenn man zwei aufeinanderfolgende Relationsschritte durch einen direkten Relationsschritt ersetzen darf:

$$\forall_{x,y,z\in M}\big((x\ R\ y \wedge y\ R\ z) \implies x\ R\ z\big).$$

Im Graphen kann man sich das so merken: Wenn es einen Weg der Länge zwei gibt, dann muss auch der direkte Pfeil vorhanden sein.



Beispiele: Die Relationen $<$ und $\leq$ auf $\mathbb{R}$ sind transitiv. Auch die Teilmengenrelation $\subseteq$ ist transitiv: Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$.

Totalität

Die Relation R heißt *total*, wenn je zwei Elemente vergleichbar sind:

$$\forall_{x,y\in M}\,(x\ R\ y \vee y\ R\ x).$$

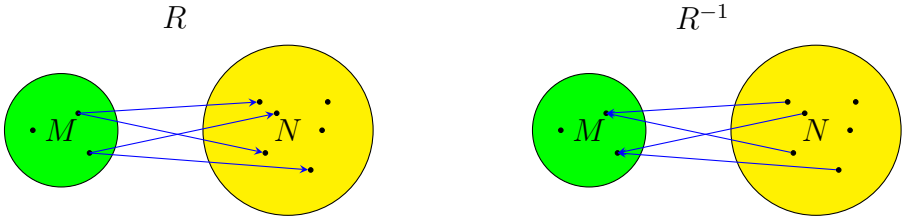
Beispiele: Die Relation $\leq$ auf $\mathbb{R}$ ist total. Die Relation $<$ auf $\mathbb{R}$ ist in diesem Sinn nicht total, denn für $x = y$ gilt weder $x < y$ noch $y < x$. Die Teilmengenrelation $\subseteq$ auf $\mathcal{P}(M)$ ist im Allgemeinen nicht total. Zum Beispiel sind $\{1\}$ und $\{2\}$ in $\mathcal{P}(\{1,2\})$ nicht vergleichbar.

6.6 Inverse Relation und Komposition

Definition 6.6.1. Sei $R \subseteq M \times N$ eine Relation von M nach N. Die *inverse Relation* R^{-1} ist die Relation von N nach M mit

$$R^{-1} := \{(n,m) \in N \times M \colon (m,n) \in R\}\,.$$

Anschaulich werden bei der inversen Relation alle Pfeile umgedreht.



Beispiel 6.6.2. *Wenn* $R = \{(1,a),(2,a),(3,b)\} \subseteq \{1,2,3\} \times \{a,b\}$ *ist, dann ist*

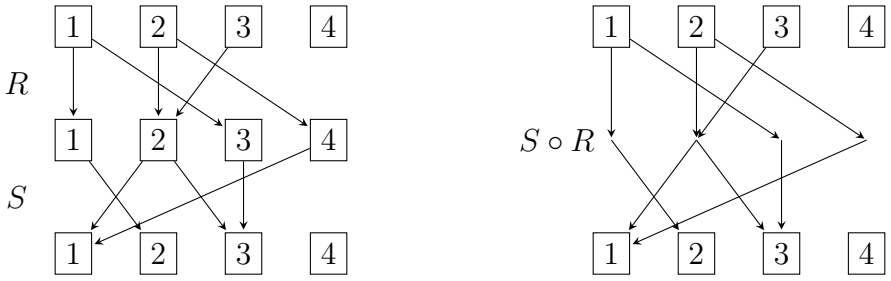
$$R^{-1} = \{(a,1),(a,2),(b,3)\}\,.$$

Definition 6.6.3. Seien $R \subseteq M \times N$ und $S \subseteq N \times P$ Relationen. Die *Komposition* $S \circ R$ ist die Relation von M nach P mit

$$S \circ R := \{(m,p) \in M \times P \colon \exists n \in N\ ((m,n) \in R \text{ und } (n,p) \in S)\}\,.$$

Man liest $S \circ R$ von rechts nach links: Zuerst geht man mit R von M nach N, dann mit S von N nach P.

In der folgenden Zeichnung sieht man links die beiden Schritte und rechts die dadurch entstehende zusammengesetzte Relation.



Beispiel 6.6.4. *Seien*

$$R = \{(1,a),(2,a),(2,b)\} \subseteq \{1,2\} \times \{a,b\}$$

und

$$S = \{(a,x),(b,y)\} \subseteq \{a,b\} \times \{x,y\}\,.$$

Dann ist

$$S \circ R = \{(1,x),(2,x),(2,y)\}\,.$$

Die Komposition von Relationen ist assoziativ. Wir begründen das kurz. Seien $R \subseteq L \times M$, $S \subseteq M \times N$ und $T \subseteq N \times P$ Relationen. Für $l \in L$ und $p \in P$ gilt

$$\begin{aligned}
(l,p) \in T \circ (S \circ R) &\iff \exists_{n \in N}\,((l,n) \in S \circ R \text{ und } (n,p) \in T) \\
&\iff \exists_{m \in M}\,\exists_{n \in N}\,((l,m) \in R \text{ und } (m,n) \in S \text{ und } (n,p) \in T) \\
&\iff \exists_{m \in M}\,((l,m) \in R \text{ und } (m,p) \in T \circ S) \\
&\iff (l,p) \in (T \circ S) \circ R.
\end{aligned}$$

Also gilt $T \circ (S \circ R) = (T \circ S) \circ R$.

6.7 Äquivalenzrelationen

Eine Äquivalenzrelation ist eine Relation, die eine Menge in Klassen von "gleichartigen" Elementen zerlegt.

Definition 6.7.1. Eine Relation $\sim$ auf einer Menge M heißt *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist.

Beispiele 6.7.2. *(i) Die Gleichheit $=$ ist eine Äquivalenzrelation auf jeder Menge M. Sie ist reflexiv, denn für jedes $x \in M$ gilt $x = x$. Sie ist symmetrisch, denn aus $x = y$ folgt $y = x$. Sie ist transitiv, denn aus $x = y$ und $y = z$ folgt $x = z$.*

(ii) Auf $\mathbb{Z}$ ist Kongruenz modulo n eine Äquivalenzrelation:

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad n \mid (a - b).$$

Diese Relation ist reflexiv, denn für jedes $a \in \mathbb{Z}$ gilt $a - a = 0$, und $n \mid 0$. Sie ist symmetrisch: Wenn $a \equiv b \pmod{n}$ gilt, dann gilt $n \mid (a - b)$. Also gibt es ein $k \in \mathbb{Z}$ mit $a - b = kn$. Dann ist $b - a = -kn$, also gilt $n \mid (b - a)$ und damit $b \equiv a \pmod{n}$. Sie ist transitiv: Wenn $a \equiv b \pmod{n}$ und $b \equiv c \pmod{n}$ gelten, dann gibt es $k, l \in \mathbb{Z}$ mit

$$a - b = kn \quad \text{und} \quad b - c = ln.$$

Dann ist

$$a - c = (a - b) + (b - c) = kn + ln = (k + l)n.$$

Also gilt $n \mid (a - c)$ und damit $a \equiv c \pmod{n}$.

(iii) Auf der Menge aller deutschen Wörter ist die Relation "hat dieselbe Länge wie" eine Äquivalenzrelation. Dabei müssen wir vorher festlegen, welche Schreibweise für jedes Wort die richtige ist; sonst wäre nicht eindeutig, wie viele Buchstaben ein Wort hat.

Die Relation ist reflexiv, denn jedes Wort hat dieselbe Länge wie sich selbst. Sie ist symmetrisch, denn wenn ein Wort w dieselbe Länge wie ein Wort v hat, dann hat auch v dieselbe Länge wie w. Sie ist transitiv, denn wenn w dieselbe Länge wie v hat und v dieselbe Länge wie u hat, dann haben auch w und u dieselbe Länge.

Wir haben oben angekündigt, dass eine Äquivalenzrelation eine Menge in Klassen von gleichartigen Elementen zerlegt. Bisher haben wir eine Äquivalenzrelation aber nur durch drei Eigenschaften definiert: Reflexivität, Symmetrie und Transitivität. Es ist an dieser Stelle noch nicht klar, dass jede Relation mit diesen drei Eigenschaften wirklich eine solche Zerlegung liefert. Genau das wollen wir jetzt verstehen. Wir beginnen mit der folgenden Definition.

Definition 6.7.3. Sei $\sim$ eine Äquivalenzrelation auf M und sei $a \in M$. Die *Äquivalenzklasse* von a ist

$$[a] := \{x \in M : x \sim a\}.$$

Die Äquivalenzklasse $[a]$ enthält also alle Elemente, die zu a äquivalent sind.

Beispiel 6.7.4. *Betrachten wir Kongruenz modulo* 3 *auf* $\mathbb{Z}$. *Dann ist*

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$

$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$

$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Diese drei Klassen zerlegen $\mathbb{Z}$.

Lemma 6.7.5. *Sei* $\sim$ *eine Äquivalenzrelation auf* M. *Für* $x, y \in M$ *gilt*

$$x \sim y \iff [x] = [y].$$

Beweis. Angenommen $x \sim y$. Sei $z \in [x]$. Dann gilt $z \sim x$. Aus $x \sim y$ folgt mit Transitivität $z \sim y$, also $z \in [y]$. Damit gilt $[x] \subseteq [y]$. Die umgekehrte Inklusion folgt genauso, also $[x] = [y]$.

Umgekehrt gelte $[x] = [y]$. Wegen Reflexivität gilt $x \in [x]$. Also gilt $x \in [y]$, und damit $x \sim y$. □

Definition 6.7.6. Eine *Zerlegung* einer Menge M ist eine Menge $\mathcal{Z}$ von nichtleeren Teilmengen von M, so dass

(i) $\bigcup_{Z \in \mathcal{Z}} Z = M$ gilt,

(ii) zwei verschiedene Mengen aus $\mathcal{Z}$ disjunkt sind.

Mit anderen Worten: Jedes Element von M liegt in genau einer Teilmenge aus $\mathcal{Z}$.

Satz 6.7.7. *Sei* $\sim$ *eine Äquivalenzrelation auf* M. *Dann bilden die Äquivalenzklassen eine Zerlegung von* M.

Beweis. Zunächst ist jede Äquivalenzklasse nichtleer: Für jedes $a \in M$ gilt $a \sim a$, also $a \in [a]$.

Außerdem liegt jedes Element $a \in M$ in mindestens einer Äquivalenzklasse, nämlich in $[a]$.

Es bleibt zu zeigen, dass zwei Äquivalenzklassen entweder gleich oder disjunkt sind. Angenommen, $[a] \cap [b]$ ist nicht leer. Dann gibt es ein $x \in M$ mit $x \in [a]$ und $x \in [b]$. Also gilt $x \sim a$ und $x \sim b$. Wegen Symmetrie gilt $a \sim x$, und wegen Transitivität folgt aus $a \sim x$ und $x \sim b$, dass $a \sim b$ gilt.

Nun zeigen wir $[a] = [b]$. Sei $y \in [a]$. Dann gilt $y \sim a$. Zusammen mit $a \sim b$ folgt durch Transitivität $y \sim b$, also $y \in [b]$. Damit ist $[a] \subseteq [b]$. Umgekehrt folgt genauso $[b] \subseteq [a]$. Also gilt $[a] = [b]$. □

Umgekehrt erzeugt jede Zerlegung eine Äquivalenzrelation. Sei dazu $\mathcal{Z}$ eine Zerlegung von M. Wir definieren eine Relation $\sim_{\mathcal{Z}}$ auf M durch

$$x \sim_{\mathcal{Z}} y \quad \iff \quad \exists_{Z \in \mathcal{Z}} (x \in Z \text{ und } y \in Z).$$

Mit anderen Worten: Zwei Elemente sind genau dann äquivalent, wenn sie im selben Teil der Zerlegung liegen. Als Übung sollte man überprüfen, dass $\sim_{\mathcal{Z}}$ tatsächlich eine Äquivalenzrelation ist und dass ihre Äquivalenzklassen genau die Elemente der ursprünglichen Zerlegung $\mathcal{Z}$ sind.

Äquivalenzrelationen und Zerlegungen sind also zwei Arten, dieselbe Information zu beschreiben.

Die Menge aller Äquivalenzklassen einer Äquivalenzrelation $\sim$ auf M wird häufig mit $M/\sim$ bezeichnet. Man nennt diese Menge den ***Quotienten*** von M nach $\sim$.

Für die Kongruenz modulo n auf $\mathbb{Z}$ schreibt man $\mathbb{Z}/n$ für die Menge der Kongruenzklassen modulo n.

6.8 Ordnungsrelationen

Definition 6.8.1. Eine Relation $\preceq$ auf einer Menge M heißt *Ordnungsrelation*, wenn sie reflexiv, antisymmetrisch und transitiv ist. In diesem Fall heißt $(M, \preceq)$ eine *teilweise geordnete Menge*. Wenn $\preceq$ zusätzlich total ist, heißt $(M, \preceq)$ eine *total geordnete Menge*.

Bemerkung 6.8.2. Wenn wir im Folgenden von einer *geordneten Menge* sprechen, meinen wir immer eine teilweise geordnete Menge. Wenn wir Totalität voraussetzen wollen, sagen wir das ausdrücklich.

Bemerkung 6.8.3. Etwas verwirrend ist vielleicht, dass jede total geordnete Menge nach dieser Definition automatisch auch eine teilweise geordnete Menge ist. Totalität ist also eine zusätzliche Eigenschaft, die eine teilweise Ordnung haben oder nicht haben kann.

Beispiele 6.8.4. *(i)* $(\mathbb{R}, \leq)$ *ist total geordnet. Reflexivität, Antisymmetrie und Transitivität sind die bekannten Eigenschaften von* $\leq$ *auf* $\mathbb{R}$*. Außerdem sind je zwei reelle Zahlen vergleichbar: Für alle* $x, y \in \mathbb{R}$ *gilt* $x \leq y$ *oder* $y \leq x$*. Also ist* $(\mathbb{R}, \leq)$ *total geordnet.*

(ii) Für jede Menge M *ist* $(\mathcal{P}(M), \subseteq)$ *teilweise geordnet. Reflexivität gilt, denn für jedes* $A \subseteq M$ *gilt* $A \subseteq A$*. Antisymmetrie gilt, denn aus* $A \subseteq B$ *und* $B \subseteq A$ *folgt* $A = B$*. Transitivität gilt, denn aus* $A \subseteq B$ *und* $B \subseteq C$ *folgt* $A \subseteq C$*.*

Hier sehen wir, dass eine teilweise Ordnung nicht total sein muss. Zum Beispiel sind die Mengen $\{1\}$ *und* $\{2\}$ *in* $\mathcal{P}(\{1, 2\})$ *nicht vergleichbar: Weder* $\{1\} \subseteq \{2\}$ *noch* $\{2\} \subseteq \{1\}$ *gilt.*

(iii) Auf $\mathbb{N}_+$ *ist die Teilbarkeitsrelation* $\mid$ *eine teilweise Ordnung. Reflexivität gilt, denn für jedes* $a \in \mathbb{N}_+$ *gilt* $a \mid a$*. Transitivität gilt, denn aus* $a \mid b$ *und* $b \mid c$ *folgt* $a \mid c$*. Für Antisymmetrie seien* $a, b \in \mathbb{N}_+$ *mit* $a \mid b$ *und* $b \mid a$*. Dann gibt es* $k, l \in \mathbb{N}_+$ *mit* $b = ka$ *und* $a = lb$*. Also gilt* $a = lka$*. Da* $a > 0$ *ist, folgt* $lk = 1$*. Mit* $k, l \in \mathbb{N}_+$ *folgt* $k = l = 1$*, also* $a = b$*.*

Kapitel 7

Funktionen

7.1 Funktionen als spezielle Relationen

Funktionen kennen wir schon aus der Schule. In diesem Kapitel wollen wir sie aber konsequent als spezielle Relationen verstehen.

Definition 7.1.1. Seien M und N Mengen. Eine *Funktion* oder *Abbildung* von M nach N ist eine Relation $f \subseteq M \times N$ mit der folgenden Eigenschaft: Für jedes $m \in M$ existiert genau ein $n \in N$ mit $(m, n) \in f$. In diesem Fall schreiben wir

$$f \colon M \to N.$$

Die Bedingung "genau ein" besteht aus zwei Teilen. Erstens muss zu jedem Element $m \in M$ überhaupt ein passendes Element $n \in N$ existieren. Diese Eigenschaft heißt *Linkstotalität*:

$$\forall_{m \in M} \exists_{n \in N} \, m \; f \; n.$$

Zweitens darf es zu einem festen $m \in M$ nicht zwei verschiedene passende Elemente geben. Diese Eigenschaft heißt *Rechtseindeutigkeit*:

$$\forall_{m \in M,\; x,y \in N} \left((m \; f \; x \wedge m \; f \; y) \implies x = y \right).$$

Wenn $(m, n) \in f$ gilt, schreiben wir meistens

$$n = f(m)$$

oder

$$m \mapsto n.$$

Das Element n heißt dann das *Bild* von m. Das Element m heißt ein *Urbild* von n. Die Menge M heißt *Definitionsbereich* von f. Die Menge N heißt *Zielmenge* oder *Wertebereich* von f.

Beispiele 7.1.2. *(i) Sei B die Menge der Bundesbürger. Die Relation*

$$\{(p, n) \in B \times \mathbb{N} \colon p \text{ hat Identifikationsnummer } n\}$$

von B nach $\mathbb{N}$ ist eine Funktion, sofern jeder Bundesbürger genau eine Identifikationsnummer hat.

(ii) Sei F die Menge der Facebook-Nutzer. Die Freundschaftsrelation

$$\{(x, y) \in F \times F \colon x \text{ ist Facebook-Freund von } y\}$$

ist keine Funktion. Sie wäre nur dann eine Funktion, wenn jeder Facebook-Nutzer genau einen Freund hätte.

(iii) Die Relation

$$f = \{(n, n') \in \mathbb{N} \times \mathbb{N} \colon n' = 2n\}$$

ist eine Funktion $f \colon \mathbb{N} \to \mathbb{N}$. Wir schreiben dafür auch kürzer

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

(iv) Für jede Menge M ist die Identität id_M eine Funktion von M nach M. Sie ist gegeben durch

$$\mathrm{id}_M(m) = m \quad \text{für alle } m \in M.$$

Für eine Teilmenge $M' \subseteq M$ definieren wir

$$f(M') := \{f(m) \colon m \in M'\}.$$

Diese Menge heißt das *Bild* von M' unter f.

