BERGISCHE
UNIVERSITÄT
WUPPERTAL

Grundlagen der Mathematik

Jochen Glück

Vorlesungsmanuskript
Sommersemester 2024

Vorläufig finale Version
22. September 2024

Inhaltsverzeichnis

Vorwort

Einige Teile dieses Manuskripts habe ich aus meinem Vorlesungsmanuskript *Lineare Algebra 1* aus dem Wintersemester 2021/22 an der Universität Passau übernommen. Dies betrifft insbesondere große Teile der Kapitel 1 und 2 und manche Teile der Kapitel 3 und 4.

Kapitel 1

Aussagen und Mengen

Einstiegsfragen. (a) Schauen Sie sich die folgende Aussage an: „Alle Matheprofessorinnen sind Star Trek-Fans."

Wie lautet die Verneinung dieser Aussage? Können Sie die Verneinung formulieren, ohne die Worte „alle" und „jede" (bzw. Synonyme dieser Worte) zu verwenden?

(b) Können Sie in einfachen Worten erklären, was die Vereinigung von zwei Mengen ist?

(c) Was sind eigentlich Variablen und wozu braucht man sie?

(d) Wie unterscheidet sich die Bedeutung des Wortes „Menge" in den folgenden drei Sätzen?

Satz 1: „Ich habe letzten Sommer eine Menge Eis gegessen."

Satz 2: „Die Eisdiele hat letzten Sommer ein geringere Menge Eis verkauft als im Jahr zuvor."

Satz 3: „Die Menge der Primzahlen ist in der Menge aller ganzen Zahlen enthalten."

1.1 Exaktheit in der Mathematik

Ein zentrales und besonderes Merkmal der Wissenschaft *Mathematik* ist, dass mathematische Resultate nicht empirisch – also beruhigend auf realen Beobachtungen und Experimenten – gewonnen werden, sondern dass alle Behauptungen stets zweifelsfrei zu beweisen sind. Dies ist nur möglich, indem eine Reihe von Regeln konsequent beachtet wird:

- Wann immer man einen mathematischen Begriff verwendet, muss man präzise beschreiben, wie dieser Begriff zu verstehen ist. Dies ist der Sinn von *Definitionen*.

- Mathematische Resultate bestehen aus *Annahmen* und *Konklusionen*, und sind von der Form: Wenn die Annahmen alle erfüllt sind, dann sind auch die Konklusionen wahr.

  Je nach Kontext werden mathematische Resultate oft als *Theorem*, *Satz*, *Lemma*, *Proposition* oder *Korollar* bezeichnet.[1] Sie werden im Laufe der Vorlesung noch häufig sehen, welcher dieser Begriffe für welche Art von mathematischem Resultat verwendet wird.

- Mathematische Resultate werden stets sauber getrennt von Ihrer Begründung: Zunächst schreibt man das Resultat auf, anschließend folgt der Beweis des Resultats. Der Zweck des Beweises ist es, darzulegen, dass aus den Annahmen des Resultats die Konklusionen logisch folgen. Erst nach dem Beweis darf man davon ausgehen, dass das Resultat tatsächlich gültig ist.

- Wichtig: Das Wort „logisch“ im vorangehenden Punkt darf auf keinen Fall umgangssprachlich im Sinne von „plausibel“ verstanden werden. Mit dem Begriff *logisch folgen* meint man in der Mathematik stattdessen eine Situation, in der die Richtigkeit der Annahmen zwangsläufig und in jedem Fall dazu führt, dass auch die Konklusionen richtig sind.

  Damit es hier nicht zu Missverständnissen oder Ungenauigkeiten kommt, bedient man sich der *Aussagenlogik*, in der genau festgelegt ist, wie man mit mathematischen Aussagen umgehen darf, und wann eine Aussage logisch aus einer anderen folgt.

Wir werden uns in den nachfolgenden Abschnitten 1.2 und 1.4 mit der Aussagenlogik beschäftigen.

Außerdem werden Sie in den weiteren Abschnitten dieses Kapitels einige weitere Konzepte lernen, die in allen mathematischen Teilgebieten eine wichtige Rolle spielen: *Mengen und Tupel* (Abschnitt 1.3) dienen dazu, mehrere mathematische Objekte (z.B. mehrere Zahlen) zu einem größeren Objekt zusammenzufassen. *Funktionen* (Kapitel 2) sind wichtig, um verschiedene mathematische Objekte zueinander in Beziehung setzen zu können.

1.2 Aussagen und Wahrheitswerte

In der *Aussagenlogik* geht es darum, Aussagen über mathematische Objekte zu treffen und festzulegen, wie man mit diesen Aussagen arbeiten darf.

[1] Wobei die Unterscheidung zwischen diesen Begriffen recht subjektiv und häufig auch etwas willkürlich ist. Dies ist aber kein Problem, da es für den Inhalt eines mathematischen Resultats nicht von Bedeutung ist, ob man das Resultat z.B. als Theorem oder als Lemma bezeichnet.

Was ist eine Aussage?

In der Mathematik möchte man wahre Dinge über mathematische Objekte sagen – dazu muss man stets sauber unterscheiden können, was wahr und was falsch ist. Formulierungen, bei denen diese Unterscheidung möglich ist, bezeichnen wir als *Aussagen*:

Definition 1.2.1 (Aussagen und Wahrheitswerte)**.** (a) Unter einer **Aussage** verstehen wir einen sprachlichen Ausdruck[2], von dem eindeutig feststeht, ob er wahr oder falsch ist.

(b) Wenn eine Aussage wahr ist, dann sagen wir, sie hat den **Wahrheitswert** „wahr“; wenn sie hingegen falsch ist, dann sagen wir, sie hat den **Wahrheitswert** „falsch“.

Es folgen sowohl einige alltägliche Beispiele als auch einige mathematische Beispiele.

Beispiele 1.2.2. (a) Der Ausdruck „*Friedrich Schiller*“ ist keine Aussage, denn es ergibt keinen Sinn zu sagen, dass eine Person war oder falsch sei.

(b) Der Ausdruck „*Friedrich Schiller hat das Drama ‘Der Götz von Berlichingen’ geschrieben.*“ ist eine Aussage. Sie ist falsch[3], hat also den Wahrheitswert „falsch“.

(c) Der Ausdruck „*Friedrich Schiller hat das Drama ‘Die Räuber’ geschrieben.*“ ist eine Aussage. Sie ist wahr, hat also den Wahrheitswert „wahr“.

(d) Der Ausdruck „*Friedrich Schiller hat vielleicht die Ballade ‘Die Bürgschaft’ geschrieben*“ ist keine Aussage[4], denn aufgrund des Wortes „vielleicht“ ist es nicht möglich zu sagen, ob der Ausdruck wahr oder falsch ist.

(e) Der Ausdruck „$2 + 2$“ ist keine Aussage, denn „$2 + 2$“ ist weder wahr noch falsch.

(f) Der Ausdruck „$2 + 2 = 5 - 1$“ ist eine Aussage. Sie ist wahr, hat also den Wahrheitswert „wahr“.

(g) Der Ausdruck „$2+2 = 4$“ ist eine Aussage. Sie hat ebenfalls den Wahrheitswert „wahr“.

(h) Der Ausdruck „$2 + 2 = 5 + 2$“ ist eine Aussage. Sie hat den Wahrheitswert „falsch“.

[2] Man könnte auch sagen: Eine sprachliche Formulierung.
[3] Das Drama ‘Der Götz von Berlichingen’ wurde von Goethe verfasst.
[4] Im mathematischen Sinne.

Inhalt der Mathematik ist es, wahre Aussagen über mathematische Objekte zu machen und zu beweisen. Deshalb hat man wenig Lust, zu jeder wahren Aussage stets explizit dazuzuschreiben, dass sie wahr ist. Denken Sie zum Beispiel an die Aussage aus Beispiel 1.2.2(c): Wenn Sie einem Kommilitonen mitteilen möchten, dass Schiller 'Die Räuber' geschrieben hat, dann sagen Sie nicht etwa

Die Aussage „*Friedrich Schiller hat das Drama 'Die Räuber' geschrieben.*“ ist wahr.

Sondern Sie sagen einfach:

Friedrich Schiller hat das Drama 'Die Räuber' geschrieben.

Damit wollen Sie selbstverständlich zum Ausdruck bringen, dass diese Aussage wahr ist. Ebenso hält man es auch in der Mathematik:

Konvention 1.2.3. Wenn wir eine Aussage machen ohne Ihren Wahrheitsgehalt zu spezifizieren, so wollen wir damit zum Ausdruck bringen, dass die Aussage wahr ist.

Verknüpfungen von Aussagen und Wahrheitstabellen

Einzelne Aussagen sind aus mathematischer Sicht recht unspektakulär. Interessant wird es erst, wenn man mehrere Aussagen verknüpft – das bedeutet, man baut aus mehreren gegebenen Aussagen eine neue. Ein einfaches Beispiel für solche eine Verknüpfung ist die *Verundung*[5] von zwei Aussagen. Sehen wir uns das zunächst an einem Beispiel an:

Beispiel 1.2.4. Die beiden Aussagen *Friedrich Schiller hat das Drama 'Die Räuber' geschrieben* und *Johann Wolfgang von Goethe hat die Ballade 'Der Erlkönig' geschrieben* können wir mit Hilfe des Wortes „und“ zu einer neuen Aussage verknüpfen:

Friedrich Schiller hat das Drama 'Die Räuber' geschrieben und Johann Wolfgang von Goethe hat die Ballade 'Der Erlkönig'.

Diese neue Aussage ist wahr, weil die beiden Aussagen, mit denen wir begonnen hatten, wahr sind.

Dasselbe kann man natürlich auch für beliebige andere Aussagen machen: Wenn A and B Aussagen sind, dann können wir daraus eine neue Aussage „A und B“ konstruieren.[6]

An dieser Stelle sollten Sie kurz innehalten und an Abschnitt 1.1 zurückdenken: Als allererstes haben wir besprochen, dass jeder Begriff, den wir verwenden, sauber definiert werden muss, damit wir stets genau wissen, wovon wir eigentlich sprechen.

[5] Häufig auch *Konjunktion* genannt.

[6] Hier sehen Sie bereits eine Vorgehensweise, die in der Mathematik sehr üblich und sehr nützlich ist: Wenn man etwas nicht nur für ein konkretes Beispiel tun möchte, sondern ganz allgemein, so verwendet man Platzhalter – häufig bezeichnet man diese Platzhalter mit Buchstaben, wie hier A und B.

Wenn also A und B zwei Aussagen sind, was genau ist dann mit der und-Verknüpfung „A und B“ gemeint?

Wir meinen mit „A und B“ eine neue Aussage, und damit keine Meinungsverschiedenheit darüber auftreten kann, ob diese Aussage wahr oder falsch ist, müssen wir *definieren*, welchen Wahrheitswert „A und B“ hat. Dies wird natürlich davon abhängen, welchen Wahrheitswert A und B jeweils haben. Allerdings gibt es für die Wahrheitswerte von A und B nur vier mögliche Fälle, und wenn wir für jeden dieser Fälle den Wahrheitswert von „A und B“ festlegen, dann ist immer eindeutig bestimmt, ob „A und B“ wahr oder falsch ist. Also tun wir genau das:

Definition 1.2.5 (und-Verknüpfung)**.** Seien A und B beliebige Aussagen. Wir definieren eine neue Aussage, die wir als $A \wedge B$ notieren und als „A und B“ aussprechen, indem wir die folgenden Wahrheitswerte für $A \wedge B$ festlegen:

- Wenn A wahr ist und B wahr ist, dann ist $A \wedge B$ ebenfalls wahr.
- Wenn A wahr ist und B falsch ist, dann ist $A \wedge B$ falsch.
- Wenn A falsch ist und B wahr ist, dann ist $A \wedge B$ falsch.
- Wenn A falsch ist und B falsch ist, dann ist $A \wedge B$ ebenfalls falsch.

Die Aussage $A \wedge B$ wird als **Konjunktion** von A und B bezeichnet.

Diese Definition orientiert sich an der Bedeutung des Wortes „und“ in der Alltagssprache: „Es gilt A und B“ ist in der Alltagssprache gleichbedeutend mit „Es gilt sowohl A als auch B“. Diese Aussage ist wahr, wenn A, B beide wahr sind, sie ist jedoch falsch, wenn mindestens eine der beiden Aussagen A, B falsch ist.

Dies ist eine passende Stelle für einige allgemeine Kommentare zu Definitionen in der Mathematik:

Bemerkungen 1.2.6. (a) Grundsätzlich darf man definieren, was immer man möchte – solange die Definition sich nicht selbst widerspricht. Wenn man einen mathematischen Begriff oder ein mathematisches Symbol definiert, muss man sich also nicht zwangsläufig daran halten, wie dieser Begriff oder dieses Symbol in der alltäglichen Sprache verwendet werden.

