Grundlagen der Mathematik 1: Lineare Algebra

Andreas Gathmann

Vorlesungsskript RPTU Kaiserslautern 2024/25

– vorläufige Version –

Inhaltsverzeichnis (Grundlagen der Mathematik 1)

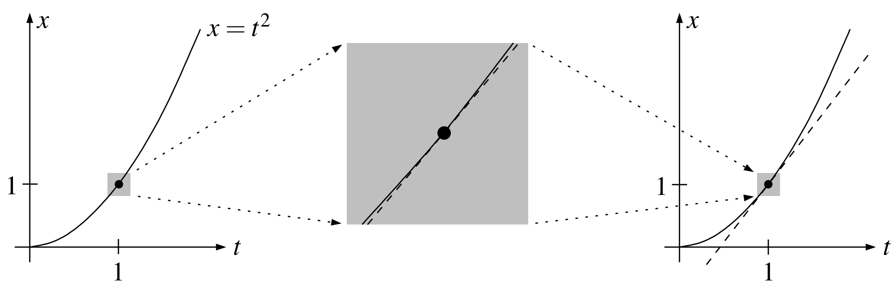
Grundlagen der Mathematik 1: Lineare Algebra

0. Einleitung und Motivation

In diesem Skript – so verspricht es der Titel – wollen wir uns die Grundlagen der Mathematik erarbeiten. Aber was ist das überhaupt, die „Grundlagen der Mathematik"? Es handelt sich hierbei um die Kombination zweier Themengebiete, die in der Tat das grundlegende Handwerkszeug für nahezu die gesamte Mathematik darstellen, nämlich

- der *Analysis*, d. h. der Untersuchung von Folgen und Grenzwerten, Stetigkeit, sowie der Differential- und Integralrechnung (zunächst in einer und im zweiten Semester dann auch in mehreren Variablen), und
- der *linearen Algebra*, d. h. der Theorie der Vektorräume, linearen Abbildungen und Gleichungssysteme.

Von beiden Gebieten habt ihr ja aus der Schule wahrscheinlich schon eine ungefähre Vorstellung. In der *Analysis* geht es grob gesagt darum, reelle Funktionen *lokal*, also in der Umgebung eines gewählten Punktes, zu untersuchen, und aus diesen Untersuchungen dann wieder Aussagen über die gesamte Funktion zurückzugewinnen. Betrachten wir z. B. ein Auto, das sich entlang einer geraden Strecke bewegt. Der Einfachheit halber nehmen wir an, dass die Position x des Autos nach der Zeit t (in geeigneten Einheiten) durch die Gleichung $x = t^2$ beschrieben werden kann, so dass die Bewegung durch die Kurve im folgenden Bild links dargestellt wird:



Wir wollen diese Bewegung nun nur in einer kleinen Umgebung eines fest gewählten Zeitpunkts, z. B. des Zeitpunkts $t = 1$ (und damit auch $x = 1$) betrachten. Im Bild oben haben wir diese Umgebung grau markiert und in der Mitte stark vergrößert dargestellt. Wir sehen, dass die Kurve in dieser Umgebung fast wie eine *Gerade* aussieht; wir haben diese Gerade gestrichelt eingezeichnet und im Bild rechts auch außerhalb der gewählten Umgebung fortgesetzt. Geometrisch ist diese Gerade natürlich einfach die *Tangente* an die Kurve an der Stelle $t = 1$. Physikalisch repräsentiert die Steigung dieser Geraden die *Geschwindigkeit* des Autos zum betrachteten Zeitpunkt, denn sie gibt ja gerade an, in welchem Verhältnis sich dort die Strecke x mit der Zeit t verändert. Aus der Schule wisst ihr auch schon, wie man diese Steigung ausrechnet: Man muss dazu die gegebene Funktion t^2 *differenzieren* – so dass man die Ableitung $2t$ erhält – und dort die betrachtete Stelle $t = 1$ einsetzen. Die Steigung ist in unserem Fall also gerade $2 \cdot 1 = 2$, und man rechnet sofort nach, dass $x = 2t - 1$ die Gleichung der oben eingezeichneten Tangente ist. Man sagt, dass die Gerade $x = 2t - 1$ eine *lineare Approximation* der ursprünglich gegebenen Funktion $x = t^2$ im Punkt $t = 1$ ist.

Wir können aus der Kenntnis der zurückgelegten Strecke zu jedem Zeitpunkt also die Geschwindigkeit des Autos durch Differenzieren bestimmen. Man kann sich natürlich auch die umgekehrte Frage stellen: Angenommen, der Kilometerzähler eures Autos ist kaputt, aber ihr beobachtet auf eurer Fahrt ständig eure Geschwindigkeit. Könnt ihr dann am Ende der Fahrt trotzdem ausrechnen, wie weit ihr gefahren seid? Dies ist offensichtlich die „Umkehrung" des Differenzierens – und auch hier wisst ihr aus der Schule natürlich schon, dass dies auf die *Integralrechnung* führen wird.

In der Praxis bewegt man sich mit dem Auto aber nicht immer nur auf einer geraden Strecke, und demzufolge braucht man für die Beschreibung solch einer Bewegung (und natürlich auch vieler anderer natürlich auftretender Prozesse) mehrere Variablen. Wir werden daher auch Abbildungen betrachten, die mehrere Variablen auf mehrere andere abbilden, wie z. B. die folgende Vorschrift, die zwei reelle Zahlen y_1 und y_2 in Abhängigkeit von zwei anderen x_1 und x_2 ausdrückt:

$$\begin{aligned} y_1 &= 2x_1 + x_2 \cos x_1 \\ y_2 &= x_1 \, \mathrm{e}^{x_2} - x_2 \end{aligned}$$

Genau wie oben werden wir uns auch hier wieder die Frage stellen, ob wir diese (in diesem Fall recht komplizierte) Funktion in der Nähe eines gegebenen Punktes nicht vielleicht durch eine einfache *lineare* Abhängigkeit annähern können. In der Tat ist dies möglich: Wir werden sehen, dass z. B. in einer kleinen Umgebung des Nullpunkts $(x_1, x_2) = (0,0)$ die obige Vorschrift näherungsweise die gleichen Ergebnisse liefert wie das lineare Gleichungssystem

$$\begin{aligned} y_1 &= 2x_1 + x_2 \\ y_2 &= x_1 - x_2. \end{aligned}$$

Auch wenn diese Gleichungen natürlich viel einfacher als die ursprünglichen sind, sollte offensichtlich sein, dass auch solche linearen Gleichungssysteme bei wachsender Zahl von Variablen (und in der Praxis sind Hunderte oder Tausende von Variablen keine Seltenheit) recht kompliziert werden können. Wir werden daher einen wesentlichen Teil dieser Vorlesung mit der *linearen Algebra*, also dem Studium derartiger linearer Gleichungssysteme, verbringen. Um dabei überhaupt erst einmal den Notationsaufwand in Grenzen zu halten, tut man dabei gut daran, die Start- und Zielvariablen nicht alle einzeln hinzuschreiben, sondern sie zu sogenannten *Vektoren* zusammenzufassen. In der Tat kann man in dieser Sichtweise die lineare Algebra als das Studium von linearen Abbildungen zwischen Vektorräumen beschreiben.

Wenn wir dann die linearen Abbildungen zwischen mehreren Variablen gut genug verstanden haben, können wir uns im zweiten Teil der Analysis schließlich daran machen, die Differential- und Integralrechnung auf den Fall von mehreren Variablen auszuweiten.

Wir haben damit jetzt relativ kurz umrissen, welcher mathematische Stoff uns in dieser Vorlesung erwartet. Es wird in diesem Skript aber nicht nur darum gehen, mathematische Resultate kennenzulernen. Mindestens ebenso wichtig ist es, das „mathematische Denken“ zu lernen, d. h. die Fähigkeit zu entwickeln, mit abstrakten Konzepten umzugehen, exakte logische Schlüsse zu ziehen und Beweise zu führen. Anders als in der Schule oder im Studium z. B. ingenieurswissenschaftlicher Fächer werden wir genau darauf achten, eine „wasserdichte“ Theorie aufzubauen: Jeder neue Begriff bzw. jeder neue Satz wird nur unter Verwendung des bisher Bekannten exakt definiert bzw. bewiesen. So sind z. B. Formulierungen in dem Stil „eine Funktion wird durch eine Gerade angenähert“ oder „eine Funktion heißt stetig, wenn man sie zeichnen kann, ohne den Stift abzusetzen“ als Veranschaulichung unserer Ideen zwar sehr sinnvoll, als exakte mathematische Formulierung jedoch schlichtweg unbrauchbar. Wir werden daher in dieser Vorlesung viel exakter arbeiten als ihr es wahrscheinlich aus der Schule gewohnt seid, und es ist wichtig, dass ihr diese exakte Denkweise verinnerlicht und anzuwenden lernt. Die Mathematik ist ein riesiges Gebäude – viel größer und komplexer als ihr es euch wahrscheinlich im Moment vorstellen könnt – das ständig höher gebaut wird, indem schon bewiesene Sätze auf neue Fälle angewendet oder wieder für neue Beweise verwendet werden. Wir starten gerade beim Fundament dieses Gebäudes und können es uns da wirklich nicht leisten herumzupfuschen.

Diese konsequent logische und exakte Herangehensweise ist zwar am Anfang wahrscheinlich ungewohnt, hat jedoch für euch auch einen Vorteil: Etwas überspitzt formuliert erzählen wir euch während des gesamten Studiums eigentlich nur Dinge, die logisch aus dem folgen, was ihr ohnehin schon wusstet. Dadurch ist die Mathematik wahrscheinlich das Studienfach, in dem man am wenigsten auswendig lernen muss – in dem es aber im Gegenzug auch am meisten auf das *Verständnis* des Stoffes ankommt. Je besser euer Verständnis für die Mathematik wird, um so mehr Dinge werden euch letztlich einfach „klar“ werden, so dass es euch dann auch viel leichter fällt, sie zu lernen.

Dieses Verständnis für die Mathematik bekommt man aber natürlich nur durch intensiven und *aktiven* Umgang mit dem Stoff, weswegen neben dem Studium der Vorlesung auch die Bearbeitung der Übungsaufgaben besonders wichtig ist.

Heißt das alles nun, dass wir nur mit logischen Argumenten die Mathematik sozusagen „aus dem Nichts“ aufbauen können? Nein, das geht natürlich nicht ... von nichts kommt nichts. Man muss am Anfang immer gewisse Dinge als gegeben annehmen, also Aussagen als wahr voraussetzen, die man nicht mehr beweist bzw. beweisen kann, und auf denen dann die gesamte Theorie beruht. Derartige Annahmen bezeichnet man als **Axiome**. Natürlich versucht man in der Mathematik, mit möglichst wenigen und sehr elementaren Axiomen auszukommen, die hoffentlich niemand anzweifeln würde. In der modernen Mathematik ist es üblich, hierfür die grundlegenden Prinzipien der Logik und Mengenlehre zu verwenden (zu denen wir auch gleich in Kapitel 1 Genaueres sagen werden).

In dieser Vorlesung wollen wir uns das Leben allerdings etwas leichter machen und zusätzlich auch die *Existenz und elementaren Eigenschaften der reellen Zahlen* axiomatisch voraussetzen (um welche Eigenschaften es sich hierbei handelt, werden wir natürlich genau angeben). Man kann zwar nur aus den Axiomen der Logik und Mengenlehre beweisen, dass die reellen Zahlen existieren und dass sie die erwarteten Eigenschaften haben, der Beweis wäre zu diesem frühen Zeitpunkt im Studium aber sehr verwirrend und würde euch auch keine großartigen neuen Erkenntnisse bringen. In diesem Sinne starten wir also sozusagen doch nicht ganz beim Fundament unseres „Gebäudes Mathematik“, sondern bereits im ersten Stock.

Im weiteren Verlauf ist dieses Skript dann wie im Inhaltsverzeichnis angegeben in mehrere Teile gegliedert. Diese bauen der Reihe nach aufeinander auf, mit einer Ausnahme: Nach den in jedem Fall benötigten grundlegenden Anfangskapiteln 1 bis 3 sind die Teile „Grundlagen der Mathematik 1: Analysis“ (Kapitel **??** bis **??**) und „Grundlagen der Mathematik 1: Lineare Algebra“ (Kapitel 13 bis **??**) *unabhängig voneinander* und können somit in beliebiger Reihenfolge oder auch parallel studiert werden.

Aber jetzt genug der Vorrede ... beginnen wir nun also unser Studium der Mathematik mit den „Grundlagen der Grundlagen“, den für uns wesentlichen Prinzipien der Logik und Mengenlehre.

1. Etwas Logik und Mengenlehre

Bevor wir mit dem eigentlichen Inhalt der Vorlesung beginnen, müssen wir in diesem Kapitel kurz die exakte mathematische Sprache beschreiben, in der wir unsere Ergebnisse formulieren werden: die der Logik und Mengenlehre. Zentral hierbei sind die Begriffe der *Aussage* (in der Logik) und der *Menge* (in der Mengenlehre).

Da wir es hier mit den ersten beiden Begriffen überhaupt zu tun haben, die in der Mathematik vorkommen, können wir sie natürlich nicht durch bereits bekannte Dinge definieren oder mit bereits bekannten Resultaten ihre Eigenschaften herleiten. Wir müssen sie daher (wie schon in der Einleitung erwähnt) axiomatisch voraussetzen. Wir müssen *voraussetzen*, dass es sinnvoll ist, über logische Aussagen und deren Wahrheit zu reden, dass Mengen überhaupt existieren, dass man Mengen vereinigen und schneiden kann, aus ihnen Elemente auswählen kann, und noch einiges mehr. Wenn ihr euch zum Beispiel auf den Standpunkt stellt, dass ihr nicht an die Existenz von Mengen glaubt, wird euch niemand widerlegen können. Allerdings zweifelt ihr damit dann auch die Existenz der gesamten Mathematik an, wie sie heutzutage betrieben wird – und aus der Tatsache, dass ihr in dieser Vorlesung sitzt, schließe ich einmal, dass das nicht der Fall ist.

Glücklicherweise sind die Dinge, die wir benötigen, jedoch allesamt anschaulich sofort einleuchtend. Ich möchte es euch (und mir) daher ersparen, an dieser Stelle eine vollständige und präzise axiomatische Formulierung der Logik und Mengenlehre hinzuschreiben, zumal das momentan sicher mehr verwirren als helfen würde und außerdem gerade im Bereich der Logik auch zu sehr in die Philosophie abdriften würde. Stattdessen wollen wir uns in diesem (für den Rest der Vorlesung sehr untypischen) ersten Kapitel damit begnügen, die für uns wichtigsten Prinzipien und Notationen sowie beliebte Fehlerquellen in verständlicher Sprache zu erklären, auch wenn ein paar Dinge (insbesondere die Begriffsfestlegung – „Definition“ möchte ich es eigentlich gar nicht nennen – einer Aussage und einer Menge) dadurch recht schwammig klingen werden. Außerdem werden wir in Beispielen zur besseren Verdeutlichung bereits hier die reellen Zahlen und ihre einfachsten Eigenschaften (die euch sicherlich bekannt sein werden) benutzen, auch wenn wir diese erst später formalisieren werden. Da es sicher niemanden von euch verwirren wird, werden wir auch die Schreibweise „$x \in \mathbb{R}$“ für „x ist eine reelle Zahl“ schon verwenden, bevor sie in den Notationen 1.12 und 1.14 offiziell eingeführt wird. Ab Kapitel 2 werden wir dann mit dem strukturierten Aufbau der Grundlagen der Mathematik beginnen, also alle Definitionen mit bereits eingeführten Notationen präzise formulieren und alle Aussagen aus vorherigen exakt beweisen.

1.A Logik

Beginnen wir also mit der Logik. Unter einer **Aussage** verstehen wir (grob gesagt) ein sprachliches Gebilde, das entweder wahr oder falsch ist (wobei wir in der Mathematik natürlich letztlich daran interessiert sind, *wahre* Aussagen herzuleiten – wenn wir später mathematische Sätze formulieren, ist damit also stets gemeint, dass die dort gemachte Aussage wahr ist). Wichtig sind auch sprachliche Gebilde, in denen freie **Variablen**, also Platzhalter, vorkommen, und die erst beim Einsetzen von Werten für diese Variablen Aussagen liefern. Man bezeichnet sie als **Aussageformen**.

Beispiel 1.1.

(a) $1+1=2$ ist eine wahre, $1+1=3$ eine falsche, und $1+1$ überhaupt keine Aussage.

(b) $x+1=2$ ist eine Aussageform, die beim Einsetzen von $x=1$ in eine wahre, beim Einsetzen jeder anderen reellen Zahl in eine falsche Aussage übergeht.

Bemerkung 1.2. Als Variablen in Aussageformen kann man beliebige Symbole benutzen. Üblich sind neben den normalen lateinischen Klein- und Großbuchstaben auch die griechischen Buchstaben, die wir zur Erinnerung hier auflisten:

Α α alpha	Β β beta	Γ γ gamma	Δ δ delta	Ε ε epsilon	Ζ ζ zeta	Η η eta	Θ ϑ theta
Ι ι iota	Κ κ kappa	Λ λ lambda	Μ μ my	Ν ν ny	Ξ ξ xi	Ο o omikron	Π π pi
Ρ ρ rho	Σ σ sigma	Τ τ tau	Υ υ ypsilon	Φ φ phi	Χ χ chi	Ψ ψ psi	Ω ω omega

Oft verziert man Buchstaben auch noch mit einem Symbol oder versieht sie mit einem Index, um neue Variablen zu erhalten: So sind z. B. $x, x', \tilde{x}, \bar{x}, x_1, x_2, \dots$ alles Symbole für verschiedene Variablen, die zunächst einmal nichts miteinander zu tun haben (aber möglichst für irgendwie miteinander zusammenhängende Objekte eingesetzt werden sollten, wenn man den Leser nicht vollends verwirren will).

Notation 1.3 (Zusammengesetzte Aussagen)**.** Sind A und B Aussagen, so lassen sich daraus wie folgt neue bilden:

Symbol	Wahrheitstafel				Bedeutung
A	w	f	w	f	
B	w	w	f	f	
$\neg A$	f	w			nicht A
$A \wedge B$	w	f	f	f	A und B
$A \vee B$	w	w	w	f	A oder B (oder beides): „nicht-ausschließendes Oder“
$A \Leftrightarrow B$	w	f	f	w	A und B sind gleichbedeutend / *äquivalent*, bzw. A genau dann, wenn B
$A \Rightarrow B$	w	w	f	w	aus A folgt B, bzw. wenn A dann B

Die sogenannte **Wahrheitstafel** in den mittleren vier Spalten ist dabei die eigentliche Definition der neuen zusammengesetzten Aussagen. Sie gibt in Abhängigkeit der Wahrheit von A und B (in den ersten beiden Zeilen) an, ob die zusammengesetzte Aussage wahr oder falsch ist.

Bemerkenswert ist hierbei wohl nur die Folgerungsaussage $A \Rightarrow B$, die keine Aussage über die Richtigkeit von A oder B separat macht, sondern nur sagt, dass B wahr ist, wenn auch A es ist. Ist hingegen A falsch, so ist die Folgerungsaussage $A \Rightarrow B$ stets wahr („aus einer falschen Voraussetzung kann man alles folgern“). So ist z. B. $0 = 1 \quad \Rightarrow \quad 2 = 3$ eine wahre Aussage. Wie schon erwähnt wollen wir uns in der Mathematik aber natürlich in der Regel mit wahren Aussagen beschäftigen, und neue wahre Aussagen aus alten herleiten. Gerade in Beweisen ist die übliche Verwendung der Notation $A \Rightarrow B$ daher, dass A eine bereits als wahr erkannte Aussage ist, und wir damit nun schließen wollen, dass auch B wahr ist.

Bemerkung 1.4 (Beweise mit Wahrheitstafeln)**.** Wollen wir kompliziertere zusammengesetzte Aussagen miteinander vergleichen, so können wir dies auch mit Hilfe von Wahrheitstafeln tun. So ist für zwei Aussagen A und B z. B.

$$A \Rightarrow B \quad \text{äquivalent zu} \quad (\neg A) \vee B,$$

denn wenn wir in der Wahrheitstafel

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

mit Hilfe der Definitionen von $\neg$ und $\vee$ aus Notation 1.3 zunächst $\neg A$ und dann $(\neg A) \vee B$ berechnen, sehen wir, dass das Ergebnis mit $A \Rightarrow B$ übereinstimmt. Nach der Bemerkung aus Notation 1.3 ist dies auch anschaulich klar: Die Folgerungsaussage $A \Rightarrow B$ ist ja genau dann wahr, wenn A falsch (also $\neg A$ wahr) ist, oder wenn B wahr ist (oder beides).

Genauso zeigt man die ebenfalls einleuchtende Aussage, dass

$$A \Leftrightarrow B \quad \text{äquivalent zu} \quad (A \Rightarrow B) \wedge (B \Rightarrow A)$$

ist – was auch die übliche Art ist, wie man eine Äquivalenz zeigt: Man zeigt separat die beiden Folgerungen $A \Rightarrow B$ und $B \Rightarrow A$.

Notation 1.5. Folgerungen („$\Rightarrow$“) und Äquivalenzen („$\Leftrightarrow$“) sind natürlich zwei verschiedene Dinge, die man nicht durcheinanderwerfen darf (auch wenn das in der Schule wahrscheinlich manchmal nicht so genau genommen wird). Es hat sich jedoch in der Mathematik eingebürgert, bei *Definitionen* von Begriffen durch eine äquivalente, definierende Eigenschaft die Sprechweise „wenn“ anstatt des eigentlich korrekten „genau dann, wenn“ zu verwenden: So würde man z. B. als Definition des Begriffs einer geraden Zahl hinschreiben

„Eine ganze Zahl x heißt gerade, wenn $\frac{x}{2}$ eine ganze Zahl ist“,

obwohl man genau genommen natürlich meint

„Eine ganze Zahl x heißt *genau dann* gerade, wenn $\frac{x}{2}$ eine ganze Zahl ist“.

Eine gewöhnliche Folgerungsaussage wie z. B. die wahre Aussage

„Wenn eine ganze Zahl x positiv ist, dann ist auch $x+1$ positiv“

ist dagegen immer nur in einer Richtung zu verstehen; hier wird also nicht behauptet, dass mit $x+1$ auch x immer positiv sein muss (was ja auch falsch wäre).

Notation 1.6 (Quantoren)**.** Natürlich kann man nicht nur zwei, sondern auch mehrere Aussagen wie in Notation 1.3 mit „und“ bzw. „oder“ verknüpfen – also die neue Aussage konstruieren, dass *jede* bzw. *mindestens eine* der ursprünglichen Aussagen wahr ist. Am einfachsten notiert man dies mit einer Aussageform A, in der eine freie Variable x vorkommt. Wir schreiben dies dann auch als $A(x)$ und setzen

Symbol	Bedeutung
$\forall x\colon A(x)$	für alle x gilt $A(x)$ (also eine „und“-Verknüpfung aller Aussagen $A(x)$)
$\exists x\colon A(x)$	es gibt ein x mit $A(x)$ (also eine „oder“-Verknüpfung aller Aussagen $A(x)$)

Die beiden Symbole $\forall$ und $\exists$ bezeichnet man als **Quantoren**. Beachte, dass diese beiden Quantoren *nicht* miteinander vertauschbar sind: So besagt z. B. die Aussage

$$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon\ y > x$$

„zu jeder reellen Zahl x gibt es eine Zahl y, die größer ist“ (was offensichtlich wahr ist), während die Umkehrung der beiden Quantoren die Aussage

$$\exists y \in \mathbb{R}\ \forall x \in \mathbb{R}\colon\ y > x$$

„es gibt eine reelle Zahl y, die größer als jede reelle Zahl x ist“ liefern würde (was ebenso offensichtlich falsch ist). Der Unterschied besteht einfach darin, dass im ersten Fall zuerst das x gewählt werden muss und dann ein y dazu existieren muss (das von x abhängen darf), während es im zweiten Fall *dasselbe* y für alle x sein müsste.