Für eine Teilmenge $N' \subseteq N$ definieren wir

$$f^{-1}(N') := \{m \in M \colon f(m) \in N'\}.$$

Diese Menge heißt das *Urbild* von N' unter f.

Beispiel 7.1.3. *Sei $v \colon \mathbb{N} \to \mathbb{N}$ die Funktion mit $v(n) := 2n$. Dann gilt*

$$v(\mathbb{N}) = \{2x \colon x \in \mathbb{N}\}.$$

Außerdem gilt

$$v^{-1}(\{2k + 1 \colon k \in \mathbb{N}\}) = \emptyset,$$

denn keine ungerade natürliche Zahl wird von v getroffen.

Beispiel 7.1.4. *Sei* $M := \{1, 2, 3, 4, 5, 6\}$. *Wir definieren* $f\colon M \to M$ *durch*

$$f(m) := \lceil \sqrt{m} \rceil .$$

Dann gilt

$$f(M) = \{1, 2, 3\}, \qquad f(\{1, 2\}) = \{1, 2\},$$

und

$$f^{-1}(\{2\}) = \{2, 3, 4\}.$$

Bemerkung 7.1.5. Da Funktionen in diesem Abschnitt als Relationen betrachtet werden, ist auch der Ausdruck $f \subseteq g$ sinnvoll, wenn $f, g\colon M \to N$ Funktionen sind. Als Übung sollte man überprüfen: Wenn $f, g\colon M \to N$ Funktionen sind und $f \subseteq g$ gilt, dann gilt schon $f = g$.

7.2 Injektivität, Surjektivität und Bijektivität

Definition 7.2.1. Sei $f\colon M \to N$ eine Funktion.

(i) f heißt *injektiv*, wenn für alle $x, y \in M$ gilt:

$$f(x) = f(y) \implies x = y.$$

(ii) f heißt *surjektiv*, wenn für jedes $n \in N$ ein $m \in M$ existiert mit $f(m) = n$.

(iii) f heißt *bijektiv*, wenn f injektiv und surjektiv ist.

Injektivität bedeutet: Verschiedene Elemente der Definitionsmenge werden auf verschiedene Elemente der Zielmenge abgebildet. Surjektivität bedeutet: Jedes Element der Zielmenge wird getroffen.

Beispiele 7.2.2. *(i) Die Funktion* $f\colon \mathbb{N} \to \mathbb{N}$ *mit* $f(n) = n + 1$ *ist injektiv, aber nicht surjektiv, weil* 0 *nicht getroffen wird.*

(ii) Die Funktion $f\colon \mathbb{Z} \to \mathbb{N}$ *mit* $f(n) = n^2$ *ist nicht injektiv, weil* $f(1) = f(-1)$ *gilt. Sie ist auch nicht surjektiv, weil zum Beispiel* 2 *nicht getroffen wird.*

(iii) Die Funktion $f\colon \mathbb{Z} \to \mathbb{Z}$ *mit* $f(n) = n + 1$ *ist bijektiv.*

(iv) Die Funktion $\tan\colon \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ *ist bijektiv. Anschaulich nimmt sie jeden reellen Wert genau einmal an.*

Bei endlichen Mengen stimmen Injektivität und Surjektivität in einer wichtigen Situation überein.

Satz 7.2.3. *Sei M eine endliche Menge und sei $f\colon M \to M$ eine Funktion. Dann ist f genau dann injektiv, wenn f surjektiv ist.*

Beweis. Für jedes $a \in M$ betrachten wir das Urbild

$$F_a := f^{-1}(\{a\}) = \{x \in M\colon f(x) = a\}\,.$$

Die Mengen F_a sind paarweise disjunkt, und ihre Vereinigung ist M: Jedes $x \in M$ liegt nämlich genau in der Menge $F_{f(x)}$. Da M endlich ist, gilt also

$$|M| = \sum_{a \in M} |F_a|\,.$$

Angenommen zuerst, f ist surjektiv. Dann ist jedes F_a nichtleer, also gilt $|F_a| \geq 1$ für alle $a \in M$. Wenn f nicht injektiv wäre, dann gäbe es ein $a \in M$ mit $|F_a| \geq 2$. Dann wäre

$$\sum_{a \in M} |F_a| > |M|\,,$$

im Widerspruch zu der Gleichung oben. Also ist f injektiv.

Angenommen nun, f ist injektiv. Dann enthält jedes F_a höchstens ein Element, also gilt $|F_a| \leq 1$ für alle $a \in M$. Wenn f nicht surjektiv wäre, dann gäbe es ein $a \in M$ mit $F_a = \emptyset$. Dann wäre

$$\sum_{a \in M} |F_a| < |M|\,,$$

wieder im Widerspruch zu der Gleichung oben. Also ist f surjektiv. □

Dieser Satz ist für unendliche Mengen falsch. Die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 1$ ist injektiv, aber nicht surjektiv. Außerdem ist die Funktion $: \mathbb{N} \to \mathbb{N}$ mit $f(n) = \lceil \sqrt{n} \rceil$ surjektiv, aber nicht injektiv.

7.3 Komposition von Funktionen

Da Funktionen Relationen sind, können wir Funktionen zunächst als Relationen komponieren. Seien also $f\colon M \to N$ und $g\colon N \to P$ Funktionen. Als Relationen gilt $f \subseteq M \times N$ und $g \subseteq N \times P$. Die Komposition der Relationen ist dann die Relation

$$g \circ f := \{(m, p) \in M \times P\colon \exists_{n \in N}\, ((m, n) \in f \text{ und } (n, p) \in g)\}\,.$$

Zunächst ist $g \circ f$ also nur eine Relation von M nach P. Wir müssen kurz überprüfen, dass diese Relation wieder eine Funktion ist.

Lemma 7.3.1. *Die Komposition zweier Funktionen ist wieder eine Funktion.*

Beweis. Seien $f\colon M \to N$ und $g\colon N \to P$ Funktionen. Wir zeigen, dass die Relation $g \circ f$ linkstotal und rechtseindeutig ist.

Linkstotalität. Sei $m \in M$. Da f linkstotal ist, gibt es ein $n \in N$ mit $(m, n) \in f$. Da g linkstotal ist, gibt es ein $p \in P$ mit $(n, p) \in g$. Also gilt $(m, p) \in g \circ f$. Damit ist $g \circ f$ linkstotal.

Rechtseindeutigkeit. Angenommen, $(m, p) \in g \circ f$ und $(m, p') \in g \circ f$. Dann gibt es $n, n' \in N$ mit

$$(m, n) \in f, \quad (n, p) \in g, \quad (m, n') \in f, \quad (n', p') \in g.$$

Da f rechtseindeutig ist, folgt aus $(m, n) \in f$ und $(m, n') \in f$, dass $n = n'$ gilt. Da g rechtseindeutig ist, folgt dann aus $(n, p) \in g$ und $(n, p') \in g$, dass $p = p'$ gilt. Damit ist $g \circ f$ rechtseindeutig.

Also ist $g \circ f$ eine Funktion von M nach P. □

Für diese Komposition gilt die bekannte Formel

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

Wie bei Relationen liest man $g \circ f$ von rechts nach links: zuerst f, dann g.

Satz 7.3.2. *Die folgenden Aussagen gelten.*

(i) Die Komposition injektiver Funktionen ist injektiv.

(ii) Die Komposition surjektiver Funktionen ist surjektiv.

(iii) Die Komposition bijektiver Funktionen ist bijektiv.

Beweis. Wir zeigen exemplarisch die Aussage für Injektivität. Seien $f\colon M \to N$ und $g\colon N \to P$ injektiv. Angenommen

$$(g \circ f)(x) = (g \circ f)(y).$$

Dann gilt $g(f(x)) = g(f(y))$. Da g injektiv ist, folgt $f(x) = f(y)$. Da f injektiv ist, folgt $x = y$. Also ist $g \circ f$ injektiv.

Die Aussagen für Surjektivität und Bijektivität werden ähnlich bewiesen. □

Da die Komposition von Relationen assoziativ ist, ist auch die Komposition von Funktionen assoziativ:

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

Außerdem gilt für jede Funktion $f\colon M \to N$:

$$f \circ \mathrm{id}_M = f \quad \text{und} \quad \mathrm{id}_N \circ f = f.$$

7.4 Inverse Funktionen

Wenn $f\colon M \to N$ eine Funktion ist, dann können wir immer die inverse Relation $f^{-1} \subseteq N \times M$ bilden. Diese inverse Relation muss aber nicht wieder eine Funktion sein.

Beispiel 7.4.1. *Sei $f\colon \mathbb{Z} \to \mathbb{N}$ die Funktion mit $f(n) = n^2$. Dann enthält die inverse Relation f^{-1} zum Beispiel die beiden Paare $(1,1)$ und $(1,-1)$. Als Relation von $\mathbb{N}$ nach $\mathbb{Z}$ ordnet f^{-1} dem Element 1 also zwei verschiedene Elemente zu. Deshalb ist f^{-1} in diesem Fall keine Funktion.*

Wir wollen nun genau die Funktionen beschreiben, bei denen die inverse Relation wieder eine Funktion ist.

Definition 7.4.2. Eine Funktion $f\colon M \to N$ heißt *invertierbar*, wenn es eine Funktion $g\colon N \to M$ gibt, so dass

$$g \circ f = \mathrm{id}_M$$

und

$$f \circ g = \mathrm{id}_N\,.$$

In diesem Fall heißt g die inverse Funktion von f und wird mit f^{-1} bezeichnet.

Proposition 7.4.3. *Sei $f\colon M \to N$ invertierbar. Dann ist die inverse Funktion von f eindeutig bestimmt.*

Beweis. Seien $g, h\colon N \to M$ inverse Funktionen zu f. Dann gilt

$$f \circ g = f \circ h = \mathrm{id}_N \quad \text{und} \quad g \circ f = h \circ f = \mathrm{id}_M\,.$$

Mit der Assoziativität der Komposition erhalten wir

$$g = g \circ \mathrm{id}_N = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_M \circ h = h.$$

Also ist die inverse Funktion eindeutig. □

Satz 7.4.4. *Eine Funktion ist genau dann invertierbar, wenn sie bijektiv ist.*

Beweis. Angenommen, $f\colon M \to N$ ist invertierbar mit inverser Funktion $g\colon N \to M$. Wir zeigen zuerst, dass f injektiv ist. Wenn $f(x) = f(y)$ gilt, dann folgt durch Anwenden von g:

$$x = g(f(x)) = g(f(y)) = y.$$

Also ist f injektiv. Für Surjektivität sei $n \in N$. Dann gilt $n = f(g(n))$, also wird n von $g(n) \in M$ getroffen. Damit ist f surjektiv.

Umgekehrt sei f bijektiv. Für jedes $n \in N$ gibt es dann genau ein $m \in M$ mit

$f(m) = n$. Wir definieren $g(n)$ als dieses eindeutig bestimmte m. Dann gilt $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$. □

7.5 Einseitige Inverse und die Axiome der Mengenlehre

Sei $f\colon M \to N$ eine Funktion. Eine Funktion $g\colon N \to M$ heißt eine ***Linksinverse*** zu f, wenn

$$g \circ f = \mathrm{id}_M$$

gilt. Eine Funktion $g\colon N \to M$ heißt eine ***Rechtsinverse*** zu f, wenn

$$f \circ g = \mathrm{id}_N$$

gilt.

Eine invertierbare Funktion besitzt also eine Funktion g, die gleichzeitig Links- und Rechtsinverse ist. Jetzt betrachten wir die beiden Bedingungen getrennt.

Proposition 7.5.1. *Sei $f\colon M \to N$ injektiv, und sei $M \neq \emptyset$. Dann gibt es eine Funktion $g\colon N \to M$ mit*

$$g \circ f = \mathrm{id}_M .$$

Beweis. Wir wählen ein festes Element $m_0 \in M$. Für $n \in N$ definieren wir

$$g(n) := \begin{cases} \text{das eindeutig bestimmte } m \in M \text{ mit } f(m) = n, & \text{falls } n \in f(M), \\ m_0, & \text{falls } n \notin f(M). \end{cases}$$

Diese Definition ist sinnvoll, weil f injektiv ist: Wenn $n \in f(M)$ gilt, dann gibt es genau ein $m \in M$ mit $f(m) = n$.

Für jedes $m \in M$ gilt nun $f(m) \in f(M)$, und nach Definition von g gilt daher

$$g(f(m)) = m.$$

Also gilt $g \circ f = \mathrm{id}_M$. □

Die entsprechende Aussage für surjektive Funktionen sieht auf den ersten Blick genauso harmlos aus. Wenn $f\colon M \to N$ surjektiv ist, dann ist für jedes $n \in N$ das Urbild

$$f^{-1}(\{n\}) = \{m \in M\colon f(m) = n\}$$

nichtleer. Wir würden also gerne für jedes $n \in N$ ein Element $g(n) \in f^{-1}(\{n\})$ wählen. Dann wäre

$$f(g(n)) = n$$

für alle $n \in N$, also $f \circ g = \mathrm{id}_N$.

Der Unterschied zu vielen früheren Existenzbeweisen ist, dass wir hier nicht unbedingt eine Vorschrift haben, welches Element im jeden Urbild gewählt werden soll.

In Beweisen, die wir bisher gesehen haben, war das anders. Im Euklidischen Algorithmus wird der größte gemeinsame Teiler nicht nur als existierend behauptet, sondern tatsächlich berechnet. In Bézouts Satz erhält man die Koeffizienten durch Rückwärtseinsetzen im Euklidischen Algorithmus. Im Beweis, dass es unendlich viele Primzahlen gibt, konstruiert man aus endlich vielen Primzahlen $p_1, \dots, p_k$ die Zahl

$$p_1 \cdots p_k + 1$$

und nimmt dann einen Primteiler dieser Zahl (und diese Primteiler kann mach auch algorithmish berechnen).

Bei einer beliebigen surjektiven Funktion $f\colon M \to N$ gibt es dagegen möglicherweise sehr viele Urbilde, und im jeden davon muss eine Wahl getroffen werden. Es kann sein, dass es keine Regel gibt, die sagt, welches Element des jeweiligen Bilds genommen werden soll.

An dieser Stelle berühren wir die Axiome der Mengenlehre. Wir haben Mengen bisher nicht definiert. Das ist kein Versehen: Man kann nicht alle Begriffe auf noch einfachere Begriffe zurückführen. Irgendwo muss man anfangen.

Eine sehr interessante Idee besteht darin, den Begriff der Menge nicht direkt zu definieren, sondern die Regeln festzulegen, nach denen man mit Mengen arbeiten darf. Diese Regeln sind die Axiome der Mengenlehre. Man kann sie sich als Regeln eines Spiels vorstellen: Welche Mengen dürfen wir bilden? Welche Konstruktionen sind erlaubt? Wann gelten zwei Mengen als gleich?

Auf den ersten Blick könnte man erwarten, dass alle Mathematikerinnen und Mathematiker ungefähr dieselbe Vorstellung davon haben, was Mengen sind und welche Regeln erlaubt sein sollten. Es hat sich aber herausgestellt, dass dies nicht ganz so einfach ist. Das folgende Axiom war historisch umstritten, weil es eine Existenzbehauptung macht, ohne eine konkrete Regel für die Konstruktion des gesuchten Objekts anzugeben.

Axiom (Auswahlaxiom)**.** Sei $(X_i)_{i\in I}$ eine Familie nichtleerer Mengen. Dann gibt es eine Funktion

$$c\colon I \to \bigcup_{i\in I} X_i$$

mit $c(i) \in X_i$ für alle $i \in I$.

Eine solche Funktion c heißt eine ***Auswahlfunktion***. Für endliche Familien ist diese Aussage unproblematisch: Man kann die endlich vielen Wahlen nacheinander treffen. Das Auswahlaxiom ist vor allem eine Aussage über beliebige, auch unendliche Familien von nichtleeren Mengen.

Mehr zu den Axiomen der Mengenlehre wird in der Hörsaalübung besprochen. Für uns ist im Moment vor allem die folgende Konsequenz wichtig.

Proposition 7.5.2. *Wir nehmen das Auswahlaxiom an. Sei $f\colon M \to N$ surjektiv. Dann gibt es eine Funktion $g\colon N \to M$ mit*

$$f \circ g = \mathrm{id}_N\,.$$

Beweis. Für jedes $n \in N$ ist die Faser

$$X_n := f^{-1}(\{n\})$$

nichtleer, weil f surjektiv ist. Nach dem Auswahlaxiom gibt es eine Funktion $g\colon N \to M$ mit

$$g(n) \in X_n$$

für alle $n \in N$. Das bedeutet gerade, dass

$$f(g(n)) = n$$

für alle $n \in N$ gilt. Also gilt $f \circ g = \mathrm{id}_N$. □

In der heutigen mathematischen Praxis arbeitet man fast immer mit dem Auswahlaxiom. Deshalb wird die letzte Proposition normalerweise ohne den Zusatz "wir nehmen das Auswahlaxiom an" formuliert: Eine surjektive Funktion besitzt eine Rechtsinverse.

Kapitel 8

Kardinalitäten

Im vorigen Kapitel haben wir Funktionen und Bijektionen eingeführt. In diesem Kapitel benutzen wir Bijektionen, um die Größe von Mengen zu vergleichen.

Bei endlichen Mengen ist die Situation vertraut: Eine Menge mit drei Elementen hat dieselbe Größe wie jede andere Menge mit drei Elementen. Für unendliche Mengen wird die Situation interessanter. Die Mengen $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ sind alle gleichmächtig, obwohl sie unterschiedlich aussehen.

Interessanterweise werden wir aber sehen, dass es trotzdem verschiedene Arten von Unendlichkeit gibt.

8.1 Gleichmächtigkeit

Definition 8.1.1. Zwei Mengen M und N heißen *gleichmächtig*, wenn es eine bijektive Funktion $f\colon M \to N$ gibt. In diesem Fall schreiben wir

$$|M| = |N|\,.$$

Diese Notation ist zunächst nur eine Schreibweise. Sie bedeutet nicht, dass $M = N$ als Mengen gilt. Sie bedeutet nur, dass die Elemente von M und die Elemente von N paarweise miteinander verbunden werden können.