Wichtig dabei ist natürlich: Jeder Begriff hat dann natürlich auch nur die Bedeutung, die ihm in seiner Definition zugewiesen wurde. Ob der Begriff in der Alltagssprache anders verwendet wird, spielt somit bei der Verwendung des Begriffs in der Mathematik keine Rolle – man hat sich einzig und allein an seine Definition zu halten.

(b) Trotzdem würde es vermutlich große Verwirrung stiften, wenn man einen Begriff so definiert, da seine mathematischen Definition der alltagssprachlichen Bedeutung des Begriffs stark zuwider läuft. Deshalb versucht man, Begriffe so zu definieren, dass sich die Definition eines Begriffs zumindest grob an seiner alltagssprachlichen Bedeutung orientiert. Wie oben erläutert, haben wir das auch in Definition 1.2.5 so gemacht.

(c) Beachten Sie trotzdem unbedingt: Ausschlaggebend für die Bedeutung eines mathematischen Begriffs ist letztlich immer seine mathematische Definition! Wenn Sie also unsicher sind, was ein mathematischer Begriff, den wir verwenden, bedeutet, dann lautet der erste Ratschlag immer: Blättern Sie in Ihren Unterlagen zurück und schlagen Sie die Definition des Begriffs nach!

Definition 1.2.5 ist ziemlich ausladend formuliert und wenig übersichtlich. Denselben Inhalt kann man aber auch übersichtlicher darstellen, indem man einfach eine Tabelle verwendet: Definition 1.2.5 besagt, dass die Wahrheitswerte von $A \wedge B$ folgendermaßen lauten:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

Hierbei haben wir „wahr“ mit dem Buchstaben „w“ abgekürzt und „falsch“ mit dem Buchstaben „f“. Eine Tabelle von obenstehender Form nennt man aus naheliegenden Gründen **Wahrheitstabelle**.

Wir definieren nun noch weitere Verknüpfungen von zwei Aussagen, sowie die Verneinung von Aussagen. Um die Definition dieser Begriffe übersichtlicher zu gestalten als in Definition 1.2.5, schreiben wir sie direkt mit Hilfe von Wahrheitstabellen auf.

Definition 1.2.7 (oder-Verknüpfungen und Negation)**.** Seien A und B beliebige Aussagen. Wir definieren drei weitere Aussagen $A \vee B$, $A \dot{\vee} B$, $\neg A$, deren Werte durch die folgenden Wahrheitstabellen festgelegt werden:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

A	B	$A \dot{\vee} B$
w	w	f
w	f	w
f	w	w
f	f	f

A	$\neg A$
w	f
f	w

Für die so definierten Aussagen verwenden wir die folgenden Bezeichnungen:

(a) Die Aussage $A \vee B$ wird als „A inklusiv oder B“ ausgesprochen und als **inklusive Disjunktion** von A und B bezeichnet; oft sagt man anstelle „A inklusiv oder B“ auch einfach „A oder B“.[7]

(b) Die Aussage $A \dot{\vee} B$ wird als „A exklusiv oder B“ ausgesprochen und als **exklusive Disjunktion** von A und B bezeichnet.[8]

[7] Das bedeutet, das Wort „oder“ wird in der Mathematik, solange man nichts anderes dazu sagt, immer als „inklusives Oder“ verstanden.

[8] Neben $\dot{\vee}$ gibt es noch weitere gebräuliche Symbole für das exklusive Oder. Zum Beispiel ist es in der Informatik üblich anstelle von $A \dot{\vee} B$ die Notation $A \operatorname{xor} B$ zu verwenden.

(c) Die Aussage $\neg A$ wir als „nicht A“ ausgesprochen und als **Verneinung** oder **Negation** von A bezeichnet.

Bisher haben wir nur Begriffe und Symbole definiert. Als nächstes wollen wir ein paar mathematische Resultate aus der Aussagenlogik besprechen, und uns überzeugen, dass diese tatsächlich stimmen.

Proposition 1.2.8. *Sei A eine beliebige Aussage. Dann gilt immer (d.h. unabhängig vom Wahrheitswerte von A):*[9]

(a) *Die Aussage $A \vee (\neg A)$ ist wahr.*[10]

(b) *Die Aussage $A \wedge (\neg A)$ ist falsch.*[11]

(c) *Die Aussage $A \dot{\vee} (\neg A)$ ist wahr.*

Bevor Sie weiterlesen, sollten Sie sich auf jeden Fall überlegen, warum die Resultate in Proposition 1.2.8 intuitiv wirklich so erwarten würde. Wie Sie schon wissen, reicht Intuition aber in der Mathematik als Begründung nicht aus – wir wollen absolut sicher sein, dass Proposition 1.2.8 richtig ist. Deshalb **beweisen** wir die Proposition nun mit Hilfe von Wahrheitstabellen:

Beweis von Proposition 1.2.8. Die Aussage A hat genau einen der Wahrheitswerte „wahr“ oder „falsch“. Wenn wir also diese beiden Fälle betrachten, und in jedem der Fälle den Wahrheitswert der drei Aussagen $A \vee (\neg A)$, $A \wedge (\neg A)$, $A \dot{\vee} (\neg A)$ bestimmen, können wir sicherstellen, dass diese drei Aussagen wirklich immer den Wahrheitswert „wahr“ besitzen. Am übersichtlichsten lässt sich dies mit Hilfe einer Wahrheitstabelle darstellen:

A	$\neg A$	$A \vee (\neg A)$	$A \wedge (\neg A)$	$A \dot{\vee} (\neg A)$
w	f	w	f	w
f	w	w	f	w

Die Einträge in der Tabelle sind wie folgt zustande gekommen:

- Die Definition einer Aussage (Definition 1.2.1) besagt, dass A genau einen der beiden Wahrheitswerte „wahr“ und „falsch“ besitzt. Also können nur die beiden Fälle auftreten, die in der ersten Spalte aufgelistet sind.

- Die Definition der Negation (in Definition 1.2.7) sagt uns nun, welchen Wahrheitswert $\neg A$ in jedem der Fälle besitzt. Somit sind die Wahrheitswerte in der zweiten Spalte durch Definition 1.2.7 festgelegt.

[9] An der Notation dieser Aussagen sehen Sie, dass wir Klammern verwenden, um klarzumachen, in welcher Reihenfolge der Verknüpfungen ausgewertet werden.

[10] Dieses Resultat bezeichnet man manchmal auch als Satz vom ausgeschlossenen Dritten.

[11] Dieses Resultat bezeichnet man manchmal auch als Satz vom Widerspruch.

- Aus den Wahrheitswerten in den ersten beiden Spalten und der Definition der inklusiven Disjunktion (in Definition 1.2.7) erhalten wir nun die Wahrheitswerte in der dritten Spalte.

- Aus den Wahrheitswerten in den ersten beiden Spalten und der Definition der Konjunktion (in Definition 1.2.5) erhalten wir nun die Wahrheitswerte in der dritten Spalte.

- Aus den Wahrheitswerten in den ersten beiden Spalten und der Definition der exklusiven Disjunktion (in Definition 1.2.7) erhalten wir die Wahrheitswerte in der vierten Spalte.

In der dritten Spalte der Tabelle können Sie sehen, dass die Aussage $A \vee (\neg A)$ tatsächlich in jedem Fall den Wahrheitswert „wahr“ besitzt. Damit ist (a) bewiesen.

In der vierten Spalte können Sie sehen, dass die Aussage $A \wedge (\neg A)$ immer den Wahrheitswert „falsch“ besitzt. Damit ist (b) bewiesen.

Und laut der fünften Spalte besitzt die Aussage $A \dot{\vee} (\neg A)$ immer den Wahrheitswert „wahr“. Somit ist (c) bewiesen. □

Bemerkung 1.2.9. Am Ende des vorangehenden Beweises konnten Sie eine in der Mathematik sehr weit verbreitete Notation sehen: Das Ende eines Beweises wird meist mit einem kleinen Quadrat[12] markiert. Dies wird als symbolische Abkürzung für die Wendung „was zu zeigen war“ – auf lateinisch „quot erat demonstrandum“ – verstanden. Die Abkürzung „qed“ hingegen ist in der Mathematik heute sehr aus der Mode gekommen.

Mit Hilfe von Wahrheitstabellen kann man auch komplexere Resultate über Verknüpfungen von mehreren Aussagen beweisen. Die folgenden vier Propositionen enthalten einige solcher Aussagen.

Proposition 1.2.10 (De Morgansche Regeln für die Verneinung von Konjunktionen und Disjunktionen)**.** *Seien A, B beliebige Aussagen.*

(a) *Die Aussage $\neg(A \wedge B)$ hat immer denselben Wahrheitswert wie $(\neg A) \vee (\neg B)$.*

(b) *Die Aussage $\neg(A \vee B)$ hat immer denselben Wahrheitswert wie $(\neg A) \wedge (\neg B)$.*

Es ist wichtig, dass Sie sich in Ruhe überlegen, weshalb die Resultat in Proposition 1.2.10 stimmen. Unabhängig davon muss man die Proposition aber natürlich auch beweisen, wobei man nur die Definitionen der logischen Verknüpfungen verwendet. Weil dies mit Hilfe von Wahrheitstabellen sehr einfach möglich ist, besprechen wir hier nur exemplarisch den Beweis von Teil (a). Um mit dem Konzept der Wahrheitstabelle vertraut zu werden, sollten Sie selbst versuchen, Teil (b) zu beweisen.

[12] Manche Autorinnen und Autoren verwenden stattdessen z.B. auch eine Raute.

Beweis von Proposition 1.2.10(a). Für die möglichen Wahrheitswerte der Aussagen A, B gibt es insgesamt vier Möglichkeiten. Mit Hilfe der Definitionen 1.2.5 und 1.2.7 können wir somit die folgende Wahrheitstabelle ausfüllen:

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

Die Wahrheitswerte für $A \wedge B$ sowie für die Aussage $\neg A$ und die Aussage $\neg B$ haben wir hier nur als Zwischenergebnisse eingefügt, um daraus die Wahrheitswerte der Aussage $\neg(A \wedge B)$ und der Aussage $(\neg A) \vee (\neg B)$ zu bestimmen, die uns eigentlich interessieren.

Wie Sie in der Tabelle erkennen können, hat die Aussage $\neg(A \wedge B)$ immer denselben Wahrheitswert wie die Aussage $(\neg A) \vee (\neg B)$. Somit ist die Behauptung von Proposition 1.2.10(a) bewiesen. □

Proposition 1.2.11 (Kommutativgesetz für Konjunktion und Disjunktionen)**.** *Seien A, B beliebige Aussagen.*

(a) *Die Aussage $A \wedge B$ hat immer denselben Wahrheitswert wie $B \wedge A$.*

(b) *Die Aussage $A \vee B$ hat immer denselben Wahrheitswert wie $B \vee A$.*

(c) *Die Aussage $A \dot{\vee} B$ hat immer denselben Wahrheitswert wie $B \dot{\vee} A$.*

Genau wie Proposition 1.2.10 kann man auch Proposition 1.2.11 mit Hilfe von Wahrheitstabellen beweisen. Wir verzichten darauf, diese Tabellen hier alle anzugeben.

Proposition 1.2.12 (Assoziativgesetz für Konjunktion und Disjunktionen)**.** *Seien A, B, C beliebige Aussagen.*

(a) *Die Aussage $(A \wedge B) \wedge C$ hat immer denselben Wahrheitswert wie $A \wedge (B \wedge C)$.*

(b) *Die Aussage $(A \vee B) \vee C$ hat immer denselben Wahrheitswert wie $A \vee (B \vee C)$.*

(c) *Die Aussage $(A \dot{\vee} B) \dot{\vee} C$ hat immer denselben Wahrheitswert wie $A \dot{\vee} (B \dot{\vee} C)$.*

Auch hier lässt sich der Beweis einfach mit Hilfe von Wahrheitstabellen führen. Weil in Proposition 1.2.12 drei Aussagen A, B, C vorkommen (statt wie bisher nur zwei) geben wir den Beweis für Teil (a) noch einmal explizit an. Die Beweise der anderen beiden Aussagen können Sie nach diesem Vorbild leicht selbst führen.