Bemerkung 1.7. Jede Aussage lässt sich natürlich auf viele Arten aufschreiben, sowohl als deutscher Satz als auch als mathematische Formel. Die gerade eben betrachtete Aussage könnte man z. B. auf die folgenden (absolut gleichwertigen) Arten aufschreiben:

(a) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon\ y > x$.

(b) Es sei $x \in \mathbb{R}$. Dann gibt es ein $y \in \mathbb{R}$ mit $y > x$.

(c) Zu jeder reellen Zahl gibt es noch eine größere.

Welche Variante man beim Aufschreiben wählt, ist weitestgehend Geschmackssache. Die Formulierung einer Aussage als deutscher Satz hat den Vorteil, dass wir sie oft leichter verstehen können, weil wir die deutsche Sprache schon länger kennen als die mathematische. Wenn wir uns jedoch erst einmal an die mathematische Sprache gewöhnt haben, wird auch sie ihre Vorzüge bekommen:

Sie ist deutlich kürzer und besser logisch strukturiert. Wir werden im Folgenden beide Schreibweisen mischen und jeweils diejenige wählen, mit der unsere Aussagen (hoffentlich) am einfachsten verständlich werden.

Wenn wir mathematische Symbole verwenden, müssen wir diese aber auch stets in ihrer korrekten Notation und nicht als „Abkürzungen" für deutsche Wörter verwenden: Man würde die Aussage „2 und 4 sind gerade Zahlen" sicher niemals schreiben als „$2 \wedge 4$ sind gerade Zahlen", und analog genauso wenig „Es gilt $x^2 \geq 0$ für alle $x \in \mathbb{R}$" als „Es gilt $x^2 \geq 0\ \forall x \in \mathbb{R}$".

Bemerkung 1.8 (Negationen)**.** Es ist wichtig zu wissen, wie man von einer Aussage das Gegenteil, also die Negation bzw. „Verneinung" bildet. Da hierbei oft Fehler gemacht werden, wollen wir die allgemeinen Regeln hierfür im Folgenden kurz auflisten. Dabei könnte man (a), (b) und (c) wieder schnell mit Wahrheitstafeln zeigen; die Regeln (d) und (e) sind wie in Notation 1.6 analog zu (b) und (c) für die Verknüpfung mehrerer Aussagen:

(a) $\neg(\neg A) \Leftrightarrow A$: Ist es falsch, dass A falsch ist, so bedeutet dies genau, dass A wahr ist.

(b) $\neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B)$: Das Gegenteil von „$A$ und B sind richtig" ist „A oder B ist falsch".

(c) $\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B)$: Das Gegenteil von „$A$ oder B ist richtig" ist „A und B sind falsch".

(d) $\neg(\forall x\colon A(x)) \Leftrightarrow \exists x\colon \neg A(x)$: Das Gegenteil von „für alle x gilt $A(x)$" ist „es gibt ein x, für das $A(x)$ falsch ist".

(e) $\neg(\exists x\colon A(x)) \Leftrightarrow \forall x\colon \neg A(x)$: Das Gegenteil von „es gibt ein x, für das $A(x)$ gilt" ist „für alle x ist $A(x)$ falsch".

Man kann also sagen, dass eine Verneinung dazu führt, dass „und" mit „oder" sowie „für alle" mit „es gibt" vertauscht werden. So ist z. B. das Gegenteil der Aussage

„In Frankfurt haben *alle* Haushalte Strom *und* fließendes Wasser"

die Aussage

„In Frankfurt *gibt es* einen Haushalt, der keinen Strom *oder* kein fließendes Wasser hat".

Beispiel 1.9.

(a) Wollen wir eine Folgerung $A \Rightarrow B$ verneinen, so können wir sie zunächst mit Bemerkung 1.4 zu $(\neg A) \vee B$ umformen, und erhalten nach Bemerkung 1.8 als Umkehrung dann $A \wedge \neg B$. Dies ist auch anschaulich einleuchtend: Die Folgerungsaussage „wenn A dann B" ist genau dann falsch, wenn die Voraussetzung A zwar gilt, die Behauptung B aber nicht. Wir sehen also:

$$\boxed{\text{Die Verneinung einer Folgerung } A \Rightarrow B \text{ ist } A \wedge \neg B}$$

(und nicht etwa $A \Rightarrow \neg B$, wie man vielleicht denken könnte).

(b) Eine oft vorkommende Anwendung der Regeln für die Verneinung von Aussagen ist der sogenannte **Widerspruchsbeweis** bzw. Beweis durch **Kontraposition**. Nach Bemerkung 1.4 gesehen ist die Folgerung $A \Rightarrow B$ („aus A folgt B") gleichbedeutend mit $(\neg A) \vee B$. Damit ist diese Aussage nach Bemerkung 1.8 (a) auch äquivalent zu $(\neg(\neg B)) \vee (\neg A)$, also zu $\neg B \Rightarrow \neg A$. Mit anderen Worten: Haben wir eine Schlussfolgerung $A \Rightarrow B$ zu beweisen, so können wir genauso gut $(\neg B) \Rightarrow (\neg A)$ zeigen, d. h. *wir können annehmen, dass die zu zeigende Aussage B falsch ist und dies dann zu einem Widerspruch führen bzw. zeigen, dass dann auch die Voraussetzung A falsch sein muss.*

Beispiel 1.10. Hier sind zwei Beispiele für die Anwendung der Prinzipien aus Bemerkung 1.8 und Beispiel 1.9 – und auch unsere ersten Beispiele dafür, wie man Beweise von Aussagen exakt aufschreiben kann.

(a) Einen Beweis durch Widerspruch könnte man z. B. so aufschreiben:

Behauptung: Für alle $x \in \mathbb{R}$ gilt $2x+1>0$ oder $2x-1<0$.

Beweis: Angenommen, die Behauptung wäre falsch, d. h. (nach Bemerkung 1.8 (c) und (d)) es gäbe ein $x \in \mathbb{R}$ mit

$$2x+1 \le 0 \quad (1) \qquad \text{und} \qquad 2x-1 \ge 0 \quad (2).$$

Für dieses x würde dann folgen, dass

$$0 \overset{(1)}{\ge} 2x+1 = 2x-1+2 \overset{(2)}{\ge} 0+2 = 2.$$

Dies ist aber ein Widerspruch. Also war unsere Annahme falsch und somit die zu beweisende Aussage richtig. □

Das dabei verwendete Symbol „□" ist die übliche Art, das Ende eines Beweises zu kennzeichnen. Zur Verdeutlichung haben wir die beiden Ungleichungen mit (1) und (2) markiert, um später angeben zu können, wo sie verwendet werden.

(b) Manchmal weiß man von einer Aussage aufgrund der Aufgabenstellung zunächst einmal noch nicht, ob sie wahr oder falsch ist. In diesem Fall muss man sich dies natürlich zuerst überlegen – und, falls die Aussage falsch ist, ihre Negation beweisen. Als Beispiel dafür betrachten wir die Aufgabe

Man beweise oder widerlege: Für alle $x \in \mathbb{R}$ gilt $2x+1<0$ oder $2x-1>0$.

In diesem Fall merkt man schnell, dass die Aussage falsch sein muss, weil die Ungleichungen schon für den Fall $x=0$ nicht stimmen. Man könnte als Lösung der Aufgabe unter Beachtung der Negationsregeln aus Bemerkung 1.8 also aufschreiben:

Behauptung: Die Aussage ist falsch, d. h. es gibt ein $x \in \mathbb{R}$ mit $2x+1 \ge 0$ und $2x-1 \le 0$.

Beweis: Für $x=0$ ist $2x+1=1 \ge 0$ und $2x-1=-1 \le 0$. □

Beachte, dass dies ein vollständiger Beweis ist: *Um eine allgemeine Aussage zu widerlegen, genügt es, ein Gegenbeispiel dafür anzugeben.*

Bemerkung 1.11. Bevor wir unsere kurze Auflistung der für uns wichtigen Prinzipien der Logik beenden, wollen wir noch kurz auf ein paar generelle Dinge eingehen, die man beim Aufschreiben mathematischer Beweise oder Rechnungen beachten muss.

Dass wir bei unseren logischen Argumenten sauber und exakt arbeiten – also z. B. nicht Folgerungen, die keine Äquivalenzen sind, in der falschen Richtung verwenden, „für alle" mit „es gibt" verwechseln oder ähnliches – sollte sich von selbst verstehen. Die folgende kleine Geschichte hilft vielleicht zu verstehen, was damit gemeint ist.

> Ein Ingenieur, ein Physiker und ein Mathematiker fahren mit dem Zug nach Frankreich und sehen dort aus dem Fenster des Zuges ein schwarzes Schaf.
>
> Da sagt der Ingenieur: „Oh, in Frankreich sind die Schafe schwarz!"
>
> Darauf der Physiker: „Nein ... wir wissen jetzt nur, dass es in Frankreich mindestens ein schwarzes Schaf gibt."
>
> Der Mathematiker: „Nein ... wir wissen nur, dass es in Frankreich mindestens ein Schaf gibt, das auf mindestens einer Seite schwarz ist."

Es gibt aber noch einen weiteren sehr wichtigen Punkt, der leider oft nicht beachtet wird: In der Regel werden wir beim Aufschreiben sowohl Aussagen notieren wollen, die wir erst noch zeigen wollen (um schon einmal zu sagen, worauf wir hinaus wollen), als auch solche, von denen wir bereits wissen, dass sie wahr sind (z. B. weil sie für die zu zeigende Behauptung als wahr vorausgesetzt werden oder weil sie sich logisch aus irgendetwas bereits Bekanntem ergeben haben). Es sollte offensichtlich sein, dass wir Aussagen mit derartig verschiedenen Bedeutungen für die Argumentationsstruktur nicht einfach zusammenhangslos hintereinander schreiben dürfen, wenn noch jemand in der Lage sein soll, die Argumente nachzuvollziehen. Betrachten wir z. B. noch einmal unseren

Beweis aus Beispiel 1.10 (a) oben, so wäre eine Art des Aufschreibens in folgendem Stil (wie man es leider oft sieht)

$$\begin{array}{lll} 2x+1>0 & \text{oder} & 2x-1<0 \\ 2x+1\le 0 & & 2x-1\ge 0 \\ \multicolumn{3}{l}{0\ge 2x+1=2x-1+2\ge 0+2=2} \end{array}$$

völlig inakzeptabel, obwohl hier natürlich letztlich die gleichen Aussagen stehen wie oben. Kurz gesagt:

> Von *jeder* aufgeschriebenen Aussage muss für den Leser *sofort* und *ohne eigenes Nachdenken* ersichtlich sein, welche Rolle sie in der Argumentationsstruktur spielt: Ist es z. B. eine noch zu zeigende Behauptung, eine Annahme oder eine Folgerung (und wenn ja, aus was)?

Dies bedeutet allerdings nicht, dass wir ganze Aufsätze schreiben müssen. Eine (schon recht platzoptimierte) Art, den Beweis aus Beispiel 1.10 (a) aufzuschreiben, wäre z. B.

Angenommen, es gäbe ein $x\in\mathbb{R}$ mit $2x+1\le 0$ und $2x-1\ge 0$.
Dann wäre $0\ge 2x+1=2x-1+2\ge 0+2=2$, Widerspruch. □ 01

1.B Mengenlehre

Nachdem wir die wichtigsten Regeln der Logik behandelt haben, wenden wir uns jetzt der Mengenlehre zu. Die gesamte moderne Mathematik basiert auf diesem Begriff der Menge, der ja auch schon aus der Schule hinlänglich bekannt ist. Zur Beschreibung, was eine Menge ist, zitiert man üblicherweise die folgende Charakterisierung von Georg Cantor (1845–1918):

> „Eine **Menge** ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.“

Die in einer Menge zusammengefassten Objekte bezeichnet man als ihre **Elemente**.

Notation 1.12.

(a) Wir schreiben $x\in M$, falls x ein Element der Menge M ist, und $x\notin M$ andernfalls.

(b) Die einfachste Art, eine Menge konkret anzugeben, besteht darin, ihre Elemente in geschweiften Klammern aufzulisten, wobei es auf die Reihenfolge und Mehrfachnennungen nicht ankommt. So sind z. B. $\{1,2,3\}$ und $\{2,3,1,3\}$ zwei Schreibweisen für dieselbe Menge mit den drei Elementen 1, 2 und 3.

Beachte, dass die Elemente einer Menge nicht unbedingt Zahlen sein müssen – so ist z. B. $M=\{\{2,3\},\{1,3\}\}$ eine Menge mit zwei Elementen, die selbst wieder Mengen sind, nämlich $\{2,3\}$ und $\{1,3\}$. Mit der Notation aus (a) ist also z. B. $\{1,3\}\in M$. Insbesondere ist M nicht dasselbe wie die Menge $\{1,2,3\}$.

(c) Man kann die Elemente einer Menge auch durch eine beschreibende Eigenschaft angeben: $\{x:A(x)\}$ bezeichnet die Menge aller Objekte x, für die die Aussage $A(x)$ wahr ist, wie z. B. in $\{x\in\mathbb{R}:x^2=1\}=\{-1,1\}$.

(d) Die Menge $\{\}$ ohne Elemente, die sogenannte **leere Menge**, bezeichnen wir mit $\emptyset$.

(e) Eine Menge M heißt **Teilmenge** einer Menge N (geschrieben $M\subset N$), wenn jedes Element von M auch Element von N ist, bzw. in der Quantorenschreibweise von Notation 1.6 wenn

$$\forall x\colon\ x\in M\Rightarrow x\in N.$$

Man sagt in diesem Fall auch, dass N eine **Obermenge** von M ist (geschrieben $N\supset M$).

Beachte, dass M und N dabei auch gleich sein können; in der Tat ist offensichtlich

$$M=N \quad \text{genau dann, wenn} \quad M\subset N \text{ und } N\subset M.$$

Oft wird man eine Gleichheit $M = N$ von Mengen auch so beweisen, dass man separat $M \subset N$ und $N \subset M$ zeigt.

Wenn wir ausdrücken wollen, dass M eine Teilmenge von N und nicht gleich N ist, so schreiben wir dies als $M \subsetneq N$ und sagen, dass M eine **echte Teilmenge** von N ist. Es ist wichtig, dies von der Aussage $M \not\subset N$ zu unterscheiden, die bedeutet, dass M keine Teilmenge von N ist.

Achtung: Manchmal wird in der Literatur das Symbol „$\subset$“ für *echte* Teilmengen und „$\subseteq$“ für nicht notwendig echte Teilmengen verwendet.

(f) Hat eine Menge M nur endlich viele Elemente, so nennt man M eine **endliche Menge** und schreibt die Anzahl ihrer Elemente als $|M|$. Andernfalls setzt man formal $|M| = \infty$.

Bemerkung 1.13 (Russellsches Paradoxon)**.** Die oben gegebene Charakterisierung von Mengen von Cantor ist aus mathematischer Sicht natürlich sehr schwammig. In der Tat hat Bertrand Russell kurz darauf bemerkt, dass sie sogar schnell zu Widersprüchen führt. Er betrachtet dazu

$$M = \{A : A \text{ ist eine Menge mit } A \notin A\}, \qquad (*)$$

also „die Menge aller Mengen, die sich nicht selbst als Element enthalten“. Sicherlich ist es eine merkwürdige Vorstellung, dass eine Menge sich selbst als Element enthalten könnte – im Sinne von Cantors Charakterisierung wäre die Definition $(*)$ aber zulässig. Fragen wir uns nun allerdings, ob sich die so konstruierte Menge M selbst als Element enthält, so erhalten wir sofort einen Widerspruch: Wenn $M \in M$ gilt, so würde das nach der Definition $(*)$ ja gerade bedeuten, dass $M \notin M$ ist – und das wiederum, dass doch $M \in M$ ist. Man bezeichnet dies als das *Russellsche Paradoxon*.

Die Ursache für diesen Widerspruch ist, dass die Definition $(*)$ rückbezüglich ist: Wir wollen eine neue Menge M konstruieren, verwenden dabei aber auf der rechten Seite der Definition *alle Mengen*, also u. a. auch die Menge M, die wir gerade erst definieren wollen. Das ist in etwa so, als würdet ihr im Beweis eines Satzes die Aussage des Satzes selbst verwenden – und das ist natürlich nicht zulässig.

Man muss bei der Festlegung, was Mengen sind und wie man sie bilden kann, also eigentlich viel genauer vorgehen, als es Cantor getan hat. Heutzutage verwendet man hierzu in der Regel das im Jahre 1930 aufgestellte Axiomensystem von Zermelo und Fraenkel, das genau angibt, wie man aus bekannten Mengen neue konstruieren darf: z. B. indem man sie schneidet oder vereinigt, oder aus bereits bekannten Mengen Elemente mit einer bestimmten Eigenschaft auswählt. Wir wollen dies hier in dieser Vorlesung aber nicht weiter thematisieren und uns mit der naiven Mengencharakterisierung von Cantor begnügen (sowie der Versicherung meinerseits, dass schon alles in Ordnung ist, wenn wir neue Mengen immer nur aus alten konstruieren und keine rückbezüglichen Definitionen hinschreiben). Genaueres zum Zermelo-Fraenkel-Axiomensystem könnt ihr z. B. in [E, Kapitel 13] nachlesen.

Notation 1.14 (Reelle Zahlen)**.** Unser wichtigstes Beispiel für eine Menge ist die Menge der **reellen Zahlen**, die wir mit $\mathbb{R}$ bezeichnen werden. Wir wollen die Existenz der reellen Zahlen in dieser Vorlesung axiomatisch voraussetzen und begnügen uns daher an dieser Stelle damit zu sagen, dass man sie sich als die Menge der Punkte auf einer Geraden (der „Zahlengeraden“) vorstellen kann. Zusätzlich werden wir in den nächsten beiden Kapiteln die mathematischen Eigenschaften von $\mathbb{R}$ exakt angeben (und ebenfalls axiomatisch voraussetzen) – und zwar genügend viele Eigenschaften, um $\mathbb{R}$ dadurch eindeutig zu charakterisieren.

Ich möchte hier noch einmal betonen, dass man die Existenz und die Eigenschaften der reellen Zahlen eigentlich nicht voraussetzen müsste: Man kann das auch allein aus den Axiomen der Logik und Mengenlehre herleiten! Dies wäre jedoch relativ aufwendig und würde euch im Moment mehr verwirren als helfen, daher wollen wir hier darauf verzichten. Wer sich trotzdem dafür interessiert, kann die Einzelheiten hierzu in [E, Kapitel 1 und 2] nachlesen.

Außer den reellen Zahlen sind vor allem noch die folgenden Teilmengen von $\mathbb{R}$ wichtig:

(a) die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$ der **natürlichen Zahlen** (Achtung: In der Literatur wird die 0 manchmal nicht mit zu den natürlichen Zahlen gezählt!);

(b) die Menge $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ der **ganzen Zahlen**;

(c) die Menge $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ der **rationalen Zahlen**.

Offensichtlich sind diese Mengen ineinander enthalten: Es gilt $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. Teilmengen von $\mathbb{R}$, die durch Ungleichungen gegeben sind, schreiben wir in der Regel, indem wir die Ungleichungsbedingung als Index an das Symbol $\mathbb{R}$ schreiben, z. B. $\mathbb{R}_{\geq 0}$ für die Menge $\{x \in \mathbb{R} : x \geq 0\}$ aller nicht-negativen Zahlen.

Notation 1.15. Sind M und N Mengen, so bezeichnen wir mit ...

(a) $M \cap N := \{x : x \in M \text{ und } x \in N\}$ die **Schnittmenge** von M und N. Gilt $M \cap N = \emptyset$, so sagen wir, dass M und N **disjunkt** sind.

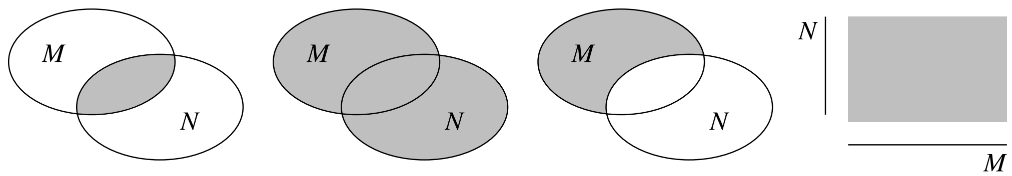
(b) $M \cup N := \{x : x \in M \text{ oder } x \in N\}$ die **Vereinigungsmenge** von M und N. Im Fall einer **disjunkten Vereinigung** mit $M \cap N = \emptyset$ schreiben wir statt $M \cup N$ auch $M \mathbin{\dot\cup} N$.

(c) $M \setminus N := \{x : x \in M \text{ und } x \notin N\}$ die **Differenzmenge** von M und N.

(d) $M \times N := \{(x, y) : x \in M, y \in N\}$ die **Produktmenge** bzw. das Produkt von M und N. Die Schreibweise (x, y) steht hierbei für ein **geordnetes Paar**, d. h. einfach für die Angabe eines Elements aus M und eines aus N (wobei es auch im Fall $M = N$ auf die Reihenfolge ankommt, d. h. (x, y) ist genau dann gleich (x', y') wenn $x = x'$ und $y = y'$). Im Fall $M = N$ schreibt man $M \times N = M \times M$ auch als M^2.

(e) $\mathscr{P}(M) := \{A : A \text{ ist Teilmenge von } M\}$ die **Potenzmenge** von M.

Das Symbol „:=“ bedeutet hierbei, dass der Ausdruck auf der linken Seite durch die rechte Seite definiert wird. Die Konstruktionen (a) bis (d) können durch die folgenden Bilder veranschaulicht werden. Natürlich sind sie auch für mehr als zwei Mengen möglich; aus der Schule kennt ihr zum Beispiel sicher den Fall $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.



$M \cap N$ $M \cup N$ $M \setminus N$ $M \times N$

Die Potenzmenge $\mathscr{P}(M)$ aller Teilmengen einer gegebenen Menge M lässt sich dagegen nicht so einfach durch ein Bild darstellen. Es ist z. B.

$$\mathscr{P}(\{0,1\}) = \big\{\emptyset, \{0\}, \{1\}, \{0,1\}\big\}.$$

Aufgabe 1.16. Wie lautet die Negation der folgenden Aussagen? Formuliere außerdem die Aussage (a) in Worten (also analog zu (b)) sowie die Aussage (b) mit Quantoren und anderen mathematischen Symbolen (also analog zu (a)).

(a) $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N} \colon n = 2m$.

(b) Zwischen je zwei verschiedenen reellen Zahlen gibt es noch eine weitere reelle Zahl.

(c) Sind M, N, R Mengen mit $R \subset N \subset M$, so ist $M \setminus N \subset M \setminus R$.