Beispiel 8.1.2. *Die Mengen* $\{a, b, c\}$ *und* $\{10, 20, 30\}$ *sind gleichmächtig. Eine Bijektion ist zum Beispiel*

$$a \mapsto 10, \qquad b \mapsto 20, \qquad c \mapsto 30.$$

Beispiel 8.1.3. *Es gilt* $|\mathbb{Z}| = |\mathbb{N}|$. *Eine mögliche Bijektion* $f\colon \mathbb{Z} \to \mathbb{N}$ *ist*

$$f(z) = \begin{cases} 2z, & \text{falls } z \geq 0, \\ -(2z+1), & \text{falls } z < 0. \end{cases}$$

Dann erhalten wir

$$0 \mapsto 0, \quad -1 \mapsto 1, \quad 1 \mapsto 2, \quad -2 \mapsto 3, \quad 2 \mapsto 4,$$

und so weiter.

Beispiel 8.1.4. *Es gilt*

$$|\mathbb{R}| = \left|\left(-\frac{1}{2}, \frac{1}{2}\right)\right|.$$

Eine Bijektion $f\colon (-\frac{1}{2}, \frac{1}{2}) \to \mathbb{R}$ *ist*

$$f(x) = \tan(\pi x).$$

Die Funktion streckt das offene Intervall auf die ganze reelle Gerade.

Übung 8.1.5. *Zeigen Sie: Für alle* $a, b \in \mathbb{R}$ *mit* $a < b$ *gilt*

$$|\mathbb{R}| = |(a, b)|.$$

Satz 8.1.6. *Gleichmächtigkeit ist eine Äquivalenzrelation.*

Beweis. Reflexivität: Für jede Menge M ist die Identität $\mathrm{id}_M\colon M \to M$ eine Bijektion. Also gilt $|M| = |M|$.

Symmetrie: Wenn $f\colon M \to N$ eine Bijektion ist, dann ist die inverse Funktion $f^{-1}\colon N \to M$ ebenfalls eine Bijektion. Also folgt aus $|M| = |N|$ auch $|N| = |M|$.

Transitivität: Wenn $f\colon M \to N$ und $g\colon N \to P$ Bijektionen sind, dann ist $g \circ f\colon M \to P$ eine Bijektion. Also folgt aus $|M| = |N|$ und $|N| = |P|$ auch $|M| = |P|$. □

Die Äquivalenzklassen dieser Relation heißen *Kardinalitäten*. Die Kardinalität einer dreielementigen Menge nennen wir einfach 3. Kardinalitäten verallgemeinern also die natürlichen Zahlen.

Bemerkung 8.1.7. Streng genommen haben wir hier eine kleine technische Schwierigkeit ignoriert. Eine Äquivalenzrelation ist immer auf einer Menge definiert, aber wir dürfen nicht einfach die Menge aller Mengen betrachten. Warum das problematisch ist, sehen wir später in Bemerkung 8.2.2 zu Russells Paradoxon. Formal müsste man also zuerst ein ausreichend großes Universum von Mengen festlegen und Gleichmächtigkeit nur für Mengen in diesem Universum betrachten. Für die Ideen in

diesem Kapitel spielt diese technische Einschränkung keine Rolle.

8.2 Cantors Diagonalargument

Wir zeigen nun, dass es tatsächlich verschiedene Arten von Unendlichkeit gibt: kleinere und größere. Das ist beim ersten Kontakt überraschend, denn man könnte meinen, dass unendlich einfach unendlich ist. Konkret werden wir zeigen, dass die Menge $\mathbb{R}$ nicht durch die natürlichen Zahlen vollständig aufgelistet werden kann. Also gibt es keine bijektive Funktion $\mathbb{N} \to \mathbb{R}$, weswegen die Mächtigkeiten $|\mathbb{N}|$ und $|\mathbb{R}|$ nicht gleich sind.

Satz 8.2.1. *Es gilt*

$$|\mathbb{N}| \neq |\mathbb{R}| .$$

Beweis. Wir zeigen eine bisschen stärkere Aussage: Es gibt keine surjektive Funktion $b\colon \mathbb{N} \to (0,1)$.

Wir führen einen Widerspruchsbeweis. Angenommen, es gäbe eine surjektive Funktion

$$b\colon \mathbb{N} \to (0,1).$$

Dann könnten wir alle Zahlen $b(0), b(1), b(2), \ldots$ als Dezimalzahlen untereinander schreiben:

$$\begin{aligned} b(0) &= 0.d_{00}d_{01}d_{02}\ldots \\ b(1) &= 0.d_{10}d_{11}d_{12}\ldots \\ b(2) &= 0.d_{20}d_{21}d_{22}\ldots \\ &\vdots \end{aligned}$$

Wir konstruieren nun eine neue Zahl

$$x = 0.e_0e_1e_2\ldots$$

so, dass sie sich von jeder Zahl in dieser Liste unterscheidet. Dazu wählen wir für jedes $i \in \mathbb{N}$ eine Ziffer

$$e_i \in \{1,2,3,4,5,6,7,8\} \setminus \{d_{ii}\} .$$

Das ist immer möglich. Wir vermeiden dabei die Ziffern 0 und 9, damit keine Probleme mit zwei verschiedenen Dezimaldarstellungen derselben Zahl entstehen.

Die Zahl x liegt in $(0,1)$. Da b surjektiv sein soll, müsste es ein $m \in \mathbb{N}$ geben mit $b(m) = x$. Aber die m-te Nachkommastelle von $b(m)$ ist d_{mm}, während die m-te Nachkommastelle von x gleich e_m ist. Nach Konstruktion gilt $e_m \neq d_{mm}$. Also kann $b(m)$ nicht gleich x sein.

Das ist ein Widerspruch zur Surjektivität von b. Daher gibt es keine solche surjektive Funktion. □

Dieses Argument heißt *Diagonalargument*, weil wir die Ziffern auf der Diagonalen der

Tabelle verändern. Es geht auf Georg Cantor zurück, der im 19. Jahrhundert zeigte, dass es verschiedene Größen von unendlichen Mengen gibt.

Die Kardinalität von $\mathbb{N}$ heißt $\aleph_0$. Die Kardinalität von $\mathbb{R}$ heißt *Kontinuum* und wird oft mit $\mathfrak{c}$ bezeichnet.

Bemerkung 8.2.2 (Russells Paradoxon)**.** Ein verwandtes diagonales Argument zeigt, warum man nicht naiv von der Menge aller Mengen sprechen darf. Angenommen, es gäbe eine Menge $\mathcal{U}$ aller Mengen. Dann könnten wir

$$V := \{M \in \mathcal{U} \colon M \notin M\}$$

definieren. Dann müsste entweder $V \in V$ oder $V \notin V$ gelten. Wenn $V \in V$ gilt, folgt aus der Definition von V, dass $V \notin V$ gilt. Wenn $V \notin V$ gilt, folgt aus der Definition von V, dass $V \in V$ gilt. Beides ist unmöglich. In der axiomatischen Mengenlehre wird dieses Problem dadurch vermieden, dass die Gesamtheit aller Mengen keine Menge ist.

8.3 Abzählbare Mengen

Definition 8.3.1. Eine Menge M heißt *abzählbar*, wenn

$$|M| \leq |\mathbb{N}|$$

gilt, also wenn es eine injektive Funktion $M \to \mathbb{N}$ gibt. Eine unendliche abzählbare Menge hat dieselbe Kardinalität wie $\mathbb{N}$.

Endliche Mengen sind abzählbar. Außerdem sind $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ abzählbar. Bei $\mathbb{Z}$ haben wir bereits eine Bijektion mit $\mathbb{N}$ gesehen, und $\mathbb{Q}$ verlassen wir als eine Übung.

Bemerkung 8.3.2. Man kann auch die positive Version der Definition verwenden: Eine Menge ist abzählbar, wenn man ihre Elemente in einer endlichen oder unendlichen Liste anordnen kann,

$$x_0, x_1, x_2, \ldots,$$

so dass jedes Element der Menge irgendwann in der Liste vorkommt. Wiederholungen sind dabei erlaubt. Diese Listenformulierung ist besonders anschaulich. Sie zeigt auch: Abzählbare Mengen sind entweder endlich, oder sie haben dieselbe Kardinalität wie $\mathbb{N}$, also Kardinalität $\aleph_0$.

8.4 Vergleich von Kardinalitäten

Wir wollen Kardinalitäten nicht nur auf Gleichheit prüfen, sondern auch ordnen.

Definition 8.4.1. Für Mengen M und N schreiben wir

$$|M| \leq |N|\,,$$

wenn es eine injektive Funktion $f\colon M \to N$ gibt.

Anschaulich bedeutet $|M| \leq |N|$: Die Elemente von M können ohne Kollisionen in N eingebettet werden.

Man muss kurz prüfen, dass diese Definition nur von den Kardinalitäten abhängt, nicht von den konkreten Repräsentanten.

Lemma 8.4.2. *Seien M, X, N, Y Mengen mit $|M| = |X|$ und $|N| = |Y|$. Dann existiert eine injektive Funktion $M \to N$ genau dann, wenn eine injektive Funktion $X \to Y$ existiert.*

Beweis. Angenommen, es gibt eine injektive Funktion $f\colon M \to N$. Da $|M| = |X|$ und $|N| = |Y|$ gelten, gibt es Bijektionen $b\colon X \to M$ und $c\colon N \to Y$. Dann ist

$$c \circ f \circ b\colon X \to Y$$

injektiv, weil Kompositionen injektiver Funktionen injektiv sind.

Die umgekehrte Richtung folgt durch dasselbe Argument mit vertauschten Rollen. □

Damit ist die Relation $\leq$ auf Kardinalitäten wohldefiniert. Tatsächlich ist es eine Ordnungsrelation. Reflexivität ist klar: $\mathrm{id}_M\colon M \to M$ ist injektiv. Transitivität ist ebenfalls klar: Die Komposition zweier Injektionen ist injektiv. Die Antisymmetrie ist nicht offensichtlich. Wenn es eine Injektion $A \to B$ und eine Injektion $B \to A$ gibt, muss es dann eine Bijektion $A \to B$ geben? Der Satz von Cantor-Schröder-Bernstein in der nächsten Sektion beantwortet genau diese Frage.

Beispiele 8.4.3. *(i) Wenn $M \subseteq N$ gilt, dann gilt $|M| \leq |N|$, denn die Inklusion $\iota\colon M \to N$ mit $\iota(m) = m$ ist injektiv.*

(ii) Es gilt $|\mathbb{N}| \leq |\mathbb{Z}|$, weil die Inklusion $\mathbb{N} \to \mathbb{Z}$ injektiv ist.

(iii) Es gilt $|\mathbb{N}| \leq |\mathbb{R}|$, weil die Inklusion $\mathbb{N} \to \mathbb{R}$ injektiv ist.

(iv) Wenn $f\colon M \to N$ surjektiv ist und man zu jedem $n \in N$ ein Urbild auswählt, erhält man eine injektive Funktion $N \to M$. In diesem Sinn folgt aus einer Surjektion $M \to N$ auch $|N| \leq |M|$.

Proposition 8.4.4. *$\aleph_0$ ist die kleinste unendliche Kardinalität. Genauer: Wenn M eine unendliche Menge ist, dann gilt*

$$\aleph_0 \leq |M| .$$

Beweis. Da M unendlich ist, können wir ein Element $m_0 \in M$ wählen. Da $M \setminus \{m_0\}$ immer noch nicht leer ist, können wir ein Element $m_1 \in M \setminus \{m_0\}$ wählen. Induktiv wählen wir, nachdem $m_0, \ldots, m_{n-1}$ gewählt wurden, ein Element

$$m_n \in M \setminus \{m_0, \ldots, m_{n-1}\} .$$

Das ist möglich, weil eine unendliche Menge nicht durch endlich viele Elemente ausgeschöpft werden kann.

Damit erhalten wir paarweise verschiedene Elemente $m_0, m_1, m_2, \ldots$ von M. Die Funktion $f\colon \mathbb{N} \to M$ mit $f(n) = m_n$ ist injektiv. Also gilt $|\mathbb{N}| \leq |M|$, das heißt $\aleph_0 \leq |M|$. □

8.5 Cantor-Schröder-Bernstein und Matchings in bipartiten Graphen

Satz 8.5.1 (Cantor-Schröder-Bernstein)**.** *Seien A und B Mengen. Wenn es eine injektive Funktion $f\colon A \to B$ und eine injektive Funktion $g\colon B \to A$ gibt, dann gibt es eine bijektive Funktion $h\colon A \to B$.*

Wir formulieren den Beweis von Cantor-Schröder-Bernstein in einer Graphensprache. Diese Sprache ist für Informatik besonders nützlich.

Definition 8.5.2. Ein *bipartiter Graph* besteht aus zwei Knotenmengen A und B und Kanten, die immer einen Knoten aus A mit einem Knoten aus B verbinden.

Ein *Matching* ist eine Menge von Kanten, so dass kein Knoten in mehr als einer gewählten Kante liegt. Ein Matching heißt *perfekt*, wenn jeder Knoten in genau einer gewählten Kante liegt.

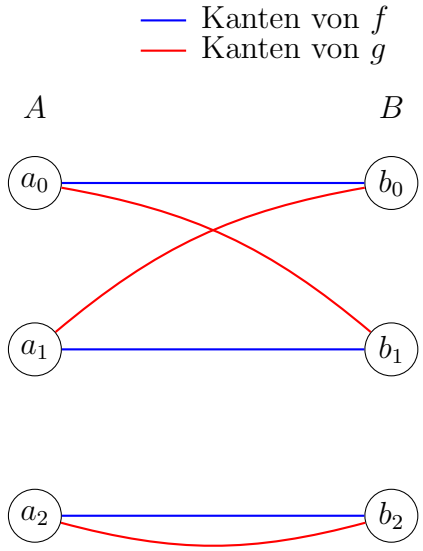
Eine Bijektion $A \to B$ ist dasselbe wie ein perfektes Matching zwischen A und B: Jedem $a \in A$ wird genau ein $b \in B$ zugeordnet, und jedes $b \in B$ wird genau einmal getroffen.

Jetzt können wir mit dem Beweis anfangen.

Beweis. Erst bauen wir aus f und g einen bipartiten Graphen mit den beiden Knotenmengen A und B.

Für jedes $a \in A$ zeichnen wir eine blaue Kante zwischen a und $f(a) \in B$. Weil f injektiv ist, liegt jeder Knoten aus B an höchstens einer blauen Kante. Außerdem liegt jeder Knoten aus A an genau einer blauen Kante.

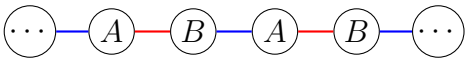
Für jedes $b \in B$ zeichnen wir eine rote Kante zwischen $g(b) \in A$ und b. Weil g injektiv ist, liegt jeder Knoten aus A an höchstens einer roten Kante. Außerdem liegt jeder Knoten aus B an genau einer roten Kante.



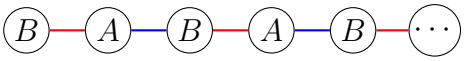
Jeder Knoten hat also höchstens eine blaue und höchstens eine rote Kante. Eine *Komponente* dieses Graphen besteht aus allen Knoten, die man von einem gegebenen Startknoten aus durch eine Folge von Kanten erreichen kann. Um den Beweis abzuschließen, betrachten wir die Komponenten einzeln und zeigen in jeder Komponente, wie man ein perfektes Matching konstruiert.

Fixieren wir also eine Komponente und wählen darin einen Knoten. Von diesem Knoten aus können wir entlang einer Kante zum nächsten Knoten gehen. Dort kann es höchstens eine Kante der anderen Farbe geben, der wir weiter folgen können. Danach kann es wieder höchstens eine Kante der ersten Farbe geben, und so weiter. Auf diese Weise können wir in der Komponente entlang von Kanten mit abwechselnden Farben laufen. Typische Komponenten sehen daher folgendermaßen aus.

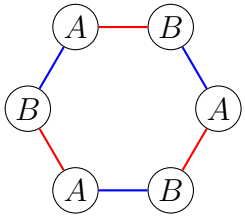
Bi-unendliche Linie:



Einseitig unendliche Linie:



Kreis:



Wir unterscheiden nun zwei Fälle.

Fall 1: Die Komponente enthält einen Knoten $b \in B$, der von keiner blauen Kante getroffen wird, also $b \notin f(A)$. Dann definieren wir in dieser ganzen Komponente ein Matching, indem wir alle roten Kanten wählen. Warum ist das ein perfektes Matching auf dieser Komponente? Jeder Knoten aus B liegt an genau einer roten Kante. Vom Startknoten b aus folgen wir einer roten Kante zu einem Knoten aus A, dann eventuell einer blauen Kante weiter zu einem Knoten aus B, dann wieder einer roten Kante, und so weiter. Auf diese Weise liegt auch jeder Knoten aus A in dieser Komponente an genau einer roten Kante.

Fall 2: Die Komponente enthält keinen Knoten aus $B \setminus f(A)$. Dann wird jeder Knoten aus B in dieser Komponente von einer blauen Kante getroffen. Außerdem liegt jeder Knoten aus A an genau einer blauen Kante. Also bilden die blauen Kanten in dieser Komponente ein perfektes Matching.

In jeder Komponente haben wir also ein perfektes Matching zwischen den A-Knoten und den B-Knoten dieser Komponente gewählt. Zusammengenommen erhalten wir ein perfektes Matching zwischen A und B. Dieses perfekte Matching definiert eine Bijektion $h\colon A \to B$. □

Bemerkung 8.5.3. In der letzten Beweiskonstruktion ist die Bijektion h explizit beschrieben. Auf Komponenten vom Typ Fall 2 setzen wir $h(a) = f(a)$. Auf Komponenten vom Typ Fall 1 verwenden wir die roten Kanten, also setzen wir $h(a) = b$, wobei b das eindeutig bestimmte Element mit $g(b) = a$ ist.

Satz 8.5.4. *Die Relation $\leq$ auf Kardinalitäten ist eine Ordnungsrelation.*

Beweis. Wie wir nach Lemma 8.4.2 geklärt haben, brauchen wir nur noch die Antisymmetrie zu begründen.

Nehmen wir dazu an, dass $|A| \leq |B|$ und $|B| \leq |A|$ gelten. Dann gibt es Injektionen $A \to B$ und $B \to A$. Nach dem Satz von Cantor-Schröder-Bernstein gibt es eine

Bijektion $A \to B$. Also gilt $|A| = |B|$. □

Mit dem Auswahlaxiom kann man sogar zeigen, dass diese Ordnungsrelation total ist: Für je zwei Mengen M und N gilt entweder $|M| \leq |N|$ oder $|N| \leq |M|$. Um diese Aussage zu beweisen, müssen wir das Auswahlaxiom allerdings noch etwas genauer betrachten, was wir im nächten Abschnitt machen werden.