Beweis von Proposition 1.2.12(a). Es gibt insgesamt acht Möglichkeiten, wie die Wahrheitswerte von A, B, C lauten können. Wir gehen alle acht Möglichkeiten in der folgenden Tabelle durch:

A	B	C	$A \wedge B$	$(A \wedge B) \wedge C$	$B \wedge C$	$A \wedge (B \wedge C)$
w	w	w	w	w	w	w
w	w	f	w	f	f	f
w	f	w	f	f	f	f
w	f	f	f	f	f	f
f	w	w	f	f	w	f
f	w	f	f	f	f	f
f	f	w	f	f	f	f
f	f	f	f	f	f	f

Also besitzen $(A \wedge B) \wedge C$ und $A \wedge (B \wedge C)$ tatsächlich immer denselben Wahrheitswert. □

Weil $(A \wedge B) \wedge C$ und $A \wedge (B \wedge C)$ immer denselben Wahrheitswert besitzen[13] ist es also nicht wichtig, wo wir die Klammern setzen. Deshalb ist es Konvention, die Klammern auch einfach ganz wegzulassen, und stattdessen die Aussage mit dem Wahrheitswert von $(A \wedge B) \wedge C$ (bzw. $A \wedge (B \wedge C)$) als $A \wedge B \wedge C$ zu notieren.[14]

Proposition 1.2.13 (Distributivgesetze für Konjunktion und Disjunktion)**.** *Seien A, B, C beliebige Aussagen.*

(a) *Es hat $(A \vee B) \wedge C$ immer denselben Wahrheitswert wie $(A \wedge C) \vee (B \wedge C)$.*

(b) *Es hat $(A \wedge B) \vee C$ immer denselben Wahrheitswert wie $(A \vee C) \wedge (B \vee C)$.*

Auch hier erfolgt der Beweis, wie bei Proposition 1.2.12, über Wahrheitstabellen. Da ist nicht allzu sehr aufschlussreich ist, fertig ausgefüllte Tabellen zu lesen, verzichten wir darauf, die Tabellen hier alle aufzuführen. Wie oben gilt stattdessen: Wenn Sie wissen möchten, weshalb die Proposition stimmt, können Sie die Wahrheitstabellen selbst erstellen und somit die Proposition beweisen.[15]

Zum Abschluss dieses Abschnitts noch zwei Bemerkungen über die bisher geführten Beweise:

Bemerkungen 1.2.14. (a) Die bisher geführten Beweise fanden Sie vielleicht, obgleich überzeugend, nicht besonders aufschlussreich oder interessant – Tabellen auszufüllen ist eine nicht besonders kreative Tätigkeit. Sie können aber unbesorgt sein: Die große Mehrzahl der Beweise, die Sie ab sofort sehen werden, hat mit dem Ausfüllen von Tabellen nichts (oder sehr wenig) zu tun.

Genau gesprochen handelt es sich bei der oben verwendeten Methoden um eine bestimmte **Beweistechnik**, nämlich um **Fallunterscheidungen**: Wenn man

[13] Später werden wir für diese Eigenschaft übrigens noch einen speziellen Begriff einführen: Wir werden zwei Aussagen **äquivalent** nennen, wenn Sie dieselben Wahrheitswerte besitzen.

[14] Ebenso kann man dann auch für noch mehr als nur drei Aussagen vorgehen. Darauf gehen wir aber an dieser Stelle erst mal nicht weiter ein, weil es nicht wirklich zu neuen Einsichten führt.

[15] Versuchen Sie das ruhig einmal, zumindest für eine oder zwei der Propositionen! Sie sollen ja kritisch sein und nicht einfach alles glauben, was Ihnen im Manuskript oder in der Vorlesung erzählt wird!

weiß, dass nur eine bestimmte Anzahl an Fällen auftreten kann (z.B. können im Beweis von Proposition 1.2.12(a) nur acht Fälle für die Wahrheitswerte von A, B, C auftreten), dann kann man all diese Fälle einzeln durchgehen, und sehen, was in jedem Fall jeweils passiert. In den obigen Beweisen war es besonders leicht, in jedem Fall zu sehen, was passiert: Wenn man nämlich die Wahrheitswerte aller gegebenen Aussagen kennt, dann kann man daraus recht mechanisch auch die Wahrheitswerte von zusammengesetzten Aussagen bestimmen.[16]

Sie werden schon bald noch weitere nützliche Beweistechniken kennenlernen, und Fallunterscheidungen werden nur noch ab und zu vorkommen.

(b) Grundsätzlich werden alle Beweise, egal wie sie im Detail ausgestaltet sind, darauf beruhen, korrekte logische Schlussfolgerungen zu ziehen: Ein „korrekte logische Schlussfolgerung zu ziehen“ bedeutet hierbei, dass man eine Aussage gegeben hat, und im nächsten Schritt eine Aussage angibt, die immer richtig ist, falls die vorangehende Aussage richtig ist.

Um dies effizient und fehlerfrei zu tun, muss man sicher mit Aussagen und deren Verknüpfungen umgehen. Man kann den Inhalt dieses Abschnitts also, wenn man möchte, als ein wenig „meta-mathematisch“ betrachten: Wir möchten im Rest der Vorlesung (während des ganzen Semesters) gerne verschiedenste mathematische Resultate beweisen. Dazu müssen wir sicher mit Aussagen umgehen können, und deshalb haben wir hier zuerst einige Dinge über Aussagen selbst bewiesen.

In Abschnitt 1.4 bauen wir die Aussagenlogik noch weiter aus, indem wir dort über **quantifizierte Aussagen** sprechen.

1.3 Mengen und Tupel

Wie Sie schon wissen, möchten wir in der Mathematik Aussagen über mathematische Objekte beweisen. Die einfachsten mathematischen Objekte, die Ihnen vielleicht einfallen, sind vermutlich Zahlen (z.B., ganze Zahlen, rationale Zahlen, reelle Zahlen).

Es gibt aber noch zahlreiche weitere mathematische Objekte, und es ist ein wichtiges Grundprinzip in der Mathematik, dass man aus bekannten Objekten neue Objekte baut, in dem man zum Beispiel mehrere Objekte zu einem Objekt zusammenfasst. In diesem Abschnitt besprechen wir zwei Möglichkeiten, um dies zu tun: **Mengen** und **Tupel**.

[16] Dass wir die Fallunterscheidungen in Tabellenform aufgeschrieben haben, liegt einfach daran, dass dies für die Bestimmung der Wahrheitswerte von Aussagen am übersichtlichsten ist. Auch im weiteren Verlauf der Vorlesung und Ihres Studiums werden Ihnen immer wieder einmal Beweise per Fallunterscheidung begegnen – allerdings sind die einzelnen Fälle dann meist komplizierter als nur eine einzelne Zeile von Wahrheitswerten, und deshalb werden solche Beweise dann meist nicht mehr in Tabellenform aufgeschrieben.

Was ist eine Menge?

Wenn Sie im Supermarkt eine Gurke, eine Flasche Bier, eine Packung Chips und eine Melone kaufen, haben Sie vermutlich Schwierigkeiten, diese einzeln nach Hause zu tragen. Eine bewährte Möglichkeit, dies zu lösen, besteht darin, all Ihre Einkäufe in eine Tüte (oder einen Korb oder einen Rucksack) zu packen und somit nur noch ein Objekt transportieren zu müssen statt vier einzelne Objekte. Kurzum: Sie fassen mehrere Objekte zu einem Objekt zusammen, indem Sie eine Art von Hülle um die Objekte legen.

Dasselbe tun wir nun in der Mathematik: Wir fassen mehrere Objekte zu einem neuen Objekt zusammen. Das zusammengefasste Objekt bezeichnen wir dann als **Menge**, in die einzelnen Objekte, die wir „hineingelegt“ haben, bezeichnen wir als **Elemente** der Menge.

Wie in Ihrer Einkaufstüte ist es dabei nicht von Belang, in welcher Reihenfolge Sie die Objekte in die Tüte legen.[17] Es gibt allerdings einen entscheidenden Unterschied zwischen der Einkaufstüte und einer Menge: In einer Menge verlangt man, dass jedes Element der Menge dort höchstens einmal vorkommt,[18] während Sie in eine Einkaufstüte durchaus zwei Flaschen Bier derselben Sorte legen können.

Was wir oben beschrieben haben, wird in der folgenden klassischen Definition des Begriffs **Menge**, die von Georg Cantor[19] stammt, kanpp zusammengefasst:

Definition 1.3.1 (Mengendefinition nach Cantor)**.** Eine **Menge** M ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens (welche die **Elemente** von M genannt werden) zu einem Ganzen.

Die Reihenfolge, in der die Objekte zusammengefasst werden, spielt hierbei keine Rolle.[20]

Das Wort „wohlunterschiedene“ in der Definition stellt klar, dass jedes Element nur einmal in der Menge M auftreten darf.

Ein Problem bei dieser Definition ist, dass nicht geklärt wird, war genau man unter einer „Zusammenfassung“ versteht, und ob es wirklich immer widerspruchsfrei möglich ist, beliebige Objekte zu einem neuen Objekt zusammenzufassen. Deshalb wurde später eine formale Mengenlehre entwickelt, die sich dieser Probleme annimmt und die viel präziser ist. Diese formale Mengenlehre ist aber viel zu abstrakt um sie im ersten Semester zu besprechen, und in vielen mathematischen Teilgebieten reicht obige Definition im Arbeitsalltag meist aus.

[17] Nun gut, vielleicht möchten Sie die Chips nicht ganz nach unten legen – aber lassen Sie uns dies hier einfach ignorieren.

[18] Manchmal kann es auch interessant sein, ein Objekt mehrmals zuzulassen – dafür gibt es das Konzept der sogenannten **Multimenge**. Allerdings kommen Multimengen im mathematischen Alltag viel seltener vor als Mengen, und in der Linearen Algebra 1 werden wir Multimengen gar nicht benötigen.

[19] Georg Cantor (1845 in St. Petersburg – 1918 in Halle) war ein deutscher Mathematiker, der als Begründer der Mengenlehre gilt.

[20] Genau genommen stammt der erste Absatz in der Definition von Cantor; den zweiten Absatz haben wir hier hinzugefügt, um Missverständnisse auszuschließen.

Um eventuelle Widersprüche auszuschließen, wollen wir Definition 1.3.1 noch um folgende Vereinbarung ergänzen:

Konvention 1.3.2. Wir vereinbaren, dass die „Zusammenfassung bestimmter, wohlunterschiedener Objekte“ zu einer Menge nur dann möglich ist, wenn sichergestellt ist, dass von jedem mathematischen Objekt entschieden werden kann, ob es ein Element der Menge ist, oder nicht.

Um zusagen, dass ein Objekt x Element einer Menge M ist, benutzen wir die Notation

$$x \in M;$$

man spricht dies beim Vorlesen folgendermaßen aus: „x Element M“. Um hingegen zu sagen, dass ein Objekt x nicht Element einer Menge ist, benutzen wir die Notation

$$x \notin M;$$

dies spricht man beim Vorlesen folgendermaßen aus: „x nicht Element M“.

Wenn Sie sich nun Definition 1.2.1 noch einmal durchlesen, dann sehen Sie: Wenn M eine Menge ist und x irgendein Objekt, dann ist „$x \in M$“ eine Aussage. Ebenso ist „$x \notin M$“ eine Aussage – nämlich die Verneinung der vorangehenden Aussage; anders gesagt hat „$x \notin M$“ immer denselben Wahrheitswert wie „$\neg(x \in M)$“.

Einige Mengen, deren Elemente bestimmte Zahlen sind, kommen in der Mathematik so häufig vor, dass man eigene Symbole für sie einführt und durchgängig benutzt. Sie kennen viele dieser Mengen und deren Symbole vermutlich bereits aus der Schule – aber der Vollständigkeit halber wiederholen wir sie hier noch einmal kurz:

Notation 1.3.3.

(a) Mit $\mathbb{Z}$ bezeichnen wir die Menge der **ganzen Zahlen**.[21]

(b) Mit $\mathbb{N}$ bezeichnen wir die Menge aller ganzen Zahlen, die größer oder gleich 0 sind.

Wir nennen $\mathbb{N}$ die Menge der **natürlichen Zahlen**.

(c) Mit $\mathbb{N}^*$ bezeichnen wir die Menge der ganzen Zahlen, die größer oder gleich 1 sind.

[21] An dieser Stelle sehen Sie, dass wir mathematisch nicht komplett von vorne beginnen: An einigen Stellen setzen wir Wissen aus der Schule voraus, zum Beispiel ein intuitives Verständnis, was die ganzen Zahlen, die rationalen Zahlen und die reellen Zahlen sind, und was es bedeutet, dass eine Zahl größer oder größer gleich ist als eine andere Zahl.

Für all diese Zahlenmengen und deren Eigenschaft kann man präzise angeben, wie Sie definiert sind – dies erfordert jedoch einiges an Zusatzaufwand und gehört thematisch nicht zur Linearen Algebra 1. Möglicherweise werden Sie in der Vorlesung Analysis 1 ansprechen, wie man z.B. die reellen Zahlen konstruieren kann, und welche axiomatischen Eigenschaften sie besitzen.

(d) Mit $\mathbb{Q}$ bezeichnen wir die Menge aller **rationalen Zahlen**.[22]

(e) Mit $\mathbb{R}$ bezeichnen wir die Menge der **reellen Zahlen**.