Aufgabe 1.17. Es seien A, B, C Aussagen und M, N, R Mengen. Man zeige:

(a) $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ und $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$.

(b) $M \cup (N \cap R) = (M \cup N) \cap (M \cup R)$ und $M \cap (N \cup R) = (M \cap N) \cup (M \cap R)$.

Aufgabe 1.18. Welche der folgenden Aussagen sind für beliebige gegebene x und M äquivalent zueinander? Zeige jeweils die Äquivalenz bzw. widerlege sie durch ein Gegenbeispiel.

(a) $x \in M$	(b) $\{x\} \subset M$	(c) $\{x\} \cap M \neq \emptyset$
(d) $\{x\} \in M$	(e) $\{x\} \setminus M = \emptyset$	(f) $M \setminus \{x\} = \emptyset$

Aufgabe 1.19. Man beweise oder widerlege: Für alle Mengen $A \subset M$ und $A' \subset M'$ gibt es Teilmengen B und C von M sowie B' und C' von M', so dass

$$(M \times M') \setminus (A \times A') = (B \times B') \mathbin{\dot\cup} (C \times C').$$

Könnt ihr die Aussage durch eine Skizze veranschaulichen?

2. Relationen und Funktionen

Nachdem wir Mengen eingeführt haben, wollen wir nun auch mehrere von ihnen miteinander in Beziehung setzen können. Das Grundkonzept hierfür ist das einer Relation.

Definition 2.1 (Relationen)**.** Es seien M und N zwei Mengen. Eine **Relation** zwischen M und N ist eine Teilmenge R des Produkts $M \times N$. Für $x \in M$ und $y \in N$ mit $(x,y) \in R$ sagen wir dann „*x steht (bezüglich R) in Relation zu y*". Ist $M = N$, so nennen wir R auch eine *Relation auf M*.

Bemerkung 2.2. Um eine Relation R anzugeben, also eine Teilmenge $R \subset M \times N$ zu definieren, müssen wir demzufolge einfach für alle Paare (x,y) mit $x \in M$ und $y \in N$ festlegen, ob $(x,y) \in R$ gelten, also ob x in Relation zu y stehen soll.

Wie wir in diesem Kapitel sehen werden, werden Relationen in der Mathematik für sehr unterschiedliche Konzepte verwendet – z. B. um Zahlen miteinander zu vergleichen wie in Beispiel 2.3, um eine Menge auf eine andere abzubilden wie in Abschnitt 2.A, oder um die Elemente einer Menge nach bestimmten Kriterien zu Klassen zusammenzufassen wie in Abschnitt 2.B. Dementsprechend sind für die Aussage „x steht bezüglich R in Relation zu y" auch je nach Anwendung ganz unterschiedliche Notationen üblich. Für allgemeine, nicht näher spezifizierte Relationen schreibt man hierfür oft $x R y$.

Beispiel 2.3 (Kleiner-Relation)**.** Für $M = N = \mathbb{R}$ betrachten wir die Relation

$$R = \{(x,y) : x,y \in \mathbb{R} \text{ mit } x < y\},$$

für die x also genau dann in Relation zu y steht, wenn $x < y$ gilt. Man nennt R deshalb auch die *Kleiner-Relation* auf $\mathbb{R}$. Die Notation „$x R y$" aus Bemerkung 2.2 stimmt in diesem Fall also mit der Schreibweise „$x < y$" überein, wenn man die Relation R direkt mit dem Symbol „$<$" bezeichnet. In der Tat ist es aus diesem Grund bei manchen Relationen üblich, sie gleich mit Symbolen statt mit Buchstaben zu benennen.

2.A Funktionen

Die mit Abstand wichtigsten Relationen sind ohne Zweifel die Funktionen, die ihr natürlich bereits hinlänglich aus der Schule kennt. Wir wollen sie hier nun exakt einführen und ihre ersten Eigenschaften untersuchen.

Definition 2.4 (Funktionen)**.** Es seien M und N zwei Mengen.

(a) Eine **Funktion** oder **Abbildung** f von M nach N, geschrieben $f: M \to N$, ist eine Relation zwischen M und N, bezüglich der jedes Element x von M zu *genau einem* Element y von N in Relation steht. Wir schreiben dies dann als $x \mapsto y$ oder $y = f(x)$ und sagen, y ist das **Bild** von x unter f bzw. der **Wert** von f in x.

(b) Für eine Funktion $f: M \to N$ bezeichnet man die Menge M als **Definitionsmenge**, **Startmenge** oder **Startraum** von f. Die Menge N heißt **Zielmenge** oder **Zielraum** von f.

Bemerkung 2.5.

(a) Um eine Funktion komplett festzulegen, müssen wir zuerst einmal den Start- und Zielraum angeben, und dann schließlich noch von jedem Element des Startraums sagen, auf welches Element des Zielraums es abgebildet wird. In welcher Form wir diese Zuordnung angeben – ob durch eine Formel, durch explizites Auflisten der Funktionswerte aller Elemente des Startraums, oder irgendwie anders – spielt dabei keine Rolle. So sind z. B.

$$f: \{0,1\} \to \mathbb{R},\ x \mapsto 2x^2, \quad g: \{0,1\} \to \mathbb{R},\ x \mapsto 2x^3, \quad h: \{0,1\} \to \mathbb{R},\ x \mapsto \begin{cases} 0 & \text{für } x = 0, \\ 2 & \text{für } x = 1 \end{cases}$$

trotz ihrer verschieden aussehenden Vorschriften dieselbe Funktion (d. h. es gilt $f = g = h$), da alle drei den gleichen Start- und Zielraum haben und aus den gleichen Zuordnungen $0 \mapsto 0$ und $1 \mapsto 2$ bestehen. Mit anderen Worten sind zwei Funktionen $f,g\colon M \to N$ also genau dann gleich, wenn sie an jedem Punkt die gleichen Werte besitzen, also wenn gilt

$$\forall x \in M\colon\ f(x) = g(x).$$

(b) Man sieht leider oft, dass eine Funktion $f\colon M \to N$ als $f(x)$ geschrieben wird. Es ist wichtig zu verstehen, dass diese Notation gemäß Definition 2.4 falsch ist: Mit $f(x)$ wird *der Wert der Funktion f in einem Punkt $x \in M$* bezeichnet. Somit ist $f(x)$ (für gegebenes x) ein Element von N, und damit ein ganz anderes mathematisches Objekt als die Funktion selbst, die wir nur mit f bezeichnen und die eine Relation zwischen M und N ist. Dies mag auf den ersten Blick spitzfindig erscheinen – wir werden aber später noch oft Mengen sehen, deren Elemente Funktionen sind, und dann ist es natürlich wichtig, dies von der Menge ihrer Funktions*werte* zu unterscheiden.

Beispiel 2.6.

(a) Die Zuordnungen

$$f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \frac{1}{x} \qquad \text{und} \qquad g\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \begin{cases} x+1 & \text{für } x \le 0 \\ x & \text{für } x \ge 0 \end{cases}$$

sind in dieser Form keine zulässigen Funktionsdefinitionen, weil im Fall von f der Zahl 0 kein gültiger Funktionswert zugeordnet wird und im Fall g für die Zahl 0 zwei (sich widersprechende) Festlegungen des Funktionswertes gemacht werden. Dies lässt sich jedoch in beiden Fällen leicht reparieren, z. B. indem man die Festlegungen abändert in

$$f\colon \mathbb{R}\backslash\{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x} \qquad \text{und} \qquad g\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \begin{cases} x+1 & \text{für } x < 0 \\ x & \text{für } x \ge 0 \end{cases}.$$

(b) Zu jeder Menge M gibt es die **identische Abbildung**

$$\mathrm{id}_M\colon M \to M,\ x \mapsto x,$$

die jedes Element auf sich selbst abbildet.

(c) Ist $f\colon M \to N$ eine Abbildung und $A \subset M$ eine Teilmenge des Startraums, so erhält man durch die Einschränkung der Definitionsmenge von M auf A eine neue Abbildung, die wir mit

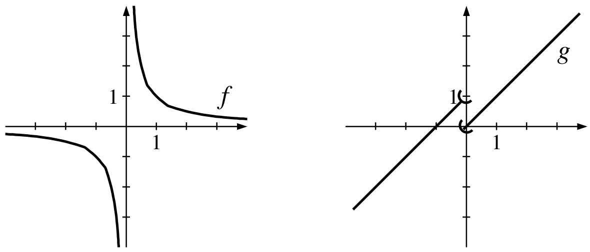
$$f|_A\colon A \to N,\ x \mapsto f(x)$$

bezeichnen und die die **Einschränkung** von f auf A genannt wird. Genauso kann man natürlich auch die Zielmenge N auf eine Teilmenge B einschränken, wenn f nur Werte in B annimmt. Es ist üblich, bei einer derartigen Einschränkung der Zielmenge immer noch den gleichen Namen für die Abbildung zu verwenden, also dann $f\colon M \to B$ zu schreiben (auch wenn es sich dabei um eine andere Funktion als das ursprüngliche $f\colon M \to N$ handelt).

Bemerkung 2.7 (Graph einer Abbildung)**.** Zu einer Abbildung $f\colon M \to N$ heißt die Menge

$$\{(x, f(x)) : x \in M\} \quad \subset M \times N$$

der **Graph** von f. Sind M und N Teilmengen von $\mathbb{R}$, so ist dieser Graph also eine Teilmenge von $\mathbb{R}^2$, und man kann ihn leicht zeichnen und dadurch die Abbildung veranschaulichen. Für die Abbildungen aus Beispiel 2.6 (a) sieht dies z. B. so aus:



Beachte, dass dieser Graph nach den Definitionen 2.1 und 2.4 eigentlich sogar genau das gleiche ist wie die Funktion selbst, nämlich die Teilmenge des Produkts $M \times N$, die aus den Paaren (x,y) besteht, für die x bezüglich f in Relation zu y steht, also $y = f(x)$ gilt. Der Begriff des Graphen soll hier also nur noch einmal deutlich machen, dass man sich die Funktion gerade wirklich als ein derart „grafisches" Objekt vorstellt und nicht als eine „Zuordnung" von M nach N.

In der Definition 2.4 einer Abbildung $f\colon M \to N$ verlangen wir, dass jedem Element von M genau ein Element von N zugeordnet wird. Wir fordern jedoch nicht auch umgekehrt, dass jedes Element des Zielraums N das Bild von genau einem Element von M ist, oder dass es überhaupt als Bild eines Elements von M auftritt. Abbildungen, die diese Eigenschaften dennoch besitzen, haben spezielle Namen, die wir jetzt einführen wollen.

Definition 2.8 (Eigenschaften von Abbildungen)**.** Es sei $f\colon M \to N$ eine Abbildung.

(a) Ist $y \in N$ und $x \in M$ mit $f(x) = y$, so heißt x ein **Urbild** von y unter f.

(b) Hat jedes $y \in N$ ...

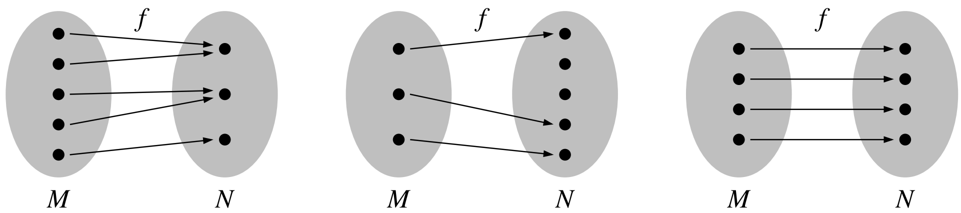
- *mindestens* ein Urbild, so heißt f **surjektiv**.

  In Quantoren bedeutet dies: $\forall y \in N \ \exists x \in M\colon \ f(x) = y$.

- *höchstens* ein Urbild, so heißt f **injektiv**.

  In Quantoren bedeutet dies: $\forall x_1, x_2 \in M\colon \ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. (Also: Haben zwei Elemente des Startraums das gleiche Bild, so müssen sie bereits dasselbe Element sein.)

- *genau* ein Urbild, ist f also surjektiv und injektiv, so heißt f **bijektiv**.



surjektiv injektiv bijektiv 02

Beispiel 2.9. Betrachten wir noch einmal die Funktionen aus Beispiel 2.6 (a), so ist die Funktion f nicht surjektiv (und damit auch nicht bijektiv), da das Element 0 des Zielraums kein Urbild hat. Sie ist jedoch injektiv: Sind $x_1, x_2 \in \mathbb{R}\backslash\{0\}$ mit $f(x_1) = f(x_2)$, also $\frac{1}{x_1} = \frac{1}{x_2}$, so folgt durch Multiplikation mit $x_1 x_2$ sofort $x_1 = x_2$.

Die Funktion g dagegen ist surjektiv: Eine Zahl $y \in \mathbb{R}$ hat als Urbild $x = y$ für $y \geq 0$, und $x = y - 1$ für $y < 0$. Sie ist allerdings nicht injektiv, denn es ist $g(-1) = g(0) = 0$.

Beachte, dass diese Eigenschaften auch an den Graphen in Bemerkung 2.7 ablesbar sind: Surjektivität bzw. Injektivität bedeuten gerade, dass jede horizontale Gerade auf der Höhe eines Wertes im Zielraum den Funktionsgraphen in mindestens bzw. höchstens einem Punkt schneidet. Wichtig ist auch, dass diese Eigenschaften von der Wahl des Start- und Zielraums abhängen: So wird z. B. f bijektiv, wenn man den Zielraum $\mathbb{R}$ durch $\mathbb{R}\backslash\{0\}$ ersetzt, und g injektiv, wenn man den Startraum auf $\mathbb{R}_{\geq 0}$ einschränkt (in der Notation von Beispiel 2.6 (c) also $g|_{\mathbb{R}_{\geq 0}}$ betrachtet).

Aufgabe 2.10. Wie viele Abbildungen gibt es zwischen den Mengen $\{1,2,3,4\}$ und $\{1,2,3,4,5,6\}$? Wie viele von ihnen sind injektiv?

Bilder und Urbilder unter Abbildungen betrachtet man oft auch von ganzen Mengen statt nur von Punkten:

Definition 2.11 (Bild und Urbild von Mengen)**.** Es sei $f\colon M\to N$ eine Abbildung.

(a) Für $A\subset M$ heißt die Menge

$$f(A):=\{f(x):x\in A\}\quad\subset N$$

(also die Menge aller Bilder von Punkten in A) das **Bild** von A unter f.

(b) Ist $B\subset N$, so heißt die Menge

$$f^{-1}(B):=\{x\in M:f(x)\in B\}\quad\subset M$$

(also die Menge aller Urbilder von Punkten in B) das **Urbild** von B unter f.

Bemerkung 2.12. Die Grundidee der Notation in Definition 2.11 (a) ist: Schreiben wir als Argument einer Funktion $f\colon M\to N$ eine *Teilmenge* statt einem *Element* von M, so bedeutet dies, dass wir alle Werte $f(x)$ für $x\in M$ zusammen nehmen und diese wieder in einer Menge zusammenfassen. Diese Schreibweise verwendet man auch oft, wenn die Funktion aus einer Rechenverknüpfung besteht, wie z. B. in

$$\mathbb{N}+\tfrac{1}{2}:=\left\{n+\tfrac{1}{2}:n\in\mathbb{N}\right\}=\left\{\tfrac{1}{2},\tfrac{3}{2},\tfrac{5}{2},\dots\right\}\quad\text{oder}\quad 3\mathbb{Z}:=\{3n:n\in\mathbb{Z}\}=\{\dots,-6,-3,0,3,6,\dots\}.$$

Beispiel 2.13. Für die Funktion $f\colon\mathbb{R}\backslash\{0\}\to\mathbb{R}$, $x\mapsto\frac{1}{x}$ aus Beispiel 2.6 (a) ist $f(\mathbb{R}_{>0})=\mathbb{R}_{>0}$ und $f^{-1}(\{0\})=\emptyset$.

Beispiel 2.14. Zwischen den Konstruktionen von Bild und Urbild aus Definition 2.11 und den Mengenoperationen aus Abschnitt 1.B gibt es sehr viele Beziehungen. Um einmal exemplarisch zu sehen, wie derartige Beziehungen aussehen und bewiesen werden können, wollen wir nun zeigen, dass für jede Abbildung $f\colon M\to N$ und zwei beliebige Teilmengen $A,B\subset M$ stets

$$f(A)\backslash f(B)\subset f(A\backslash B)\tag{$*$}$$

gilt.

Zum Beweis müssen wir zeigen, dass jedes Element der linken Menge auch in der rechten Menge liegt. Es sei also $y\in f(A)\backslash f(B)$ beliebig. Insbesondere ist damit $y\in f(A)$, nach Definition 2.11 (a) also $y=f(x)$ für ein $x\in A$. Würde nun auch $x\in B$ gelten, so hätten wir wegen $y=f(x)$ auch $y\in f(B)$, im Widerspruch zu $y\in f(A)\backslash f(B)$. Also ist $x\notin B$, und damit $x\in A\backslash B$. Damit besagt $y=f(x)$ aber gerade $y\in f(A\backslash B)$. Insgesamt haben wir somit die behauptete Teilmengenbeziehung $(*)$ gezeigt.

Beachte allerdings, dass in $(*)$ im Allgemeinen keine Gleichheit gilt: Für $f\colon\mathbb{R}\to\mathbb{R}$, $x\mapsto x^2$ mit $A=\{-1,1\}$ und $B=\{-1\}$ ist

$$f(A)\backslash f(B)=\{1\}\backslash\{1\}=\emptyset,\quad\text{aber}\quad f(A\backslash B)=f(\{1\})=\{1\}.$$

Aufgabe 2.15. Beweise die folgenden Teilmengenbeziehungen und untersuche jeweils, ob auch die Gleichheit gilt.

(a) Für alle Mengen M,A,B gilt $M\backslash(A\cup B)\subset(M\backslash A)\cap(M\backslash B)$.

(b) Ist $f\colon M\to N$ eine Abbildung und $A\subset N$, so ist $f\left(f^{-1}(A)\right)\subset A$.

Aufgabe 2.16. Es sei $f\colon M\to N$ eine Abbildung. Finde für das Symbol $\square$ jeweils eine der Mengenbeziehungen $\subset,=,\supset$, so dass die folgenden Aussagen wahr werden, und beweise die so entstandenen Aussagen!

(a) $f(A)\cap f(B)\;\square\;f(A\cap B)$ für alle $A,B\subset M$.

(b) $f^{-1}(A)\cap f^{-1}(B)\;\square\;f^{-1}(A\cap B)$ für alle $A,B\subset N$.

Als Nächstes wollen wir nun die euch sicher bereits bekannte Verkettung, also die Hintereinanderausführung von Funktionen einführen.

Definition 2.17 (Verkettung von Funktionen)**.** Es seien $f: M \to N$ und $g: N \to R$ zwei Abbildungen (also so dass die Zielmenge von f gleich der Startmenge von g ist). Dann heißt die Abbildung

$$g \circ f : M \to R,\ x \mapsto g(f(x))$$

die **Verkettung** von f und g.

Bemerkung 2.18. Bei der Verkettung zweier Funktionen kommt es natürlich auf die Reihenfolge an, allein schon weil in der Situation von Definition 2.17 in der Regel der Zielraum von g ja nicht mit dem Startraum von f übereinstimmt und die „umgekehrte Verkettung" $f \circ g$ damit gar nicht definierbar wäre. Beachte dabei, dass die Notation $g \circ f$ lautet, obwohl wir zuerst f (von M nach N) und dann g (von N nach R) anwenden – man liest $g \circ f$ daher manchmal auch als „g nach f". Diese vielleicht etwas merkwürdig erscheinende Notation kommt einfach daher, dass die Buchstaben in der gleichen Reihenfolge stehen sollen wie bei der Abbildungsvorschrift $x \mapsto g(f(x))$.

Wir werden nun unser erstes *Lemma* beweisen – „Lemma" ist griechisch und bedeutet eigentlich „Annahme", aber in der Mathematik wird dieser Begriff für einen *Hilfssatz* verwendet, also für ein kleines Zwischenresultat, das vielleicht für sich genommen nicht übermäßig überraschend oder interessant ist, aber das in späteren Beweisen immer wieder nützlich sein wird. In unserem momentanen Fall geht es einfach darum, dass die Verkettung von Abbildungen *assoziativ* ist (siehe auch Definition 3.1):

Lemma 2.19 (Assoziativität der Verkettung)**.** *Sind $f: M \to N$, $g: N \to R$ und $h: R \to S$ drei Abbildungen, so gilt $h \circ (g \circ f) = (h \circ g) \circ f$. (Man schreibt für diese Abbildung daher oft auch einfach $h \circ g \circ f$.)*

Beweis. Nach Definition 2.4 können wir die Gleichheit zweier Funktionen zeigen, indem wir für jedes Element der Startmenge nachweisen, dass sein Bild unter beiden Funktionen übereinstimmt. Dies rechnen wir nun einfach durch wiederholtes Einsetzen von Definition 2.17 nach: Es gilt

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

und

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

Da diese beiden Ausdrücke übereinstimmen, ist das Lemma bewiesen. □

Am Ende dieses Abschnitts wollen wir schließlich noch das Konzept von Umkehrfunktionen bijektiver Funktionen einführen.

Definition 2.20 (Umkehrfunktionen)**.** Es sei $f: M \to N$ eine bijektive Funktion. Dann heißt

$$f^{-1} : N \to M,\ y \mapsto \text{das eindeutige Urbild von } y \text{ unter } f$$

die **Umkehrfunktion** bzw. **Umkehrabbildung** von f.

Bemerkung 2.21. Für die Umkehrfunktion f^{-1} einer bijektiven Funktion $f: M \to N$ gilt nach Konstruktion offensichtlich $f^{-1} \circ f = \mathrm{id}_M$ und $f \circ f^{-1} = \mathrm{id}_N$.

Gibt es umgekehrt zu einer Funktion $f: M \to N$ eine Abbildung $g: N \to M$ mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$, so ist f bijektiv:

- f ist surjektiv: Ist $y \in N$ beliebig, so ist $x := g(y) \in M$ ein Urbild von y unter f, denn es ist $f(x) = f(g(y)) = y$.
- f ist injektiv: Sind $x_1, x_2 \in M$ mit $f(x_1) = f(x_2)$, so folgt durch Anwenden von g sofort auch $g(f(x_1)) = g(f(x_2))$, und damit $x_1 = x_2$.

Beispiel 2.22. Die Funktion $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x+1$ ist bijektiv, und ihre Umkehrabbildung ist $f^{-1}: \mathbb{R} \to \mathbb{R}$, $x \mapsto x-1$. In der Tat gilt nämlich für alle $x \in \mathbb{R}$

$$(f^{-1} \circ f)(x) = (x+1) - 1 = x \quad \text{und} \quad (f \circ f^{-1})(x) = (x-1) + 1 = x.$$

Bemerkung 2.23 (Urbilder und Umkehrabbildungen)**.** Beachte, dass wir das Urbild einer Menge unter einer Abbildung $f: M \to N$ in Definition 2.11 (b) mit dem gleichen Symbol f^{-1} bezeichnet haben wie (im Fall einer bijektiven Abbildung) die Umkehrabbildung aus Definition 2.20. Das ist vielleicht etwas unglücklich gewählt, aber in der Literatur so fest verankert, dass wir hier nicht davon abweichen wollen. Bei genauem Hinschauen kann man aber auch immer feststellen, was gemeint ist:

> Ist $f: M \to N$ eine Abbildung, so bezeichnet ...
>
> ... $f^{-1}(B)$ für eine *Menge* $B \subset N$ das *Urbild* von B wie in Definition 2.11 (b); es existiert für jede Abbildung f.
>
> ... $f^{-1}(y)$ für ein *Element* $y \in B$ den *Wert der Umkehrabbildung* bei y wie in Definition 2.20; er existiert nur für bijektives f.