8.6 Lemma von Zorn

In der mathematischen Alltagspraxis verwendet man das Auswahlaxiom nur selten direkt in der Form einer Auswahlfunktion. Die allermeisten Anwendungen laufen über die folgende äquivalente Formulierung.

Satz 8.6.1 (Lemma von Zorn)**.** *Sei $(M, \leq)$ eine nichtleere teilweise geordnete Menge. Angenommen, jede Kette $K \subseteq M$ besitzt eine obere Schranke in M, das heißt: Für jede Kette $K \subseteq M$ gibt es ein $x \in M$, so dass*

$$k \leq x$$

für alle $k \in K$ gilt. Dann besitzt M ein maximales Element.

Das Lemma von Zorn heißt auch ***Lemma von Kuratowski–Zorn***. Eine eng verwandte äquivalente Formulierung ist das ***Hausdorffsche Maximalitätsprinzip***. Über den übrigen ZF-Axiomen ist das Lemma von Zorn äquivalent zum Auswahlaxiom.

Die Richtung vom Auswahlaxiom zum Lemma von Zorn ist etwas aufwendig und würde uns zu weit weg von der linearen Algebra führen. Dafür müsste man insbesondere Ordnungstypen und Ordinalzahlen genauer besprechen. Für diese Notizen können wir das Lemma von Zorn daher als eine alternative Form des Auswahlaxioms auffassen.

Wir zeigen aber kurz die umgekehrte Richtung: Aus dem Lemma von Zorn folgt das Auswahlaxiom.

Proposition 8.6.2. *Das Lemma von Zorn impliziert das Auswahlaxiom.*

Beweis. Sei $(X_i)_{i \in I}$ eine Familie nichtleerer Mengen. Wir müssen eine Funktion

$$c \colon I \to \bigcup_{i \in I} X_i$$

finden, so dass $c(i) \in X_i$ für alle $i \in I$ gilt.

Wir betrachten die Menge P aller partiellen Auswahlfunktionen. Ein Element von P ist also eine Funktion

$$c \colon J \to \bigcup_{i \in I} X_i$$

für eine Teilmenge $J \subseteq I$, so dass

$$c(j) \in X_j$$

für alle $j \in J$ gilt. Wir ordnen P durch Fortsetzung: Für $c, d \in P$ schreiben wir $c \leq d$, wenn d die Funktion c fortsetzt, also $c \subseteq d$ wenn wir c und d als Relationen betrachten.

Wir wollen das Lemma von Zorn auf P anwenden. Sei dazu $K \subseteq P$ eine Kette. Dann sind die Funktionen in K miteinander verträglich, weil je zwei von ihnen durch Fortsetzung vergleichbar sind. Daher können wir ihre Vereinigung bilden:

$$u := \bigcup_{c \in K} c.$$

Diese Vereinigung ist wieder eine partielle Auswahlfunktion. Außerdem ist u eine obere Schranke von K in P.

Nach dem Lemma von Zorn besitzt P also ein maximales Element c. Wir zeigen, dass c auf ganz I definiert ist. Sei $J \subseteq I$ der Definitionsbereich von c. Angenommen, es gäbe ein $i_0 \in I \setminus J$. Da X_{i_0} nichtleer ist, gibt es ein Element $x_0 \in X_{i_0}$. Dann können wir c zu einer größeren partiellen Auswahlfunktion erweitern, indem wir zusätzlich

$$c(i_0) := x_0$$

setzen. Das widerspricht der Maximalität von c.

Also gilt $J = I$. Damit ist c eine Auswahlfunktion für die ganze Familie $(X_i)_{i \in I}$. □

Übung 8.6.3. *Seien M und N Mengen.*

(a) Zeigen Sie mit dem Lemma von Zorn: Es gibt eine injektive Funktion $M \to N$ oder eine injektive Funktion $N \to M$.

(b) Folgern Sie mit dem Satz von Cantor–Schröder–Bernstein, dass die Relation

$$|M| \leq |N| \quad \Longleftrightarrow \quad \textit{es gibt eine injektive Funktion } M \to N$$

eine totale Ordnung auf den Kardinalitäten definiert.

8.7 Mehr über unendliche Kardinalitäten

Wir haben gesehen, dass $\mathbb{N}$ und $\mathbb{R}$ nicht gleichmächtig sind. Es gibt also mindestens zwei verschiedene unendliche Kardinalitäten:

$$|\mathbb{N}| = \aleph_0, \qquad |\mathbb{R}| = \mathfrak{c}.$$

Die Kardinalität $\mathfrak{c}$ heißt die ***Kardinalität des Kontinuums***.

Satz 8.7.1. *Die Kardinalität $\aleph_0 = |\mathbb{N}|$ ist die kleinste unendliche Kardinalität. Anders gesagt: Ist M eine unendliche Menge, dann gilt*

$$|\mathbb{N}| \leq |M|\,.$$

Beweis. Wir müssen eine injektive Funktion $f\colon \mathbb{N} \to M$ konstruieren.

Da M unendlich ist, ist M nicht leer. Wir wählen ein Element $x_0 \in M$ und setzen $f(0) := x_0$.

Angenommen, $f(0), \dots, f(k)$ seien bereits definiert und paarweise verschieden. Die Menge

$$M \setminus \{f(0), \dots, f(k)\}$$

ist nicht leer, denn sonst wäre M endlich. Wir wählen also ein Element

$$x_{k+1} \in M \setminus \{f(0), \dots, f(k)\}$$

und setzen $f(k+1) := x_{k+1}$.

So erhalten wir rekursiv eine Funktion $f\colon \mathbb{N} \to M$. Nach Konstruktion sind die Werte $f(0), f(1), f(2), \dots$ paarweise verschieden. Also ist f injektiv. □

Bemerkung 8.7.2. Formal benutzt dieser rekursive Beweis eine Wahlmöglichkeit: In jedem Schritt wählen wir ein neues Element aus einer nichtleeren Menge. In unserer üblichen Mengenlehre mit Auswahlaxiom ist das erlaubt.

Satz 8.7.3 (Cantor 1874)**.** *Es gilt*

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|\,.$$

Beweis. Nach dem Satz von Cantor–Schröder–Bernstein genügt es, Injektionen in beide Richtungen zu konstruieren.

Zuerst konstruieren wir eine Injektion $\mathbb{R} \to \mathcal{P}(\mathbb{N})$. Da $\mathbb{Q}$ abzählbar ist, wählen wir eine Bijektion

$$e\colon \mathbb{N} \to \mathbb{Q}.$$

Jeder reellen Zahl $x \in \mathbb{R}$ ordnen wir die Menge

$$A_x := \{n \in \mathbb{N}\colon e(n) < x\}$$

zu. Damit erhalten wir eine Funktion

$$\mathbb{R} \to \mathcal{P}(\mathbb{N}), \qquad x \mapsto A_x.$$

Diese Funktion ist injektiv: Sind $x < y$, so gibt es eine rationale Zahl $q \in \mathbb{Q}$ mit $x < q < y$. Schreibe $q = e(n)$. Dann gilt $n \notin A_x$, aber $n \in A_y$. Also ist $A_x \neq A_y$.

Nun konstruieren wir eine Injektion $\mathcal{P}(\mathbb{N}) \to \mathbb{R}$. Einer Teilmenge $A \subseteq \mathbb{N}$ ordnen wir die reelle Zahl

$$r_A := \sum_{n \in A} \frac{2}{3^{n+1}}$$

zu. Diese Zahl liegt im Intervall $[0, 1]$.

Die Zuordnung $A \mapsto r_A$ ist injektiv. Sind nämlich $A \neq B$, so gibt es ein kleinstes $n \in \mathbb{N}$, für das sich A und B unterscheiden. Der Beitrag an der Stelle n ist dann $\frac{2}{3^{n+1}}$, während alle späteren Beiträge zusammen höchstens

$$\sum_{k>n} \frac{2}{3^{k+1}} = \frac{1}{3^{n+1}}$$

ausmachen. Der Unterschied an der ersten verschiedenen Stelle kann also durch die späteren Stellen nicht aufgehoben werden. Daher gilt $r_A \neq r_B$.

Damit haben wir Injektionen

$$\mathbb{R} \to \mathcal{P}(\mathbb{N}) \qquad \text{und} \qquad \mathcal{P}(\mathbb{N}) \to \mathbb{R}$$

konstruiert. Nach Cantor–Schröder–Bernstein folgt $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. □

8.8 Cantors Satz und die Kontinuumshypothese

Wir wissen nun:

$$|\mathbb{N}| = \aleph_0, \qquad |\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}.$$

Damit stellt sich sofort die nächste Frage: Gibt es noch größere unendliche Kardinalitäten?

Satz 8.8.1 (Cantor)**.** *Für jede Menge M gilt*

$$|M| < |\mathcal{P}(M)|\,.$$

Beweis. Zuerst gilt $|M| \leq |\mathcal{P}(M)|$, denn die Funktion

$$M \to \mathcal{P}(M), \qquad m \mapsto \{m\}$$

ist injektiv.

Wir zeigen nun, dass $|M| \neq |\mathcal{P}(M)|$. Angenommen, es gäbe eine bijektive Funktion

$$g\colon M \to \mathcal{P}(M).$$

Wir betrachten die Menge

$$X := \{x \in M : x \notin g(x)\}.$$

Da $X \subseteq M$ gilt, ist $X \in \mathcal{P}(M)$. Da g surjektiv ist, gibt es also ein $m \in M$ mit

$$g(m) = X.$$

Nun fragen wir, ob $m \in X$ gilt. Nach Definition von X gilt

$$m \in X \quad \Longleftrightarrow \quad m \notin g(m).$$

Da aber $g(m) = X$, erhalten wir

$$m \in X \quad \Longleftrightarrow \quad m \notin X.$$

Das ist ein Widerspruch. Also gibt es keine Bijektion $M \to \mathcal{P}(M)$, und somit gilt

$$|M| < |\mathcal{P}(M)|.$$

□

Damit gibt es nicht nur zwei verschiedene unendliche Kardinalitäten, sondern unendlich viele:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \cdots.$$

Da $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ gilt, können wir auch schreiben:

$$\aleph_0 < \mathfrak{c} < |\mathcal{P}(\mathbb{R})| < \cdots.$$

Eine naheliegende Frage bleibt offen: Gibt es eine Kardinalität strikt zwischen $\aleph_0$ und $\mathfrak{c}$? Anders gefragt: Gibt es eine Teilmenge $A \subseteq \mathbb{R}$, die überabzählbar ist, aber nicht dieselbe Kardinalität wie $\mathbb{R}$ hat?

Cantor vermutete, dass dies nicht der Fall ist.

Definition 8.8.2. Die ***Kontinuumshypothese*** ist die Aussage: Für jede Teilmenge $A \subseteq \mathbb{R}$ gilt entweder

$$|A| \leq \aleph_0$$

oder

$$|A| = \mathfrak{c}.$$

Die Kontinuumshypothese sagt also: Es gibt keine Kardinalität strikt zwischen der Kardinalität der natürlichen Zahlen und der Kardinalität der reellen Zahlen.

Bemerkung 8.8.3. Die Kontinuumshypothese kann aus den üblichen ZFC-Axiomen weder bewiesen noch widerlegt werden. Man sagt: Die Kontinuumshypothese ist ***unabhängig von ZFC***. Die beiden Richtungen dieser Unabhängigkeit gehen auf Arbeiten von Gödel und Cohen zurück.

Informell bedeutet das: Es gibt Modelle der ZFC-Axiome, in denen die Kontinuumshypothese gilt, und es gibt Modelle der ZFC-Axiome, in denen sie nicht gilt. Alle diese Modelle erfüllen dieselben Grundregeln der Mengenlehre, unterscheiden sich aber darin, welche Teilmengen der reellen Zahlen vorhanden sind.

Kapitel 9

Lineare Gleichungssysteme

In den bisherigen Kapiteln haben wir Grundlagen der mathematischen Sprache besprochen: Aussagen, Prädikate, Mengen, Relationen, Funktionen und Kardinalitäten. Ab diesem Kapitel beginnen wir mit der eigentlichen linearen Algebra.

Unser erstes Thema sind ***lineare Gleichungssysteme***. Einfache Beispiele sind

$$5X + 2Y = 3, \qquad 3.4X + \pi Y = 4,$$

oder auch

$$12X + 3Y + 4Z = 0, \qquad 3X + 12Y + 2Z = 0.$$

Allgemein betrachtet man Unbekannte $X_1, \ldots, X_n$ und Gleichungen, in denen keine Potenzen oder Produkte von Unbekannten auftreten. Zum Beispiel ist

$$2X + 3Y + 4XY = 0$$

keine lineare Gleichung, weil der Term XY ein Produkt von Unbekannten enthält.

Wir schreiben lineare Gleichungssysteme meistens so, dass die Terme mit Unbekannten auf der linken Seite stehen und die freien Terme auf der rechten Seite. Ein allgemeines lineares Gleichungssystem mit m Gleichungen und n Unbekannten hat die Form

$$\begin{array}{rcrcccrcl} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1, \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2, \\ & & & & \vdots & & & & \vdots \\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & + & a_{mn}X_n & = & b_m. \end{array}$$

Dabei sind die Koeffizienten a_{ij} und die rechten Seiten b_i Elemente einer festen Menge, in der wir rechnen dürfen. Eine Lösung ist ein Tupel $(x_1, \ldots, x_n)$, so dass alle Gleichungen nach Einsetzen von $X_i := x_i$ erfüllt sind.

Ein lineares Gleichungssystem kann keine Lösung, genau eine Lösung oder mehrere Lösungen haben. Zum Beispiel haben die Systeme

$$\begin{array}{rcl} 12X + 4Y + 2Z & = & 1, \\ 6X + 2Y + Z & = & 0 \end{array} \qquad \begin{array}{rcl} 5X + 2Y & = & 0, \\ 4X + 2Y & = & 0 \end{array} \qquad \begin{array}{rcl} X + Y & = & 1, \\ 2X + 2Y & = & 2 \end{array}$$

beziehungsweise keine, genau eine, und mehrere Lösungnen.

Bevor wir solche Systeme systematisch lösen können, müssen wir festlegen, in welcher Menge die Koeffizienten und die Lösungen liegen.

9.1 Körper

In der linearen Algebra nehmen wir meistens an, dass alle Koeffizienten und alle Lösungen Elemente eines festen ***Körpers*** sind. Ein Körper ist eine Verallgemeinerung der bekannten Zahlbereiche $\mathbb{Q}$ und $\mathbb{R}$: Man kann addieren, subtrahieren, multiplizieren und durch von Null verschiedene Elemente dividieren.

Definition 9.1.1. Ein ***Körper*** ist ein Tupel $(\mathbb{K}, +, \cdot)$, wobei $\mathbb{K}$ eine Menge mit mindestens zwei Elementen ist und

$$+ \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}, \qquad \cdot \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

zwei Verknüpfungen sind, die folgende Eigenschaften erfüllen.

(i) Addition und Multiplikation sind assoziativ: Für alle $a, b, c \in \mathbb{K}$ gilt

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

(ii) Addition und Multiplikation sind kommutativ: Für alle $a, b \in \mathbb{K}$ gilt

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

(iii) Es gilt das Distributivgesetz: Für alle $a, b, c \in \mathbb{K}$ gilt

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

(iv) Es gibt ein Element $0 \in \mathbb{K}$, so dass für alle $a \in \mathbb{K}$ gilt $a + 0 = a$. Außerdem gibt es zu jedem $a \in \mathbb{K}$ ein Element $b \in \mathbb{K}$ mit $a + b = 0$.

(v) Es gibt ein Element $1 \in \mathbb{K}$, so dass für alle $a \in \mathbb{K}$ gilt $a \cdot 1 = a$. Außerdem gibt es zu jedem $a \in \mathbb{K}$ mit $a \neq 0$ ein Element $b \in \mathbb{K}$ mit $a \cdot b = 1$.

Normalerweise sagen wir einfach "sei $\mathbb{K}$ ein Körper", auch wenn genauer das Tupel $(\mathbb{K}, +, \cdot)$ gemeint ist. Außerdem schreiben wir meistens ab statt $a \cdot b$.

Proposition 9.1.2. *In einem Körper ist das Nullelement eindeutig bestimmt.*

Beweis. Seien 0 und $0'$ zwei Elemente von $\mathbb{K}$, die beide die Eigenschaft eines neutralen Elements für die Addition haben. Dann gilt

$$0 = 0 + 0' = 0'.$$

Also sind sie gleich. □

Ähnlich zeigt man, dass das Einselement 1 eindeutig bestimmt ist.

Proposition 9.1.3. *Sei $\mathbb{K}$ ein Körper und sei $a \in \mathbb{K}$. Dann gibt es genau ein Element $b \in \mathbb{K}$ mit $a + b = 0$.*

Beweis. Die Existenz gehört zur Definition eines Körpers. Wir zeigen die Eindeutigkeit. Seien $b, b' \in \mathbb{K}$ mit

$$a + b = 0 \qquad \text{und} \qquad a + b' = 0.$$

Dann gilt

$$b = b + 0 = b + (a + b') = (b + a) + b' = (a + b) + b' = 0 + b' = b'.$$

Also ist $b = b'$. □

Dieses eindeutig bestimmte Element heißt das ***additive Inverse*** von a. Wir bezeichnen es mit $-a$. Außerdem schreiben wir $c + (-a)$ meistens als $c - a$.

Analog gilt: Für jedes $a \in \mathbb{K}$ mit $a \neq 0$ gibt es genau ein Element $b \in \mathbb{K}$ mit $ab = 1$. Dieses Element heißt das ***multiplikative Inverse*** von a. Wir bezeichnen es mit a^{-1} oder $\frac{1}{a}$. Außerdem schreiben wir $c \cdot a^{-1}$ meistens als $\frac{c}{a}$.

Beispiele 9.1.4. *Die Mengen $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.*

Die Mengen $\mathbb{N}$ und $\mathbb{Z}$ sind keine Körper. In $\mathbb{N}$ kann man zum Beispiel nicht beliebig subtrahieren. In $\mathbb{Z}$ kann man nicht durch jedes von Null verschiedene Element dividieren: Es gibt kein $b \in \mathbb{Z}$ mit $2b = 1$.

Auch die Menge $\mathbb{Q}[X]$ der Polynome mit rationalen Koeffizienten ist kein Körper, denn das Polynom X besitzt in $\mathbb{Q}[X]$ kein multiplikatives Inverses.