Bemerkung 1.3.4. Bezüglich des Begriffs **natürliche Zahlen** herrscht Uneinheitlichkeit in der Literatur: Manche Autorinnen und Autoren verwenden dieselbe Nomenklatur wie in diesem Manuskript, d.h., sie setzen $\mathbb{N}^* \coloneqq \{1, 2, \dots\}$ und $\mathbb{N} \coloneqq \{0, 1, 2, \dots\}$, und nennen die erstgenannte Menge die **natürlichen Zahlen**. Andere hingegen setzen zum Beispiel $\mathbb{N} \coloneqq \{1, 2, \dots\}$ und $\mathbb{N}_0 \coloneqq \{0, 1, 2, \dots\}$ und nennen die erstgenannte Menge die **natürlichen Zahlen**. Wenn Sie etwas in einem Buch oder Manuskript nachlesen, ist es also wichtig darauf zu achten, wie die natürlichen Zahlen dort definiert sind, und welches Symbol hierfür benutzt wird.

Methoden zur Beschreibung von Mengen

Definition 1.3.1 und Vereinbarung 1.3.2 sagen uns zwar, was wir unter einer Menge verstehen – aber um mit Mengen zu arbeiten, braucht man auch Möglichkeiten um Mengen effizient aufzuschreiben.

Dazu gibt es in der Mathematik mehrere Möglichkeiten, die im folgenden aufgezählt werden:

Konvention 1.3.5 (Beschreibung von Mengen)**.** (a) Eine Menge, die nur endlich viele Elemente besitzt, kann man beschreiben, indem man alle Ihre Elemente aufzählt.[23]

(b) Man kann eine Menge (egal ob sie endlich oder unendlich viele Elemente besitzt) beschreiben, in dem man Bedingungen angibt, die ein Objekt erfüllen muss, um Element der Menge zu sein.

(c) Man kann eine Menge (egal ob sie endlich oder unendlich viele Elemente besitzt) beschreiben, in dem man eine Regel angibt, nach der alle ihre Elemente konstruiert werden.[24]

Einige Beispiele für die Möglichkeit (b) haben Sie bereits in Notation 1.3.3 gesehen, denn zum Beispiel kann man die dort verwendete Formulierung „Mit $\mathbb{Z}$ bezeichnen wir die Menge der ganzen Zahlen“ auch ewas ausführlicher schreiben als „Mit $\mathbb{Z}$ bezeichnen wir die Menge aller Objekte, die eine ganze Zahl sind.“

Jedes der drei Möglichkeiten in Vereinbarung 1.3.5 kann man auf verschiedene Weise umsetzen, zum Beispiel indem man eine geeignete natürlichsprachliche Formulierung verwendet oder indem man die in der Mathematik sehr übliche Notation

[22] Zur Erinnerung: Eine Zahl heißt rational, wenn man sie als Bruch schreiben kann, wobei der Zähler eine ganze Zahl und der Nenner eine von Null verschiedene ganze Zahl ist.

[23] Für Mengen mit sehr vielen Elementen ist das aber manchmal äußerst unpraktisch, und für Mengen mit unendlichen vielen Elementen geht es gar nicht.

[24] Im nächsten Abschnitt, 1.4, werden Sie sehen, dass Möglichkeit (c) im Grunde ein Spezialfall von Möglichkeit (b) ist.

mit geschweiften Klammern verwendet. Das lässt sich am einfachsten anhand eines Beispiels demonstrieren:

Beispiel 1.3.6. Die folgenden Formulierungen beschreiben jeweils dieselbe Menge M:

(a) *Aufzählen der Elemente*:

- Natürlichsprachliche Formulierung:

  „Es sei M die Menge, deren Elemente die Zahlen 2, 4 und 6 sind."

- Notation mit geschweiften Klammern:

  „Es sei $M = \{2, 4, 6\}$."

(b) *Angeben von Bedingungen, die Objekte erfüllen müssen, um Elemente von M zu sein:*

- Natürlichsprachliche Formulierung:

  „Es sei M die Menge aller ganzen Zahlen, die gerade sind, und die größer oder gleich 2 und kleiner oder gleich 6 sind."

- Natürlichsprachliche Formulierung, etwas knapper: Dieses Mal drücken wir uns etwas kürzer aus, indem wir eine Variable verwenden:[25]

  „Es sei M die Menge aller Objekte z, die die folgenden Bedingungen erfüllen: $z \in \mathbb{Z}$ und z ist gerade und $2 \leq z \leq 6$."

- Notation mit geschweiften Klammern:

  „Es sei $M = \{z \mid \ z \in \mathbb{Z}$ und z ist gerade und $2 \leq z \leq 6\}$."

  Den Strich „$\mid$ " liest man hier als „mit den Eigenschaften" oder „welche die folgenden Eigenschaften erfüllen". Die gesamte Beschreibung von M kann man zum Beispiel folgendermaßen lesen:

  „Es sei M die Menge aller Objekte z, welche die folgenden Eigenschaften erfüllen: z ist in $\mathbb{Z}$, und z ist gerade, und $2 \leq z \leq 6$."

- Notation mit geschweiften Klammern, noch knapper: Wir drücken uns noch etwas kürzer aus, indem wir die Symbole zur Verknüpfungen von Aussagen verwenden, die wir im vorangehenden Abschnitt 1.2 besprochen haben:

  „Es sei $M = \{z \mid \ z \in \mathbb{Z} \ \wedge \ z$ ist gerade $\ \wedge \ 2 \leq z \leq 6\}$."

[25] Mehr Informationen zu Variablen folgen zu Beginn des Abschnitts 1.4.

- Notation mit geschweiften Klammern, nochmals effizienter: Wir verkürzen die Schreibweise ein wenig mehr, indem wir die Bedingung „$z \in \mathbb{Z}$“ vor den Strich | schreiben:

  $$\text{„Es sei } M = \{z \in \mathbb{Z} \mid \quad z \text{ ist gerade } \quad \wedge \quad 2 \leq z \leq 6\}.\text{“}$$

  Anschaulich kann man diese Notation so lesen, dass die Elemente von M diejenigen Elemente aus einer anderen Menge – in diesem Fall $\mathbb{Z}$ – sind, welche die nach dem Strich | folgenden Bedingungen erfüllen.

  Man kann diese Beschreibung von M zum Beispiel folgendermaßen aussprechen: „Es sei M die Menge aller Elemente z von $\mathbb{Z}$, welche die folgenden Eigenschaften erfüllen: z ist gerade, und $2 \leq z \leq 6$.“

(c) *Angeben einer Regel um alle Elemente von M zu konstruieren:*

- Natürlichsprachliche Formulierung:

  „Es sei M die Menge der Zahlen, die man erhält, indem man alle ganzen Zahlen, die größer oder gleich 1 und kleiner oder gleich 3 sind, mit 2 multipliziert.“

- Notation mit geschweiften Klammern:

  $$\text{„Es sei } M = \{2y \mid \quad y \in \mathbb{Z} \quad \wedge \quad 1 \leq y \leq 3\}\text{“}.$$

  Diese Notation kann man zum Beispiel folgendermaßen aussprechen: „Es sei M die Menge aller Objekte von der Form $2y$, wobei folgendes gilt: $y \in \mathbb{Z}$ and $1 \leq y \leq 3$.“

Das korrekte Beschreiben von Mengen ist für alles, was in dieser Vorlesung folgt – und auch für jede weitere Mathematikvorlesung – absolut essentiell. Beim Üben sollten Sie die folgende Bemerkung beachten.

Bemerkung 1.3.7. In Beispiel 1.3.6 ist für die verschiedenen Notationsmöglichkeiten jeweils angegeben, wie Sie diese aussprechen können (und die lässt sich natürlich auch auf verschiedene Weise variieren).

Üben Sie auf jeden Fall, Mengen nicht nur zu lesen und aufzuschreiben, sondern auf jeden Fall auch vorzulesen. Dies wird Ihre Intuition für den Umgang mit Mengen stärken und es wird Ihnen regelmäßig ins Gedächtnis rufen, dass auf dem Blatt Papier oder Computerbildschirm vor Ihnen nicht irgendein Symbolsalat steht, sondern Dinge mit einer ganz konkreten Bedeutung, die man auch natürlichsprachlich formulieren kann.[26]

Wichtig: Man kann – und soll! – die mathematische Beschreibung einer Menge immer so vorlesen, dass das, was man sagt, ein grammatisch sinnvoller Satz in der

[26] Wenn Sie mit Kommilitoninnen und Kommilitonen über die Vorlesungsinhalte und Übungsaufgaben diskutieren (was Sie auf jeden Fall tun sollten!), sollten Sie aus demselben Grund ebenfalls eine Kombination aus Aufschreiben und mündlicher Diskussion wählen.

verwendeten Sprache (in Ihrem Fall vermutlich: Deutsch) ist. Mathematische Notation so vorzulesen, dass Sie grammatisch sinnvolle Sätze sagen, ist wichtig, damit Ihr Gegenüber Sie verstehen kann, und damit Sie sicher sind, dass Sie das Vorgelesene selbst verstehen. Üben Sie deshalb das Vorlesen von Mengen unbedingt solange, bis Sie dies stets in vollständigen und grammatisch richtigen Sätzen tun!

Als ein weiteres wichtiges Beispiel erwähnen wir noch die leere Menge:

Beispiel 1.3.8 (Leere Menge)**.** Die Menge, die gar kein Element enthält, bezeichnet man als **leere Menge**. Man notiert sie häufig mit dem Symbol $\emptyset$.

Auch diese Menge kann man mithilfe von geschweiften Klammern aufschreiben, indem man alle Elemente dieser Menge zwischen den geschweiften Klammern aufzählt: Mit dieser Schreibeweise erhält man die Notation $\{\}$ für die leere Menge.[27]

Beziehungen zwischen Mengen

Weil wir sehr viel mit Mengen arbeiten werden und dabei keine Missverständnisse zur Bedeutung bestimmter Begriffe aufkommen lassen wollen, wollen wir im folgenden klären, wann genau wir zwei Menge als gleich auffassen:

Definition 1.3.9 (Gleichheit von Mengen)**.** Zwei Mengen M_1, M_2 heißen **gleich**, falls sie genau die gleichen Elemente haben.

Wir verwenden die Notation $M_1 = M_2$ um auszudrücken, dass die Mengen M_1 und M_2 gleich sind und die Notation $M_1 \neq M_2$ um auszudrücken, dass M_1 und M_2 nicht gleich sind.

Für zwei Mengen M_1, M_2 ist „$M_1 = M_2$“ also ein Aussage; ihre Verneinung „$\neg(M_1 = M_2)$“ ist genau die Aussage $M_1 \neq M_2$.

Beispiele 1.3.10. (a) Es gilt $\{7, -1, \pi\} = \{-1, \pi, 7\}$ (denn die Reihenfolge der Elemente spielt für eine Menge keine Rolle.[28]

(b) Es gilt $\{n \in \mathbb{N} \mid\ 5 \leq n \leq 8\} = \{5, 6, 7, 8\}$.

(c) Es gilt $\{k \in \mathbb{Z} \mid\ k^2 = 9\} \neq \{3\}$.[29]

(d) Es gilt $\{\} \neq \big\{\{\}\big\}$.[30]

Neben der Gleichheit der Mengen sind auch noch Teilmengenbeziehungen[31] zwischen Mengen von großer Bedeutung. Diese sind folgendermaßen definiert:

[27] Die beiden Schreibweise $\emptyset$ und $\{\}$ für die leere Menge sind beide gebräuchlich, allerdings ist $\emptyset$ erfahrungsgemäß verbreiteter.

[28] Siehe Definition 1.3.1.

[29] Denn die Menge auf der linken Seite besteht aus den Elementen 3 und -3.

[30] Denn die Menge auf der linken Seite hat kein Element, während die Menge auf der rechten Seite das Element $\{\}$ besitzt.

Wichtig um das zu verstehen, ist die Beobachtung, dass die leere Menge $\{\}$ nicht „nichts“ ist, sondern ein mathematisches Objekt: nämlich eine Menge, die nichts enthält.

[31] Die man oft auch **Inklusionen** nennt.

Definition 1.3.11 (Teilmengen und Obermengen)**.** Eine Menge M_1 heißt **Teilmenge** von M_2, falls jedes Element von M_1 auch ein Element von M_2 ist. In diesem Fall nennt man M_2 auch **Obermenge** von M_1.

Um auszudrücken, dass M_1 Teilmenge von M_2 ist, verwenden wir die Notation $M_1 \subseteq M_2$ oder, alternativ, die Notation $M_2 \supseteq M_1$.

Ähnlich wie zuvor schreiben wir $M_1 \not\subseteq M_2$ (oder $M_2 \not\supseteq M_1$) als Abkürzung für die Aussage $\neg(M_1 \subseteq M_2)$.