Letztlich hängen diese beiden Notationen aber auch eng miteinander zusammen: Ist f bijektiv und ist $x \in M$ mit $f(x) = y$, so ist $f^{-1}(y) = x$ (mit f^{-1} im Sinne der Umkehrabbildung) und $f^{-1}(\{y\}) = \{x\}$ (mit f^{-1} im Sinne des Urbildes).

Aufgabe 2.24.

(a) Untersuche die Abbildung $f: \mathbb{Z} \to \mathbb{Z},\ x \mapsto 3x+2$ auf Injektivität und Surjektivität.

(b) Untersuche die Abbildung $f: \mathbb{R}^2 \to \mathbb{R}^2,\ (x,y) \mapsto (xy, x+1)$ auf Injektivität und Surjektivität.

(c) Man zeige: Sind $f: M \to N$ und $g: N \to R$ surjektiv, so ist auch $g \circ f: M \to R$ surjektiv.

Aufgabe 2.25. Es seien $f: M \to N$ und $g: N \to R$ bijektiv. Zeige, dass dann auch $f^{-1}: N \to M$ und $g \circ f: M \to R$ bijektiv sind.

Aufgabe 2.26. Man beweise oder widerlege:

(a) Sind $f: M \to N$ und $g: N \to R$ zwei Abbildungen und ist $g \circ f$ injektiv, so ist auch f injektiv.

(b) Sind $f: M \to N$ und $g: N \to R$ zwei Abbildungen und ist $g \circ f$ injektiv, so ist auch g injektiv.

Aufgabe 2.27. Es sei $f: M \to N$ eine Abbildung zwischen nicht-leeren Mengen. Man zeige:

(a) f ist genau dann surjektiv, wenn es eine Abbildung $g: N \to M$ gibt mit $f \circ g = \mathrm{id}_N$.

(b) f ist genau dann injektiv, wenn es eine Abbildung $g: N \to M$ gibt mit $g \circ f = \mathrm{id}_M$.

Aufgabe 2.28. Es sei $f: M \to N$ eine Abbildung zwischen zwei Mengen. Man beweise:

$$f \text{ ist surjektiv} \quad \Leftrightarrow \quad \text{für alle } A,B \subset N \text{ mit } f^{-1}(A) = f^{-1}(B) \text{ gilt } A = B.$$

Aufgabe 2.29. Für diese Aufgabe nennen wir eine Funktion $f: \mathbb{R} \to \mathbb{R}$ ...

- *monoton wachsend*, wenn gilt: $\forall x,y \in \mathbb{R} : x < y \Rightarrow f(x) \le f(y)$;
- *irgendwann konstant*, wenn gilt: $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R} : x \le y \Rightarrow f(x) = f(y)$;
- *interessant*, wenn gilt: $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R} : x < y$ und $f(x) < f(y)$.

Man zeige:

(a) Die Funktion $f: \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ ist interessant.

(b) Für die Eigenschaften „monoton wachsend" und „irgendwann konstant" gilt, dass mit $f: \mathbb{R} \to \mathbb{R}$ und $g: \mathbb{R} \to \mathbb{R}$ auch deren Summenfunktion

$$f+g: \mathbb{R} \to \mathbb{R},\ x \mapsto f(x)+g(x)$$

diese Eigenschaft hat.

(c) Ist $f: \mathbb{R} \to \mathbb{R}$ monoton wachsend, aber nicht interessant, so ist f irgendwann konstant.

2.B Äquivalenzrelationen

Am Anfang dieses Kapitels haben wir allgemeine Relationen eingeführt, als einzigen Spezialfall davon aber bisher nur die Funktionen ausführlicher betrachtet. Wir wollen daher nun noch einen ganz anderen wichtigen Typ von Relationen studieren, die sogenannten Äquivalenzrelationen.

Angenommen, wir möchten eine Menge M untersuchen, die uns zunächst einmal zu groß oder zu kompliziert erscheint. Es gibt dann zwei prinzipiell verschiedene Möglichkeiten, wie man daraus eine kleinere bzw. einfachere Menge machen kann:

- Wir können uns auf eine Teilmenge von M beschränken – dann schließen wir allerdings manche Elemente von M von unserer Untersuchung aus.
- Wir können zwar alle Elemente von M betrachten, aber manche von ihnen miteinander identifizieren bzw. zu Klassen zusammenfassen – d. h. sie als gleich bzw. „äquivalent“ ansehen, wenn sie für das zu untersuchende Problem ähnliche Eigenschaften haben.

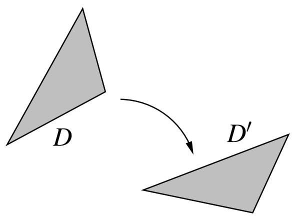
Diese zweite Idee der Identifizierung ähnlicher Elemente führt zum Begriff der Äquivalenzrelationen. Sie klingt vielleicht zunächst etwas abstrakt, ist euch aber sicher schon an vielen Stellen begegnet. Hier sind zwei einfache Beispiele dafür.

Beispiel 2.30.

(a) Eine analoge Uhr vereinfacht die recht große Menge aller (vergangenen und zukünftigen) Zeitpunkte, die wir uns als Zeitachse $M = \mathbb{R}$ vorstellen können, indem sie nach jeweils 12 Stunden wieder dasselbe anzeigt. Sie identifiziert also zwei Zeitpunkte $x, y \in \mathbb{R}$ (gemessen in Stunden) miteinander, wenn $x - y$ ein ganzzahliges Vielfaches von 12 ist. Dadurch „verkleinert“ sie die ursprüngliche Zeitachse auf ein gut überschaubares Intervall von 12 Stunden – und wir alle wissen, dass uns ein Blick auf die Uhr in vielen Fällen ausreicht, wenn wir den aktuellen Zeitpunkt wissen wollen, auch wenn uns das nichts über das Datum oder die Tageszeit (vormittags oder nachmittags) sagt.

(b) Als „mathematischeres“ Beispiel können wir die Menge M aller Dreiecke in der Ebene $\mathbb{R}^2$ betrachten.

Bekanntlich heißen zwei solche Dreiecke $D, D' \in M$ zueinander *kongruent*, wenn sie wie im Bild rechts durch eine Drehung und / oder Verschiebung auseinander hervorgehen – wir schreiben dies im Folgenden als $D \sim D'$. Zueinander kongruente Dreiecke werden oft miteinander identifiziert, nämlich immer dann, wenn es uns nur auf die Form bzw. Größe der Dreiecke, aber nicht auf ihre Lage in der Ebene ankommt.



Wenn wir z. B. sagen, dass die drei Seitenlängen ein Dreieck eindeutig bestimmen, dann meinen wir damit in Wirklichkeit, dass sie das Dreieck *bis auf Kongruenz* eindeutig bestimmen, also nur die Form und Größe festlegen, aber nicht die Lage des Dreiecks in $\mathbb{R}^2$. Formal kann man dies so ausdrücken: zu einem Dreieck D nennt man

$$\overline{D} := \{D' \in M : D' \sim D\},$$

also die Menge aller zu D kongruenten Dreiecke, die *Kongruenzklasse* von D. Die Menge aller dieser Kongruenzklassen bezeichnen wir mit

$$M/\sim \; := \; \{\overline{D} : D \in M\}.$$

Man kann dann z. B. sagen, dass die Seitenlängen eines Dreiecks ein eindeutiges Element in $M/\sim$ bestimmen, also eine eindeutige Kongruenzklasse von Dreiecken festlegen – nicht aber ein eindeutiges Element von M.

Mit der Idee dieser Beispiele im Kopf wollen wir nun den Begriff der Äquivalenzrelation exakt definieren.

Definition 2.31 (Äquivalenzrelationen)**.** Es sei $\sim$ wie in Definition 2.1 eine Relation auf einer Menge M. Wie in Bemerkung 2.2 schreiben wir $x \sim y$, wenn x und y bezüglich $\sim$ in Relation stehen.

Man nennt $\sim$ eine **Äquivalenzrelation** auf M, wenn die folgenden Eigenschaften gelten:

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

(b) (**Symmetrie**) Sind $x, y \in M$ mit $x \sim y$, so gilt auch $y \sim x$.

(c) (**Transitivität**) Sind $x, y, z \in M$ mit $x \sim y$ und $y \sim z$, so gilt auch $x \sim z$.

In diesem Fall sagt man statt $x \sim y$ auch, dass x (bezüglich dieser Relation) zu y **äquivalent** ist. Zu $x \in M$ heißt dann die Menge

$$\overline{x} := \{y \in M : y \sim x\}$$

aller Elemente, die zu x äquivalent sind, die **Äquivalenzklasse** bzw. einfach **Klasse** von x; jedes Element dieser Menge nennt man einen **Repräsentanten** dieser Klasse. Die Menge aller Äquivalenzklassen schreiben wir als

$$M/\sim \; := \; \{\overline{x} : x \in M\}.$$

Beispiel 2.32.

(a) Das Beispiel 2.30 (a) einer analogen Uhr lässt sich mathematisch exakt wie folgt definieren: Auf $M = \mathbb{R}$ betrachten wir die Relation

$$x \sim y \;:\Leftrightarrow\; \text{es gibt ein } k \in \mathbb{Z} \text{ mit } x - y = 12k. \qquad (*)$$

Dies ist in der Tat eine Äquivalenzrelation, denn für alle $x, y, z \in \mathbb{R}$ gilt:

- Reflexivität: Es gilt $x - x = 12 \cdot 0 = 12k$ mit $k = 0 \in \mathbb{Z}$, also $x \sim x$.
- Symmetrie: Es gelte $x \sim y$, also $x - y = 12k$ für ein $k \in \mathbb{Z}$. Durch Multiplikation mit -1 folgt dann auch $y - x = 12 \cdot (-k) = 12k'$ mit $k' := -k \in \mathbb{Z}$, und damit $y \sim x$.
- Transitivität: Es gelte $x \sim y$ und $y \sim z$, nach Definition der Relation also $x - y = 12k$ und $y - z = 12k'$ für gewisse $k, k' \in \mathbb{Z}$ (beachte, dass der Wert von k in $(*)$ von x und y abhängt und wir daher für die Differenz $y - z$ eine neue Variable k' brauchen). Durch Addition dieser beiden Gleichungen erhalten wir $x - z = 12(k + k') = 12k''$ mit $k'' := k + k' \in \mathbb{Z}$, und damit $x \sim z$.

Die Äquivalenzklasse z. B. von $2 \in \mathbb{R}$ ist

$$\overline{2} = \{x \in \mathbb{R} : x \sim 2\} = \{x \in \mathbb{R} : \text{es gibt ein } k \in \mathbb{Z} \text{ mit } x - 2 = 12k\} = \{2 + 12k : k \in \mathbb{Z}\},$$

also die Menge aller Zeitpunkte, zu denen die Uhr auf 2 steht. Jeder beliebige Zeitpunkt $x \in \mathbb{R}$, zu dem die Uhr auf 2 steht, ist ein Repräsentant dieser Klasse. Die Menge $M/\sim$ entspricht allen möglichen Ständen der Uhr; wir können sie uns anschaulich als einen „Kreis mit Umfang 12“ vorstellen.

(b) Die Kongruenz von Dreiecken aus Beispiel 2.30 (b) ist ebenfalls eine Äquivalenzrelation (es ist offensichtlich, dass sie die Eigenschaften aus Definition 2.31 erfüllt). Die Äquivalenzklassen sind in diesem Fall genau die Kongruenzklassen.

(c) Die Kleiner-Relation auf $\mathbb{R}$ aus Beispiel 2.3, also die Relation, für die für $x, y \in \mathbb{R}$ genau dann $x \sim y$ gilt, wenn $x < y$ ist, ist keine Äquivalenzrelation, da sie weder reflexiv noch symmetrisch ist.

Beachte, dass bei unseren Äquivalenzrelationen aus Beispiel 2.32 (a) und (b) jedes Element von M in genau einer Äquivalenzklasse liegt: Zu jedem Zeitpunkt hat eine analoge Uhr genau einen Stand, und jedes Dreieck in der Ebene liegt in genau einer Kongruenzklasse. Dies beschreibt genau unsere Idee, dass wir die Elemente von M auf eine bestimmte Art zu Klassen zusammenfassen wollen. Allgemein sind die Axiome einer Äquivalenzrelation aus Definition 2.31 anschaulich genau diejenigen, die man braucht, damit die Relation sinnvoll eine solche Identifizierung von Elementen zu Klassen beschreiben kann. Dies zeigt auch noch einmal der folgende zentrale Satz über Äquivalenzrelationen.

Satz 2.33 (Eigenschaften von Äquivalenzrelationen)**.** *Es sei $\sim$ eine Äquivalenzrelation auf einer Menge M.*

(a) *Für $x,y \in M$ gilt $x \sim y$ genau dann, wenn $\overline{x} = \overline{y}$. (Zwei Elemente sind also genau dann äquivalent zueinander, wenn sie die gleiche Äquivalenzklasse bestimmen.)*

(b) *Jedes Element $x \in M$ liegt in genau einer Äquivalenzklasse (nämlich in $\overline{x}$). Insbesondere ist M also die disjunkte Vereinigung aller Äquivalenzklassen. Man sagt dafür auch, dass die Äquivalenzklassen eine* Partition *von M bilden.*

Beweis.

(a) Es seien $x,y \in M$.

„$\Rightarrow$": Es gelte $x \sim y$. Ist dann $z \in M$ mit $z \in \overline{x}$, also $z \sim x$, so ist nach der Transitivität wegen $x \sim y$ auch $z \sim y$, also $z \in \overline{y}$. Damit gilt $\overline{x} \subset \overline{y}$. Da mit $x \sim y$ wegen der Symmetrie aber auch $y \sim x$ gilt, folgt analog auch umgekehrt $\overline{y} \subset \overline{x}$, und somit insgesamt $\overline{x} = \overline{y}$.

„$\Leftarrow$": Es sei nun $\overline{x} = \overline{y}$. Wegen der Reflexivität ist $x \sim x$, also $x \in \overline{x} = \overline{y}$, und damit $x \sim y$.

(b) Wegen der Reflexivität liegt wie im Beweis von (a) jedes $x \in M$ in seiner eigenen Äquivalenzklasse $\overline{x}$. Liegt x nun zusätzlich auch in $\overline{y}$ für ein $y \in M$, gilt also $x \sim y$, so folgt nach (a) sofort $\overline{x} = \overline{y}$. Also waren die beiden Äquivalenzklassen schon gleich, d. h. x liegt in nur einer Äquivalenzklasse (nämlich in $\overline{x}$). □

Aufgabe 2.34. Es sei $M = \{n \in \mathbb{Z} : |n| \leq 100\} = \{-100, -99, \dots, 0, \dots, 99, 100\}$. Welche der folgenden Relationen sind Äquivalenzrelationen auf M? Gib im Fall einer Äquivalenzrelation außerdem die Äquivalenzklasse $\overline{-34}$ explizit an.

(a) $x \sim y \;:\Leftrightarrow\;$ es gibt ein $n \in \mathbb{Z}$ mit $x = 2^n y$.

(b) $x \sim y \;:\Leftrightarrow\; xy \geq 0$.

Aufgabe 2.35. Welche der folgenden Relationen sind Äquivalenzrelationen auf $\mathbb{R}^2$? Im Fall einer Äquivalenzrelation berechne und skizziere man außerdem die Äquivalenzklassen von $(0,1) \in \mathbb{R}^2$ und $(1,1) \in \mathbb{R}^2$.

(a) $(x,y) \sim (x',y') \;:\Leftrightarrow\;$ es gibt ein $a \in \mathbb{R}\backslash\{0\}$ mit $x = a^2 x'$ und $y = ay'$;

(b) $(x,y) \sim (x',y') \;:\Leftrightarrow\;$ es gibt ein $a \in \mathbb{R}\backslash\{0\}$ mit $x = ay'$ und $y = ax'$. 03

3. Erste Eigenschaften der reellen Zahlen

In Notation 1.14 haben wir bereits die reellen Zahlen $\mathbb{R}$ als „Menge der Punkte auf einer Geraden“ eingeführt. Man kann aber natürlich noch viel mehr Dinge mit den reellen Zahlen tun als sie als eine einfache Punktmenge zu betrachten: Man kann sie addieren, multiplizieren, die Größe von zwei Zahlen miteinander vergleichen, und noch einiges mehr. Wir wollen die Eigenschaften der reellen Zahlen in diesem und dem nächsten Kapitel exakt formalisieren, damit wir danach genau wissen, welche Eigenschaften von $\mathbb{R}$ wir in dieser Vorlesung axiomatisch voraussetzen. In der Tat werden diese Eigenschaften letztlich sogar ausreichen, um die reellen Zahlen eindeutig zu charakterisieren. Wir beginnen in diesem Kapitel aber zunächst einmal nur mit den „Grundrechenarten“, also mit der Addition und der Multiplikation sowie ihren Umkehrungen, der Subtraktion und Division.

3.A Gruppen und Körper

Die Eigenschaften von Verknüpfungen wie der Addition oder Multiplikation reeller Zahlen werden mathematisch durch die Begriffe einer Gruppe bzw. eines Körpers beschrieben, die wir jetzt einführen wollen.

Definition 3.1 (Gruppen)**.** Eine **Gruppe** ist eine Menge G zusammen mit einer „Verknüpfung“, d. h. einer Abbildung

$$*\colon G\times G\to G,\ (x,y)\mapsto x*y,$$

so dass die folgenden Eigenschaften (auch *Gruppenaxiome* genannt) gelten:

(a) (**Assoziativität**) Für alle $x,y,z\in G$ gilt $(x*y)*z=x*(y*z)$. Man schreibt diesen Ausdruck dann in der Regel auch einfach als $x*y*z$, weil die Reihenfolge der Klammerung ja egal ist.

(b) (Existenz eines neutralen Elements) Es gibt ein $e\in G$, für das $e*x=x*e=x$ für alle $x\in G$ gilt. Man nennt ein solches e ein **neutrales Element**, und verlangt davon zusätzlich:

(c) (Existenz von inversen Elementen) Für alle $x\in G$ gibt es ein $x'\in G$ mit $x'*x=x*x'=e$. Man nennt x' dann ein **inverses Element** zu x.

Wir bezeichnen eine solche Gruppe mit $(G,*)$. Wenn aus dem Zusammenhang klar ist, welche Verknüpfung gemeint ist, schreiben wir oft auch einfach nur G für die Gruppe.

Gilt zusätzlich zu den obigen Eigenschaften noch

(d) (**Kommutativität**) $x*y=y*x$ für alle $x,y\in G$,

so heißt $(G,*)$ eine **kommutative** oder **abelsche Gruppe**.

Bemerkung 3.2. Manchmal wird in der Definition einer Gruppe in Teil (b) lediglich $e*x=x$ und in Teil (c) lediglich $x'*x=e$ gefordert (man spricht dann auch von einem **linksneutralen** bzw. **linksinversen** Element). Man kann jedoch unter Verwendung der übrigen Gruppenaxiome zeigen, dass in diesem Fall automatisch auch $x*e=x$ und $x*x'=e$ gelten muss, also dass linksneutrale Elemente bereits immer neutrale und linksinverse Elemente immer inverse Elemente sind [G, Satz 1.7]. Die beiden Varianten der Definition einer Gruppe stimmen also letztlich überein.

Beispiel 3.3.

(a) $(\mathbb{R},+)$ ist eine abelsche Gruppe, denn die Addition ist (wie wir axiomatisch voraussetzen werden) eine Verknüpfung auf $\mathbb{R}$ mit den Eigenschaften:

- $(x+y)+z=x+(y+z)$ für alle $x,y,z\in\mathbb{R}$;
- $0\in\mathbb{R}$ ist ein neutrales Element, denn $0+x=x+0=x$ für alle $x\in\mathbb{R}$;
- zu jedem $x\in\mathbb{R}$ ist $-x\in\mathbb{R}$ ein inverses Element, denn $(-x)+x=x+(-x)=0$;

- $x+y=y+x$ für alle $x,y \in \mathbb{R}$.

Auf die gleiche Art sind auch $(\mathbb{Q},+)$ und $(\mathbb{Z},+)$ abelsche Gruppen, jedoch nicht $(\mathbb{N},+)$: Hier existiert zwar noch ein neutrales Element 0, aber die Zahl $1 \in \mathbb{N}$ hat kein Inverses mehr, denn es gibt kein $x \in \mathbb{N}$ mit $x+1=0$.

(b) $(\mathbb{R},\cdot)$ ist keine Gruppe: Die Multiplikation ist zwar assoziativ und kommutativ und hat das neutrale Element 1, aber die Zahl 0 hat kein Inverses – denn dies müsste ja eine Zahl $x \in \mathbb{R}$ sein mit $x \cdot 0 = 1$.

Nimmt man jedoch die 0 aus $\mathbb{R}$ heraus, so erhält man mit $(\mathbb{R}\backslash\{0\},\cdot)$ wieder eine abelsche Gruppe, bei der das neutrale Element 1 und das zu einem x inverse Element $\frac{1}{x}$ ist. Genauso funktioniert dies für $(\mathbb{Q}\backslash\{0\},\cdot)$, aber z. B. nicht für $(\mathbb{Z}\backslash\{0\},\cdot)$: Hier gibt es zwar noch ein neutrales Element 1, aber die Zahl $2 \in \mathbb{Z}\backslash\{0\}$ hat kein Inverses mehr, denn es gibt kein $x \in \mathbb{Z}\backslash\{0\}$ mit $2 \cdot x = 1$.

(c) Hier ist noch ein Beispiel von einem ganz anderen Typ: Es sei M eine beliebige Menge und

$$G = \{f : f \text{ ist eine bijektive Abbildung von } M \text{ nach } M\}.$$

Da die Verkettung bijektiver Abbildungen nach Aufgabe 2.25 wieder bijektiv ist, definiert sie eine Verknüpfung auf G. In der Tat wird G damit zu einer Gruppe, denn die Verkettung ist assoziativ nach Lemma 2.19, die Identität id_M ist ein neutrales Element, und zu einem $f \in G$ ist die Umkehrabbildung f^{-1} aus Definition 2.20 ein inverses Element: Sie ist nach Aufgabe 2.25 selbst wieder bijektiv (also in G) und erfüllt $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}_M$ nach Bemerkung 2.21. Im Allgemeinen ist diese Gruppe jedoch nicht kommutativ.

Wir wollen nun ein paar einfache Eigenschaften von Gruppen beweisen, u. a. dass die in Definition 3.1 geforderten neutralen und inversen Elemente eindeutig sind und wir daher in Zukunft auch von *dem* neutralen und *dem* zu einem gegebenen Element inversen Element sprechen können.

Lemma 3.4 (Eigenschaften von Gruppen)**.** *Es seien $(G,*)$ eine Gruppe und $x,y \in G$.*

(a) *Es gibt genau ein neutrales Element (wie in Definition 3.1 (b)).*

(b) *Es gibt genau ein inverses Element zu x (wie in Definition 3.1 (c)).*

(c) *Sind x' und y' die inversen Elemente zu x bzw. y, so ist $y' * x'$ das inverse Element zu $x * y$.*

(d) *Ist x' das inverse Element zu x, so ist x das inverse Element zu x' („das Inverse des Inversen ist wieder das Ausgangselement“).*

Beweis.