Die einelementige Menge $\{0\}$ ist ebenfalls kein Körper, da in einem Körper $0 \neq 1$ gelten muss.

9.1.1 Der Körper der komplexen Zahlen

Neben $\mathbb{Q}$ und $\mathbb{R}$ ist der wichtigste Körper für uns der Körper $\mathbb{C}$ der komplexen Zahlen. Als Menge ist

$$\mathbb{C} := \{a + bi \colon a, b \in \mathbb{R}\},$$

wobei i die ***imaginäre Einheit*** ist und die Eigenschaft $i^2 = -1$ hat. Formal kann man $\mathbb{C}$ als $\mathbb{R} \times \mathbb{R}$ auffassen.

Die Addition und Multiplikation sind definiert durch

$$(a + bi) + (c + di) := (a + c) + (b + d)i$$

und

$$(a + bi)(c + di) := (ac - bd) + (ad + bc)i.$$

Ist $z = a + bi \in \mathbb{C}$, so definieren wir die ***komplex konjugierte Zahl***

$$\overline{z} := a - bi$$

und den ***Betrag***

$$|z| := \sqrt{a^2 + b^2}.$$

Dann gilt

$$z\overline{z} = |z|^2 .$$

Falls $z \neq 0$, folgt daraus

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Insbesondere besitzt jede von Null verschiedene komplexe Zahl ein multiplikatives Inverses.

Bemerkung 9.1.5. Eine komplexe Zahl $z = a + bi$ kann man als Punkt der Ebene mit Koordinaten (a, b) visualisieren. Ist $z \neq 0$, so kann man schreiben

$$z = |z| (\cos \varphi + i \sin \varphi)$$

für ein $\varphi \in \mathbb{R}$. Wählt man $\varphi \in [0, 2\pi)$, so ist φ eindeutig bestimmt und heißt das ***Argument*** von z.

Die Addition komplexer Zahlen entspricht der Addition von Vektoren in der Ebene. Die Multiplikation hat eine geometrische Bedeutung: Sie multipliziert die Beträge und addiert die Argumente. Genauer gilt

$$\big(|z| (\cos \varphi + i \sin \varphi)\big)\big(|w| (\cos \psi + i \sin \psi)\big) = |z|\ |w| \big(\cos(\varphi + \psi) + i \sin(\varphi + \psi)\big).$$

Der wichtigste Grund dafür, dass $\mathbb{C}$ in der Mathematik eine so zentrale Rolle spielt, ist im folgenden Satz enthalten.

Satz 9.1.6 (Fundamentalsatz der Algebra)**.** *Sei $P(X) \in \mathbb{C}[X]$ ein nichtkonstantes Polynom. Dann gibt es ein $z \in \mathbb{C}$ mit*

$$P(z) = 0.$$

Wir werden diesen Satz im Modul Algebra 1 beweisen. Der Körper $\mathbb{R}$ hat diese Eigenschaft nicht: Die Gleichung

$$X^2 + 1 = 0$$

hat keine Lösung in $\mathbb{R}$.

Eine wichtige Folgerung des Fundamentalsatzes ist: Ist

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$$

ein Polynom vom Grad d mit komplexen Koeffizienten, dann gibt es $\lambda_1, \ldots, \lambda_d \in \mathbb{C}$, so dass

$$P(X) = (X - \lambda_1) \cdots (X - \lambda_d).$$

9.1.2 Endliche Körper der Form $\mathbb{Z}/p$

Sei $n \in \mathbb{N}_+$. Wir bezeichnen mit $\mathbb{Z}/n$ die Menge der Kongruenzklassen modulo n:

$$\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}.$$

Addition und Multiplikation definieren wir durch

$$[a] + [b] := [a + b], \qquad [a] \cdot [b] := [ab].$$

Diese Operationen sind wegen Satzes 2.3.2 wohldefiniert.

In der Praxis schreiben wir Rechnungen in $\mathbb{Z}/n$ meistens mit Kongruenzen. Statt $[a] = [b]$ schreiben wir also häufig $a \equiv b \mod n$. Die Kongruenzklassen sind vor allem wichtig, um die Menge $\mathbb{Z}/n$ und ihre Operationen formal korrekt zu definieren. Zum Beispiel bedeutet $[7] \cdot [6] = [1]$ in $\mathbb{Z}/41$ genau dasselbe wie $7 \cdot 6 \equiv 1 \mod 41$.

Proposition 9.1.7. *Ist p eine Primzahl, dann ist $\mathbb{Z}/p$ ein Körper.*

Beweis. Alle Körperaxiome außer der Existenz multiplikativer Inverser folgen direkt aus den Rechenregeln in $\mathbb{Z}$. Sei also $[a] \neq [0]$ in $\mathbb{Z}/p$. Dann gilt $p \nmid a$. Da p prim ist, folgt $\mathrm{ggT}(a, p) = 1$. Nach Bézout gibt es $r, s \in \mathbb{Z}$ mit

$$ra + sp = 1.$$

Modulo p erhalten wir

$$[r][a] = [1].$$

Also besitzt $[a]$ das multiplikative Inverse $[r]$. □

Zum Beispiel gilt in $\mathbb{Z}/41$, dass $[7]^{-1} = [6]$.

Von nun an bedeutet ein ***lineares Gleichungssystem über einem Körper*** $\mathbb{K}$, dass alle Koeffizienten a_{ij}, alle rechten Seiten b_i und alle gesuchten Lösungen x_i Elemente von $\mathbb{K}$ sind. Das allgemeine Problem lautet also:

Gegeben seien $a_{ij}, b_i \in \mathbb{K}$. Finde alle Tupel

$$(x_1, \ldots, x_n) \in \mathbb{K}^n,$$

so dass für alle $i = 1, \ldots, m$ gilt

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i.$$

9.2 Gleichungssysteme und die Zeilenstufenform

Wir haben nun Körper offiziell eingeführt. Deshalb können wir den Begriff eines linearen Gleichungssystems präzise formulieren.

Definition 9.2.1. Sei $\mathbb{K}$ ein Körper. Ein ***lineares Gleichungssystem über*** $\mathbb{K}$ mit m Gleichungen und n Unbekannten ist ein System der Form

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1, \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & b_2, \\ & & & & \vdots & & & & \vdots \\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & + & a_{mn}X_n & = & b_m, \end{array}$$

wobei alle Koeffizienten a_{ij} und alle rechten Seiten b_i Elemente von $\mathbb{K}$ sind.

Eine ***Lösung*** dieses Gleichungssystems ist ein Tupel $(x_1, \ldots, x_n) \in \mathbb{K}^n$, so dass nach Einsetzen von $X_i := x_i$ alle Gleichungen erfüllt sind.

Unser Ziel ist es, alle Lösungen eines gegebenen linearen Gleichungssystems zu finden. Das wichtigste Verfahren dafür ist das ***Gaußsche Eliminationsverfahren***. Die Idee ist, das Gleichungssystem durch einfache Umformungen Schritt für Schritt in eine besonders übersichtliche Form zu bringen.

Definition 9.2.2. Ein lineares Gleichungssystem ist in ***Zeilenstufenform***, wenn es ein $r \in \{0, \ldots, m\}$ gibt, so dass die folgenden Bedingungen erfüllt sind.

(i) Die ersten r Gleichungen haben auf der linken Seite mindestens einen von Null verschiedenen Koeffizienten. Die letzten $m - r$ Gleichungen haben die Form

$$0 = b_i.$$

(ii) Für $i = 1, \ldots, r$ sei $j(i)$ der kleinste Index mit $a_{i,j(i)} \neq 0$. Dann gilt

$$j(1) < j(2) < \cdots < j(r).$$

Die Koeffizienten $a_{i,j(i)}$ heißen die ***Pivots*** des Systems. Die zugehörigen Variablen $X_{j(1)}, \ldots, X_{j(r)}$ heißen die ***Pivotvariablen*** oder ***gebundenen Variablen***. Alle anderen Variablen heißen ***freie Variablen***.

Beispiele 9.2.3. *(i) Das Gleichungssystem*

$$\begin{aligned} X + 2Y - Z &= 3, \\ 3Y + 2Z &= 5, \\ 4Z &= 8 \end{aligned}$$

ist in Zeilenstufenform. Die Pivotvariablen sind X, Y, Z, und es gibt keine freien Variablen.

Man kann dieses System von unten nach oben lösen. Aus der letzten Gleichung folgt $Z = 2$. Dann folgt aus der zweiten Gleichung

$$3Y + 2 \cdot 2 = 5,$$

also $Y = \frac{1}{3}$. Schließlich folgt aus der ersten Gleichung

$$X + 2 \cdot \frac{1}{3} - 2 = 3,$$

also $X = \frac{13}{3}$. Das System hat also genau eine Lösung.

(ii) Das Gleichungssystem

$$\begin{aligned} X + 2Y - Z + 3W &= 1, \\ Y + 4Z - W &= 2 \end{aligned}$$

ist ebenfalls in Zeilenstufenform. Die Pivotvariablen sind X und Y. Die Variablen Z und W sind frei.

Wir können also Z und W beliebig wählen. Schreiben wir

$$Z := s, \qquad W := t$$

mit $s, t \in \mathbb{K}$. Dann folgt aus der zweiten Gleichung

$$Y + 4s - t = 2,$$

also

$$Y = 2 - 4s + t.$$

Aus der ersten Gleichung folgt anschließend

$$X + 2(2 - 4s + t) - s + 3t = 1,$$

also

$$X = -3 + 9s - 5t.$$

Die Lösungen sind daher genau die Tupel

$$(X, Y, Z, W) = (-3 + 9s - 5t,\ 2 - 4s + t,\ s,\ t), \qquad s, t \in \mathbb{K}.$$

Bemerkung 9.2.4. An diesen Beispielen sieht man den Vorteil der Zeilenstufenform: Solche Systeme lassen sich durch Rückwärtseinsetzen lösen. Man beginnt mit der untersten nichttrivialen Gleichung und arbeitet sich nach oben. Freie Variablen dürfen beliebig gewählt werden; danach sind die gebundenen Variablen eindeutig bestimmt. Auf dieselbe Weise lässt sich jedes Gleichungssystem in Zeilenstufenform lösen.

9.3 Gaußsches Eliminationsverfahren

Das Gaußsche Eliminationsverfahren ist ein Verfahren, mit dem man jedes lineare Gleichungssystem in Zeilenstufenform bringen kann. Da Systeme in Zeilenstufenform leicht zu lösen sind, liefert dies zugleich ein systematisches Verfahren zum Lösen beliebiger linearer Gleichungssysteme.

Dazu müssen wir zuerst erklären, welche Umformungen eines Gleichungssystems erlaubt sind. Erlaubt sollen genau solche Umformungen sein, die die Lösungsmenge nicht verändern.

Wir bezeichnen die Zeilen eines Gleichungssystems (L) mit

$$Z_1, \ldots, Z_m.$$

Eine Zeile meint hier die ganze Gleichung, also linke und rechte Seite.

Definition 9.3.1. Seien (L) und (R) zwei lineare Gleichungssysteme über $\mathbb{K}$ mit denselben Unbekannten und derselben Anzahl von Gleichungen. Wir sagen, dass (R) aus (L) durch eine ***elementare Zeilenumformung*** entsteht, wenn eine der folgenden beiden Operationen ausgeführt wird.

(1) Zwei Zeilen werden vertauscht.

(2) Zu einer Zeile wird ein Vielfaches einer anderen Zeile addiert:

$$Z_i \longmapsto Z_i + \lambda Z_j,$$

wobei $i \neq j$ und $\lambda \in \mathbb{K}$ gilt. Alle anderen Zeilen bleiben unverändert.

Zwei lineare Gleichungssysteme heißen ***äquivalent***, wenn eines aus dem anderen durch eine Folge elementarer Zeilenumformungen entsteht.

Jede elementare Zeilenumformung kann wieder rückgängig gemacht werden: Ein Zeilentausch ist seine eigene Umkehrung, und die Umformung $Z_i \mapsto Z_i + \lambda Z_j$ wird durch $Z_i \mapsto Z_i - \lambda Z_j$ rückgängig gemacht. Deshalb ist Äquivalenz von Gleichungssystemen tatsächlich eine Äquivalenzrelation.

Beispiel 9.3.2. *Betrachten wir das Gleichungssystem*

$$\begin{aligned} X + Y - Z &= 2, \\ 2X + 3Y + Z &= 5, \\ -X + Y + 2Z &= 1. \end{aligned}$$

Wir bezeichnen die drei Zeilen mit Z_1, Z_2, Z_3.

Zuerst vertauschen wir die erste und die dritte Zeile. Dann erhalten wir das äquivalente System

$$\begin{aligned} -X + Y + 2Z &= 1, \\ 2X + 3Y + Z &= 5, \\ X + Y - Z &= 2. \end{aligned}$$

Dies ist eine elementare Zeilenumformung vom ersten Typ.

Nun addieren wir das Doppelte der ersten Zeile zur zweiten Zeile, also ersetzen wir Z_2 durch $Z_2 + 2Z_1$. Die zweite Zeile wird dadurch zu

$$(2X + 3Y + Z) + 2(-X + Y + 2Z) = 5 + 2 \cdot 1,$$

also zu

$$5Y + 5Z = 7.$$

Wir erhalten das System

$$\begin{aligned} -X + Y + 2Z &= 1, \\ 5Y + 5Z &= 7, \\ X + Y - Z &= 2. \end{aligned}$$

Dies ist eine elementare Zeilenumformung vom zweiten Typ.

Beide Umformungen können rückgängig gemacht werden. Den Zeilentausch machen wir durch denselben Zeilentausch rückgängig. Die Umformung $Z_2 \mapsto Z_2 + 2Z_1$ machen wir durch $Z_2 \mapsto Z_2 - 2Z_1$ rückgängig.

Lemma 9.3.3. *Äquivalente lineare Gleichungssysteme haben dieselbe Lösungsmenge.*

Beweis. Es genügt, den Fall zu betrachten, in dem (R) aus (L) durch eine einzige elementare Zeilenumformung entsteht.

Beim Vertauschen zweier Zeilen ändert sich offensichtlich nicht, welche Tupel $(x_1, \ldots, x_n)$

alle Gleichungen erfüllen.

Betrachten wir also eine Umformung der Form

$$Z_i \longmapsto Z_i + \lambda Z_j.$$

Schreiben wir die i-te und j-te Gleichung von (L) als

$$a_{i1}X_1 + \cdots + a_{in}X_n = b_i$$

und

$$a_{j1}X_1 + \cdots + a_{jn}X_n = b_j.$$

Dann lautet die neue i-te Gleichung

$$(a_{i1} + \lambda a_{j1})X_1 + \cdots + (a_{in} + \lambda a_{jn})X_n = b_i + \lambda b_j.$$

Jede Lösung der alten beiden Gleichungen erfüllt auch diese neue Gleichung. Also ist jede Lösung von (L) auch eine Lösung von (R).

Da die Zeilenumformung umkehrbar ist, gilt umgekehrt auch: Jede Lösung von (R) ist eine Lösung von (L). Also haben (L) und (R) dieselbe Lösungsmenge. □

Wir sind nun bereit, das ***Gaußsche Eliminationsverfahren*** zu formulieren. Wie oft in der Mathematik ist die Aussage des nächsten Satzes zunächst nur eine Existenzbehauptung: Es gibt ein äquivalentes System in Zeilenstufenform. Der Beweis liefert aber mehr als das. Er beschreibt ein konkretes Verfahren, mit dem man ein solches System findet. Dieses Verfahren heißt das Gaußsche Eliminationsverfahren.

Satz 9.3.4. *Jedes lineare Gleichungssystem über einem Körper ist äquivalent zu einem linearen Gleichungssystem in Zeilenstufenform.*

Beweis. Wir beschreiben ein Verfahren, das ein gegebenes System durch elementare Zeilenumformungen in Zeilenstufenform bringt.

Zuerst suchen wir in der ersten Spalte nach einem von Null verschiedenen Koeffizienten. Gibt es einen solchen Koeffizienten a_{i1}, dann vertauschen wir die erste Zeile mit der i-ten Zeile. Danach ist der Koeffizient a_{11} von Null verschieden. Für jede Zeile $k = 2, \ldots, m$ ersetzen wir dann

$$Z_k \quad \text{durch} \quad Z_k - \frac{a_{k1}}{a_{11}} Z_1.$$

Danach sind alle Einträge unterhalb des ersten Pivots in der ersten Spalte gleich Null.

Falls es in der ersten Spalte keinen von Null verschiedenen Koeffizienten gibt, gehen wir zur nächsten Spalte über, und so weiter, bis wir eine Spalte finden, die mindestens einen von Null verschiedenen Koeffizienten enthält. Diese Spalte behandeln wir dann als die erste relevante Spalte.

Nach diesem ersten Schritt betrachten wir nur noch die Zeilen $Z_2, \ldots, Z_m$. Die erste Zeile wird von nun an nicht mehr verändert. Im verbleibenden Teil des Systems suchen wir wieder eine Spalte, die in den Zeilen $Z_2, \ldots, Z_m$ einen von Null verschiedenen Koeffizienten enthält, und die so weit links wie möglich liegt. Durch einen Zeilentausch bringen wir einen solchen Koeffizienten in die zweite Zeile. Danach addieren wir geeignete Vielfache der zweiten Zeile zu den darunterliegenden Zeilen, so dass unter diesem Pivot nur noch Nullen stehen.

Anschließend wird auch die zweite Zeile nicht mehr verändert. Wir arbeiten dann nur noch mit den Zeilen $Z_3, \ldots, Z_m$ weiter und wiederholen dasselbe Verfahren. Nach endlich vielen Schritten erhalten wir ein System, bei dem die Pivotpositionen von Zeile zu Zeile nach rechts wandern und alle Nullzeilen unten stehen. Das ist genau ein System in Zeilenstufenform. □

Damit erhalten wir ein systematisches Verfahren zum Lösen linearer Gleichungssysteme, das wir im nächsten Satz zusammenfassen.

Satz 9.3.5. *Sei ein lineares Gleichungssystem über $\mathbb{K}$ gegeben. Wir bringen es durch das Gaußsche Eliminationsverfahren in Zeilenstufenform.*

(i) Falls eine Gleichung der Form

$$0 = b$$

mit $b \neq 0$ auftritt, dann hat das Gleichungssystem keine Lösung.