Bemerkung 1.3.12. Mit diesen Begriffsbildungen folgt für alle Mengen M_1, M_2 sofort die folgende Beobachtung: Die Aussage $M_1 = M_2$ ist gleichbedeutend mit der Aussage $M_1 \subseteq M_2 \ \wedge \ M_1 \supseteq M_2$.

Beispiele 1.3.13. (a) Es gilt $\{1, 3\} \subseteq \{3, 2, 1\}$, aber $\{3, 2, 1\} \not\subseteq \{1, 3\}$.

(b) Es gilt $\{\frac{3}{2}, 5\} \not\subseteq \{-3, 10\}$ und $\{-3, 10\} \not\subseteq \{\frac{3}{2}, 5\}$.

(c) Für jede Menge M gilt $M \supseteq \emptyset$.

(d) Für jede nicht-leere Menge M gilt $M \not\subseteq \emptyset$.

(e) Es gilt $\emptyset \subseteq \emptyset$.[32]

(f) Es gilt $\{2\} \subseteq \big\{2, \{2, 3\}\big\}$, aber $\{2, 3\} \not\subseteq \big\{2, \{2, 3\}\big\}$.[33]

Mengenoperationen

Aus gegebenen Mengen kann man neue Mengen bauen – unter anderem folgendermaßen:

Definition 1.3.14 (Durchschnitt, Vereinigung und Differenz zweier Mengen)**.** Seien L, M Mengen.

(a) Die Menge $L \cap M \coloneqq \{x \mid \ x \in L \ \wedge \ x \in M\}$ heißt der **Durchschnitt** von L und M.[34]

(b) Die Menge $L \cup M \coloneqq \{x \mid \ x \in L \ \vee \ x \in M\}$ heißt die **Vereinigung** von L und M.

(c) Die Menge $L \setminus M \coloneqq \{x \mid \ x \in L \ \wedge \ x \notin M\}$ heißt die **mengentheoretische Differenz** – oder kürzer die **Differenz** – von L und M.

[32] Weil ja sogar $\emptyset = \emptyset$ gilt.

[33] Denn die Menge $\big\{2, \{2, 3\}\big\}$ hat nur die beiden Elemente 2 und $\{2, 3\}$.

[34] Das Gleichheitszeichen mit Doppelpunkt auf einer Seite benutzt man in der Mathematik häufig; es bedeutet: Das Objekt auf der Seite des Gleichheitszeichen, wo der Doppelpunkt steht, wird **definiert** als das Objekt auf der anderen Seite des Gleichheitszeichens. Die Verwendung dieses Symbols ergibt natürlich nur Sinn, wenn das Objekt auf der Seite, wo der Doppelpunkt steht, bisher noch nicht definiert ist.

Die obenstehenden Mengenoperationen wurden alle mit Hilfe der logischen Verknüpfungen definiert, die Sie bereits aus Abschnitt 1.2 kennen. In diesem Abschnitt hatten wir mithilfe von Wahrheitstabellen verschiedene Eigenschaften für die Verknüpfungen von Aussagen bewiesen. Diese Eigenschaften können wir nun verwenden, um interessante Eigenschaften von Mengenoperationen zu beweisen.

Als ein erstes einfaches Beispiel zeigen wir, dass die Durchschnittsbildung zweier Mengen kommutativ ist:

Proposition 1.3.15. *Seien L, M Mengen. Dann gilt $L \cap M = M \cap L$.*

Beweis. Um die Proposition zu beweisen, verwenden wir die Beobachtung aus Bemerkung 1.3.12. Es genügt demnach, wenn wir die beiden Inklusionen „$L \cap M \subseteq M \cap L$“ und „$L \cap M \supseteq M \cap L$“ beweisen.

„$\subseteq$“ Um die Inklusion „$L \cap M \subseteq M \cap L$“ zu zeigen, müssen wir laut Definition 1.3.11 beweisen, dass jedes Element von $L \cap M$ auch ein Element von $M \cap L$ ist.

Sei also x ein beliebiges Element von $L \cap M$. Dann gilt laut Definition 1.3.14(a)

$$x \in L \ \wedge \ x \in M.$$

Aus Proposition 1.2.11(a) wissen wir, dass dann auch die Aussage

$$x \in M \ \wedge \ x \in L$$

wahr ist. Dies bedeutet laut Definition 1.3.14(a), dass $x \in M \cap L$ ist.

„$\supseteq$“ Der Beweis der umgekehrten Inklusion „$L \cap M \supseteq M \cap L$“ ist sehr ähnlich:[35] Laut Definition 1.3.11 müssen wir, um diese Inklusion zu beweisen, zeigen, dass jedes Element von $M \cap L$ auch ein Element von $L \cap M$ ist.

Sei also x ein beliebiges Element von $M \cap L$. Dann gilt laut Definition 1.3.14(a) die Aussage.

$$x \in M \ \wedge \ x \in L.$$

Somit ist laut Proposition 1.2.11(a) auch die Aussage

$$x \in L \ \wedge \ x \in M$$

wahr. Dies bedeutet gemäß Definition 1.3.14(a), dass $x \in L \cap M$ ist. □

Mithilfe der Resultate aus Abschnitt 1.2 kann man noch viele weitere Regeln für Durchschnitt, Vereinigung und Differenz von Mengen beweisen. Darauf kommen wir in den Übungen zurück.

[35] Wir werden aber schon bald Beweise von Mengengleichheiten führen, in denen die beiden Inklusionen auf sehr verschiedene Weise bewiesen werden.

Tupel und kartesische Produkte

Sie haben bereits gelernt, dass Mengen in der Mathematik genutzt werden, um mehrere Objekte zu einem Objekt zusammenzufassen – wobei jedes der Objekte, die zusammengefasst werden, nur einmal in der Menge auftauchen darf, und die Reihenfolge der Objekte beim Zusammenfassen keine Rolle spielt.

In diesem Abschnitt besprechen wir, die entgegengesetzte Situation: Wir fassen mehrere Objekte zu einem neuen Objekt zusammen, wobei wir aber die Reihenfolge beachten wollen und wobei ein Objekt auch mehrmals vorkommen darf. Außerdem wollen wir uns in diesem Abschnitt darauf beschränken, nur endlich viele Objekte zusammenzufassen.[36]

Definition 1.3.16 (Tupel)**.** (a) Die Zusammenfassung endlich vieler Objekte (wobei auch einige oder alle dieser Objekte gleich sein dürfen) in einer bestimmten Reihenfolge zu einem einzelnen Objekt bezeichnet man als **Tupel**. Die so zusammengefassten Objekte heißen **Einträge** des Tupels.

(b) Zur Notation eines Tupels verwenden wir runde Klammern, innerhalb derer die Einträge in entsprechender Reihenfolge aufgezählt werden. Ist x ein Tupel, so bezeichnen wir mit x_1 den ersten Eintrag des Tupels, mit x_2 den zweiten Eintrag, und so weiter (wobei der Index nicht größer sein darf als die Anzahl der Einträge des Tupels).

(c) Zwei Tupel x und y heißen **gleich**, falls die Anzahl Ihrer Einträge die gleiche Zahl $n \in \mathbb{N}$ ist, und falls für jede natürliche Zahl k zwischen 1 und n gilt: $x_k = y_k$.

Wir verwenden die Notation $x = y$ um zu sagen, dass zwei Tupel x und y gleich sind, und wir verwenden erneut die Notation $x \neq y$ als Abkürzung für die Aussage $\neg(x = y)$.

Konkret schreibt man die Objekte, aus denen ein Tupel besteht, innerhalb der runden Klammern oft von links nach rechts auf und trennt sie durch Kommata. Eine häufig gebrauchte Alternative, die manchmal übersichtlicher ist, besteht darin, die Einträge von oben nach unten aufzuzählen. Zum Beispiel könnten wir das Tupel $(5, \pi, 5)$ auch in der Form

$$\begin{pmatrix} 5 \\ \pi \\ 5 \end{pmatrix}$$

schreiben, und meinen damit dasselbe.[37]

[36] Man kann natürlich auch unendlich viele Objekte auf diese Weise zusammenzufassen; es ist aber etwas schwieriger, dies sauber aufzuschreiben – insbesondere, weil man darauf achten muss, was bei unendlich vielen Objekten mit dem Begriff „Reihenfolge“ überhaupt gemeint ist.

[37] Hier muss man aber ein wenig aufpassen, insbesondere in der Linearen Algebra: Wenn man mit Matrizen und mit sogenannten Spaltenvektoren und Zeilenvektoren arbeitet, dann muss man tatsächlich sauber unterscheiden, ob die Einträge nebeneinander oder übereinander stehen.

Es folgen ein paar Beispiele:

Beispiel 1.3.17. Die Tupel

$$(5, \pi, 5), \qquad (5, 5, \pi), \qquad (5, 5, \pi, 5), \qquad ()$$

sind alle verschieden. Das letztgenannte ist das Tupel mit Null Einträgen, das sogenannte **leere Tupel**. Es gilt beispielsweise

$$(5, \pi, 5)_1 = 5, \quad (5, \pi, 5)_2 = \pi, \quad (5, \pi, 5)_3 = 5,$$

während $(5, \pi, 5)_4$ nicht definiert ist, weil das Tupel $(5, \pi, 5)$ nur drei Einträge hat.

Tupel ermöglichen die äußerst nützliche Begriffsbildung des kartesischen Produktes von Mengen. Kartesische Produkte von $\mathbb{R}$ mit sich selbst werden später eines der häufigsten Beispiele in der Vorlesung sein.

Definition 1.3.18 (Kartesisches Produkt)**.** Sei $n \in \mathbb{N}$.

(a) Seien $M_1, \ldots, M_n$ Mengen.[38] Die Menge

$$M_1 \times \cdots \times M_n := \big\{(x_1, \ldots, x_n) \mid \ x_1 \in M_1 \ \wedge \cdots \wedge \ x_n \in M_n\big\}$$

nennt man das *kartesische Produkt* der Mengen $M_1, \ldots M_n$.

(b) Sei M eine Menge. Dann verwendet man die Abkürzung

$$M^n := \underbrace{M \times \cdots \times M}_{n \text{ Faktoren}}$$

für das n-fache kartesische Produkt mit sich selbst.

Die vorangehende Definition wirkt auf den ersten Blick sehr abstrakt; sie wird aber deutlich klarer, wenn man sich einige einfache Beispiele ansieht:

Beispiele 1.3.19. (a) Sei $L = \{5, 6\}$ und $M = \{-2, -1, 0\}$. Dann gilt

$$L \times M = \big\{(5, -2),\ (5, -1),\ (5, 0),\ (6, -2),\ (6, -1),\ (6, 0)\big\}.$$

(b) Es ist $\mathbb{R}^2 = \big\{(x_1, x_2) \mid \ x_1 \in \mathbb{R} \ \wedge \ x_2 \in \mathbb{R}\big\}$.

Die Menge $\mathbb{R}^2$ kann man geometrisch interpretieren; dies besprechen wir auf dem dritten Übungsblatt genauer.

[38] Von diesen Mengen dürfen auch mehrere gleich sein. Dies ist eine generelle Regel in der Mathematik: Wenn man mehrere Objekte mit verschiedenen Namen aufzählt, ist trotzdem zugelassen, dass manche dieser Objekte gleich sind – es sei denn, man sagt explizit dazu, dass die Objekte alle verschieden sein sollen.

1.4 Verknüpfung beliebig vieler Aussagen: Quantoren

Variablen

Variablen (oder **Platzhalter**) werden in der Mathematik verwendet, um nicht nur Aussagen über einzelne mathematische Objekte, sondern über viele (oder unendliche viele) mathematische Objekte zu treffen. Zur Einstimmung besprechen wir kurz einige sehr einfache Beispiele:

Beispiele 1.4.1. (a) Sehen Sie sich die folgenden drei (wahren) Aussagen an:

$$\begin{aligned} &\text{Es gilt } (1+1)^2 \leq 1^2 + 3 \cdot 1. \\ &\text{Es gilt } (2+1)^2 \leq 2^2 + 3 \cdot 2. \\ &\text{Es gilt } (3+1)^2 \leq 3^2 + 3 \cdot 3. \end{aligned} \tag{1.4.1}$$

Diese drei Aussagen können wir komprimierter aufschreiben, indem wir eine Variable – nennen wir sie zum Beispiel r – verwenden:

$$\text{Für jede Zahl } r \in \{1,2,3\} \text{ gilt } (r+1)^2 \leq r^2 + 3 \cdot r. \tag{1.4.2}$$

Beachten Sie unbedingt, dass der Beginn dieses Satzes, also die Formulierung „Für jede Zahl $r \in \{1,2,3\}$“, benötigt wird um zu erkennen, dass (1.4.2) eine Kurzfassung von genau den drei Aussagen in (1.4.1) ist.