(a) Sind e und $\tilde{e}$ neutrale Elemente, so folgt

$$\begin{aligned} e &= \tilde{e} * e && \text{(denn } \tilde{e} \text{ ist ein neutrales Element)} \\ &= \tilde{e} && \text{(denn } e \text{ ist ein neutrales Element).} \end{aligned}$$

(b) Sind x' und $\tilde{x}'$ inverse Elemente zu x, so gilt

$$\begin{aligned} x' &= e * x' && (e \text{ neutrales Element}) \\ &= (\tilde{x}' * x) * x' && (\tilde{x}' \text{ ist ein inverses Element zu } x) \\ &= \tilde{x}' * (x * x') && \text{(Assoziativität)} \\ &= \tilde{x}' * e && (x' \text{ ist ein inverses Element zu } x) \\ &= \tilde{x}' && (e \text{ neutrales Element).} \end{aligned}$$

(c) Es gilt

$$(y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e$$

und analog auch $(x * y) * (y' * x') = e$. Damit ist $y' * x'$ das inverse Element zu $x * y$.

(d) Die Gleichung $x' * x = x * x' = e$ besagt direkt, dass x das inverse Element zu x' ist. □

Wie wir in Beispiel 3.3 (a) und (b) gesehen haben, erlauben die reellen Zahlen *zwei* grundlegende Gruppenstrukturen: die Addition und (nach Herausnahme der 0) die Multiplikation. Diese beiden Strukturen sind jedoch nicht unabhängig voneinander, da sie durch das Distributivgesetz $(x+y)\cdot z = xz + yz$ für alle $x,y,z \in \mathbb{R}$ miteinander verbunden sind. Eine derartige Kombination zweier Gruppenstrukturen bezeichnet man als einen Körper.

Definition 3.5 (Körper)**.** Ein **Körper** ist eine Menge K zusammen mit zwei Verknüpfungen

$$+ \colon K \times K \to K \quad (\text{genannt } \textit{Addition}) \qquad \text{und} \qquad \cdot \colon K \times K \to K \quad (\text{genannt } \textit{Multiplikation}),$$

so dass die folgenden Eigenschaften (auch *Körperaxiome* genannt) gelten:

(a) $(K,+)$ ist eine abelsche Gruppe. Wir bezeichnen ihr neutrales Element mit 0 und das zu einem $x \in K$ inverse Element mit $-x$.

(b) $(K\backslash\{0\},\cdot)$ ist ebenfalls eine abelsche Gruppe. Wir bezeichnen ihr neutrales Element mit 1 und das zu einem $x \in K\backslash\{0\}$ inverse Element mit x^{-1}.

(c) (**Distributivität**) Für alle $x,y,z \in K$ gilt $(x+y)\cdot z = (x\cdot z) + (y \cdot z)$.

Mit dieser Definition wollen wir nun also axiomatisch voraussetzen:

$$\boxed{\mathbb{R} \text{ ist ein Körper.}}$$

Um Verwirrungen zu vermeiden, werden wir die beiden Verknüpfungen in einem Körper immer mit den Symbolen „$+$“ und „$\cdot$“ bezeichnen. Ebenso werden wir (wie ihr es natürlich gewohnt seid) vereinbaren, dass man den Punkt bei der Multiplikation auch weglassen darf und bei ungeklammerten Ausdrücken zuerst die Multiplikationen und dann die Additionen ausgeführt werden, so dass man also z. B. die Distributivität aus Definition 3.5 (c) auch als $(x+y)z = xz + yz$ schreiben kann.

Es ist jedoch wichtig zu verstehen, dass wir ab jetzt *nicht* mehr voraussetzen werden, dass Addition und Multiplikation in einem Körper wie z. B. $\mathbb{R}$ genau die Verknüpfungen sind, „an die man als Erstes denken würde“ – was auch immer das heißen mag. Stattdessen sind es einfach irgendwelche zwei Verknüpfungen, die die Eigenschaften aus Definition 3.5 haben. Unsere zukünftigen Beweise über Körper wie z. B. $\mathbb{R}$ müssen wir also ausschließlich auf diesen Eigenschaften aufbauen.

Dieser axiomatische Zugang hat zwei Vorteile:

- Zum einen wissen wir dadurch genau, welche Eigenschaften der Grundrechenarten auf den reellen Zahlen wir eigentlich voraussetzen. Es sollte schließlich klar sein, dass wir eine *exakte* Mathematik nicht auf einer *anschaulichen* Vorstellung von $\mathbb{R}$ aufbauen können. Solltet ihr euch also z. B. später einmal dafür interessieren, wie man die Existenz der reellen Zahlen beweisen kann, so wüsstet ihr dann genau, was eigentlich zu beweisen ist: nämlich die Existenz einer Menge mit genau den Eigenschaften, die wir jetzt axiomatisch voraussetzen.
- Zum anderen werdet ihr im Laufe eures Studiums noch viele weitere Körper kennenlernen, z. B. in Kapitel **??** den sehr wichtigen Körper der komplexen Zahlen. Alle Resultate, die nur auf den Körperaxiomen aufbauen, übertragen sich dann also sofort auf diese neuen Fälle, ohne dass man sich darüber noch einmal neu Gedanken machen muss.

Beispiel 3.6.

(a) Neben $\mathbb{R}$ ist auch $\mathbb{Q}$ (mit den gleichen Verknüpfungen wie auf $\mathbb{R}$) ein Körper. Die ganzen Zahlen $\mathbb{Z}$ bilden mit diesen Verknüpfungen jedoch keinen Körper, da $(\mathbb{Z}\backslash\{0\},\cdot)$ nach Beispiel 3.3 (b) keine Gruppe ist. Ebenso ist $\mathbb{N}$ mit diesen Verknüpfungen kein Körper, da hier nach Beispiel 3.3 (a) bereits die Addition keine Gruppenstruktur liefert.

(b) Hier ist ein Beispiel für einen Körper, der sich ganz anders verhält als $\mathbb{R}$ und $\mathbb{Q}$: Wir definieren auf der Menge $K = \{g,u\}$ zwei Verknüpfungen durch die folgenden Tabellen.

$$\begin{array}{c|cc} + & g & u \\ \hline g & g & u \\ u & u & g \end{array} \qquad \text{und} \qquad \begin{array}{c|cc} \cdot & g & u \\ \hline g & g & g \\ u & g & u \end{array}$$

Dabei sind g und u einfach nur Namen für die beiden Elemente von K, die für „gerade“ und „ungerade“ stehen sollen und damit auch die Verknüpfungstafeln erklären: Wir haben z. B. $g+u$ als u definiert, weil die Addition einer geraden und einer ungeraden Zahl eine ungerade Zahl ergibt.

Man kann zeigen, dass K mit diesen beiden Verknüpfungen einen Körper bildet. Er wird in der Literatur mit $\mathbb{Z}_2$ bezeichnet, da seine Elemente die Reste ganzer Zahlen bei Division durch 2 beschreiben. Um zu beweisen, dass $\mathbb{Z}_2$ ein Körper ist, könnte man z. B. einfach die geforderten Eigenschaften für alle Elemente – es gibt ja nur zwei – explizit nachprüfen. In der Vorlesung „Algebraische Strukturen“ zeigt man allerdings, dass man die Körperaxiome hier auch viel eleganter direkt aus den Eigenschaften von $\mathbb{Z}$ folgern kann [G, Satz 7.10]. Wir wollen uns hier damit begnügen, die neutralen und inversen Elemente anzugeben:

- Das additive neutrale Element ist g, wie man leicht aus der Tabelle abliest. Im Sinne der Notationen von Definition 3.5 ist also $0 = g$. Wegen $g+g = u+u = g = 0$ sind die additiven inversen Elemente $-g = g$ und $-u = u$. Dies stimmt natürlich auch mit der Interpretation als gerade und ungerade Zahlen überein, da das Negative von einer geraden bzw. ungeraden Zahl ebenfalls wieder gerade bzw. ungerade ist.
- Das multiplikative neutrale Element in $\mathbb{Z}_2\backslash\{0\}$ ist u – in der Tat ist es ja auch das einzige Element in $\mathbb{Z}_2\backslash\{0\}$. Gemäß der Notation von Definition 3.5 ist also $1 = u$.

Beachte, dass in diesem Körper $\mathbb{Z}_2$ die Gleichung $1+1 = u+u = g = 0$ gilt. Die Körperaxiome lassen es also zu, dass man bei fortgesetzter Addition der 1 irgendwann wieder zur 0 zurück kommt. Wir werden in dieser Vorlesung nicht viel mit dem Körper $\mathbb{Z}_2$ zu tun haben – wir haben ihn hier nur als Beispiel dafür angegeben, dass die Körperaxiome noch weit davon entfernt sind, die rationalen oder reellen Zahlen eindeutig zu charakterisieren.

Anschaulich kann man die Körperaxiome so interpretieren, dass ein Körper eine Menge ist, auf der „die vier Grundrechenarten existieren und die erwarteten Eigenschaften haben“. Wir wollen nun noch ein paar weitere dieser erwarteten Eigenschaften zeigen, die bereits aus den Körperaxiomen folgen und die wir dann beim Rechnen z. B. in $\mathbb{R}$ natürlich ständig benutzen werden.

Bemerkung 3.7. Es seien K ein Körper und $x,y \in K$.

(a) Wenden wir Lemma 3.4 (c) und (d) auf die (kommutative) Addition und Multiplikation an, so sehen wir sofort, dass

$$-(x+y) = (-x)+(-y) \quad \text{und} \quad -(-x) = x$$

sowie für $x,y \neq 0$

$$(xy)^{-1} = x^{-1} \cdot y^{-1} \quad \text{und} \quad (x^{-1})^{-1} = x.$$

(b) Etwas versteckt in Definition 3.5 steht in Teil (b) u. a. die Aussage, dass die Multiplikation überhaupt eine Verknüpfung auf $K\backslash\{0\}$ ist, also dass für $x,y \in K\backslash\{0\}$ auch $xy \in K\backslash\{0\}$ gilt. Äquivalent dazu bedeutet das:

$$\text{Ist } xy = 0, \text{ so gilt } x = 0 \text{ oder } y = 0.$$

Lemma 3.8 (Eigenschaften von Körpern)**.** *In jedem Körper K gilt für alle $x,y \in K$:*

(a) $0 \cdot x = 0$.

(b) $x \cdot (-y) = -(xy)$.

(c) *Für $x \neq 0$ ist $-(x^{-1}) = (-x)^{-1}$.*

Beweis.

(a) Es gilt

$$\begin{aligned} 0 \cdot x &= (0+0) \cdot x && \text{(0 ist additives neutrales Element)} \\ &= 0 \cdot x + 0 \cdot x, && \text{(Distributivität)} \end{aligned}$$

woraus durch Addition des additiven Inversen von $0 \cdot x$ auf beiden Seiten die gewünschte Gleichung $0 = 0 \cdot x$ folgt.

(b) Es ist

$$\begin{aligned} x \cdot (-y) + xy &= x \cdot (-y+y) && \text{(Distributivität)} \\ &= x \cdot 0 && (-y \text{ ist additives Inverses zu } y) \\ &= 0 && \text{(nach (a))}, \end{aligned}$$

daher ist $x \cdot (-y)$ das additive Inverse zu xy, d. h. es gilt $x \cdot (-y) = -(xy)$.

(c) Doppeltes Anwenden von (b), einmal für den linken und einmal für den rechten Faktor, ergibt

$$(-(x^{-1})) \cdot (-x) = -(x^{-1} \cdot (-x)) = -(-(x^{-1} \cdot x)) = -(-1) \overset{3.7(a)}{=} 1.$$

Also ist $-(x^{-1})$ das multiplikative Inverse zu $-x$, d. h. es ist $-(x^{-1}) = (-x)^{-1}$. □

Notation 3.9. In einem Körper K verwendet man üblicherweise die folgenden Notationen, von denen euch die meisten sicher bekannt sein werden:

(a) Für $x, y \in K$ setzt man $x - y := x + (-y)$. Ist $y \neq 0$, so setzt man $\frac{x}{y} := x \cdot y^{-1}$.

(b) Für $x \in K$ und $n \in \mathbb{N}$ definiert man die n-te **Potenz** von x als

$$x^n := \underbrace{x \cdot \cdots \cdot x}_{n\text{-mal}},$$

wobei dieser Ausdruck für $n = 0$ als $x^0 := 1$ zu verstehen ist. Insbesondere legen wir also auch $0^0 := 1$ fest. Beachte, dass aus dieser Definition (und der Kommutativität der Multiplikation) unmittelbar die Potenzrechenregeln

$$x^m \cdot x^n = x^{m+n} \quad \text{und} \quad (xy)^n = x^n \cdot y^n$$

für alle $x, y \in K$ folgen. Ist $x \neq 0$, so definiert man zusätzlich Potenzen mit negativen ganzzahligen Exponenten durch $x^{-n} := (x^{-1})^n$.

Beachte, dass auch in einem beliebigen Körper K die Exponenten einer Potenz stets *ganze Zahlen* sind und keine Elemente aus K. Eine Potenz x^y für $x, y \in K$ lässt sich im Allgemeinen nicht definieren (auch wenn dies für $K = \mathbb{R}$ in vielen Fällen möglich ist, siehe Definition **??**).

(c) Manchmal möchte man mehrere Elemente $x_m, x_{m+1}, x_{m+2}, \dots, x_n$ in einem Körper (oder allgemeiner in einer additiv geschriebenen abelschen Gruppe) aufsummieren, die durch eine ganzzahlige Laufvariable indiziert werden, die von einem $m \in \mathbb{Z}$ bis zu einem $n \in \mathbb{Z}$ (mit $n \geq m$) läuft. Man schreibt dies dann als

$$\sum_{i=m}^{n} x_i := x_m + x_{m+1} + x_{m+2} + \cdots + x_n$$

(also mit einem großen griechischen Sigma, das an das Wort „Summe" erinnern soll). So steht z. B.

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 \qquad (*)$$

für die Summe aller Quadratzahlen bis n^2. Natürlich ist der Name der Laufvariablen dabei egal, und der Ausdruck $(*)$ hängt nicht von einem i ab (wie man auf der rechten Seite ja auch sieht). Außerdem kann man die Laufvariable verschieben, ohne den eigentlichen Ausdruck zu ändern: Setzt man z. B. $i = j + 1$, also $j = i - 1$, in der obigen Summe $(*)$, so läuft j dort von 0 bis $n - 1$, wenn i von 1 bis n läuft, und wir können dieselbe Summe auch schreiben als

$$\sum_{j=0}^{n-1} (j+1)^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2.$$

Natürlich kann man diesen Ausdruck nun auch wieder genauso gut mit dem Buchstaben i statt j als $\sum_{i=0}^{n-1}(i+1)^2$ schreiben, oder den Index um mehr als 1 in die eine oder andere Richtung verschieben. Also:

> Der Wert einer Summe ändert sich nicht, wenn man zur Laufvariablen im zu summierenden Ausdruck eine Konstante addiert, und dafür von der Ober- und Untergrenze der Summe diese Konstante abzieht.

Wir sagen in diesem Fall, dass die neue Darstellung der Summe durch eine **Indexverschiebung** (im Beispiel oben $i \mapsto i+1$) aus der alten hervorgeht. 04

Analog schreibt man

$$\prod_{i=m}^{n} x_i := x_m \cdot x_{m+1} \cdot x_{m+2} \cdot \;\cdots\; \cdot x_n$$

(mit einem großen griechischen Pi für das Produkt), wenn man die Körperelemente multiplizieren statt addieren möchte. Ist schließlich die Obergrenze einer Summe oder eines Produkts kleiner als die Untergrenze (man spricht dann von der **leeren Summe** bzw. dem **leeren Produkt**), so definiert man dies als

$$\sum_{i=m}^{n} x_i := 0 \quad \text{und} \quad \prod_{i=m}^{n} x_i := 1 \quad \text{für } n < m,$$

also als das additive bzw. multiplikative neutrale Element.

(d) Ist n eine natürliche Zahl, so fasst man diese oft auch als das Element

$$\sum_{i=1}^{n} 1 = \underbrace{1 + \cdots + 1}_{n\text{-mal}}$$

von K auf. Im Fall $K = \mathbb{R}$ ist dies dann einfach die natürliche Zahl $n \in \mathbb{N} \subset \mathbb{R}$ und liefert somit keine neue Notation, aber z. B. in $K = \mathbb{Z}_2$ aus Beispiel 3.6 (b) ist $2 = 1 + 1 = 0$.

Aufgabe 3.10. Zeige, dass in jedem Körper K die üblichen Rechenregeln

$$\frac{x}{y} + \frac{z}{w} = \frac{xw + yz}{yw} \quad \text{und} \quad \frac{x}{y} \cdot \frac{z}{w} = \frac{xz}{yw}$$

für Brüche gelten, wobei $x, y, z, w \in K$ mit $y, w \neq 0$.

Aufgabe 3.11. Es sei $a \in \mathbb{R}$ fest gegeben. Wir definieren auf $\mathbb{R}^2$ eine „Addition“ und „Multiplikation“ durch

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2) \quad \text{und} \quad (x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1 + a x_2 y_2, x_1 y_2 + x_2 y_1).$$

Man prüft leicht durch explizite Rechnung nach, dass $\mathbb{R}^2$ mit dieser Addition eine kommutative Gruppe mit neutralem Element $(0,0)$ ist, dass auch die Multiplikation kommutativ ist, und dass diese beiden Operationen das Distributivgesetz erfüllen – ihr solltet euch kurz überlegen, warum das so ist, braucht das aber nicht aufzuschreiben. Man zeige stattdessen:

(a) Die Multiplikation ist assoziativ und besitzt ein neutrales Element.

(b) Im Fall $a = -1$ ist $(\mathbb{R}^2, +, \cdot)$ ein Körper, im Fall $a = 1$ jedoch nicht.

(Für $a = -1$ ist $(\mathbb{R}^2, +, \cdot)$ der sogenannte Körper der komplexen Zahlen, den wir in Kapitel **??** noch genau untersuchen werden.)

Aufgabe 3.12. Zu einem Körper K und einer Menge D mit $|D| \geq 2$ sei

$$V = \{f : f \text{ ist eine Abbildung von } D \text{ nach } K\}$$

die Menge aller reellwertigen Funktionen auf D. Für $f, g \in V$ definieren wir die Addition $f + g$ und Multiplikation $f \cdot g$ dieser Funktionen punktweise durch

$$f + g \colon D \to K,\; x \mapsto f(x) + g(x) \quad \text{und} \quad f \cdot g \colon D \to K,\; x \mapsto f(x) \cdot g(x).$$

(a) Zeige, dass V mit dieser Addition eine abelsche Gruppe ist.

(b) Ist V mit dieser Addition und Multiplikation ein Körper?

3.B Vollständige Induktion

Häufig möchte man in der Mathematik Aussagen beweisen, die von einer natürlichen Zahl abhängen – z. B. bei Formeln, die Summen oder Produkte wie in Notation 3.9 mit variablen Unter- oder Obergrenzen beinhalten. Die einfachste und bekannteste solcher Aussagen ist vermutlich die folgende Formel für die Summe aller natürlichen Zahlen bis zu einer gegebenen Obergrenze.

Satz 3.13 (Summenformel von Gauß). *Für alle $n \in \mathbb{N}$ gilt*

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

Beispiel 3.14. Für $n = 5$ ist z. B.

$$\sum_{k=1}^{5} k = 1+2+3+4+5 = 15 = \frac{5 \cdot 6}{2}.$$

Um derartige Aussagen zu beweisen, ist oft das Beweisverfahren der **(vollständigen) Induktion** nützlich, das wir jetzt einführen wollen.

Angenommen, wir wollen (wie z. B. in Satz 3.13) eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ beweisen. Dann können wir dies tun, indem wir die folgenden beiden Dinge zeigen:

(a) (**Induktionsanfang**) Die Aussage $A(0)$ ist wahr.

(b) (**Induktionsschritt**) Für alle $n \in \mathbb{N}$ gilt $A(n) \Rightarrow A(n+1)$, d. h. *wenn* die Aussage $A(n)$ für ein gegebenes $n \in \mathbb{N}$ gilt (die „Induktionsannahme“ bzw. „Induktionsvoraussetzung“), *dann* gilt auch die Aussage $A(n+1)$ (der „Induktionsschluss“).

Haben wir diese beiden Dinge gezeigt, so folgt daraus nämlich die Gültigkeit von $A(n)$ für alle $n \in \mathbb{N}$: Die Aussage $A(0)$ haben wir mit dem Induktionsanfang gezeigt, und durch fortgesetztes Anwenden des Induktionsschritts $A(n) \Rightarrow A(n+1)$ für $n = 0, 1, 2, \dots$ erhalten wir dann auch

$$A(0) \Rightarrow A(1) \Rightarrow A(2) \Rightarrow A(3) \Rightarrow \cdots,$$

also die Gültigkeit von $A(n)$ für alle $n \in \mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Derartige Induktionsbeweise sind immer dann sinnvoll, wenn die Aussagen $A(n)$ und $A(n+1)$ „ähnlich genug“ sind, so dass es beim Beweis von $A(n+1)$ hilft, die Gültigkeit von $A(n)$ voraussetzen zu dürfen.

Mit diesem Verfahren können wir nun die Summenformel aus Satz 3.13 beweisen:

Beweis von Satz 3.13. Wir zeigen die Formel mit Induktion über n.

Induktionsanfang ($n = 0$): Für $n = 0$ stimmen die beiden Seiten der zu zeigenden Gleichung überein, denn es ist

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

Induktionsschritt ($n \to n+1$): Als Induktionsvoraussetzung nehmen wir an, dass die zu beweisende Formel für ein gegebenes $n \in \mathbb{N}$ richtig ist, d. h. dass

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

gilt. (Beachte, dass wir diese Gleichung nicht für alle $n \in \mathbb{N}$ voraussetzen – dies wäre ja schon die gesamte zu zeigende Aussage!) Wir müssen zeigen, dass die entsprechende Gleichung dann auch für $n+1$ gilt, also dass

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

Dies ergibt sich nun leicht aus der folgenden Rechnung:

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) && \text{(Abspalten des letzten Summanden für } k = n+1\text{)} \\
&= \frac{n(n+1)}{2} + (n+1) && \text{(nach Induktionsvoraussetzung)} \\
&= (n+1) \cdot \left(\frac{n}{2} + 1\right) \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

Damit ist der Satz mit vollständiger Induktion bewiesen. □

Bemerkung 3.15. Offensichtlich erlaubt das Beweisverfahren der vollständigen Induktion die folgenden Abwandlungen:

(a) Im Induktionsschritt kann man, wenn es hilfreich ist, beim Beweis der Aussage $A(n+1)$ nicht nur die direkt vorangegangene Aussage $A(n)$, sondern *alle bereits gezeigten Aussagen* $A(0), A(1), \dots, A(n)$ voraussetzen.

(b) Möchte man die Aussage $A(n)$ nicht für alle $n \in \mathbb{N}$, sondern für alle $n \in \mathbb{Z}$ ab einem gewissen Startwert $n_0 \in \mathbb{Z}$ zeigen, so kann man als Induktionsanfang die Aussage $A(n_0)$ zeigen, und im Induktionsschritt dann die Folgerung $A(n) \Rightarrow A(n+1)$ für alle $n \geq n_0$.