(ii) Falls keine solche Gleichung auftritt, entfernen wir alle Gleichungen der Form $0 = 0$. Sei r die Anzahl der verbleibenden Gleichungen, und seien $X_{j(1)}, \ldots, X_{j(r)}$ die gebundenen Variablen.

Wenn es keine freien Variablen gibt, dann hat das Gleichungssystem genau eine Lösung.

Wenn es freie Variablen gibt, dann erhält man für jede Belegung der freien Variablen genau eine Lösung.

Beweis. Nach dem Lemma 9.3.3 verändern die elementaren Zeilenumformungen die Lösungsmenge nicht. Wir dürfen also das System in Zeilenstufenform betrachten.

Eine Gleichung der Form $0 = b$ mit $b \neq 0$ kann von keinem Tupel $(x_1, \ldots, x_n)$ erfüllt werden. In diesem Fall gibt es also keine Lösung.

Nehmen wir nun an, dass nur Gleichungen der Form $0 = 0$ unten auftreten. Diese Gleichungen liefern keine Einschränkung und können entfernt werden.

In einer Zeilenstufenform kann man die gebundenen Variablen von unten nach oben bestimmen. In der letzten nichttrivialen Gleichung kommt die letzte gebundene Variable mit einem von Null verschiedenen Koeffizienten vor, und die späteren Variablen, falls vorhanden, sind frei.

Nach der Belegund den freien Variablen in dieser letzten Zeile,kann man eindeutig nach gebundenen Variable auflösen. Danach geht man eine Zeile nach oben und wiederholt dasselbe Argument.

Wenn es gar keine freien Variablen in der Zeilenstufenform gibt, ist dadurch jede Variable eindeutig bestimmt. Es gibt also genau eine Lösung.

Wenn es freie Variablen gibt, können diese beliebig gewählt werden. Nach jeder solchen Wahl bestimmt das Rückwärtseinsetzen eindeutig alle gebundenen Variablen. Also erhält man für jede Belegung der freien Variablen genau eine Lösung. □

Kapitel 10

Vektorräume

10.1 Was jetzt?

Im letzten Kapitel haben wir das Gaußsche Eliminationsverfahren kennengelernt. Es ist ein sehr effizientes Verfahren, um lineare Gleichungssysteme zu lösen.

In gewissem Sinne könnte man nun fragen: Gibt es jetzt noch etwas zu tun, oder können wir nach Hause gehen? Zumindest können wir versuchen, die Lösungsmengen linearer Gleichungssysteme besser zu verstehen.

Als motivierende Frage betrachten wir die folgende. Beim Gaußschen Eliminationsverfahren können wir manchmal verschiedene Pivots wählen. Dadurch können verschiedene äquivalente Systeme in Zeilenstufenform entstehen. Ist die Anzahl der freien Variablen trotzdem immer gleich?

Für endliche Körper ist das schon jetzt plausibel. Angenommen, $\mathbb{K}$ hat endlich viele Elemente und unser Gleichungssystem ist lösbar. Eine Zeilenstufenform mit r Pivotvariablen liefert eine Bijektion zwischen $\mathbb{K}^{n-r}$ und der Lösungsmenge. Die Lösungsmenge selbst hängt aber nur vom ursprünglichen Gleichungssystem ab, nicht von unseren Entscheidungen im Gaußschen Verfahren. Also ist auch

$$\left|\mathbb{K}^{n-r}\right| = |\mathbb{K}|^{n-r}$$

unabhängig von diesen Entscheidungen. Da $|\mathbb{K}| > 1$, folgt daraus, dass $n - r$ unabhängig von den Pivotwahlen ist. Also ist auch r unabhängig von den Pivotwahlen.

Dieses Argument funktioniert für unendliche Körper nicht. Zum Beispiel gibt es eine Bijektion

$$\mathbb{Q} \to \mathbb{Q}^2.$$

Die reine Mächtigkeit einer Menge unterscheidet also nicht zwischen "einem Parameter" und "zwei Parametern". Wenn wir über unendlichen Körpern arbeiten, brauchen wir einen feineren Begriff als nur die Kardinalität der Lösungsmenge. Dieser feinere Begriff wird die Dimension eines Vektorraums sein, und wir werden es in diesem Kapitel einführen.

Es gibt noch eine zweite Perspektive. Wir hatten am Anfang des Semesters das Motto: Alles ist eine Menge. Was ist dann eigentlich ein Gleichungssystem?

Die linke Seite eines linearen Gleichungssystems definiert eine Funktion

$$A\colon \mathbb{K}^n \to \mathbb{K}^m.$$

Sie ordnet einem Tupel $(x_1, \dots, x_n) \in \mathbb{K}^n$ das Tupel

$$\begin{aligned}(&a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n,\\ &a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n,\\ &\dots,\\ &a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n)\end{aligned}$$

in $\mathbb{K}^m$ zu. Das Gleichungssystem fragt dann nach dem Urbild des Elements

$$(b_1, \dots, b_m) \in \mathbb{K}^m.$$

Es fragt also nach allen $\mathbf{x} \in \mathbb{K}^n$ mit

$$A(\mathbf{x}) = \mathbf{b},$$

wobei $\mathbf{b} = (b_1, \dots, b_m)$.

Lineare Algebra beschäftigt sich genau mit solchen Funktionen und ihren Eigenschaften. Um diese Eigenschaften systematisch zu untersuchen, führen wir zuerst Vektorräume ein.

10.2 Vektorräume

Ein Vektorraum ist eine Verallgemeinerung von $\mathbb{R}^2$ oder $\mathbb{R}^3$. Er besteht aus Objekten, die wir addieren können und die wir mit Skalaren multiplizieren können. Die eigentliche Definition ist etwas länger, weil wir genau alle üblichen Eigenschaften der Addition von Vektoren in $\mathbb{R}^2$ oder $\mathbb{R}^3$ auflisten sollen.

Definition 10.2.1. Sei $\mathbb{K}$ ein Körper. Ein ***Vektorraum über*** $\mathbb{K}$ ist ein Tupel $(V, +, \mu)$, wobei V eine Menge ist,

$$+\colon V \times V \to V$$

eine Addition und

$$\mu\colon \mathbb{K} \times V \to V$$

eine Skalarmultiplikation ist. Wir schreiben $\mu(a, \mathbf{v})$ meistens als $a\mathbf{v}$ oder $a \cdot \mathbf{v}$. Die folgenden Eigenschaften müssen erfüllt sein.

(i) Die Addition ist kommutativ und assoziativ: Für alle $\mathbf{v}, \mathbf{w}, \mathbf{u} \in V$ gilt

$$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$$

und

$$(\mathbf{v} + \mathbf{w}) + \mathbf{u} = \mathbf{v} + (\mathbf{w} + \mathbf{u}).$$

(ii) Es gibt ein Element $\mathbf{0} \in V$, so dass für alle $\mathbf{v} \in V$ gilt

$$\mathbf{v} + \mathbf{0} = \mathbf{v}.$$

(iii) Zu jedem $\mathbf{v} \in V$ gibt es ein $\mathbf{w} \in V$ mit

$$\mathbf{v} + \mathbf{w} = \mathbf{0}.$$

(iv) Die Skalarmultiplikation ist assoziativ: Für alle $a, b \in \mathbb{K}$ und alle $\mathbf{v} \in V$ gilt

$$a(b\mathbf{v}) = (ab)\mathbf{v}.$$

(v) Die Skalarmultiplikation ist distributiv gegenüber der Addition in V: Für alle $a \in \mathbb{K}$ und alle $\mathbf{v}, \mathbf{w} \in V$ gilt

$$a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}.$$

(vi) Die Skalarmultiplikation ist distributiv gegenüber der Addition in $\mathbb{K}$: Für alle $a, b \in \mathbb{K}$ und alle $\mathbf{v} \in V$ gilt

$$(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}.$$

(vii) Für alle $\mathbf{v} \in V$ gilt

$$1\mathbf{v} = \mathbf{v}.$$

Die Elemente von V heißen ***Vektoren***. Die Elemente von $\mathbb{K}$ heißen ***Skalare***. Wenn $\mathbb{K} = \mathbb{R}$, dann nennen wir V einen ***reellen Vektorraum***. Wenn $\mathbb{K} = \mathbb{C}$, dann nennen wir V einen ***komplexen Vektorraum***.

Jeder komplexe Vektorraum ist auch ein reeller Vektorraum: Man vergisst dabei einen Teil der Skalarmultiplikation und erlaubt nur noch Multiplikation mit reellen Zahlen $\lambda \in \mathbb{R} \subseteq \mathbb{C}$.

Die nächsten zwei Propositionen beschreiben einige grundlegeneden Eigenschaften eines Vektorraums, die leicht aus den Axiomen folgen.

Proposition 10.2.2. *In einem Vektorraum ist der Nullvektor* $\mathbf{0}$ *eindeutig bestimmt. Außerdem besitzt jeder Vektor* $\mathbf{v} \in V$ *ein eindeutig bestimmtes additives Inverses.*

Beweis. Der Beweis ist derselbe wie bei Körpern. Sind $\mathbf{0}$ und $\mathbf{0}'$ beide neutrale Elemente der Addition, dann gilt

$$\mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}'.$$

Also ist der Nullvektor eindeutig.

Seien nun $\mathbf{w}, \mathbf{w}' \in V$ beide additive Inverse zu $\mathbf{v}$. Dann gilt

$$\mathbf{v} + \mathbf{w} = \mathbf{0} \qquad \text{und} \qquad \mathbf{v} + \mathbf{w}' = \mathbf{0}.$$

Daher erhalten wir

$$\mathbf{w} = \mathbf{w} + \mathbf{0} = \mathbf{w} + (\mathbf{v} + \mathbf{w}') = (\mathbf{w} + \mathbf{v}) + \mathbf{w}' = (\mathbf{v} + \mathbf{w}) + \mathbf{w}' = \mathbf{0} + \mathbf{w}' = \mathbf{w}'.$$

Also ist auch das additive Inverse eindeutig. □

Das eindeutig bestimmte additive Inverse von $\mathbf{v}$ bezeichnen wir mit $-\mathbf{v}$. Außerdem schreiben wir

$$\mathbf{x} - \mathbf{y} := \mathbf{x} + (-\mathbf{y}).$$

Proposition 10.2.3. *Sei V ein Vektorraum über $\mathbb{K}$. Dann gelten für alle $\mathbf{v} \in V$ und alle $a \in \mathbb{K}$:*

$$0\mathbf{v} = \mathbf{0}, \qquad a\mathbf{0} = \mathbf{0}.$$

Außerdem gilt: Wenn

$$a\mathbf{v} = \mathbf{0},$$

dann ist $a = 0$ oder $\mathbf{v} = \mathbf{0}$.

Beweis. Zuerst gilt

$$0\mathbf{v} = (0 + 0)\mathbf{v} = 0\mathbf{v} + 0\mathbf{v}.$$

Addieren wir auf beiden Seiten das additive Inverse von $0\mathbf{v}$, so erhalten wir $0\mathbf{v} = \mathbf{0}$.

Ebenso gilt

$$a\mathbf{0} = a(\mathbf{0} + \mathbf{0}) = a\mathbf{0} + a\mathbf{0}.$$

Also ist $a\mathbf{0} = \mathbf{0}$.

Sei nun $a\mathbf{v} = \mathbf{0}$. Falls $a = 0$, sind wir fertig. Angenommen also $a \neq 0$. Dann existiert $a^{-1} \in \mathbb{K}$, und es folgt

$$\mathbf{v} = 1\mathbf{v} = (a^{-1}a)\mathbf{v} = a^{-1}(a\mathbf{v}) = a^{-1}\mathbf{0} = \mathbf{0}.$$

□

Beispiele 10.2.4. *(i) Für jeden Körper $\mathbb{K}$ und jedes $n \in \mathbb{N}$ ist $\mathbb{K}^n$ ein Vektorraum über $\mathbb{K}$. Die Elemente sind Tupel*

$$(a_1, \ldots, a_n), \qquad a_i \in \mathbb{K}.$$

Addition und Skalarmultiplikation sind komponentenweise definiert:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$$

und

$$\lambda(a_1, \dots, a_n) := (\lambda a_1, \dots, \lambda a_n).$$

Häufig schreiben wir Vektoren als Spalten, zum Beispiel

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \in \mathbb{R}^3, \qquad \begin{pmatrix} i \\ 1+i \end{pmatrix} \in \mathbb{C}^2.$$

Manchmal möchten wir einen Vektor als Spalte auffassen, aber aus Platzgründen als Zeile schreiben. Dann schreiben wir zum Beispiel $(1,2,3)^T$ *für den Spaltenvektor* $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$. *Der Buchstabe* T *steht für* ***Transposition****.*

(ii) Die Menge $\mathbb{K}[X]$ *aller Polynome mit Koeffizienten in* $\mathbb{K}$ *ist ein Vektorraum über* $\mathbb{K}$*. Auch*

$$\mathbb{K}_{\leqslant n}[X]$$

ist ein Vektorraum; das ist die Menge aller Polynome vom Grad höchstens n*, zusammen mit dem Nullpolynom.*

Ebenso sind die Mengen

$$\mathbb{K}[X_1, \dots, X_\ell]$$

und

$$\mathbb{K}_{\leqslant d}[X_1, \dots, X_\ell]$$

Vektorräume über $\mathbb{K}$*.*

(iii) Die Menge

$$\mathcal{F}([0,1], \mathbb{C})$$

aller Funktionen $f\colon [0,1] \to \mathbb{C}$ *ist ein komplexer Vektorraum. Die Addition und Skalarmultiplikation sind punktweise definiert:*

$$(f+g)(x) := f(x) + g(x), \qquad (\lambda f)(x) := \lambda f(x).$$

(iv) Die Menge $\{\mathbf{0}\}$ *ist ein Vektorraum über* $\mathbb{K}$*. Dieser Vektorraum heißt der* ***Nullvektorraum****. Wir bezeichnen auch diesen Vektorraum mit* $\mathbf{0}$*; aus dem Kontext wird klar sein, ob das Element* $\mathbf{0}$ *oder der Nullvektorraum gemeint ist.*

Beispiel 10.2.5. *Betrachten wir ein homogenes lineares Gleichungssystem über* $\mathbb{K}$*:*

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & 0, \\ a_{21}X_1 & + & a_{22}X_2 & + & \cdots & + & a_{2n}X_n & = & 0, \\ & & & & \vdots & & & & \vdots \\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & + & a_{mn}X_n & = & 0. \end{array}$$

Sei $V \subseteq \mathbb{K}^n$ die Menge aller Lösungen. Dann ist V ein Vektorraum über $\mathbb{K}$.

Tatsächlich: Der Nullvektor $\mathbf{0} \in \mathbb{K}^n$ ist eine Lösung. Sind $\mathbf{x}, \mathbf{y} \in V$ Lösungen, dann ist auch $\mathbf{x} + \mathbf{y}$ eine Lösung. Ist außerdem $\lambda \in \mathbb{K}$, dann ist auch $\lambda\mathbf{x}$ eine Lösung. Also ist V unter Addition und Skalarmultiplikation abgeschlossen, und damit ein Vektorraum.

Zum Beispiel ist die Lösungsmenge der Gleichung

$$X + Y + Z = 0$$

in $\mathbb{R}^3$ ein Vektorraum, den wir als eine Ebene durch den Ursprung visualisieren können.

10.3 Linearkombinationen und Basen

Sei V ein Vektorraum über dem Körper $\mathbb{K}$, und seien $\mathbf{v}_1, \ldots, \mathbf{v}_p \in V$. Eine ***Linearkombination*** der Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_p$ ist ein Vektor der Form

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_p\mathbf{v}_p = \sum_{k=1}^{p} a_k\mathbf{v}_k,$$

wobei $a_1, \ldots, a_p \in \mathbb{K}$.

Definition 10.3.1. Sei V ein Vektorraum über $\mathbb{K}$. Eine endliche Folge $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ heißt eine ***Basis*** von V, wenn jeder Vektor $\mathbf{v} \in V$ eine eindeutige Darstellung als Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$ besitzt. Das heißt: Für jeden Vektor $\mathbf{v} \in V$ gibt es eindeutig bestimmte Skalare $a_1, \ldots, a_n \in \mathbb{K}$ mit

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \sum_{k=1}^{n} a_k\mathbf{v}_k.$$

Die Skalare $a_1, \ldots, a_n$ heißen die ***Koordinaten*** von $\mathbf{v}$ bezüglich der Basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Bemerkung 10.3.2. Man könnte auch sagen, dass eine endliche Teilmenge $B \subseteq V$ eine Basis von V ist. Das bedeutet, dass jeder Vektor $\mathbf{v} \in V$ eine eindeutige Darstellung

$$\mathbf{v} = \sum_{\mathbf{w} \in B} a_{\mathbf{w}}\mathbf{w}$$

mit $a_{\mathbf{w}} \in \mathbb{K}$ besitzt.

Es ist aber häufig bequem, von einer Basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ zu sprechen. Die Reihenfolge ist für die Definition der Basis nicht wichtig, aber sie ist wichtig, wenn wir die Koordinaten eines Vektors als Tupel schreiben wollen.

Beispiele 10.3.3. *(i) Sei $V = \mathbb{K}^n$. Die Vektoren*

$$\mathbf{e}_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \mathbf{e}_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad \mathbf{e}_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

*bilden eine Basis von $\mathbb{K}^n$. Sie heißt die **Standardbasis** von $\mathbb{K}^n$.*

Tatsächlich gilt für

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$$

die Darstellung

$$\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n.$$

Diese Darstellung ist eindeutig: Wenn auch

$$\mathbf{x} = y_1\mathbf{e}_1 + y_2\mathbf{e}_2 + \cdots + y_n\mathbf{e}_n$$

gilt, dann folgt durch Vergleich der Koordinaten $x_1 = y_1, \ldots, x_n = y_n$.

(ii) Sei $V = \mathbb{K}_{\leq n}[X]$. Dann bilden die Polynome

$$1,\ X,\ X^2,\ \ldots,\ X^n$$

eine Basis von V. Denn jedes Polynom $P \in \mathbb{K}_{\leq n}[X]$ besitzt eine eindeutige Darstellung

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n.$$

(iii) Der Nullvektorraum $\mathbf{0}$ besitzt die leere Menge als Basis. Anders gesagt: Die leere Folge von Vektoren ist eine Basis des Nullvektorraums.