(b) Mit Hilfe einer binomischen Formel können Sie sich überlegen, dass die Aussage $(r+1)^2 \leq r^2 + 3 \cdot r$ nicht nur für $r \in \{1,2,3\}$ stimmt, sondern sogar für alle reellen Zahlen r, die größer oder gleich 1 sind.[39] Um dies kurz und knapp zum Ausdruck zu bringen, können Sie schreiben:

$$\text{Für jede reelle Zahl } r \geq 1 \text{ gilt } (r+1)^2 \leq r^2 + 3 \cdot r.$$

Sie können hier einen großen Vorteil der Verwendung von Variablen erkennen: Mit ihrer Hilfe kann man in einem einzigen Satz Aussagen über unendlich viele Objekte formulieren.

(c) Variablen sind nicht nur nützlich um auszudrücken, dass eine Formel für mehrere (oder sogar unendlich viele) Objekte gilt; auch wenn Sie etwas ausdrücken möchten, wozu Sie gar keine Formel benötigen, können Sie – und sollten Sie häufig auch – Variablen verwenden, um sich möglichst verständlich auszudrücken. Betrachten Sie zum Beispiel die folgende Geschichte:

„Nehmen wir an, dass Adrian und Berta jeweils eine Geldsumme an Christina verschenken. Anschließend verschenkt Christina das Doppelte der von Adrian erhaltenen Summe an die Berta und die Hälfte der von Berta erhaltene

[39] Das können Sie so sehen: Wenn r eine reelle Zahl ist, die größer oder gleich 1 ist, dann gilt $(r+1)^2 = r^2 + 2r + 1 \leq r^2 + 2r + r = r^2 + 3r$.

Summe an Adrian. Ob Christina dabei insgesamt einen Gewinn oder Verlust gemacht hat, hängt davon ab, wieviel sie zu Beginn jeweils von Adrian und Berta erhalten hatte."

Sind Sie noch dabei? Lassen Sie uns dasselbe noch einmal formulieren, aber diedes Mal verwenden wir Variablen um die Geldummen zu bezeichnen:

„Nehmen wir an, dass Adrian und Berta Geldsummen s_A bzw. s_B an Christina verschenken. Anschließend schenkt Christina das Doppelte von s_A weiter an Berta und die Hälfte von s_B weiter an Adrian. Ob Christina dabei insgesamt einen Gewinn oder Verlust gemacht hat, hängt von der Größe der Beträge s_A und s_B ab."

Wir haben beides mal denselben Sachverhalt beschrieben. Der Vorteil der zweiten Formulierung besteht darin, dass man umständliche sprachliche Konstruktionen wie „das Doppelte der von Adrian erhaltenen Summe" durch einfachere Formulierungen wie „das Doppelte von s_A" ersetzen kann.[40]

Eine weitere Beobachtung: Sogar in der ersten Formulierung kommen genau genommen schon Variablen vor: Für den beschriebenen Sachverhalt ist es ja völlig irrelevant, ob die Personen tatsächlich Adrian, Berta und Christina heißen – wir verstehen intuitiv sofort, dass sich nichts ändert, wenn wir die Namen durch andere ersetzen. Solange wir uns nicht auf eine ganze konkrete Situation beziehen, sind also „Adrian", „Berta" und „Christina" auch nur Variablen, die für generische Personen stehen. Wir könnten stattdessen z.B. auch „Person P_1", „Person P_2" und „Person P_3" schreiben.

In Beispiel 1.4.1 kam die Aussage $(r+1)^2 \leq r^2 + 3 \cdot r$ vor. Laut Definition 1.2.1 können wir diesen Ausdruck nur dann als Aussage $(r+1)^2 \leq r^2 + 3 \cdot r$ bezeichnen, wenn feststeht, ob die Ungleichung wahr oder falsch ist. Ob die Ungleichung wahr oder falsch ist, hängt aber vom Wert von r ab – zum Beispiel ist sie für $r = 0$ falsch!

Deshalb ist es sehr wichtig, dass es sich bei der Ungleichung $(r+1)^2 \leq r^2 + 3 \cdot r$ für jede reelle Zahl r um eine eigene Aussage handelt! Für $r = 4$ handelt es sich beispielsweise um die (wahre) Aussage $(4+1)^2 \leq 4^2 + 3 \cdot 4$; für $r = 0$ handelt es sich um die (falsche) Aussage $(0+1)^2 \leq 0^2 + 3 \cdot 0$.

D.h. die Ungleich $(r+1)^2 \leq r^2 + 3 \cdot r$ ist eine Kurzform für unendlich viele Aussagen, von denen manche wahr und manche falsch sind. Um generell mit solche Situationen umgehen zu können, ist die folgende Notation nützlich:

Notation 1.4.2. Wenn wir mehrere Aussagen betrachten, die von einer Variablen abhängen, so ist die folgende Notation häufig nützlich: Wir fassen die Aussagen mit einem Buchstaben – zum Beispiel A – zusammen und bringen die Abhängigkeit

[40] Noch etwas einfacher wird es natürlich, wenn man auch Formeln verwendet. Dann kann man z.B. anstelle von „Das Doppelte von s_A" einfach „$2s_A$" schreiben.

von der Variablen zum Ausdruck, in dem wir anschließend die Variablen in runden Klammern angeben.

Um das zu erläutern, betrachten wir nochmals das zuvor besprochene Beispiel:

Beispiel 1.4.3. Für jede reelle Zahl r bezeichnen wir mit die Aussage $A(r)$ die Aussage „$(r+1)^2 \leq r^2 + 3 \cdot r$“.

Aus Beispiel 1.4.1(b) wissen Sie bereits, dass die Aussage $A(r)$ für jede reelle Zahl $r \geq 1$ wahr ist.

Andererseits ist die Aussage $A(r)$ für jede reelle Zahl $r < 1$ falsch.[41]

Folgende Bemerkung ist wichtig, um korrekt mit Aussagen umzugehen, die von einer Variablen abhängen:

Bemerkung 1.4.4. Wenn Sie über Aussagen sprechen, die von einer Variablen abhängen – nennen wir die Variable zum Beispiel x und die Aussage $A(x)$ –, ist es wichtig, klar zum Ausdruck zu bringen, welche Werte für x Sie betrachten. Dies ist erstens nötig, um der Leserin oder dem Leser den richtigen Kontext zu vermitteln; und zweitens um sicherzustellen, dass $A(x)$ überhaupt eine sinnvolle Aussage ist (egal, ob die Aussage wahr oder falsch ist, zunächst muss es überhaupt eine Aussage sein).

Lassen Sie uns drei einfache Beispiele hierzu ansehen:

(a) Stellen Sie sich vor, jemand schreibt folgendes auf:

$$\text{Mit } A(x) \text{ bezeichnen wir die Aussage „}\tfrac{1}{x} \leq x\text{“.}$$

Es ist im Prinzip gar nicht möglich, zu verstehen, was genau hier gemeint ist, denn Sie können als Leserin oder Leser gar nicht wissen, was x überhaupt sein soll.[42]

(b) Geringfügig besser wäre es, wenn jemand folgendes schreibt:

$$\text{Für jede reelle Zahl } x \text{ bezeichnen wir mit } A(x) \text{ die Aussage „}\tfrac{1}{x} \leq x\text{“.}$$

Nun wissen Sie beim Lesen zumindest, dass x eine reelle Zahl sein soll. Wirklich Sinn ergibt das ganze trotzdem noch nicht, denn was genau soll mit $A(0)$ gemeint sein?

Beachten Sie hier unbedingt, dass $A(0)$ nicht etwa falsch ist – es lässt sich gar nicht entscheiden, ob $A(0)$ wahr oder falsch ist, denn der Bruch $\frac{1}{0}$ in der

[41] Versuchen Sie sich – als eine kleine Aufgabe – herauszufinden, warum $A(r)$ für $r < 1$ falsch ist.

[42] In diesem einfachen Fall können Sie mit etwas Fantasie vielleicht noch erraten, dass mit x wohl eine reelle Zahl gemeint ist – aber selbst das ist nicht wirklich klar, und Sie werden schon bald so viele verschiedene mathematische Objekte kennenlernen, dass es unmöglich sein wird, einfach zu erraten, welcher Typ von Objekt mit einer bestimmten Variable gemeint ist.

Ungleichung „$\frac{1}{0} \leq 0$“ ist schlichtweg nicht definiert. Also handelt es sich bei $A(0)$ gar nicht um eine Aussage.[43]

(c) Sinnvoll ist es zum Beispiel, wenn jemand schreibt:

Für jede Zahl $x \in \mathbb{R} \setminus \{0\}$ bezeichnen wir mit $A(x)$ die Aussage „$\frac{1}{x} \leq x$.“

Für jede reelle Zahl x, die nicht 0 ist, ist $A(x)$ nun tatsächlich eine Aussage. Die Aussage $A(2)$ ist zum Beispiel wahr, die Aussage $A(\frac{1}{2})$ ist hingegen falsch.[44]

Und-Verknüpfung und oder-Verknüpfung beliebig vieler Aussagen: Der Allquantor und der Existenzquantor

In Definitionen 1.2.5 und 1.2.7 haben wir aus zwei Aussagen durch und-Verknüpfung bzw. oder-Verknüpfung eine neue Aussage konstruiert. Mit Hilfe von Variablen können wir, wie soeben beschrieben, auch über unendlich viele Aussagen sprechen. Man kann auch unendlich viele Aussagen mit einem „und“ bzw. einem „oder“ verknüpfen. Um dies sprachlich präzise zu machen, benutzt man den sogenannten **Allquantor** und den sogenannten *Existenzquantor*:

Definition 1.4.5 (Allquantor und Existenzquantor)**.** Sei M eine Menge, und für jedes $x \in M$ sei eine Aussage $A(x)$ gegeben.

(a) Wir definieren mit Hilfe der gegebenen Aussagen $A(x)$ eine neue Aussage

$$\forall x \in M : \ A(x)$$

folgendermaßen:[45] Sie hat den Wahrheitswert „wahr“, wenn $A(x)$ für jedes x in M wahr ist, und sie hat den Wahrheitswert „falsch“, wenn es mindestes ein $x \in M$ gibt, für welches $A(x)$ falsch ist.

Man liest diese Aussage vor als „Für alle x in M gilt A von x.“ Das Symbol $\forall$ bezeichnet man als **Allquantor**.[46]

[43] Für mathematische Behauptungen, die weder wahr noch falsch, sondern in Wirklichkeit gar keine mathematischen Aussagen sind, verwenden Zyniker manchmal die englische Beschreibung „not even false“, was sich in etwa mit „noch nicht einmal falsch“ übersetzen lässt.

[44] Überlegen Sie sich bei Gelegenheit einmal, für welche $x \in \mathbb{R} \setminus \{0\}$ die Aussage $A(x)$ wahr ist und für welche $x \in A(x)$ sie falsch ist.

[45] Den Doppelpunkt hinter „$\forall x \in M$“ kann man genau genommen auch weglassen. Im täglichen Umgang mit logischen Ausdrücken ist es aber oft nützlich, ihn zu verwenden, da komplizierte Aussagen hierdurch etwas übersichtlicher werden.

[46] Man kann es etwas unglücklich finden, dass als Allquantor das „nach oben geöffnete“ Symbol $\forall$ verwendet wird, während das logische und mit dem „nach unten geöffneten“ Symbol $\wedge$ bezeichnet wird. Allerdings haben sich diese Symbole eingebürgert, und man gewöhnt sich recht schnell daran.

Vielleicht hilft Ihnen am Anfang auch die folgende Eselsbrücke: Der Allquantor $\forall$ sieht aus wie ein umbedrehtes „A“ aus dem Wort „Alle“.

(b) Sei M eine Menge, und für jedes $x \in M$ sei eine Aussage $A(x)$ gegeben. Dann definieren wir eine neue Aussage

$$\exists x \in M : \ A(x)$$

folgendermaßen:[47] Sie hat den Wahrheitswert „wahr“, wenn es mindestes ein $x \in M$ gibt, für welches $A(x)$ wahr ist, und sie hat den Wahrheitswert „falsch“, wenn $A(x)$ für alle x in M falsch ist.

Man liest diese Aussage vor als „Es gibt x in M, für das A von x gilt“, oder als „Es gibt ein x in M, für das gilt: A von x.“[48] Das Symbol $\exists$ bezeichnet man als **Existenzquantor**.

Es ist wichtig, sich den Zusammenhang mit der und-Verknüpfung und der oder-Verknüpfung von Aussagen klarzumachen:

Beispiel 1.4.6. Lassen Sie uns mit $A(1)$ die Aussage

„Friedrich Schiller hat das Drama *Die Räuber* geschrieben“

bezeichnen, mit $A(2)$ die Aussage

„Conrad F. Meyer hat das Gedicht *Die Brück' am Tay* geschrieben“,

und mit $A(3)$ die Aussage

„Max Frisch hat *Herr Biedermann und die Brandstifter* geschrieben“.