Aufgabe 3.16. Zeige für alle $n \in \mathbb{N}$:

$$\text{(a)} \quad \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}, \qquad \text{(b)} \quad \prod_{k=1}^{n} \left(1 + \frac{1}{n+k}\right) = 2 - \frac{1}{n+1}.$$

Aufgabe 3.17. Zeige mit vollständiger Induktion: Ist $a \in \mathbb{R} \backslash \{0\}$ mit $a + \frac{1}{a} \in \mathbb{Z}$, so gilt für alle $n \in \mathbb{N}$ auch $a^n + \frac{1}{a^n} \in \mathbb{Z}$.

3.C Polynomfunktionen

Als erste Anwendung der Körpereigenschaften wollen wir zum Abschluss dieses Kapitels die euch sicher schon aus der Schule bekannten Polynomfunktionen behandeln – also die Funktionen, die sich aus den grundlegenden Körperoperationen Addition und Multiplikation bilden lassen.

Definition 3.18 (Polynomfunktionen und Nullstellen)**.** Es seien D eine Teilmenge eines Körpers K und $f \colon D \to K$ eine Funktion.

(a) Ist f von der Form

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + \cdots + a_1 x + a_0 \quad \text{für alle } x \in D$$

mit gewissen $a_0, \dots, a_n \in K$, so sagt man, dass f eine **Polynomfunktion** mit **Koeffizienten** $a_0, \dots, a_n$ ist. Ist n dabei so gewählt, dass der erste Koeffizient a_n ungleich Null ist, so heißt f eine Polynomfunktion vom **Grad** n und mit **Leitkoeffizient** a_n. Ist der Leitkoeffizient 1, so heißt f eine **normierte** Polynomfunktion.

Sind in der obigen Darstellung alle Koeffizienten $a_0, \dots, a_n$ gleich 0 (und ist f damit die Nullfunktion), so nennen wir f formal eine Polynomfunktion vom Grad $-\infty$. In diesem Fall hat f keinen Leitkoeffizienten.

(b) Ist $x_0 \in D$ mit $f(x_0) = 0$, so nennt man x_0 eine **Nullstelle** von f.

Das Besondere an Nullstellen von Polynomfunktionen ist, dass man sie wie im folgenden Satz als Linearfaktoren abspalten kann.

Satz 3.19 (Abspalten von Nullstellen in Polynomfunktionen)**.** *Es seien K ein Körper, $D \subset K$ und $f \colon D \to K$ eine Polynomfunktion vom Grad $n \in \mathbb{N}$.*

(a) *Ist $x_0 \in D$ eine Nullstelle von f, so gibt es eine Polynomfunktion $g\colon D \to K$ vom Grad $n-1$ mit $f(x) = (x-x_0)\,g(x)$ für alle $x \in D$ (d. h. man kann „den Linearfaktor $x-x_0$ abspalten“).*

(b) *Die Funktion f hat höchstens n Nullstellen.*

Beweis. Wir zeigen die beiden Aussagen mit Induktion über n. Der Beweis von (a) ist dabei konstruktiv, d. h. er gibt auch ein Verfahren an, wie g berechnet werden kann (siehe Beispiel 3.20).

Der Induktionsanfang für $n = 0$ ist trivial, denn f ist dann eine Konstante ungleich 0 und hat somit keine Nullstellen. Für den Induktionsschluss nehmen wir an, dass die Aussagen des Satzes bis zu einem gegebenen n gelten, und betrachten $f\colon D \to K$, $x \mapsto a_{n+1}x^{n+1} + \cdots + a_1x + a_0$ vom Grad $n+1$, also mit $a_{n+1} \neq 0$.

(a) Wir definieren eine Polynomfunktion $\tilde{f}\colon D \to K$ durch

$$\begin{aligned}\tilde{f}(x) &:= f(x) - a_{n+1}x^n(x-x_0)\\ &= a_{n+1}x_0x^n + a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\end{aligned}$$

für alle x. Ist $\tilde{f}$ die Nullfunktion, so sind wir fertig, da dann ja $f(x) = a_{n+1}x^n(x-x_0)$ für alle $x \in D$ gilt. Andernfalls ist $\tilde{f}$ nach Konstruktion eine Polynomfunktion vom Grad höchstens n (der x^{n+1}-Term hebt sich ja gerade heraus), die immer noch die Nullstelle x_0 hat. Nach Induktionsvoraussetzung gibt es dann also eine Polynomfunktion $\tilde{g}\colon D \to K$ vom Grad höchstens $n-1$ mit $\tilde{f}(x) = (x-x_0)\,\tilde{g}(x)$ für alle $x \in D$, und somit ist

$$f(x) = a_{n+1}x^n(x-x_0) + \tilde{f}(x) = (x-x_0)\cdot(\underbrace{a_{n+1}x^n + \tilde{g}(x)}_{=:g(x)})$$

für alle $x \in D$, wobei g offensichtlich vom Grad n ist.

(b) Hat f keine Nullstelle, so sind wir fertig. Andernfalls wählen wir eine Nullstelle x_0 von f und schreiben $f(x) = (x-x_0)\,g(x)$ für alle $x \in D$ wie in (a) mit einer Polynomfunktion g vom Grad n. Nach Induktionsvoraussetzung hat g höchstens n Nullstellen, und nach Bemerkung 3.7 (b) sind die Nullstellen von f genau x_0 zusammen mit den Nullstellen von g. Also hat f höchstens $n+1$ Nullstellen. Damit ist die Behauptung mit Induktion bewiesen. □

Beispiel 3.20 (Polynomdivision)**.** Das Verfahren aus dem Beweis von Satz 3.19 (a) wird als *Polynomdivision* [G, Satz 10.19] bezeichnet: Man subtrahiert fortlaufend geeignete Vielfache von $x-x_0$ von f, so dass sich der jeweils höchste Term von f weghebt, und sammelt die dabei verwendeten Faktoren in g. Das folgende Schema, das genauso aussieht wie eine normale schriftliche Division, verdeutlicht dieses Verfahren am Beispiel der Funktion $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 3x - 4$ mit Nullstelle $x_0 = 1$, die wir als $f(x) = (x-1)\,g(x)$ für alle $x \in \mathbb{R}$ schreiben wollen. Das Ergebnis ist in diesem Fall $g\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x+4$.

$$\begin{array}{lcrl}
f(x) & \longrightarrow & (x^2+3x-4) & : (x-1) = x+4 \longleftarrow g(x)\\
 & & -\;(x^2-\;\;x) & \quad \cdot x\\ \cline{3-3}
\tilde{f}(x) & \longrightarrow & 4x-4 & \\
 & & -\;(4x-4) & \quad \cdot 4\\ \cline{3-3}
 & & 0 &
\end{array}$$

Bemerkung 3.21. Satz 3.19 liefert uns zwar die neue Funktion nach dem Abspalten des Linearfaktors, er sagt uns hingegen nicht, wie wir überhaupt erst einmal eine Nullstelle von f finden können, oder ob es überhaupt Nullstellen gibt (die reelle Polynomfunktion $f(x) = x^2 + 1$ hat ja z. B. keine Nullstellen). In der Tat gibt es im Allgemeinen kein Verfahren, wie man Nullstellen von Polynomfunktionen exakt berechnen kann! Genauer gesagt gilt:

- Für Polynomfunktionen vom Grad höchstens 4 gibt es explizite Verfahren zur exakten Bestimmung der Nullstellen (für Grad 1 ist das klar, für Grad 2 gibt es die bekannte „*p*-*q*-Formel“ bzw. die quadratische Ergänzung, und für Grad 3 bzw. 4 sind die Formeln so lang, dass man im Allgemeinen nicht mehr mit ihnen arbeiten möchte).

- Für Polynomfunktionen vom Grad größer als 4 kann man beweisen(!), dass es keine derartigen Verfahren zur exakten Bestimmung der Nullstellen geben kann (das beweist man z. B. in der Vorlesung „Einführung in die Algebra“, die ihr im nächsten Studienjahr hören könnt). Aber:
- Für reelle Polynomfunktionen beliebigen Grades gibt es zumindest numerische Verfahren, die die Nullstellen (mit beliebiger Genauigkeit) näherungsweise bestimmen können.

Zum Schluss wollen wir nun noch zwei wichtige Konzepte für Polynomfunktionen untersuchen, die ihr beide im reellen Fall vielleicht schon aus der Schule kennt: den sogenannten Koeffizientenvergleich (also dass eine Polynomfunktion eindeutig ihre Koeffizienten bestimmt) und die Vielfachheit von Nullstellen. Es stellt sich jedoch heraus, dass man hierfür im allgemeinen Fall die Voraussetzung benötigt, dass die Definitionsmenge der betrachteten Funktionen unendlich viele Elemente besitzt.

Lemma 3.22 (**Koeffizientenvergleich**). *Es seien K ein Körper, $D \subset K$ mit $|D| = \infty$, und $f: D \to K$ eine Polynomfunktion mit zwei Darstellungen*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 = b_n x^n + \cdots + b_1 x + b_0 \quad \text{für alle } x \in D$$

für gewisse $a_0, \dots, a_n, b_0, \dots, b_n \in K$. (Beachte, dass wir dabei in beiden Darstellungen den gleichen höchsten Exponenten n wählen können, da wir nicht $a_n \neq 0$ und $b_n \neq 0$ vorausgesetzt haben.)

Dann gilt bereits $a_i = b_i$ für alle $i = 0, \dots, n$. Es ist also nicht möglich, „eine Polynomfunktion auf zwei verschiedene Arten hinzuschreiben“.

Beweis. Nach Voraussetzung ist die Polynomfunktion

$$D \to K,\ x \mapsto (a_n - b_n)x^n + \cdots + (a_1 - b_1)x + (a_0 - b_0) = f(x) - f(x) = 0$$

die Nullfunktion auf D. Da sie damit wegen $|D| = \infty$ unendlich viele Nullstellen besitzt, muss sie nach Satz 3.19 (b) vom Grad $-\infty$ sein. Also sind alle Koeffizienten dieser Polynomfunktion gleich 0, d. h. es ist $a_i = b_i$ für alle $i = 0, \dots, n$. □

Bemerkung und Notation 3.23 (Polynome). Die Voraussetzung $|D| = \infty$ in Lemma 3.22 ist wirklich notwendig: So sind für $D = K = \mathbb{Z}_2$ wie in Beispiel 3.6 (b) z. B. $x \mapsto x$ und $x \mapsto x^2$ dieselbe Funktion, da sie beide 0 auf 0 und 1 auf 1 abbilden und in $\mathbb{Z}_2$ keine weiteren Elemente existieren.

In der Literatur bezeichnet man einen formalen Ausdruck der Form $a_n x^n + \cdots + a_1 x + a_0$ mit $a_0, \dots, a_n \in K$ als ein **Polynom** über K [G, Kapitel 9]. Jedes solche Polynom bestimmt natürlich eine Polynomfunktion von jeder Teilmenge D von K nach K, allerdings können verschiedene Polynome wie im eben angegebenen Beispiel durchaus dieselbe Polynomfunktion definieren: Über $\mathbb{Z}_2$ sind x und x^2 verschiedene Polynome, sie bestimmen aber dieselbe Polynomfunktion.

Mit dieser Notation ist die Aussage von Lemma 3.22 also, dass Polynome und Polynomfunktionen im Fall von unendlichen Definitionsmengen dasselbe sind. Da wir Polynomfunktionen im Folgenden in der Regel nur in diesem Fall unendlicher Definitionsmengen benötigen, werden wir die Begriffe Polynom und Polynomfunktion oft synonym verwenden. Wegen der Eindeutigkeit der Koeffizienten sind dann auch der Grad (und der Leitkoeffizient) einer Polynomfunktion f wie in Definition 3.18 (a) eindeutig bestimmt. Wir können daher eine Bezeichnung dafür einführen:

Definition 3.24 (Grad eines Polynoms). Wir bezeichnen den **Grad** einer Polynomfunktion f (mit unendlicher Definitionsmenge) mit $\deg f \in \mathbb{N} \cup \{-\infty\}$ (vom englischen Wort „degree“).

In den Fällen $\deg f = 1$ bzw. $\deg f = 2$ nennt man f ein **lineares** bzw. **quadratisches Polynom**.

Satz und Definition 3.25 (Vielfachheit von Nullstellen). *Es seien K ein Körper, $D \subset K$ mit $|D| = \infty$ und $f: D \to K$ eine Polynomfunktion, die nicht die Nullfunktion ist. Dann lässt sich f (bis auf die Reihenfolge der Faktoren) eindeutig als*

$$f(x) = g(x) \cdot (x - x_1)^{a_1} \cdot \cdots \cdot (x - x_k)^{a_k} \quad \text{für alle } x \in D$$

schreiben, wobei $x_1, \dots, x_k \in D$ die verschiedenen Nullstellen von f sind, $a_1, \dots, a_k \in \mathbb{N}_{>0}$ gilt, und g ein Polynom ohne Nullstellen in D ist. In dieser Darstellung nennt man a_i für $i = 1, \dots, k$ die

Vielfachheit *der Nullstelle x_i von f (in der Literatur sind auch die Bezeichnungen* ***Ordnung*** *und* ***Multiplizität*** *der Nullstelle üblich).*

Beweis. Die Existenz einer solchen Darstellung ergibt sich sofort durch fortgesetztes Abspalten von Nullstellen gemäß Satz 3.19 (a). Wir zeigen nun die Eindeutigkeit mit Induktion über den Grad $n := \deg f$ des Polynoms. Dabei ist der Induktionsanfang für $n = 0$ trivial, denn dann hat f keine Nullstellen, und es ist zwangsläufig $k = 0$ und $g = f$.

Für den Induktionsschritt $n \to n+1$ bemerken wir zuerst, dass $x_1, \dots, x_k$ natürlich in jedem Fall als die Nullstellen von f eindeutig bestimmt sind. Wir nehmen also an, dass wir zwei Darstellungen

$$f(x) = g(x) \cdot (x-x_1)^{a_1} \cdot \dots \cdot (x-x_k)^{a_k} = h(x) \cdot (x-x_1)^{b_1} \cdot \dots \cdot (x-x_k)^{b_k}$$

eines Polynoms vom Grad $n+1$ wie in der Behauptung des Satzes haben. Im nullstellenfreien Fall $k = 0$ sind wir natürlich bereits fertig. Andernfalls liefert Division durch $x - x_1$ für alle $x \in D \backslash \{x_1\}$ (wir müssen x_1 hier herausnehmen, da wir sonst durch 0 teilen würden!)

$$\begin{aligned} & g(x) \cdot (x-x_1)^{a_1-1} \cdot (x-x_2)^{a_2} \cdot \dots \cdot (x-x_k)^{a_k} \\ = \; & h(x) \cdot (x-x_1)^{b_1-1} \cdot (x-x_2)^{b_2} \cdot \dots \cdot (x-x_k)^{b_k}. \end{aligned} \qquad (*)$$

Wir haben also wieder zwei Darstellungen eines Polynoms auf der immer noch unendlichen Menge $D \backslash \{x_1\}$. Da der Grad dieses Polynoms n ist, müssen diese Darstellungen aber nach der Induktionsvoraussetzung bereits übereinstimmen. Also gilt $g = h$, $a_1 - 1 = b_1 - 1$, $a_2 = b_2$, ..., $a_k = b_k$, und damit stimmen auch die beiden ursprünglichen Darstellungen von f überein. □

Aufgabe 3.26. Bestimme die Nullstellen des reellen Polynoms $x^4 + 3x^3 - 4x$ und ihre Vielfachheiten.

Aufgabe 3.27. Es sei f ein reelles Polynom mit $f(x) = x^3$ für alle $x \in \{1, 2, 3, \dots, 8\}$. Welchen Grad kann f haben?

Aufgabe 3.28. Es sei f das reelle Polynom mit $f(x) = (x^2 - x + 1)^{2023}$ für alle $x \in \mathbb{R}$.

(a) Bestimme die Summe aller Koeffizienten von f.

(b) Bestimme die Summe aller Koeffizienten von geraden Potenzen von x in f.

Aufgabe 3.29.

(a) Bestimme alle reellen Polynome f mit $x\,f(x+1) = (x-1)\,f(x)$ für alle $x \in \mathbb{R}$.

05 (b) Bestimme alle reellen Polynome f mit $x\,f(x-1) = (x-1)\,f(x)$ für alle $x \in \mathbb{R}$.

Grundlagen der Mathematik 1: Lineare Algebra

13. Vektorräume

Ausgehend von den elementaren Konzepten in den Kapiteln 1 bis 3 wollen wir in dieser Vorlesung zwei grundlegende Gebiete der Mathematik entwickeln: die Analysis und die lineare Algebra. Während sich dabei die eindimensionale Analysis in den Kapiteln **??** bis **??** hauptsächlich mit allgemeinen (in der Regel stetigen oder sogar differenzierbaren) Funktionen in einer reellen Variablen beschäftigt hat, wollen wir nun im folgenden Teil des Skripts zunächst unabhängig davon *lineare* Funktionen in *mehreren* Variablen studieren, wie sie in der Praxis z. B. in Form von linearen Gleichungssystemen auftreten. Später werden wir die erarbeiteten Resultate dann mit der Analysis kombinieren, um Funktionen in mehreren Variablen mit Hilfe von Ableitungen linear approximieren zu können.

In der Analysis arbeitet man ja hauptsächlich über den reellen Zahlen, und das ist in der linearen Algebra auch nicht viel anders. Allerdings haben wir in Kapitel 3 ja auch schon gesehen, dass viele Dinge auch über einem beliebigen Körper funktionieren. Die lineare Algebra verhält sich hier sehr „gutartig“: Da wir letztlich nur lineare Funktionen bzw. Gleichungen betrachten werden, benötigen wir gar nicht mehr Struktur der reellen Zahlen als die Körperaxiome. Wir können daher nahezu die gesamte lineare Algebra über einem beliebigen Grundkörper studieren, also z. B. auch über $\mathbb{Q}$, dem Körper $\mathbb{Z}_2$ aus Beispiel 3.6 (b), oder anderen Körpern, die ihr vielleicht inzwischen kennt oder noch kennenlernen werdet. Wir vereinbaren daher:

Im Folgenden (bis zum Ende von Kapitel **??**) sei K immer ein fest gewählter Grundkörper.

Beim ersten Lesen könnt ihr euch K aber auch gerne einfach als $\mathbb{R}$ vorstellen.

13.A Der Vektorraumbegriff

Wie ihr ja sicher aus der Schule wisst, werden die Elemente von $\mathbb{R}^2$ oder $\mathbb{R}^3$ in der Regel *Vektoren* genannt. Aber was genau ist im Allgemeinen eigentlich ein Vektor? Genau wie bei Gruppen und Körpern in Abschnitt 3.A werden Vektoren über die Operationen definiert, die man mit ihnen durchführen kann: In einer Gruppe gibt es *eine* Verknüpfung, die gewisse Eigenschaften erfüllt (siehe Definition 3.1), in einem Körper *zwei* Verknüpfungen „$+$“ und „$\cdot$“ mit den erwarteten Eigenschaften (siehe Definition 3.5). Was sind nun die analogen definierenden Verknüpfungen und Eigenschaften für Vektoren? Wir wissen alle aus der Schule, dass man Vektoren addieren und „strecken“, also mit einer reellen Zahl (bzw. mit einer Zahl des gewählten Grundkörpers K) multiplizieren kann. Genau diese beiden Strukturen definieren einen allgemeinen Vektorraum:

Definition 13.1 (Vektorräume)**.** Ein **Vektorraum** über K (oder K-Vektorraum) ist eine Menge V zusammen mit zwei Verknüpfungen

$$\begin{aligned} & +\colon V\times V\to V \quad (\textit{Vektoraddition}) \\ \text{und} \quad & \cdot\,\colon K\times V\to V \quad (\textit{Skalarmultiplikation}) \end{aligned}$$

so dass gilt:

(a) $(V,+)$ ist eine abelsche Gruppe (siehe Definition 3.1).

(b) (1. Distributivität) Für alle $\lambda,\mu\in K$ und $x\in V$ gilt $(\lambda+\mu)\cdot x=\lambda\cdot x+\mu\cdot x$.

(c) (2. Distributivität) Für alle $\lambda\in K$ und $x,y\in V$ gilt $\lambda\cdot(x+y)=\lambda\cdot x+\lambda\cdot y$.

(d) (Assoziativität) Für alle $\lambda,\mu\in K$ und $x\in V$ gilt $(\lambda\cdot\mu)\cdot x=\lambda\cdot(\mu\cdot x)$.

(e) Für alle $x \in V$ gilt $1 \cdot x = x$.

Die Elemente von V heißen **Vektoren**, die Elemente von K **Skalare**.

Bemerkung 13.2.

(a) Beachte, dass man einen Vektorraum nur dann definieren kann, wenn man vorher einen Körper K gewählt hat. Wenn klar ist, welcher Körper gemeint ist, werden wir jedoch auch oft nur von einem Vektorraum (statt einem K-Vektorraum) sprechen.

(b) In Definition 13.1 haben wir mehrfach die gleichen Symbole für unterschiedliche Dinge verwendet: Es gibt z. B. zwei Additionen, die wir beide mit „$+$" bezeichnet haben, nämlich die Addition $+\colon K \times K \to K$ zweier Körperelemente und die Addition $+\colon V \times V \to V$ der Vektoren. Da man aus der Art der verknüpften Elemente eindeutig ablesen kann, um welche Verknüpfung es sich handeln muss, können dadurch aber keine Mehrdeutigkeiten entstehen: So werden z. B. beim ersten Pluszeichen in Definition 13.1 (b) zwei Skalare, beim zweiten jedoch zwei Vektoren addiert. Nur wenn wir auch in der Notation explizit deutlich machen wollen, um welche der beiden Verknüpfungen es sich handelt, schreiben wir diese als „$+_K$" bzw. „$+_V$". Analog gibt es auch die Multiplikation zweimal, einmal als Multiplikation „$\cdot_K$" in K und einmal als Skalarmultiplikation „$\cdot_V$", und auch zweimal die Null, nämlich einmal als Null 0_K im Körper K und einmal als *Nullvektor* 0_V, d. h. als das neutrale Element von $(V,+)$. In dieser ausführlichen Notation könnte man z. B. die Bedingung aus Definition 13.1 (b) als

$$(\lambda +_K \mu) \cdot_V x = \lambda \cdot_V x +_V \mu \cdot_V x$$

schreiben. In der Regel werden wir diese Indizes K und V jedoch weglassen, genauso wie die Malzeichen sowohl für „$\cdot_K$" als auch für „$\cdot_V$".

(c) Vielleicht seid ihr es aus der Schule oder anderen Studienfächern gewohnt, einen Vektor x durch eine besondere Schreibweise wie z. B. $\vec{x}$ zu kennzeichnen. Dies ist in der Mathematik eher unüblich, da wir gleich in Beispiel 13.3 noch sehen werden, dass sehr viele Objekte der Mathematik als Vektoren aufgefasst werden können und dementsprechend mit dieser Notation versehen werden müssten. Da wir außerdem ohnehin immer von jeder Variablen angeben, um was für ein Objekt es sich handelt bzw. aus welcher Menge sie kommt, brauchen wir auch keine weitere besondere Kennzeichnung für Vektoren.

Beispiel 13.3.