Beispiel 10.3.4. *Das lineare Gleichungssystem*

$$\begin{array}{ccccccccc} a_{11}X_1 & + & a_{12}X_2 & + & \cdots & + & a_{1n}X_n & = & b_1, \\ & & & & \vdots & & & & \vdots \\ a_{m1}X_1 & + & a_{m2}X_2 & + & \cdots & + & a_{mn}X_n & = & b_m \end{array}$$

können wir auch in Vektorform schreiben. Dazu betrachten wir die Spalten

$$\mathbf{a}_1 := \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \quad \mathbf{a}_2 := \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix}, \quad \ldots, \quad \mathbf{a}_n := \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

und

$$\mathbf{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Dann ist das Gleichungssystem äquivalent zu

$$X_1\mathbf{a}_1 + \cdots + X_n\mathbf{a}_n = \mathbf{b}.$$

Die Vektoren $\mathbf{a}_1, \ldots, \mathbf{a}_n$ sind also genau dann eine Basis von $\mathbb{K}^m$, wenn für jedes $\mathbf{b} \in \mathbb{K}^m$ das Gleichungssystem

$$X_1\mathbf{a}_1 + \cdots + X_n\mathbf{a}_n = \mathbf{b}$$

genau eine Lösung besitzt.

Bemerkung 10.3.5. Sei $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ eine Basis von V. Für einen Vektor

$$\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$$

bezeichnen wir den Koeffizientenvektor von $\mathbf{v}$ bezüglich $\mathcal{B}$ mit

$$[\mathbf{v}]_{\mathcal{B}} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n.$$

Da die Darstellung eines Vektors als Linearkombination der Basisvektoren eindeutig ist, erhalten wir eine Bijektion

$$V \to \mathbb{K}^n, \qquad \mathbf{v} \mapsto [\mathbf{v}]_{\mathcal{B}}.$$

Beispiel 10.3.6. *Sei $\mathbf{v} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \in \mathbb{R}^2$. Wir betrachten die Standardbasis*

$$\mathcal{B} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

und die Basis

$$\mathcal{C} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right).$$

Dann ist $[\mathbf{v}]_{\mathcal{B}} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$. Da

$$\mathbf{v} = 2\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

gilt außerdem $[\mathbf{v}]_{\mathcal{C}} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

10.4 Lineare Unabhängigkeit; Erzeugendensysteme

Eine Basis hat also zwei Eigenschaften: Jeder Vektor muss sich als Linearkombination darstellen lassen, und diese Darstellung muss eindeutig sein. Wir betrachten diese beiden Eigenschaften nun separat.

Definition 10.4.1. Sei V ein Vektorraum über $\mathbb{K}$, und seien $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$.

(i) Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ heißen ein ***Erzeugendensystem*** von V, wenn sich jeder Vektor $\mathbf{v} \in V$ als Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$ schreiben lässt. Das heißt: Für jedes $\mathbf{v} \in V$ gibt es $a_1, \ldots, a_n \in \mathbb{K}$ mit

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n.$$

Wir sagen auch, dass $\mathbf{v}_1, \ldots, \mathbf{v}_n$ den Vektorraum V ***aufspannen***.

(ii) Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ heißen ***linear unabhängig***, wenn die einzige Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$, die gleich $\mathbf{0}$ ist, die triviale Linearkombination ist. Das heißt: Aus

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$

folgt immer

$$a_1 = \cdots = a_n = 0.$$

Die Linearkombination

$$0\mathbf{v}_1 + \cdots + 0\mathbf{v}_n$$

heißt die ***triviale Linearkombination***. Man kann lineare Unabhängigkeit also auch so formulieren: Der Nullvektor $\mathbf{0}$ besitzt höchstens eine Darstellung als Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Wenn $\mathbf{v}_1, \ldots, \mathbf{v}_n$ nicht linear unabhängig sind, dann heißen sie ***linear abhängig***. Das bedeutet: Es gibt $a_1, \ldots, a_n \in \mathbb{K}$, nicht alle gleich Null, so dass

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}.$$

Bemerkung 10.4.2. Man kann die beiden Begriffe auch mit Gleichungen formulieren.

Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sind genau dann ein Erzeugendensystem von V, wenn für jedes $\mathbf{b} \in V$ die Gleichung

$$X_1\mathbf{v}_1 + \cdots + X_n\mathbf{v}_n = \mathbf{b}$$

mindestens eine Lösung besitzt.

Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sind genau dann linear unabhängig, wenn die Gleichung

$$X_1\mathbf{v}_1 + \cdots + X_n\mathbf{v}_n = \mathbf{0}$$

genau eine Lösung besitzt, nämlich die triviale Lösung $X_1 = \cdots = X_n = 0$.

Proposition 10.4.3. *Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ sind genau dann linear unabhängig, wenn jeder Vektor $\mathbf{v} \in V$ höchstens eine Darstellung als Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$ besitzt.*

Beweis. Angenommen, jeder Vektor besitzt höchstens eine Darstellung als Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Dann besitzt insbesondere $\mathbf{0}$ höchstens eine solche Darstellung. Da

$$\mathbf{0} = 0\mathbf{v}_1 + \cdots + 0\mathbf{v}_n$$

eine Darstellung ist, ist dies die einzige Darstellung von $\mathbf{0}$. Also sind $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear unabhängig.

Seien nun umgekehrt $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear unabhängig. Angenommen, ein Vektor $\mathbf{v} \in V$ habe zwei Darstellungen

$$\mathbf{v} = \sum_{i=1}^{n} x_i\mathbf{v}_i \qquad \text{und} \qquad \mathbf{v} = \sum_{i=1}^{n} y_i\mathbf{v}_i.$$

Dann gilt

$$\mathbf{0} = \sum_{i=1}^{n} x_i\mathbf{v}_i - \sum_{i=1}^{n} y_i\mathbf{v}_i = \sum_{i=1}^{n} (x_i - y_i)\mathbf{v}_i.$$

Aus der linearen Unabhängigkeit folgt $x_i - y_i = 0$ für alle i. Also gilt $x_i = y_i$ für alle i, und die beiden Darstellungen waren gleich. □

Folgerung 10.4.4. *Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ bilden genau dann eine Basis von V, wenn sie ein Erzeugendensystem von V und linear unabhängig sind.*

Proposition 10.4.5. *Die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ sind genau dann linear abhängig, wenn einer der Vektoren $\mathbf{v}_i$ eine Linearkombination der anderen Vektoren ist.*

Beweis. Seien $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear abhängig. Dann gibt es Skalare $a_1, \ldots, a_n \in \mathbb{K}$, nicht alle gleich Null, mit

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}.$$

Wähle ein i mit $a_i \neq 0$. Dann können wir nach $\mathbf{v}_i$ auflösen:

$$\mathbf{v}_i = \sum_{j \neq i} \frac{-a_j}{a_i} \mathbf{v}_j.$$

Also ist $\mathbf{v}_i$ eine Linearkombination der anderen Vektoren.

Sei umgekehrt ein Vektor $\mathbf{v}_i$ eine Linearkombination der anderen Vektoren, also

$$\mathbf{v}_i = \sum_{j \neq i} a_j \mathbf{v}_j.$$

Dann gilt

$$\mathbf{0} = \mathbf{v}_i - \sum_{j \neq i} a_j \mathbf{v}_j.$$

Dies ist eine nichttriviale Linearkombination von $\mathbf{v}_1, \ldots, \mathbf{v}_n$, die gleich $\mathbf{0}$ ist. Also sind die Vektoren linear abhängig. □

Proposition 10.4.6. *Jedes endliche Erzeugendensystem enthält eine Basis.*

Beweis. Sei $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ ein Erzeugendensystem von V. Falls $V = \mathbf{0}$, dann enthält dieses System die leere Basis von V, und wir sind fertig. Wir nehmen also $V \neq \mathbf{0}$ an.

Falls $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear unabhängig sind, dann bilden sie eine Basis.

Falls sie linear abhängig sind, dann ist nach der vorherigen Proposition einer der Vektoren, sagen wir $\mathbf{v}_i$, eine Linearkombination der anderen Vektoren:

$$\mathbf{v}_i = \sum_{j \neq i} a_j \mathbf{v}_j.$$

Wir behaupten, dass die übrigen Vektoren immer noch ein Erzeugendensystem von V bilden. Sei dazu $\mathbf{v} \in V$. Da $\mathbf{v}_1, \ldots, \mathbf{v}_n$ ein Erzeugendensystem sind, gibt es Skalare $b_1, \ldots, b_n \in \mathbb{K}$ mit

$$\mathbf{v} = \sum_{j=1}^{n} b_j \mathbf{v}_j.$$

Setzen wir die Darstellung von $\mathbf{v}_i$ ein, so erhalten wir

$$\mathbf{v} = \sum_{j \neq i} b_j \mathbf{v}_j + b_i \sum_{j \neq i} a_j \mathbf{v}_j.$$

Also ist $\mathbf{v}$ eine Linearkombination der Vektoren $\mathbf{v}_j$ mit $j \neq i$. Wir können $\mathbf{v}_i$ daher entfernen, ohne die Erzeugendeneigenschaft zu verlieren.

Wiederholen wir dieses Argument, so erhalten wir nach endlich vielen Schritten ein Erzeugendensystem, das linear unabhängig ist. Dieses System ist dann eine Basis.

Falls am Ende nur ein Vektor $\mathbf{w}$ übrig bleibt, so ist $\mathbf{w} \neq \mathbf{0}$, weil $V \neq \mathbf{0}$, und daher ist $\mathbf{w}$ linear unabhängig. □

Kapitel 11

Lineare Abbildungen

Im vorigen Kapitel haben wir Vektorräume und ihre Basen untersucht. Nun betrachten wir Funktionen zwischen Vektorräumen, die mit der Addition und der Skalarmultiplikation verträglich sind.

Definition 11.0.1. Sei $\mathbb{K}$ ein Körper, und seien V und W Vektorräume über $\mathbb{K}$. Eine Funktion

$$T\colon V \to W$$

heißt ***lineare Abbildung***, wenn die folgenden beiden Eigenschaften erfüllt sind:

(i) (Additivität) Für alle $a \in \mathbb{K}$ und $\mathbf{v} \in V$ gilt

$$T(a\mathbf{v}) = aT(\mathbf{v}).$$

(ii) (Homogenität) Für alle $\mathbf{v}, \mathbf{w} \in V$ gilt

$$T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w}).$$

Eine lineare Abbildung wird auch eine ***lineare Transformation*** genannt. Wenn wir betonen möchten, über welchem Körper die Skalarmultiplikation betrachtet wird, sprechen wir von einer ***$\mathbb{K}$-linearen Abbildung***. Eine lineare Abbildung $T\colon V \to V$ nennt man auch ein ***Endomorphismus von*** V.

Die Menge aller linearen Abbildungen von V nach W bezeichnen wir mit $\mathrm{Lin}(V, W)$, und zusätzlich setzen wir $\mathrm{Lin}(V) := \mathrm{Lin}(V, W)$.

Die beiden Bedingungen aus der Definition können auch zu einer einzigen Bedingung zusammengefasst werden: Eine Funktion $T\colon V \to W$ ist genau dann linear, wenn für alle $a, b \in \mathbb{K}$ und $\mathbf{v}, \mathbf{w} \in V$ gilt

$$T(a\mathbf{v} + \mathbf{w}) = aT(\mathbf{v}) + T(\mathbf{w}).$$

Die beiden Bedingungen aus der Definition können auch zu einer einzigen Bedingung zusammengefasst werden.

Übung 11.0.2. *Zeigen Sie, dass eine Funktion $T\colon V \to W$ genau dann linear ist, wenn für alle $a \in \mathbb{K}$ und $\mathbf{v}, \mathbf{w} \in V$ gilt*

$$T(a\mathbf{v} + \mathbf{w}) = aT(\mathbf{v}) + T(\mathbf{w}).$$

Hinweis: *Zeigen Sie zunächst, dass $T(\mathbf{0}) = \mathbf{0}$ gilt.*

Beispiel 11.0.3. *Sei $n \geq 1$. Die Ableitung*

$$T\colon \mathbb{R}_{\leq n}[X] \to \mathbb{R}_{\leq n-1}[X], \qquad T(f) := f',$$

ist eine lineare Abbildung. Für $f, g \in \mathbb{R}_{\leq n}[X]$ und $a \in \mathbb{R}$ gilt nämlich

$$T(f+g) = (f+g)' = f' + g' = T(f) + T(g)$$

und

$$T(af) = (af)' = af' = aT(f).$$

Beispiel 11.0.4. *Jede lineare Abbildung $T\colon \mathbb{K} \to \mathbb{K}$ ist die Multiplikation mit einem festen Skalar. Genauer gibt es ein $a \in \mathbb{K}$ mit*

$$T(x) = ax$$

für alle $x \in \mathbb{K}$.

Tatsächlich gilt für eine lineare Abbildung

$$T(x) = T(x \cdot 1) = xT(1).$$

Wir können also $a := T(1)$ setzen.

Wir betrachten nun eine allgemeine lineare Abbildung

$$T\colon \mathbb{K}^n \to \mathbb{K}^m.$$

Eine solche Abbildung ist bereits durch ihre Werte auf der Standardbasis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ bestimmt. Ist nämlich

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n,$$

so folgt aus der Linearität

$$T(\mathbf{x}) = T(x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n) = x_1T(\mathbf{e}_1) + \cdots + x_nT(\mathbf{e}_n).$$

Sobald die Vektoren $T(\mathbf{e}_1), \ldots, T(\mathbf{e}_n)$ bekannt sind, ist also auch $T(\mathbf{x})$ für jeden Vektor $\mathbf{x} \in \mathbb{K}^n$ bestimmt.

Umgekehrt können die Bilder der Standardbasis beliebig gewählt werden.

Proposition 11.0.5. *Zu beliebigen Vektoren* $\mathbf{a}_1, \dots, \mathbf{a}_n \in \mathbb{K}^m$ *gibt es genau eine lineare Abbildung*

$$T\colon \mathbb{K}^n \to \mathbb{K}^m$$

mit

$$T(\mathbf{e}_i) = \mathbf{a}_i$$

für alle $i = 1, \dots, n$.

Beweis. Wir definieren

$$T\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n.$$

Wir überprüfen zunächst, dass diese Abbildung linear ist. Für $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ gilt

$$\begin{aligned} T(\mathbf{x}+\mathbf{y}) &= \sum_{i=1}^{n}(x_i + y_i)\mathbf{a}_i \\ &= \sum_{i=1}^{n} x_i\mathbf{a}_i + \sum_{i=1}^{n} y_i\mathbf{a}_i \\ &= T(\mathbf{x}) + T(\mathbf{y}). \end{aligned}$$

Für $a \in \mathbb{K}$ gilt außerdem

$$T(a\mathbf{x}) = \sum_{i=1}^{n} ax_i\mathbf{a}_i = a\sum_{i=1}^{n} x_i\mathbf{a}_i = aT(\mathbf{x}).$$

Die Abbildung T ist somit linear. Für die Vektoren der Standardbasis gilt nach der Definition $T(\mathbf{e}_i) = \mathbf{a}_i$.

Die Eindeutigkeit folgt daraus, dass jede lineare Abbildung $\mathbb{K}^n \to \mathbb{K}^m$ durch ihre Werte auf der Standardbasis bestimmt ist. □

Eine lineare Abbildung $T\colon \mathbb{K}^n \to \mathbb{K}^m$ zu definieren, ist somit dasselbe, wie n Vektoren

$$\mathbf{a}_1, \dots, \mathbf{a}_n \in \mathbb{K}^m$$

auszuwählen, auf welche die Standardbasisvektoren $\mathbf{e}_1, \dots, \mathbf{e}_n$ abgebildet werden sollen.

11.1 Matrizen als lineare Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$

Eine $m \times n$-Matrix über $\mathbb{K}$ ist ein rechteckiges Tableau mit m Zeilen und n Spalten, dessen Einträge Elemente von $\mathbb{K}$ sind. Zum Beispiel ist

$$\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 2 & 3 & 3 \\ 4 & 4 & 8 \end{pmatrix}$$

eine 4×3-Matrix.

Ist A eine $m \times n$-Matrix und $\mathbf{x} \in \mathbb{K}^n$, so definieren wir die Multiplikation von A mit $\mathbf{x}$. Das Produkt $A\mathbf{x}$ soll ein Vektor in $\mathbb{K}^m$ sein. Seien also

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \qquad \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Dann ist

$$A\mathbf{x} := \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix}.$$

Beispiel 11.1.1. *Zum Beispiel gilt*

$$\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 2 & 3 & 3 \\ 4 & 4 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} y + 2z \\ 3x + 4y + 5z \\ 2x + 3y + 3z \\ 4x + 4y + 8z \end{pmatrix}.$$

Bemerkung 11.1.2. Die Definition von $A\mathbf{x}$ ist durch Gleichungssyteme motiviert. Wir können nähmlich ein lineares Gleichungssystem

$$\begin{aligned} a_{11}X_1 + \dots + a_{1n}X_n &= b_1, \\ a_{21}X_1 + \dots + a_{2n}X_n &= b_2, \\ &\vdots \\ a_{m1}X_1 + \dots + a_{mn}X_n &= b_m \end{aligned}$$

kurz als Matrixgleichung schreiben. Setzen wir $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und $\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$, so ist

$(x_1, \ldots, x_n)$ genau dann eine Lösung des Gleichungssystems, wenn

$$A\mathbf{x} = \mathbf{b}.$$

Die Menge aller $m \times n$-Matrizen mit Einträgen in $\mathbb{K}$ bezeichnen wir mit

$$M_{m\times n}(\mathbb{K}).$$

Ist der Körper $\mathbb{K}$ aus dem Kontext klar, so schreiben wir auch kurz $M_{m\times n}$. Im quadratischen Fall $m = n$ verwenden wir die Abkürzungen $M_n(\mathbb{K})$ beziehungsweise M_n.

Jede Matrix $A \in M_{m\times n}$ liefert jetzt durch die obige Multiplikation die folgende lineare Abbildung:

$$T_A \colon \mathbb{K}^n \to \mathbb{K}^m, \qquad T_A(\mathbf{x}) := A\mathbf{x}.$$

Lemma 11.1.3. *Sei A eine $m \times n$-Matrix. Dann ist die Abbildung $T_A \colon \mathbb{K}^n \to \mathbb{K}^m$ linear.*

Beweis. Seien $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ und $c \in \mathbb{K}$. Für die i-te Koordinate gilt

$$\begin{aligned} \big(T_A(\mathbf{x}+\mathbf{y})\big)_i &= \sum_{j=1}^{n} a_{ij}(x_j + y_j) \\ &= \sum_{j=1}^{n} a_{ij}x_j + \sum_{j=1}^{n} a_{ij}y_j \\ &= \big(T_A(\mathbf{x}) + T_A(\mathbf{y})\big)_i. \end{aligned}$$

Da dies für jede Koordinate gilt, folgt $T_A(\mathbf{x}+\mathbf{y}) = T_A(\mathbf{x}) + T_A(\mathbf{y})$.