Für jedes $n \in \{1, 2, 3\}$ haben wir hier also eine Aussage $A(n)$.[49] Die Aussage $A(1)$ ist wahr, die Aussage $A(2)$ is falsch, und die Aussage $A(3)$ ist wahr. Aus diesen Aussagen können wir neue Aussagen konstruieren:

(a) Die Aussage $A(1) \wedge A(2) \wedge A(3)$ kann man auch in der Form

$$\forall n \in \{1, 2, 3\} : \ A(n)$$

schreiben. Sie ist falsch (weil $A(2)$ falsch ist).

(b) Die Aussage $A(1) \wedge A(3)$ kann man auch in der Form

$$\forall n \in \{1, 3\} : \ A(n)$$

schreiben. Sie ist wahr (weil $A(1)$ und $A(3)$ beide wahr sind).

[47] Auch hier kann man den Doppelpunkt hinter „$\exists x \in M$“ genau genommen weglassen, aber es ist häufig übersichtlicher, ihn mit anzuschreiben.

[48] Wenn man sich noch etwas klarer und unmissverständlicher ausdrücken will, kann man zum Beispiel die Formulierung „Es gibt mindestens ein x in $M \ldots$“ anstelle von „Es gibt ein x in $M \ldots$“ verwenden.

[49] Hier können Sie übrigens beobachten: Variablen, die für Zahlen stehen, müssen nicht unbedingt verwendet werden, um Größen zu beschreiben, mit denen man rechnen möchte. Man kann sie auch schlicht benutzen, um Ding durchzunummerieren.

(c) Die Aussage $A(1) \vee A(2) \vee A(3)$ kann man auch in der Form

$$\exists n \in \{1, 2, 3\} : \ A(n)$$

schreiben. Sie ist wahr (weil z.B. $A(1)$ wahr ist).

(d) Die Aussage $A(2) \vee A(3)$ kann man auch in der Form

$$\exists n \in \{2, 3\} : \ A(n)$$

schreiben. Sie ist wahr (weil $A(3)$ wahr ist).

Sie fragen sich vermutlich, wozu der Allquantor und der Existenzquantor taugen, wenn wir doch auch einfach die Symbole $\wedge$ bzw. $\vee$ verwenden können. Hier sind einige Situationen, in denen der Allquantor (bzw. Existenzquantor) sehr nützlich ist:

- Wenn Sie sehr viele Aussagen mit einer und-Verknüpfung (bzw. einer oder-Verknüpfung) verknüpfen möchten.
- Wenn Sie sogar unendlich viele Aussagen mit einer und-Verknüpfung (bzw. einer oder-Verknüpfung) verknüpfen möchten.
- Wenn Sie die Menge, aus der die Variablen stammen, die Sie mit einer und-Verknüpfung (bzw. einer oder-Verknüpfung) verknüpfen möchten, nicht genauer spezifiziert ist.

Lassen Sie uns für die und- bzw. oder-Verknüpfung von unendlich vielen Aussagen mit Hilfe von Quantoren noch ein Beispiel besprechen:

Beispiele 1.4.7. Lassen Sie uns noch einmal die Ungleichung $(r+1)^2 \leq r^2 + 3r$ für reelle Zahlen r betrachten.

(a) Die Aussage

$$\forall r \in \mathbb{R} : \ (r+1)^2 \leq r^2 + 3r$$

ist falsch (weil die Ungleichung zum Beispiel für $r = 0$ falsch ist).

(b) Wenn wir aber die Menge $L \coloneqq \{x \in \mathbb{R} \mid \ x \geq 1\}$ betrachten, dann ist die Aussage

$$\forall r \in L : \ (r+1)^2 \leq r^2 + 3r$$

wahr.

Übrigens ist es natürlich etwas umständlich, extra die Menge L einzuführen um auszudrücken, dass der Allquantor sich auf alle reellen Zahl, die größer oder gleich 1 sind, bezieht. Deshalb kombiniert man den Quantor häufig mit einfach

natürlichsprachlichen Ausdrücken um dasselbe zum Ausdruck zu bringen; zum Beispiel so:

$$\forall r \in \mathbb{R} \text{ mit } r \geq 1 : \ (r+1)^2 \leq r^2 + 3r.$$

Diese Aussage kann man zum Beispiel folgendermaßen vorlesen: „Für alle r in $\mathbb{R}$ mit $r \geq 1$ gilt $(r+1)^2 \leq r^2 + 3r$.“ Oder noch etwas ausführlicher: „Für alle r in $\mathbb{R}$ mit der Eigenschaft $r \geq 1$ gilt $(r+1)^2 \leq r^2 + 3r$.“

(c) Die Aussage

$$\exists r \in \mathbb{R} : \ (r+1)^2 \leq r^2 + 3r$$

ist wahr, weil z.B. Ungleichung $(4+1)^2 \leq 4^2 + 3 \cdot 4$ wahr ist.

Im Kontext der vorangehenden Beispiele hier nochmals ein wichtiger Hinweis: Bitte achten Sie, wie bereits früher erwähnt, darauf, dass alle Aussagen, die Sie vorlesen, grammatisch sinnvolle Sätze ergeben müssen. Wenn Sie eine Aussage vorlesen und den Eindruck haben, dass das, was Sie sagen, grammatisch keinen Sinn ergibt, dann halten Sie inne und versuchen Sie, das Vorgelesene zu korrigieren.

Bemerkung 1.4.8 (Quantifizierung über die leere Menge)**.** In Definition 1.4.5 ist auch der Fall zugelassen, dass die Menge M leer ist. In diesem Fall ist die Aussage

$$\forall x \in M : \ A(x)$$

wahr[50], und die Aussage

$$\exists x \in M : \ A(x)$$

falsch.[51]

In der formalen Logik wird übrigens sehr präzise beschrieben, wie genau die Quantoren $\forall$ und $\exists$ zu verwenden sind (wesentlich genauer, als wir dies hier tun). Für den alltäglichen Gebrauch in der Mathematik genügt es aber oft, sich das Symbol $\forall$ tatsächlich als Abkürzung für „für alle“ zu denken, und sich das Symbol $\exists$ als Abkürzung von „es gibt ein“ zu denken.

Entsprechend wird es häufig vorkommen, dass wir anstelle der Symbole $\forall$ und $\exists$ einfach die Worte „für alle“ und „es gibt ein“ ausschreiben.

Exklusiv-oder-Verknüpfung beliebig vieler Aussagen

Es gibt noch einen weiteren Quantor, der immer von Bedeutung ist, weil er eine die exklusiv-oder-Verknüpfung auf beliebig viele Aussagen verallgemeinert:

[50] Bitte überlegen Sie sich in Ruhe, weshalb.
[51] Bitte überlegen Sie sich auch hier in Ruhe, weshalb.

Definition 1.4.9 (Existenz- und Eindeutigkeitsquantor)**.** Sei M eine Menge, und für jedes $x \in M$ sei eine Aussage $A(x)$ gegeben. Dann definieren wir eine neue Aussage

$$\exists! x \in M : \ A(x)$$

folgendermaßen:[52] Sie hat den Wahrheitswert „wahr“, wenn es genau ein $x \in M$ gibt, für welches $A(x)$ wahr ist (und $A(x)$ somit für alle anderens $x \in M$ falsch ist). Sie hat den Wahrheitswert „falsch“, wenn $A(x)$ für alle $x \in M$ falsch ist oder wenn $A(x)$ für mindestens zwei verschiedene $x \in M$ wahr ist.

Man liest diese Aussage vor als „Es gibt genau ein x in M, für das A von x gilt“.

Beispiele 1.4.10. (a) Die Aussage

$$\exists! x \in \mathbb{R} : \quad x^2 = 4$$

ist falsch, denn es gibt zwei reelle Zahlen, deren Quadrat gleich 4 ist (nämlich 2 und -2).

(b) Die Aussage

$$\exists! x \in \mathbb{R} : \quad x^2 = 4 \ \wedge \ x \geq 0$$

ist hingegen wahr, denn es gibt genau eine reelle Zahl, deren Quadrat gleich 4 ist und die zugleich größer oder gleich 0 ist (nämlich die Zahl 2).

(c) Die Aussage

$$\exists! x \in \mathbb{R} : \quad x^2 = -1$$

ist falsch, denn es gibt gar keine reelle Zahl, deren Quadrat gleich -1 ist.

Verneinung und Verschachtelung von Quantoren

Sie werden sehr häufig in die Situation kommen (insbesondere in der Analysis, aber auch bereits im aktuellen Semester in der Linearen Algebra 1), die Sie Aussagen, die Quantoren enthalten, verneinen müssen. Anhand der Definition des All- und de Existenzquantors in Definition 1.4.5 kann man sich leicht überlegen, wie das funktioniert:

Bemerkung 1.4.11 (Verneinung von Aussagen, die Quantoren enthalten)**.** Sei M eine Menge und für jedes $x \in M$ sei eine Aussage $A(x)$ gegeben. Dann gilt:

(a) Die Aussage

$$\neg(\forall x \in M : \ A(x))$$

hat denselben Wahrheitswert wie die Aussage

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

[52] Manche Autorinnen und Autoren verwenden anstelle des Symboll $\exists!$ das Symbol $\exists_1$.

(b) Die Aussage

$$\neg(\exists x \in M : \ A(x))$$

hat denselben Wahrheitswert wie die Aussage

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

Richtig interessant wird es, wenn man Aussagen baut, in denen mehrere Quantoren verschachtelt sind. Auch dies kommt sehr häufig vor; hier ein Beispiel mit einer ersten Kostprobe:

Beispiel 1.4.12 (Verschachtelung von Quantoren)**.** Es bezeichne A die Aussage

$$\forall k \in \mathbb{N} : \ \exists n \in \mathbb{N} : \ n^2 \geq k + 1,$$

und es bezeichne B die Aussage

$$\exists n \in \mathbb{N} : \ \forall k \in \mathbb{N} : \ n^2 \geq k + 1.$$

Dann ist A wahr, B hingegen nicht.

Daran können Sie erkennen, dass man Quantoren nicht einfach vertauschen darf – es kommt auf die Reihenfolge an! Dieses Beispiel werden Sie in den Tutorien noch genauer besprechen.

Durchschnitte und Vereinigungen von Mengen: Noch einmal

In Definition 1.3.14 hatten wir mit Hilfe des logischen Unds und des logischen Oders den Durchschnitt und die Vereinigung von je zwei Mengen definiert. Ebenso kann man mit Hilfe des Allquantors- und mit Hilfe des Existenz-Quantors den Durchschnitt und die Vereinigung von beliebig vielen Mengen definieren:

Definition 1.4.13 (Durchschnitt und Vereinigung beliebig vieler Mengen)**.** Sei I eine nicht-leere Menge und für jedes $i \in I$ sei eine Menge M_i gegeben.

(a) Die Menge

$$\bigcap_{i \in I} M_i \coloneqq \{x \mid \ \forall i \in I : \ x \in M_i\}$$

heißt der **Durchschnitt** der Mengen M_i für $i \in I$.

(b) Die Menge

$$\bigcup_{i \in I} M_i \coloneqq \{x \mid \ \exists i \in I : \ x \in M_i\}$$

heißt die **Vereinigung** der Mengen M_i für $i \in I$.

Wenn man zwei Mengen M_1, M_2 gegeben hat (d.h., wenn $I = \{1, 2\}$ ist), kann man sehen, dass

$$\bigcap_{i\in\{1,2\}} M_i = \{x \mid \forall i \in \{1,2\} : \ x \in M_i\} = \{x \mid \ x \in M_1 \ \wedge \ x \in M_2\} = M_1 \cap M_2.$$

gilt.[53] Ebenso kann man sehen, dass in diesem Fall

$$\bigcup_{i\in\{1,2\}} M_i = M_1 \cup M_2$$

gilt.[54]

Implikationen und Äquivalenz

Nun kommen wir noch einmal zurück zur Verknüpfung von Aussagen (zunächst ganz ohne Variablen; in Abschnitt 1.2 hatten wir bereits mehrere Verknüpfungen von Aussagen eingeführt. Nun folgen noch drei weitere Verknüpfungen:

Definition 1.4.14 (Implikationen und Äquivalenz)**.** Seien A und B beliebige Aussagen. Wir definieren drei weitere Aussagen $A \Rightarrow B$, $A \Leftarrow B$, $A \Leftrightarrow B$, deren Werte durch die folgenden Wahrheitstabellen festgelegt werden:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

A	B	$A \Leftarrow B$
w	w	w
w	f	w
f	w	f
f	f	w

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

Für die so definierten Aussagen verwenden wir die folgenden Sprechweisen:

(a) Die Aussage $A \Rightarrow B$ wird als „A impliziert B“ ausgesprochen, oder als „Wenn A, dann auch B“, oder als „Aus A folgt B“. Manchmal sagt man stattdessen auch „A ist hinreichend für B“ oder „B ist notwendig für A“.[55]

[53] Hier haben wir also die Mengengleichheit $\bigcap_{i\in\{1,2\}} M_i = M_1 \cap M_2$ bewiesen, indem wir die Menge $\bigcap_{i\in\{1,2\}} M_i$ solange anders dargestellt haben – ohne die Menge selbst dabei zu verändern – bis wir die Menge $M_1 \cap M_2$ erhalten haben. Selbstverständlich kann man die Mengengleichheit $\bigcap_{i\in\{1,2\}} M_i = M_1 \cap M_2$ aber auch zeigen, indem man die Methode verwendet, die im Beweis von Proposition 1.3.15 vorgestellt wurde – d.h., indem man die beiden Inklusionen „$\subseteq$“ und „$\supseteq$“ einzeln beweist.. Davon überzeugen Sie sich am besten, indem Sie es auf einem Blatt Papier (oder auf einem Tablet) selbst versuchen.