(a) Für jeden Körper K ist $V = \{0\}$ (mit den trivialen Verknüpfungen) ein K-Vektorraum, der sogenannte **Nullvektorraum**.

(b) Das mit Abstand wichtigste Beispiel ist für eine gegebene Zahl $n \in \mathbb{N}$ die Menge

$$K^n := \underbrace{K \times \cdots \times K}_{n\text{-mal}} = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_1, \dots, x_n \in K \right\}$$

aller „geordneten n-Tupel in K" – d. h. ein Element von K^n wird dadurch angegeben, dass man n Elemente $x_1, \dots, x_n$ von K angibt (die nicht notwendig verschieden sein müssen und auf deren Reihenfolge es ankommt). Dass wir die Elemente $x_1, \dots, x_n$ dabei untereinander und nicht nebeneinander schreiben, ist momentan eine reine Konvention, die sich später bei der Einführung von Matrizen in Abschnitt **??** als nützlich erweisen wird. Definiert man nun auf K^n die komponentenweisen Verknüpfungen

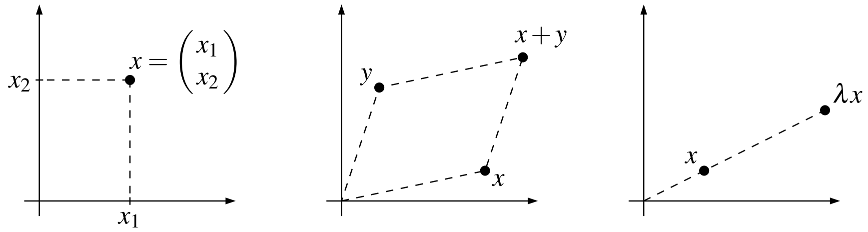
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad \text{und} \quad \lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

für alle $\lambda \in K$, so ist K^n mit diesen Verknüpfungen ein K-Vektorraum. In der Tat folgen die Vektorraumeigenschaften alle aus den Körpereigenschaften von K; wir zeigen hier exemplarisch Teil (b) der Definition 13.1: Für alle $\lambda, \mu, x_1, \dots, x_n \in K$ gilt

$$(\lambda+\mu)\cdot\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = \begin{pmatrix}(\lambda+\mu)x_1\\ \vdots\\ (\lambda+\mu)x_n\end{pmatrix} = \begin{pmatrix}\lambda x_1+\mu x_1\\ \vdots\\ \lambda x_n+\mu x_n\end{pmatrix} = \lambda\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}+\mu\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},$$

wobei das mittlere Gleichheitszeichen genau die Distributivität in K ist und die beiden anderen aus der Definition der Vektoraddition und Skalarmultiplikation in K^n folgen.

Im Fall $K = \mathbb{R}$ und $n = 2$ ist $K^n = \mathbb{R}^2$ einfach die bekannte reelle Ebene, und Addition und Skalarmultiplikation können wie im folgenden Bild veranschaulicht werden. Die geometrische Interpretation im Fall von $\mathbb{R}^n$ für andere n ist natürlich analog.



Wenn wir im Folgenden vom Vektorraum K^n sprechen, werden wir diesen Raum immer als Vektorraum über dem Körper K mit diesen komponentenweisen Verknüpfungen betrachten (sofern wir nichts anderes angeben).

Im Fall $n = 1$ erhält man $K^1 = K$, also K selbst als K-Vektorraum; der Fall $n = 0$ wird konventionsgemäß als der Nullvektorraum $K^0 = \{0\}$ aufgefasst.

(c) Die axiomatische Herangehensweise an die Vektorraumtheorie hat den großen Vorteil, dass sie auch auf viele andere Fälle als K^n anwendbar ist. Als weiteres wichtiges Beispiel ist z. B. für eine beliebige Menge D

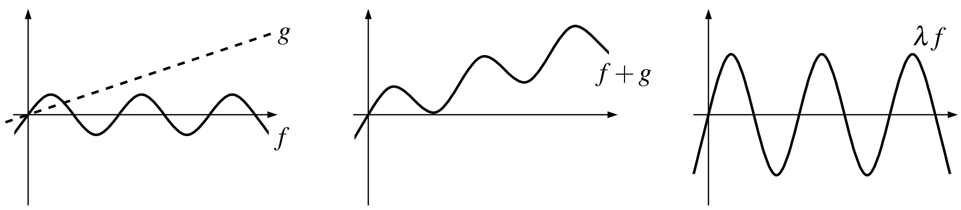
$$\mathrm{Abb}(D,K) := \{f : f \text{ ist eine Abbildung von } D \text{ nach } K\}$$

ein K-Vektorraum, indem wir die Addition und Multiplikation solcher Abbildungen punktweise definieren als

$$(f+g)(x) := f(x)+g(x) \quad \text{und} \quad (\lambda f)(x) := \lambda f(x)$$

für alle $\lambda \in K$, $x \in D$ und $f, g \colon D \to K$ (also $f, g \in \mathrm{Abb}(D,K)$). In der Tat haben wir in Aufgabe 3.12 (a) bereits gesehen, dass $\mathrm{Abb}(D,K)$ eine abelsche Gruppe ist (der Nullvektor ist hierbei die Funktion, die jedes Element von D auf 0 abbildet, und das zu einer Funktion $f \colon D \to K$ additive Inverse die Funktion $-f \colon D \to K$, $x \mapsto -f(x)$). Die anderen Vektorraumeigenschaften zeigt man wieder analog.

Beachte, dass die anschauliche Bedeutung in diesem Beispiel trotz der gleichen algebraischen Eigenschaften aus Definition 13.1 eine ganz andere ist als in (b): Zeichnen wir z. B. wie im Bild unten Abbildungen $f, g \in \mathrm{Abb}(\mathbb{R},\mathbb{R})$ als ihre Graphen in $\mathbb{R}^2$, so entsprechen Vektoraddition und Skalarmultiplikation der Addition bzw. Streckung der Funktionswerte in vertikaler Richtung.



Ein wichtiger Spezialfall dieser Konstruktion ist der Vektorraum $\operatorname{Abb}(\mathbb{N},K)$, dessen Elemente $f \in \operatorname{Abb}(\mathbb{N},K)$ wir als „unendliche Folgen“ $(f(0), f(1), f(2), \dots)$ mit Elementen in K schreiben können. Im Fall $K = \mathbb{R}$ sind dies natürlich gerade die in der Analysis betrachteten reellen Zahlenfolgen aus Abschnitt **??**.

Darüber hinaus lässt sich auf die gleiche Art auch die Menge $\operatorname{Abb}(D,W)$ aller Abbildungen von einer beliebigen Menge D in einen K-Vektorraum W zu einem Vektorraum machen.

(d) Sind V und W zwei K-Vektorräume, so ist (in Verallgemeinerung von (b)) auch ihr Produkt $V \times W$ mit komponentenweiser Addition und Skalarmultiplikation ein K-Vektorraum.

(e) $\mathbb{R}$ ist ein $\mathbb{Q}$-Vektorraum. In der Tat kann man reelle Zahlen addieren und mit einer rationalen multiplizieren, und es ist klar, dass mit diesen Definitionen alle Vektorraumeigenschaften erfüllt sind.

Wir sehen also schon, dass es ganz verschiedene Vektorräume gibt; in den nächsten Kapiteln werden wir auch noch viele weitere kennenlernen. Bei der Einführung neuer Konzepte der linearen Algebra ist es für die Anschauung aber vermutlich empfehlenswert, sich immer zuerst den Fall des Vektorraums $\mathbb{R}^n$ mit $n \in \mathbb{N}$ vorzustellen.

Als Erstes wollen wir jetzt ein paar elementare Eigenschaften von Vektorräumen zeigen. Sie haben einen ähnlichen Charakter wie die Axiome in Definition 13.1, folgen aber bereits aus diesen (so dass man sie nicht separat als Axiome fordern muss).

Lemma 13.4 (Eigenschaften von Vektorräumen)**.** *In jedem K-Vektorraum V gilt für alle $\lambda \in K$ und $x \in V$:*

(a) $0_K \cdot x = \lambda \cdot 0_V = 0_V$.

(b) *Ist $\lambda \cdot x = 0_V$, so ist $\lambda = 0_K$ oder $x = 0_V$.*

(c) $(-1) \cdot x = -x$.

Beweis.

(a) Der Beweis ist ganz analog zu dem von Lemma 3.8 (a): Wegen der 1. Distributivität aus Definition 13.1 (b) gilt $0_K \cdot x = (0_K + 0_K) \cdot x = 0_K \cdot x + 0_K \cdot x$, nach Subtraktion von $0_K \cdot x$ also wie behauptet $0_V = 0_K \cdot x$.

Genauso erhalten wir mit der 2. Distributivität $\lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V$, nach Subtraktion von $\lambda \cdot 0_V$ also $0_V = \lambda \cdot 0_V$.

(b) Ist $\lambda x = 0_V$ und $\lambda \neq 0_K$, so folgt

$$\begin{aligned} x &= 1 \cdot x && \text{(Definition 13.1 (e))} \\ &= (\lambda^{-1} \cdot \lambda) x \\ &= \lambda^{-1}(\lambda x) && \text{(Definition 13.1 (d))} \\ &= 0_V && \text{(Teil (a)).} \end{aligned}$$

(c) Es gilt

$$\begin{aligned} (-1) \cdot x + x &= (-1) \cdot x + 1 \cdot x && \text{(Definition 13.1 (e))} \\ &= (-1+1) \cdot x && \text{(Definition 13.1 (b))} \\ &= 0_K \cdot x \\ &= 0_V && \text{(Teil (a)),} \end{aligned}$$

also ist $(-1) \cdot x$ das additive Inverse zu x. □

Oft möchte man mit der Vektoraddition und Skalarmultiplikation nicht nur zwei, sondern mehrere Vektoren miteinander kombinieren. Um damit in Zukunft besser arbeiten zu können, führen wir hier schon einmal die folgenden Notationen ein.

Definition 13.5 (Familien und Linearkombinationen)**.** Es sei V ein Vektorraum.

(a) Eine (endliche) **Familie** von Vektoren in V ist gegeben durch n Vektoren $x_1,\dots,x_n \in V$ für ein $n \in \mathbb{N}$. Wir schreiben eine solche Familie als $B = (x_1,\dots,x_n)$ und nennen die Vektoren $x_1,\dots,x_n$ ihre **Elemente**.

(b) Sind $B = (x_1,\dots,x_n)$ eine Familie von Vektoren in V und $\lambda_1,\dots,\lambda_n \in K$, so heißt

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \quad \in V$$

eine **Linearkombination** der Vektoren aus B. Wir bezeichnen die Menge aller dieser Linearkombinationen mit

$$\operatorname{Lin} B := \{\lambda_1 x_1 + \cdots + \lambda_n x_n : \lambda_1,\dots,\lambda_n \in K\} \quad \subset V.$$

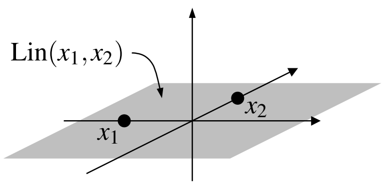
Im Fall $n = 0$ der leeren Familie fassen wir dies (im Sinne einer leeren Summe wie in Notation 3.9 (c)) als $\operatorname{Lin}() := \{0\}$ auf.

Bemerkung 13.6.

(a) Beachte, dass $x_1,\dots,x_n$ in Definition 13.5 im Gegensatz zu Beispiel 13.3 (b) Vektoren in V, und nicht die Komponenten *eines* Vektors in K^n sind. In der Tat ist diese Indexnotation in der Praxis für beide Bedeutungen üblich. Aus dem Zusammenhang ist aber immer offensichtlich, was gemeint ist, da $x_1,\dots,x_n$ in Beispiel 13.3 (b) ja Elemente des Grundkörpers K sind, hier jedoch Elemente des betrachteten Vektorraums V.

(b) Eine Familie $B = (x_1,\dots,x_n)$ ist etwas Ähnliches wie eine Menge $\{x_1,\dots,x_n\}$, allerdings haben ihre Elemente $x_1,\dots,x_n$ eine vorgegebene Reihenfolge und können in der Familie auch mehrfach auftreten. Für die Definition von $\operatorname{Lin} B$ ist dieser Unterschied noch irrelevant (wir hätten $\operatorname{Lin} B$ genauso gut auch für eine *Menge* B definieren können), später in Bemerkung 14.10 (b) bzw. Abschnitt **??** wird er jedoch noch wichtig werden.

(c) Mit der geometrischen Interpretation der Vektoraddition und Skalarmultiplikation aus Beispiel 13.3 (b) kann man sich die Mengen $\operatorname{Lin} B$ auch anschaulich gut vorstellen: So ist z. B. $\operatorname{Lin}(x_1,x_2) \subset \mathbb{R}^3$ im Bild rechts die Ebene durch den Nullpunkt und die beiden Vektoren x_1 und x_2.



Aufgabe 13.7. Es sei V ein K-Vektorraum.

Wenn wir das Vektorraumaxiom (e) „$1 \cdot x = x$ für alle $x \in V$“ in Definition 13.1 weglassen würden, könnten wir versuchen, für ein gegebenes $a \in K$ eine geänderte Skalarmultiplikation

$$\lambda \odot x := \lambda a x \quad \text{für alle } \lambda \in K \text{ und } x \in V$$

zu definieren. Für welche a wäre K^n mit der gewöhnlichen Vektoraddition „$+$“ und dieser geänderten Skalarmultiplikation „$\odot$“ dann ein Vektorraum?

13.B Untervektorräume

Sehr viele weitere Beispiele von Vektorräumen können wir erhalten, indem wir in bereits bekannten Vektorräumen nach Teilmengen suchen, die mit der gegebenen Vektoraddition und Skalarmultiplikation selbst wieder die Axiome aus Definition 13.1 erfüllen. Solche Teilmengen werden als Untervektorräume bezeichnet.

Definition 13.8 (Untervektorräume)**.** Es sei V ein Vektorraum über einem Körper K. Eine Teilmenge $U \subset V$ heißt **Untervektorraum** oder **Unterraum** von V, in Zeichen $U \leq V$, wenn gilt:

(a) $0 \in U$.

(b) (Abgeschlossenheit bzgl. Vektoraddition) Für alle $x,y \in U$ ist $x+y \in U$.

(c) (Abgeschlossenheit bzgl. Skalarmultiplikation) Für alle $x \in U$ und $\lambda \in K$ ist $\lambda x \in U$.

Bemerkung 13.9. Äquivalent zu Definition 13.8 kann man dort die Bedingung (a) auch durch die scheinbar schwächere Bedingung $U \neq \emptyset$ ersetzen: Ist nämlich U nicht leer, so gibt es ein Element $x \in U$, und nach (c) folgt dann mit Lemma 13.4 (a) auch $0 = 0 \cdot x \in U$.

Die Abgeschlossenheit eines Unterraums bezüglich Vektoraddition und Skalarmultiplikation bedeutet gerade, dass sich diese beiden Verknüpfungen zu Verknüpfungen

$$+ : U \times U \to U \quad \text{und} \quad \cdot : K \times U \to U$$

auf U einschränken lassen. Wie schon angekündigt wollen wir nun sehen, dass dies die Menge U selbst wieder zu einem Vektorraum macht.

Lemma 13.10. *Jeder Unterraum eines K-Vektorraums ist (mit den eingeschränkten Verknüpfungen) selbst wieder ein K-Vektorraum.*

Beweis. Wir müssen die Eigenschaften aus Definition 13.1 für U nachweisen. Dazu beginnen wir mit (a) und zeigen zunächst, dass $(U,+)$ eine Gruppe ist.

- (Assoziativität der Vektoraddition) Weil V ein Vektorraum ist, gilt $(x+y)+z = x+(y+z)$ für alle $x,y,z \in V$ und damit erst recht für alle $x,y,z \in U$. Die Assoziativität der Addition überträgt sich also direkt von V auf U.
- (Additives neutrales Element) Nach Definition 13.8 (a) liegt der Nullvektor in U. Dieser erfüllt $x+0 = 0+x = x$ für alle $x \in V$ und damit auch für alle $x \in U$, und ist damit ein neutrales Element für die Addition in U.
- (Additive inverse Elemente) Für jedes $x \in U$ gilt nach Definition 13.8 (c) auch $(-1) \cdot x \in U$, und dies ist nach Lemma 13.4 (c) genau das additive inverse Element zu x.

Also ist $(U,+)$ eine Gruppe. Die Kommutativität der Vektoraddition und die übrigen Vektorraumeigenschaften (b) bis (e) in Definition 13.1 sind nun alle von der Form, dass für alle Vektoren aus U eine bestimmte Gleichung gelten muss – und dies folgt jetzt genauso wie die Assoziativität oben sofort daraus, dass die betreffenden Gleichungen sogar für alle Vektoren aus V gelten. □

Das wichtigste Beispiel für Unterräume eines Vektorraums V sind wie im folgenden Lemma die Teilmengen der Form $\operatorname{Lin} B$ für eine Familie B in V wie in Definition 13.5. In der Tat ist $\operatorname{Lin} B$ sogar der kleinste Unterraum, der B enthält:

Lemma 13.11 (Erzeugte Unterräume)**.** *Für jede Familie $B = (x_1, \dots, x_n)$ in einem Vektorraum V gilt:*

(a) *$\operatorname{Lin} B$ ist ein Unterraum von V, der die Vektoren $x_1, \dots, x_n$ enthält.*

(b) *Ist U ein beliebiger Unterraum von V, der die Vektoren $x_1, \dots, x_n$ enthält, so ist $\operatorname{Lin} B \subset U$.*

*Anschaulich ist $\operatorname{Lin} B$ also „der kleinste Unterraum von V, der B enthält". Man nennt ihn daher auch den von B **erzeugten** oder **aufgespannten Unterraum**.*

Beweis.

(a) Natürlich sind sowohl der Nullvektor als auch jedes x_i für $i \in \{1, \dots, n\}$ eine Linearkombination der Vektoren in $B = (x_1, \dots, x_n)$, denn es ist

$$0 = 0 \cdot x_1 + \cdots + 0 \cdot x_n \quad \text{und} \quad x_i = 0 \cdot x_1 + \cdots + 1 \cdot x_i + \cdots + 0 \cdot x_n.$$

Wir müssen also nur noch die Abgeschlossenheit von $\operatorname{Lin} B$ überprüfen. Dies ist aber sehr einfach: Sind

$$x = \mu_1 x_1 + \cdots + \mu_n x_n \quad \text{und} \quad y = \nu_1 x_1 + \cdots + \nu_n x_n$$

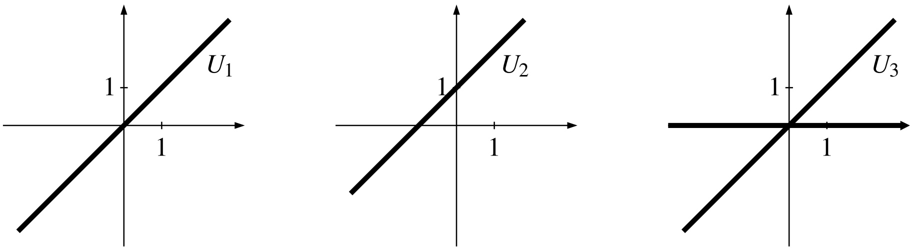
(mit $\mu_1, \dots, \mu_n, \nu_1, \dots, \nu_n \in K$) zwei beliebige Vektoren in $\operatorname{Lin} B$, so gilt für alle $\lambda \in K$ auch

$$x+y = (\mu_1+\nu_1)x_1 + \cdots + (\mu_n+\nu_n)x_n \in \operatorname{Lin} B \quad \text{und} \quad \lambda x = (\lambda\mu_1)x_1 + \cdots + (\lambda\mu_n)x_n \in \operatorname{Lin} B.$$

(b) Ist U ein solcher Unterraum, so enthält er wegen der Abgeschlossenheit mit $x_1, \dots, x_n$ auch alle Linearkombinationen dieser Vektoren, also die Menge $\operatorname{Lin} B$. □

Beispiel 13.12.

(a) Für jeden Vektor $x \in \mathbb{R}^2 \backslash \{0\}$ ist die von x aufgespannte Ursprungsgerade
$$\mathrm{Lin}(x) = \{\lambda x : \lambda \in \mathbb{R}\} \quad \subset \mathbb{R}^2$$
nach Lemma 13.11 ein Unterraum von $\mathbb{R}^2$ (und damit nach Lemma 13.10 auch ein Vektorraum). Damit gilt im folgenden Bild also $U_1 \leq \mathbb{R}^2$.



$$U_1 = \mathrm{Lin}\begin{pmatrix}1\\1\end{pmatrix} \qquad U_2 = \begin{pmatrix}0\\1\end{pmatrix} + \mathrm{Lin}\begin{pmatrix}1\\1\end{pmatrix} \qquad U_3 = \mathrm{Lin}\begin{pmatrix}1\\1\end{pmatrix} \cup \mathrm{Lin}\begin{pmatrix}1\\0\end{pmatrix}$$

Dagegen ist die verschobene Ursprungsgerade U_2 nach Definition 13.8 (a) kein Unterraum von $\mathbb{R}^2$, da sie den Ursprung nicht enthält. Auch die Vereinigung U_3 von zwei Ursprungsgeraden ist kein Unterraum, denn sie ist bzgl. der Vektoraddition nicht abgeschlossen: Es gilt
$$\begin{pmatrix}1\\1\end{pmatrix} \in U_3 \text{ und } \begin{pmatrix}1\\0\end{pmatrix} \in U_3, \quad \text{aber} \quad \begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}2\\1\end{pmatrix} \notin U_3.$$
29

(b) Für jeden Vektorraum V sind der Nullvektorraum $\{0\} \subset V$ und der gesamte Raum $V \subset V$ natürlich stets Unterräume von V. Sie werden die **trivialen Unterräume** genannt.

(c) Für eine gegebene Teilmenge $D \subset \mathbb{R}$ ist die Teilmenge
$$\mathrm{Pol}(D,\mathbb{R}) := \{f \in \mathrm{Abb}(D,\mathbb{R}) : f \text{ ist eine Polynomfunktion}\}$$
aller Polynomfunktionen $f : D \to \mathbb{R}$ ein Unterraum des Vektorraums $\mathrm{Abb}(D,\mathbb{R})$ aus Beispiel 13.3 (c), denn sie enthält die Nullfunktion, und mit f und g sind auch $f+g$ und λf für alle $\lambda \in \mathbb{R}$ Polynomfunktionen. Genauso ist für festes $n \in \mathbb{N}$ auch die Menge
$$\mathrm{Pol}_n(D,\mathbb{R}) := \{f \in \mathrm{Abb}(D,\mathbb{R}) : f \text{ ist eine Polynomfunktion vom Grad höchstens } n\}$$
ein Unterraum von $\mathrm{Abb}(D,\mathbb{R})$.