Ebenso gilt

$$\begin{aligned} \big(T_A(c\mathbf{x})\big)_i &= \sum_{j=1}^{n} a_{ij}cx_j \\ &= c\sum_{j=1}^{n} a_{ij}x_j \\ &= \big(cT_A(\mathbf{x})\big)_i. \end{aligned}$$

Also ist auch $T_A(c\mathbf{x}) = cT_A(\mathbf{x})$, und T_A ist linear. □

Schauen wir uns an, wohin die Standardbasisvektoren $\mathbf{e}_1, \ldots, \mathbf{e}_n$ durch T_A abgebildet werden. Für $i = 1, \ldots, n$ gilt

$$T_A(\mathbf{e}_i) = A\mathbf{e}_i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix}.$$

Der Standardbasisvektor $\mathbf{e}_i$ wird also auf den i-ten Spaltenvektor von A abgebildet.

Umgekehrt sei $F\colon \mathbb{K}^n \to \mathbb{K}^m$ eine lineare Abbildung. Wir setzen

$$\mathbf{a}_i := F(\mathbf{e}_i) = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix}$$

und betrachten die Matrix, deren i-te Spalte der Vektor $\mathbf{a}_i$ ist:

$$A = (\mathbf{a}_1\, \mathbf{a}_2\, \ldots\, \mathbf{a}_n) = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}.$$

Nach der Konstruktion gilt

$$T_A(\mathbf{e}_i) = \mathbf{a}_i = F(\mathbf{e}_i)$$

für jedes i. Da die beiden linearen Abbildungen T_A und F auf allen Standardbasisvektoren übereinstimmen, gilt $T_A = F$.

Wir haben also den folgenden Satz bewiesen.

Satz 11.1.4. *Jede $m \times n$-Matrix A bestimmt eine lineare Abbildung*

$$T_A\colon \mathbb{K}^n \to \mathbb{K}^m, \qquad \mathbf{x} \mapsto A\mathbf{x}.$$

Umgekehrt gibt es zu jeder linearen Abbildung $F\colon \mathbb{K}^n \to \mathbb{K}^m$ genau eine $m \times n$-Matrix A mit $F = T_A$. □

Bemerkung 11.1.5. Streng genommen sind die Matrix A und die zugehörige lineare Abbildung T_A verschiedene Objekte. Matrizen werden jedoch sehr häufig mit den linearen Abbildungen identifiziert, die sie bezüglich der Standardbasen darstellen. Wenn keine Verwechslung zu befürchten ist, schreiben wir daher auch

$$A\colon \mathbb{K}^n \to \mathbb{K}^m$$

und verwenden $A(\mathbf{x})$ oder $A\mathbf{x}$ anstelle von $T_A(\mathbf{x})$.

11.2 Matrix-Beispiele

Wir betrachten einige wichtige Beispiele linearer Abbildungen und ihrer Matrizen bezüglich der jeweiligen Standardbasen.

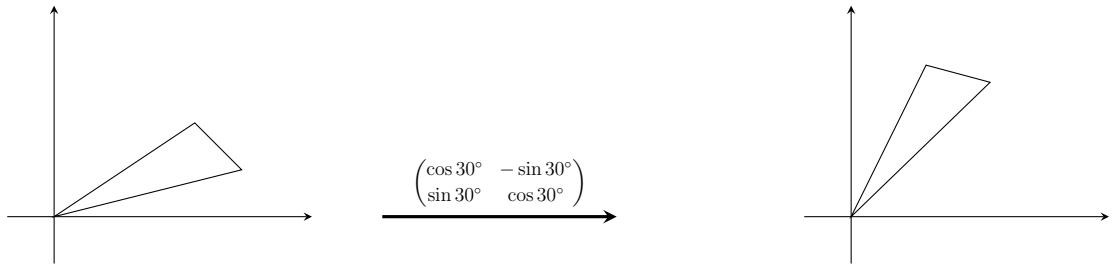
Beispiel 11.2.1. *Die Rotation in $\mathbb{R}^2$ um den Winkel φ ist die lineare Abbildung mit der Matrix*

$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

Sie bildet also den Vektor $\begin{pmatrix} x \\ y \end{pmatrix}$ auf

$$\begin{pmatrix} x\cos(\varphi) - y\sin(\varphi) \\ x\sin(\varphi) + y\cos(\varphi) \end{pmatrix}$$

ab.



Beispiel 11.2.2. *Die Spiegelung in $\mathbb{R}^3$ an der XZ-Ebene ist durch*

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \\ z \end{pmatrix}$$

gegeben. Ihre Matrix ist

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Beispiel 11.2.3. *Die Identitätsabbildung $\mathrm{Id}\colon \mathbb{K}^n \to \mathbb{K}^n$ hat die Matrix*

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

*Diese Matrix heißt die **Einheitsmatrix**. Auf ihrer Hauptdiagonale stehen Einsen, alle anderen Einträge sind null.*

Beispiel 11.2.4. *Allgemeiner heißt eine Matrix, deren Einträge außerhalb der Hauptdiagonale null sind, eine* ***Diagonalmatrix****. Wir schreiben*

$$\operatorname{diag}(a_1, \dots, a_n) := \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}.$$

Die zugehörige lineare Abbildung ist

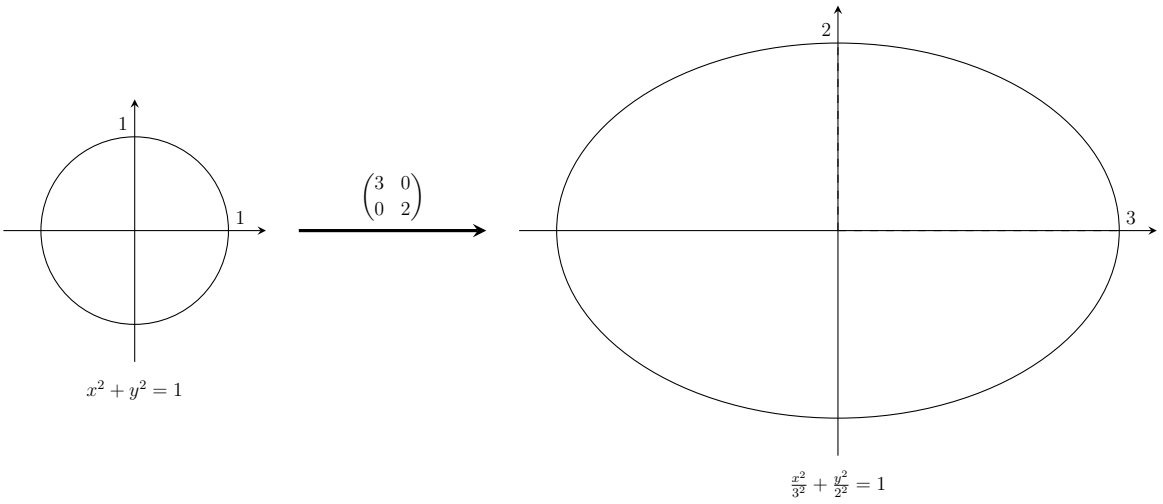
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} a_1 x_1 \\ \vdots \\ a_n x_n \end{pmatrix}.$$

Sie streckt also die einzelnen Koordinatenrichtungen mit verschiedenen Faktoren. Solche Abbildungen werden wir später genauer untersuchen.

Zum Beispiel bildet $\operatorname{diag}(a, b)$ *für* $a, b > 0$ *den Einheitskreis in* $\mathbb{R}^2$ *auf die Ellipse*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

mit Halbachsen a *und* b *ab.*



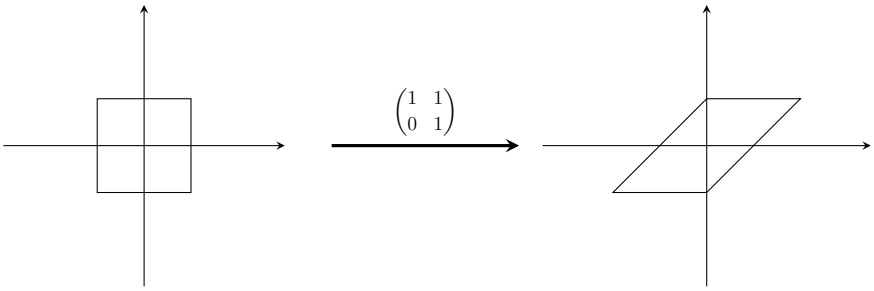
Beispiel 11.2.5. *Die lineare Abbildung*

$$T\colon \mathbb{R}^2 \to \mathbb{R}^2, \qquad T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ y \end{pmatrix},$$

*heißt eine **Scherung**. Ihre Matrix ist*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Dabei werden horizontale Geraden parallel zur x-Achse verschoben.



Beispiel 11.2.6. *Wir betrachten den Körper $\mathbb{F}_2 = \mathbb{Z}/2$ und die Matrix*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Sie definiert eine lineare Abbildung

$$G\colon \mathbb{F}_2^4 \to \mathbb{F}_2^7.$$

*Einen Vektor $\mathbf{v} \in \mathbb{F}_2^4$ können wir als ein binäres Wort der Länge 4 auffassen. Der Vektor $G\mathbf{v} \in \mathbb{F}_2^7$ ist die **Kodierung** dieses Wortes und heißt ein **Codewort**.*

*Diese Kodierung ist fehlererkennend: Zwei verschiedene Codewörter unterscheiden sich in mindestens drei Stellen. Daher können bis zu zwei Fehler erkannt werden. Außerdem kann ein einzelner Fehler eindeutig korrigiert werden. Dieser Code heißt der binäre $(7,4)$-**Hamming-Code**.*

11.3 $M_{m\times n}(\mathbb{K})$ und $\mathrm{Lin}(V,W)$ als Vektorräume

Die Menge $M_{m\times n}(\mathbb{K})$ trägt auf natürliche Weise die Struktur eines Vektorraums. Für Matrizen

$$A = (a_{ij}), \qquad B = (b_{ij})$$

definieren wir die Summe $A + B$ eintragsweise durch

$$A + B = (a_{ij} + b_{ij}).$$

Für $c \in \mathbb{K}$ definieren wir ebenso

$$cA = (ca_{ij}).$$

Mit diesen Operationen ist $M_{m\times n}(\mathbb{K})$ ein Vektorraum über $\mathbb{K}$.

Auch lineare Abbildungen können addiert und mit Skalaren multipliziert werden. Sind $S, T\colon V \to W$ linear und ist $c \in \mathbb{K}$, so definieren wir

$$(S+T)(\mathbf{v}) := S(\mathbf{v}) + T(\mathbf{v}), \qquad (cT)(\mathbf{v}) := cT(\mathbf{v}).$$

Diese Abbildungen sind wieder linear. Somit ist auch die Menge $\mathrm{Lin}(V, W)$ aller linearen Abbildungen von V nach W ein Vektorraum.

Die Vektorraumstrukturen auf Matrizen und linearen Abbildungen sind mit der oben beschriebenen Zuordnung $A \mapsto T_A$ verträglich.

Lemma 11.3.1. *Seien $S, T\colon \mathbb{K}^n \to \mathbb{K}^m$ lineare Abbildungen, deren Matrizen bezüglich der Standardbasen $A = (a_{ij})$ beziehungsweise $B = (b_{ij})$ sind. Dann ist die Matrix von $S + T$ gleich $A + B$.*

Beweis. Seien $\mathbf{e}_1, \dots, \mathbf{e}_n$ und $\mathbf{f}_1, \dots, \mathbf{f}_m$ die Standardbasen von $\mathbb{K}^n$ beziehungsweise $\mathbb{K}^m$. Für jedes $k = 1, \dots, n$ gilt

$$\begin{aligned}(S+T)(\mathbf{e}_k) &= S(\mathbf{e}_k) + T(\mathbf{e}_k)\\ &= \sum_{i=1}^{m} a_{ik}\mathbf{f}_i + \sum_{i=1}^{m} b_{ik}\mathbf{f}_i\\ &= \sum_{i=1}^{m} (a_{ik} + b_{ik})\mathbf{f}_i.\end{aligned}$$

Der k-te Spaltenvektor der Matrix von $S + T$ ist also die Summe der k-ten Spaltenvektoren von A und B. Daher ist die Matrix von $S + T$ gleich $A + B$. □

Übung 11.3.2. *Sei $T\colon \mathbb{K}^n \to \mathbb{K}^m$ eine lineare Abbildung mit Matrix A, und sei $c \in \mathbb{K}$. Zeigen Sie, dass die Matrix der linearen Abbildung cT gleich cA ist.*

11.4 Zusammenhang zwischen beliebigen linearen Abbildungen und Matrizen

Wir haben bereits gesehen, dass jede lineare Abbildung $\mathbb{K}^n \to \mathbb{K}^m$ durch eine Matrix in $M_{m\times n}$ dargestellt wird. Nun betrachten wir lineare Abbildungen

$$T\colon V \to W$$

zwischen beliebigen Vektorräumen die endliche Basen haben.

Seien $\mathbf{e}_1, \dots, \mathbf{e}_n$ eine Basis von V und $\mathbf{f}_1, \dots, \mathbf{f}_m$ eine Basis von W. Wie im Fall der Standardvektorräume ist eine lineare Abbildung $T\colon V \to W$ bereits durch ihre Werte auf der Basis von V bestimmt.

Proposition 11.4.1. *Zu beliebigen Vektoren $\mathbf{a}_1, \dots, \mathbf{a}_n \in W$ gibt es genau eine lineare Abbildung $T\colon V \to W$ mit*

$$T(\mathbf{e}_i) = \mathbf{a}_i$$

für alle $i = 1, \dots, n$.

Beweis. Jeder Vektor $\mathbf{v} \in V$ besitzt eine eindeutige Darstellung

$$\mathbf{v} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n.$$

Wir definieren

$$T(\mathbf{v}) := x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n.$$

Wegen der Eindeutigkeit der Koeffizienten $x_1, \dots, x_n$ ist diese Definition wohldefiniert. Wie im Fall der Standardbasis überprüft man unmittelbar, dass T linear ist.

Umgekehrt muss jede lineare Abbildung mit $T(\mathbf{e}_i) = \mathbf{a}_i$ die Gleichung

$$T(x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n) = x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n$$

erfüllen. Daher ist T eindeutig bestimmt. □

Wir erinnern an Remark 10.3.5: Ist $\mathcal{B}$ eine Basis von V und $\mathbf{v} \in V$, so bezeichnet $[\mathbf{v}]_\mathcal{B}$ den Koordinatenvektor von $\mathbf{v}$ bezüglich $\mathcal{B}$.

Nach der Wahl von Basen in V und W kann die Wirkung einer linearen Abbildung durch Matrixmultiplikation mit Koordinatenvektoren beschrieben werden.

Proposition 11.4.2. *Seien $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ eine Basis von V und $\mathcal{C} = (\mathbf{f}_1, \dots, \mathbf{f}_m)$ eine Basis von W. Zu jeder linearen Abbildung $T\colon V \to W$ gibt es genau eine Matrix $A \in M_{m\times n}(\mathbb{K})$ mit*

$$[T(\mathbf{v})]_\mathcal{C} = A[\mathbf{v}]_\mathcal{B}$$

für alle $\mathbf{v} \in V$.

Beweis. Für $i = 1, \dots, n$ schreiben wir

$$T(\mathbf{e}_i) = \sum_{j=1}^{m} a_{ji}\mathbf{f}_j$$

und setzen

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

Die i-te Spalte von A ist also $[T(\mathbf{e}_i)]_{\mathcal{C}}$.

Sei nun

$$\mathbf{v} = \sum_{i=1}^{n} x_i \mathbf{e}_i.$$

Dann ist $[\mathbf{v}]_{\mathcal{B}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, und aus der Linearität folgt

$$\begin{aligned} T(\mathbf{v}) &= \sum_{i=1}^{n} x_i T(\mathbf{e}_i) \\ &= \sum_{i=1}^{n} x_i \sum_{j=1}^{m} a_{ji} \mathbf{f}_j \\ &= \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ji} x_i \right) \mathbf{f}_j. \end{aligned}$$

Somit gilt

$$[T(\mathbf{v})]_{\mathcal{C}} = A[\mathbf{v}]_{\mathcal{B}}.$$

Die Matrix A ist eindeutig bestimmt, denn ihre i-te Spalte muss der Koeffizientenvektor $[T(\mathbf{e}_i)]_{\mathcal{C}}$ sein. □

Beispiel 11.4.3. *Die Matrix einer linearen Abbildung hängt von den gewählten Basen im Definitions- und Zielraum ab. Erst nach der Wahl dieser Basen kann eine lineare Abbildung mit einer Matrix identifiziert werden.*

Betrachten wir die lineare Abbildung

$$T\colon \mathbb{R}^2 \to \mathbb{R}^2, \qquad T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x+y \end{pmatrix}.$$

Bezüglich der Standardbasis $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2)$ wird T durch die Matrix

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

dargestellt.

Betrachten wir stattdessen die Basis

$$\mathcal{C} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right).$$

Für ihre Basisvektoren gilt

$$T \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad T \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mathbf{0}.$$

Bezüglich der Basis $\mathcal{C}$ sowohl im Definitions- als auch im Zielraum wird dieselbe lineare Abbildung daher durch die Matrix

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

dargestellt.

Beispiel 11.4.4. *Betrachten wir die lineare Abbildung*

$$T \colon \mathbb{R}_{\leq 3}[X] \to \mathbb{R}_{\leq 3}[X], \qquad T(f) := f'' + f' + f.$$

Wir bestimmen ihre Matrix bezüglich der Basis $\mathcal{B} = (1, X, X^2, X^3)$ im Definitions- und Zielraum. Es gilt

$$\begin{aligned} T(1) &= 1, \\ T(X) &= 1 + X, \\ T(X^2) &= 2 + 2X + X^2, \\ T(X^3) &= 6X + 3X^2 + X^3. \end{aligned}$$

Die Spalten der gesuchten Matrix sind die Koordinatenvektoren dieser Polynome bezüglich $\mathcal{B}$. Daher ist die Matrix von T

$$A = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$