Wir wollen nun sehen, wie man aus mehreren Unterräumen eines Vektorraums neue konstruieren kann. Eine Möglichkeit besteht dabei einfach darin, ihren Durchschnitt zu bilden. Im Gegensatz dazu ist ihre Vereinigung zwar in der Regel kein Unterraum (wie wir an der Menge U_3 in Beispiel 13.12 (a) gesehen haben); es gibt aber trotzdem eine Möglichkeit, aus ihnen einen neuen zu erzeugen, der sie enthält – die korrekte Konstruktion hierfür ist nur nicht die Vereinigung, sondern die sogenannte Summe von Unterräumen:

Lemma 13.13 (Durchschnitte und Summen von Unterräumen)**.** *Es seien U_1 und U_2 Unterräume eines Vektorraums V. Dann gilt:*

(a) *Der Durchschnitt $U_1 \cap U_2$ ist ebenfalls ein Unterraum von V.*

(b) *Die **Summe** $U_1 + U_2 := \{x_1 + x_2 : x_1 \in U_1, x_2 \in U_2\}$ ist ebenfalls ein Unterraum von V.*

Analog gilt dies auch für Durchschnitte $U_1 \cap \cdots \cap U_n$ und Summen $U_1 + \cdots + U_n$ von mehr als zwei Unterräumen.

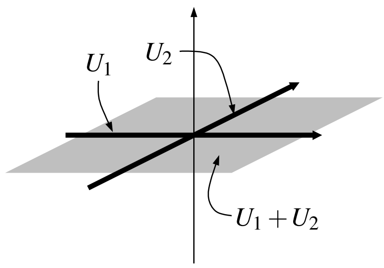
Beweis. Wir überprüfen jeweils die Bedingungen aus Definition 13.8. Dabei ist natürlich klar, dass der Nullvektor sowohl in U_1 als auch in U_2 liegt, und damit auch in $U_1 \cap U_2$ und $U_1 + U_2$. Wir müssen also nur noch die Abgeschlossenheit zeigen.

(a) Es seien $\lambda \in K$ und $x,y \in U_1 \cap U_2$, also $x,y \in U_1$ und $x,y \in U_2$. Da U_1 und U_2 Unterräume sind, liegen damit sowohl $x+y$ als auch λx in U_1 und U_2, d. h. in $U_1 \cap U_2$.

(b) Es seien $\lambda \in K$ und $x,y \in U_1 + U_2$, also $x = x_1 + x_2$ und $y = y_1 + y_2$ mit $x_1, y_1 \in U_1$ und $x_2, y_2 \in U_2$. Dann gilt wegen der Abgeschlossenheit von U_1 und U_2
$$x+y = x_1 + x_2 + y_1 + y_2 = \underbrace{(x_1+y_1)}_{\in U_1} + \underbrace{(x_2+y_2)}_{\in U_2} \in U_1 + U_2,$$
und analog auch
$$\lambda x = \lambda(x_1+x_2) = \underbrace{\lambda x_1}_{\in U_1} + \underbrace{\lambda x_2}_{\in U_2} \in U_1 + U_2. \qquad \square$$

Beispiel 13.14 (Summen von erzeugten Unterräumen)**.** Sind zwei Unterräume eines Vektorraums V durch erzeugende Vektoren gegeben als
$$U_1 = \mathrm{Lin}(x_1,\dots,x_n) = \{\lambda_1 x_1 + \cdots + \lambda_n x_n : \lambda_1,\dots,\lambda_n \in K\}$$
$$\text{und} \quad U_2 = \mathrm{Lin}(y_1,\dots,y_m) = \{\mu_1 y_1 + \cdots + \mu_m y_m : \mu_1,\dots,\mu_m \in K\},$$
so ist nach Definition der Summe natürlich
$$\begin{aligned} U_1 + U_2 &= \{\lambda_1 x_1 + \cdots + \lambda_n x_n + \mu_1 y_1 + \cdots + \mu_m y_m : \lambda_1,\dots,\lambda_n,\mu_1,\dots,\mu_m \in K\} \\ &= \mathrm{Lin}(x_1,\dots,x_k,y_1,\dots,y_l). \end{aligned}$$

Als konkretes Beispiel ist für die Unterräume
$$U_1 = \mathrm{Lin}\begin{pmatrix}1\\0\\0\end{pmatrix} \quad \text{und} \quad U_2 = \mathrm{Lin}\begin{pmatrix}0\\1\\0\end{pmatrix}$$
von $\mathbb{R}^3$ ihr Durchschnitt gleich $U_1 \cap U_2 = \{0\}$, und ihre Summe wie im Bild rechts dargestellt die Ebene
$$U_1 + U_2 = \mathrm{Lin}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}\right).$$



Aufgabe 13.15. Welche der folgenden Teilmengen sind Unterräume von $\mathbb{R}^3$ (wobei x_1, x_2, x_3 die Komponenten des Vektors $x \in \mathbb{R}^3$ bezeichnen)?

(a) $U_1 = \left\{ \begin{pmatrix}-a\\0\\b-a\end{pmatrix} : a,b \in \mathbb{R} \right\}$;

(b) $U_2 = \{x \in \mathbb{R}^3 : x_2 + a x_3 = 1 - a\}$ für ein festes, gegebenes $a \in \mathbb{R}$;

(c) $U_3 = \{x \in \mathbb{R}^3 : x_1^3 = x_2^3 = x_3^3\}$;

(d) $U_4 = \{x \in \mathbb{R}^3 : x_1, x_2, x_3 \in \mathbb{Z}\}$.

Aufgabe 13.16. Es seien U_1 und U_2 Unterräume eines K-Vektorraums V. Zeige, dass $U_1 \cup U_2$ genau dann ein Unterraum von V ist, wenn $U_1 \subset U_2$ oder $U_2 \subset U_1$ gilt.

Aufgabe 13.17. Im Vektorraum $V = \mathrm{Abb}(\mathbb{R},\mathbb{R})$ seien
$$U_1 = \{f \in \mathrm{Abb}(\mathbb{R},\mathbb{R}) : f(-x) = f(x) \text{ für alle } x \in \mathbb{R}\}$$
$$\text{und} \quad U_2 = \{f \in \mathrm{Abb}(\mathbb{R},\mathbb{R}) : f(-x) = -f(x) \text{ für alle } x \in \mathbb{R}\}$$
die Teilmengen aller sogenannten geraden bzw. ungeraden Funktionen. Man zeige:

(a) U_1 und U_2 sind Unterräume von V.

(b) $U_1 \cap U_2 = \{0\}$ und $U_1 + U_2 = V$.

14. Basen und Dimension

Im letzten Kapitel haben wir in Lemma 13.11 viele Beispiele von Vektorräumen konstruiert, indem wir zu einer (endlichen) Familie B in einem gegebenen Vektorraum den davon erzeugten Unterraum $\operatorname{Lin} B$ gebildet haben. In der Tat haben sehr viele in der Praxis auftretende Vektorräume die Eigenschaft, dass ihre Elemente als Linearkombinationen endlich vieler gegebener Vektoren geschrieben werden können – z. B. alle Unterräume von K^n für beliebige $n \in \mathbb{N}$, wie wir in Bemerkung **??** noch sehen werden. Wir wollen uns daher zur Vereinfachung oft auf solche gemäß der folgenden Definition endlich erzeugten Vektorräume beschränken. Wie man auch ohne diese Bedingung auskommen kann, werden wir kurz am Ende dieses Kapitels in Bemerkung **??** diskutieren.

Definition 14.1 (Erzeugendensysteme und endlich erzeugte Vektorräume)**.** Es sei V ein Vektorraum.

(a) Eine (endliche) Familie $B = (x_1, \dots, x_n)$ von Vektoren in V heißt ein **Erzeugendensystem** von V, wenn $\operatorname{Lin} B = V$ gilt, d. h. wenn es zu jedem $x \in V$ Skalare $\lambda_1, \dots, \lambda_n \in K$ gibt mit $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$.

(b) Der Vektorraum V heißt **endlich erzeugt**, wenn er ein solches endliches Erzeugendensystem besitzt.

Beispiel 14.2.

(a) Für ein gegebenes $n \in \mathbb{N}$ bilden die sogenannten **Einheitsvektoren**

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad \in K^n$$

ein Erzeugendensystem von K^n, denn jedes $x \in K^n$ mit Komponenten $x_1, \dots, x_n \in K$ hat die Form

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + \cdots + x_n e_n.$$

Insbesondere ist K^n damit ein endlich erzeugter Vektorraum.

(b) Für den Vektorraum $\mathbb{R}^2$ ist auch die Familie

$$B = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$$

ein Erzeugendensystem: Um dies zu zeigen, müssen wir zu jedem $x \in \mathbb{R}^2$ mit Komponenten x_1 und x_2 Skalare $\lambda_1, \lambda_2 \in \mathbb{R}$ finden mit

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \Leftrightarrow \quad \begin{array}{rl} & x_1 = \lambda_1 + \lambda_2 \\ \text{und} & x_2 = \lambda_1 - \lambda_2. \end{array}$$

Dieses Gleichungssystem lässt sich aber leicht nach λ_1 und λ_2 auflösen; wir erhalten

$$\lambda_1 = \frac{x_1 + x_2}{2} \quad \text{und} \quad \lambda_2 = \frac{x_1 - x_2}{2}, \quad \text{also} \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{x_1 + x_2}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{x_1 - x_2}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

(c) Für alle $n \in \mathbb{N}$ ist die Familie $B = (x^0, \dots, x^n)$ aller Potenzfunktionen $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^i$ für $i = 0, \dots, n$ (die wir hier kurz als x^i schreiben) ein Erzeugendensystem des Vektorraums $\operatorname{Pol}_n(\mathbb{R}, \mathbb{R})$ aller reellen Polynome vom Grad höchstens n aus Beispiel 13.12 (c), denn jedes solche Polynom ist nach Definition eine Linearkombination dieser Potenzfunktionen.

Insbesondere ist $\mathrm{Pol}_n(\mathbb{R},\mathbb{R})$ also endlich erzeugt. Der Vektorraum $\mathrm{Pol}(\mathbb{R},\mathbb{R})$ aller reellen Polynome ohne Gradbeschränkung ist dagegen nicht endlich erzeugt: In einer (endlichen) Familie B von Polynomen in $\mathrm{Pol}(\mathbb{R},\mathbb{R})$ gibt es nämlich zwangsläufig einen größten auftretenden Grad; Polynome in $\mathrm{Pol}(\mathbb{R},\mathbb{R})$ von höherem Grad können dann also nicht in $\mathrm{Lin}\,B$ liegen.

(d) Jedes Erzeugendensystem eines Vektorraums V bleibt natürlich ein Erzeugendensystem von V, wenn man beliebige Vektoren von V hinzufügt. So ist z. B. nicht nur wie in (a) die Familie der beiden Einheitsvektoren ein Erzeugendensystem von $\mathbb{R}^2$, sondern auch die Familie

$$B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right).$$

Diese Erweiterungsmöglichkeit mit beliebigen Vektoren kann Erzeugendensysteme natürlich unnötig groß machen. Wir sollten daher vor allem nach Erzeugendensystemen suchen, die keine überflüssigen Vektoren mehr beinhalten. In diesem Fall kann man dann anschaulich erwarten, dass die Anzahl der Vektoren in einem Erzeugendensystem als „Dimension“ des Vektorraums interpretiert werden kann – so wie in Beispiel 13.12 (a) ein einzelner Vektor eine (eindimensionale) Gerade und in Bemerkung 13.6 (c) zwei Vektoren eine (zweidimensionale) Ebene aufgespannt haben. Das Ziel dieses Kapitels ist es, diese Idee genau zu untersuchen und damit insbesondere auch den sehr wichtigen Dimensionsbegriff mathematisch exakt einzuführen.

14.A Lineare Unabhängigkeit und Basen

In Beispiel 14.2 (d) haben wir schon einen Fall eines Erzeugendensystems B mit überflüssigen Vektoren gesehen, nämlich

$$B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right) \quad \text{für den Vektorraum} \quad V = \mathbb{R}^2.$$

Dass hier gar nicht alle drei Vektoren von B benötigt werden, um V zu erzeugen, liegt einfach daran, dass sich einer von ihnen schon als Linearkombination der beiden anderen darstellen lässt: Es ist z. B.

$$\begin{pmatrix} 2 \\ 3 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

so dass wir diesen Vektor im Erzeugendensystem nicht benötigen. Alternativ könnten wir diese Gleichung auch nach einem der anderen Vektoren auflösen und so sehen, dass man stattdessen auch einen der anderen beiden Vektoren aus B weglassen könnte. Um hier keine Wahl treffen zu müssen, nach welchem Vektor aufgelöst werden soll, schreibt man die obige Gleichung aber in der Regel als

$$2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

also als eine Linearkombination des Nullvektors aus den gegebenen Vektoren. Um Erzeugendensysteme ohne überflüssige Vektoren zu finden, sollten wir also fordern, dass sie keine solchen Linearkombinationen des Nullvektors zulassen. Solche Erzeugendensysteme bezeichnet man als *Basen*:

Definition 14.3 (Basen)**.** Es sei $B = (x_1, \dots, x_n)$ eine Familie von Vektoren in einem Vektorraum V.

(a) Die Familie B heißt **linear abhängig**, wenn es eine Linearkombination $\lambda_1 x_1 + \dots + \lambda_n x_n = 0$ des Nullvektors gibt, in der mindestens ein λ_i ungleich 0 ist (man nennt dies auch eine *nicht-triviale Linearkombination des Nullvektors*).

Ist das Gegenteil der Fall, folgt aus einer Linearkombination $\lambda_1 x_1 + \dots + \lambda_n x_n = 0$ des Nullvektors mit zunächst beliebigen $\lambda_1, \dots, \lambda_n \in K$ also bereits, dass $\lambda_1 = \dots = \lambda_n = 0$ gelten muss, so heißt B **linear unabhängig**.

(b) Die Familie B heißt eine **Basis** von V, wenn B ein linear unabhängiges Erzeugendensystem von V ist.

Bemerkung 14.4. Es sei $B = (x_1, \dots, x_n)$ eine Familie von Vektoren in einem Vektorraum V.

(a) Enthält B den Nullvektor, d. h. gilt $x_i = 0$ für ein i, so ist B in jedem Fall linear abhängig, denn dann ist ja $1 \cdot x_i = 0$ eine nicht-triviale Linearkombination des Nullvektors.

(b) Ebenso ist B immer linear abhängig, wenn die Familie einen Vektor mehrfach enthält, also wenn $x_i = x_j$ für gewisse $i \neq j$ gilt, da dann $1 \cdot x_i - 1 \cdot x_j = 0$ eine nicht-triviale Linearkombination des Nullvektors ist.

Beispiel 14.5.

(a) Das Erzeugendensystem $B = (e_1, \dots, e_n)$ der Einheitsvektoren von K^n aus Beispiel 14.2 (a) ist linear unabhängig, denn sind $\lambda_1, \dots, \lambda_n \in K$ mit

$$0 = \lambda_1 e_1 + \cdots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix},$$

so folgt daraus natürlich sofort $\lambda_1 = \cdots = \lambda_n = 0$. Damit ist B also eine Basis von K^n; man nennt sie die **Standardbasis** von K^n.

Als Spezialfall davon für $n = 0$ ist die leere Familie eine Basis des Nullvektorraums (siehe Definition 13.5 (b)).

(b) Auch das Erzeugendensystem

$$B = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$$

von $\mathbb{R}^2$ aus Beispiel 14.2 (b) ist linear unabhängig und damit eine Basis von $\mathbb{R}^2$: Sind nämlich $\lambda_1, \lambda_2 \in \mathbb{R}$ mit

$$\lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad \begin{array}{rl} & \lambda_1 + \lambda_2 = 0 \\ \text{und} & \lambda_1 - \lambda_2 = 0, \end{array}$$

so folgt aus diesem Gleichungssystem natürlich sofort $\lambda_1 = \lambda_2 = 0$.

Neben der Standardbasis aus (a) haben wir damit also noch eine weitere Basis von $\mathbb{R}^2$ gefunden und sehen damit schon, dass Basen von Vektorräumen nicht eindeutig bestimmt sind. Allerdings werden wir in Folgerung **??** noch zeigen, dass alle Basen eines endlich erzeugten Vektorraums zumindest gleich viele Elemente haben. Dass unsere gerade gefundene Basis B genau wie die Standardbasis von $\mathbb{R}^2$ aus zwei Vektoren besteht, ist also kein Zufall.

(c) Ebenfalls in $\mathbb{R}^2$ ist wie in der Einleitung zu diesem Abschnitt die Familie

$$B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right) \quad \text{wegen} \quad 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

linear abhängig, und damit auch keine Basis von $\mathbb{R}^2$.

Beachte aber, dass mit einer Rechnung analog zu (b) je zwei der drei Vektoren dieser Familie B stets linear unabhängig sind. Die lineare Unabhängigkeit einer Familie kann also *nicht* überprüft werden, indem man immer nur zwei ihrer Vektoren miteinander vergleicht!

(d) Wir betrachten noch einmal den Vektorraum $\mathrm{Pol}_n(\mathbb{R}, \mathbb{R})$ aller reellen Polynome vom Grad höchstens n mit dem Erzeugendensystem $B = (x^0, \dots, x^n)$ der Potenzfunktionen aus Beispiel 14.2 (c). Da eine nicht-triviale Linearkombination dieser Potenzfunktionen nach dem Koeffizientenvergleich aus Lemma 3.22 nie die Nullfunktion sein kann, ist dieses Erzeugendensystem auch linear unabhängig, und damit eine Basis von $\mathrm{Pol}_n(\mathbb{R}, \mathbb{R})$.

Aufgabe 14.6. Untersuche die Familie B in den folgenden Fällen auf lineare Unabhängigkeit im Vektorraum V:

(a) $V = \mathbb{R}^3$; $B = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} \right)$.

(b) V ein beliebiger Vektorraum; $B=(x+y,x+z,y+z)$ für drei linear unabhängige Vektoren x,y,z.

(c) $V=\mathrm{Abb}(\mathbb{R}\backslash\{0\},\mathbb{R})$; $B=(\varphi_1,\varphi_2,\varphi_3)$ mit
$$\varphi_1:\mathbb{R}\backslash\{0\}\to\mathbb{R},\,x\mapsto x,\quad \varphi_2:\mathbb{R}\backslash\{0\}\to\mathbb{R},\,x\mapsto\frac{1}{x},\quad \varphi_3:\mathbb{R}\backslash\{0\}\to\mathbb{R},\,x\mapsto\begin{cases}1 & \text{falls } x>0,\\ 0 & \text{falls } x<0.\end{cases}$$

Aufgabe 14.7. Es seien $n\in\mathbb{N}_{>0}$ und $(x_1,\dots,x_n)$ eine Basis eines Vektorraums V. Wir setzen
$$y_k:=\sum_{i=1}^{k}x_i\quad\text{für alle } k=1,\dots,n.$$
Zeige, dass die Familie $(y_1,\dots,y_n)$ dann ebenfalls eine Basis von V ist.

Oft ist die folgende äquivalente Umformulierung der Basiseigenschaft nützlich:

Lemma und Definition 14.8 (Alternatives Kriterium für Basen)**.** *Eine Familie $B=(x_1,\dots,x_n)$ von Vektoren in einem Vektorraum V ist genau dann eine Basis von V, wenn es zu jedem Vektor $x\in V$ eindeutig bestimmte Skalare $\lambda_1,\dots,\lambda_n\in K$ gibt mit $x=\lambda_1x_1+\dots+\lambda_nx_n$.*

In diesem Fall nennt man $\lambda_1,\dots,\lambda_n$ die ***Koordinaten*** *von x bezüglich B.*

Beweis. Wir zeigen beide Richtungen der behaupteten Äquivalenz:

„$\Rightarrow$“: Es sei B eine Basis von V. Da B dann ein Erzeugendensystem von V ist, gibt es zu jedem $x\in V$ Skalare $\lambda_1,\dots,\lambda_n$ mit $x=\lambda_1x_1+\dots+\lambda_nx_n$.

Diese Koordinaten sind auch eindeutig bestimmt: Sind nämlich $\mu_1,\dots,\mu_n$ weitere Skalare mit $x=\mu_1x_1+\dots+\mu_nx_n$, so gilt
$$x=\lambda_1x_1+\dots+\lambda_nx_n=\mu_1x_1+\dots+\mu_nx_n\quad\Rightarrow\quad(\lambda_1-\mu_1)x_1+\dots+(\lambda_n-\mu_n)x_n=0,$$
und damit folgt wegen der linearen Unabhängigkeit von B sofort $\lambda_i-\mu_i=0$, also $\lambda_i=\mu_i$ für alle $i=1,\dots,n$.

„$\Leftarrow$“: Ist jeder Vektor in V eine Linearkombination der Vektoren aus B, so bedeutet dies natürlich $\mathrm{Lin}\,B=V$. Außerdem ist $\lambda_1=\dots=\lambda_n=0$ nach Voraussetzung die einzige Möglichkeit, den Nullvektor als Linearkombination $\lambda_1x_1+\dots+\lambda_nx_n$ zu schreiben. Damit ist B auch linear unabhängig. □

Beispiel 14.9.

(a) Die Komponenten eines Vektors $x\in K^n$ sind genau seine Koordinaten bezüglich der Standardbasis aus Beispiel 14.5 (a). Auch ohne Erwähnung einer Basis werden wir sie daher in Zukunft oft einfach seine Koordinaten nennen.

(b) Analog sind die Koeffizienten eines Polynoms in $\mathrm{Pol}_n(\mathbb{R},\mathbb{R})$ gerade seine Koordinaten bezüglich der Basis $(x^0,\dots,x^n)$ aus Beispiel 14.5 (d).

Bemerkung 14.10.

(a) Lemma 14.8 besagt anschaulich, dass wir einen Vektor in einem Vektorraum V bei gegebener Basis B genauso gut auch durch den Vektor in K^n seiner Koordinaten $\lambda_1,\dots,\lambda_n$ bezüglich B beschreiben können. Wir werden dies in den Abschnitten **??** und **??** noch genau untersuchen.

(b) Um einen Vektor wie in (a) durch seine Koordinaten bezüglich einer Basis B beschreiben zu können, ist es wichtig, dass wir Basen als *Familien* und nicht als *Mengen* definiert haben, da die Elemente einer Menge keine vorgegebene Reihenfolge haben und wir somit bei einer Menge B keine Möglichkeit hätten, die Koordinaten $\lambda_1,\dots,\lambda_n$ eindeutig den Vektoren in B zuzuordnen.

30

Literatur

[B] A. Beutelspacher, *Lineare Algebra*, Vieweg-Verlag (2003)
[BF] M. Barner, F. Flohr, *Analysis 1*, de Gruyter Lehrbuch (2000)
[E] H.-D. Ebbinghaus et al., *Zahlen*, Springer-Verlag (1988)
[Fi] G. Fischer, *Lineare Algebra*, Vieweg-Verlag (2002)
[Fo1] O. Forster, *Analysis 1*, Vieweg-Verlag (2011)
[Fo2] O. Forster, *Analysis 2*, Vieweg-Verlag (2010)
[G] A. Gathmann, *Algebraische Strukturen*, Vorlesungsskript RPTU Kaiserslautern (2023), `https://agag-gathmann.math.rptu.de/ags`
[GK] G.-M. Greuel, T. Keilen, *Lineare Algebra I und II*, Vorlesungsskript TU Kaiserslautern (1999), `www.math.uni-tuebingen.de/~keilen/download/LectureNotes/linearealgebra.pdf`
[J] K. Jänich, *Lineare Algebra*, Springer-Verlag (2010)
[K1] K. Königsberger, *Analysis 1*, Springer-Verlag (2003)
[K2] K. Königsberger, *Analysis 2*, Springer-Verlag (2003)
[M] T. Markwig, *Grundlagen der Mathematik*, Vorlesungsskript TU Kaiserslautern (2011), `www.math.uni-tuebingen.de/~keilen/download/LectureNotes/grundlagen11.pdf`

Index