[54] Überprüfen Sie für hier die Details unbedingt auf einem Blatt Papier noch einmal selbst um sicherzustellen, dass Sie das richtig verstanden haben.

[55] Bei einem Feierabendbier können Sie sich ein wenig den Kopf darüber zerbrechen, weshalb man hier die Begriffe „hinreichend“ und „notwendig“ verwendet. Oder Sie bleiben lieber bei drei erst genannten Formulierungen, die intuitiv vermutlich etwas klarer sind.

(b) Weil die Aussage $A \Leftarrow B$ immer denselben Wahrheitswert wie $B \Rightarrow A$ hat, spricht man sie genauso aus wie $B \Rightarrow A$.[56]

(c) Die Aussage $A \Leftrightarrow B$ wird ausgesprochen als „A ist äquivalent zu B“ oder als „A genau dann, wenn B“ oder als „A dann und nur dann, wenn B“.

Bevor wir genauer darauf eingehen, was es mit den Implikationen $A \Rightarrow B$ und $B \Rightarrow A$ auf sich hat, sind zwei Bemerkungen sinnvoll:

Bemerkungen 1.4.15. (a) Die Äquivalenz $A \Leftrightarrow B$ ist in genau denjenigen Fällen wahr, in denen A und B den gleichen Wahrheitswert haben. Zu sagen „Es gilt die Äquivalenz $A \Leftrightarrow B$“ ist somit eine andere Möglichkeit um zu sagen „A und B haben denselben Wahrheitswert.“

Auf diese Weise kann man einige der Resultate aus Abschnitt 1.2 formulieren, indem man Äquivalenzen verwendet. Zum Beispiel besagt Proposition 1.2.10(a) für jede Aussage A und jede Aussage B folgendes: die Aussage $\neg(A \wedge B)$ hat immer denselben Wahrheitswert wie die Aussage $(\neg A) \vee (\neg B)$. Genauso gut könnten wir auch sagen: es gilt stets

$$\Big(\neg(A \wedge B)\Big) \Leftrightarrow \Big((\neg A) \vee (\neg B)\Big).$$

(b) Mit Hilfe einer Wahrheitstabelle kann man sich leicht von folgendem überzeugen:[57] Die Aussage $A \Leftrightarrow B$ hat stets denselben Wahrheitswert wie die Aussage $(A \Rightarrow B) \wedge (A \Leftarrow B)$.[58]

Also bedeutet „A ist äquivalent zu B“ dasselbe wie „Aus A folgt B und aus B folgt A“.

Diese harmlos anmutende Beobachtung wird Sie den Rest Ihres Studiums verfolgen, den sehr viele Resultate in der Mathematik sind als Äquivalenzen formuliert, und diese werden meist bewiesen, indem man die beiden Implikationen einzeln beweist.

Wie versprochen besprechen wir nun, was es mit der Implikation $A \Rightarrow B$ auf sich hat.[59] Erfahrungsgemäß fällt es vielen Studierenden am Anfang schwer, die vorletzte Zeile in der Wahrheitstabelle von $A \Rightarrow B$ intuitiv nachzuvollziehen – warum sollte es richtig sein zu sagen, dass aus etwas Falschem etwas Wahres folgt? Am einfachsten können Sie dies vermutlich nachvollziehen, wenn Sie nicht nur einzelne Aussagen betrachten, sondern Aussagen, die von einer Variablen abhängen:

[56] Also z.B. als „B impliziert A“ oder „Aus B folgt A“.

[57] Und das sollten Sie sogleich auf einem Blatt Papier tun!

[58] Übrigens können Sie hier gleich testen, ob Sie Teil (a) der Bemerkung verstanden haben: Wie können Sie den Satz, der mit dieser Fußnote abschließt, stattdessen formulieren, wenn Sie anstelle der Worte “stets denselben Wahrheitswert” lieber einen Äquivalenzpfeil verwenden möchten?

[59] Sobald Sie diese Implikation wirklich verstanden haben, verstehen Sie automatisch auch die Bedeutung der Implikation $B \Rightarrow A$ (denn hierbei sind ja nur die Bezeichnungen der Aussagen vertauscht) und somit auch die Implikation $A \Leftarrow B$ (weil diese ja äquivalent zu $B \Rightarrow A$ ist).

Diskussion 1.4.16. Sei M eine Menge, und für jedes $x \in M$ seien Aussagen $A(x)$ und $B(x)$ gegeben. Wie Sie bereits wissen, kann es passieren, dass $A(x)$ für manche $x \in M$ wahr ist, und für andere $x \in M$ falsch; ebenso kann es passieren, dass $B(x)$ für manche x aus M wahr ist, für andere hingegen nicht. Diejenigen x, für die $A(x)$ wahr ist, müssen natürlich nicht unbedingt dieselben sein, für die auch $B(x)$ wahr ist.

Nun will man in konkreten Situationen häufig wissen, wie die Aussagen $A(x)$ und $B(x)$ zusammenhängen. Besonders interessant ist zum Beispiel die folgende Situation, die wir zunächst umgangssprachlich beschreiben:

$$\text{Für jedes } x \text{ in } M \text{ gilt: Wenn } A(x) \text{ gilt, muss auch } B(x) \text{ gelten.} \tag{1.4.3}$$

Beachten Sie, dass „Wenn $A(x)$ gilt, muss auch $B(x)$ gelten“, kein Aussage darüber macht, was passiert, wenn $A(x)$ falsch ist. Wir können (1.4.3) also auch folgendermaßen formulieren:

Für jedes x in M tritt einer der folgenden beiden Fälle auf:
(i) $A(x)$ and $B(x)$ sind beide wahr; (ii) $A(x)$ ist falsch;

oder etwas kürzer und formallastiger aufgeschrieben:

$$\forall x \in M : \ \big(A(x) \wedge B(x)\big) \vee \big(\neg A(x)\big).$$

Nun hat $\big(A(x) \wedge B(x)\big) \vee \big(\neg A(x)\big)$ stets denselben Wahrheitswert wie $A(x) \Rightarrow B(x)$ lauft Definition 1.4.14.[60,61]

Das heißt, die Wahrheitstablle für die Implikation in Definition 1.4.14 erlaubt es uns, die Aussage (1.4.3) in der Form

$$\forall x \in M : \ (A(x) \Rightarrow B(x))$$

zu schreiben[62] – und das ist ja durchaus intuitiv.

Zum Abschluss dieses Abschnitts wollen wir noch einmal demonstrieren, wie man Äquivalenzen verwenden kann um mathematische Resultate zu formulieren – und wie man Bemerkung 1.4.15(b) verwenden kann, um solche Resultate zu beweisen. Als Anschauungsobjekt verwenden wir das folgende Resultat:

Proposition 1.4.17. *Seien L, M Mengen. Dann gilt*

$$L \subseteq M \quad \Leftrightarrow \quad L \cap M = L.$$

[60] Achtung: Glauben Sie das nicht einfach! Seien Sie kritisch und überzeugen Sie sich selbst, indem Sie alle vier möglichen Fälle durchgehen.

[61] Der spannenste Fall ist hier natürlich derjenige, in dem uns die linksstehende Wahrheitstabelle aus Definition 1.4.14 auf den ersten Blick unintuitiv erscheint – also, wenn $A(x)$ falsch und $B(x)$ wahr ist. In diesem Fall ist $\big(A(x) \wedge B(x)\big) \vee \big(\neg A(x)\big)$ wahr, und dies erklärt, warum der Eintrag in der vorletzten Zeile der Wahrheitstabelle so gewählt wird, wie in Definition 1.4.14 beschrieben.

[62] Die Klammer um $A(x) \Rightarrow B(x)$ haben wir hier nur der einfacheren Lesbarkeit halber hinzugefügt.

Die Proposition besagt also in Worten: Für zwei Mengen M und L ist die Teilmengenbeziehung $L \subseteq M$ genau dann erfüllt, wenn der Durschnitt $L \cap M$ gleich L ist. Wir beweisen die Proposition in Kürze. Vorher aber ist folgende Bemerkung extrem wichtig:

Bemerkung 1.4.18. In Proposition 1.4.17 sehen Sie eine Sprechweise, die in mathematischen Resultaten sehr üblich ist: Man beginnt mit dem Wort „Seien“ und führt dann einige Objekte ein. Anschließend macht man eine Aussage über diese Objekt.

Diese Formulierung ist als eine Verwendung eines Allquantors zu verstehen, nur dass sie sprachlich über mehrere Sätze verteilt ist. Die komplette Aussage von Proposition 1.4.17 könnte man zum Beispiel ganz knapp und formal auch in folgender Form schreiben:

$$\forall \text{ Mengen } L, M: \qquad L \subseteq M \quad \Leftrightarrow \quad L \cap M = L.$$

Beweis von Proposition 1.4.17. Unser Ziel ist es, eine Äquivalenz zu beweisen. Laut Bemerkung 1.4.15(b): ist dies gleichbedeutend damit, die beiden Implikationen

$$L \subseteq M \quad \Rightarrow \quad L \cap M = L.$$

und

$$L \subseteq M \quad \Leftarrow \quad L \cap M = L.$$

zu beweisen. Dies tun wir im Folgenden.

“$\Rightarrow$” Es gelte $L \subseteq M$. Wir müssen $L \cap M = L$ zeigen, und dies tun wir wie üblich, indem wir beide Inklusionen zeigen.

- “$\subseteq$” Sei $x \in L \cap M$ beliebig, aber fest. Dann gilt wegen der Definition des Durchschnitts automatisch $x \in L$. Somit ist gezeigt, dass $L \cap M \subseteq L$ gilt.
- “$\supseteq$” Sei $x \in L$ beliebig, aber fest. Weil $L \subseteq M$ ist, gilt dann auch $x \in M$. Das heißt, insgesamt gilt $x \in L$ und $x \in M$, also $x \in L \cap M$. Somit haben wir $L \subseteq L \cap M$ gezeigt.

Insgesamt ist also $L \cap M = L$.

“$\Leftarrow$“ Sei nun $L \cap M = L$. Wir müssen $L \subseteq M$ zeigen.

Sei also $x \in L$ beliebig aber fest. Wegen der Voraussetzung $L \cap M = L$ gilt dann auch $x \in L \cap M$, und somit $x \in M$. Somit haben wir $L \subseteq M$ gezeigt. □

Kapitel 2

Funktionen

Einstiegsfragen. (a) Finden Sie eine Gemeinsamkeit zwischen den folgenden fünf Dingen? (i) Ein Telefonbuch; (ii) der Verlauf des DAX über die letzten sechs Monate; (iii) der Sachindex eines Fachbuchs; (iv) eine aktuelle Tabelle der Fußballbundesliga; (v) ein Radiosignal, dass Sie mit einem Autoradio empfangen.

(b) Können Sie eine möglichst einfache Funktion von $\mathbb{R} \to \mathbb{R}$ angeben? Und auch eine nicht ganz so einfache?

Was ist die komplizierteste Funktion von $\mathbb{R}$ nach $\mathbb{R}$, die Ihnen spontan einfällt?

(c) Wie viele Elemente hat die Menge $\{1, 2, 5, 6\}$? Wie viele Elemente hat die leere Menge?

(d) Wie viele Elemente hat $\mathbb{Z}$? Hat $\mathbb{Q}$ genauso viele Elemente von $\mathbb{Z}$? Und hat $\mathbb{R}$ genauso viele Elemente von $\mathbb{Z}$?

2.1 Was ist eine Funktion?

Was ist eine Funktion?

Bisher haben wir nicht nur über mathematisch Aussagen gesprochen, sondern auch über verschiedene mathematische Objekte: Zum Beispiel Zahlen, Mengen und Tupel. Um die Mathematik wirklich „zum Leben zu erwecken“, brauchen wir aber noch einen weiteren Typ von mathematischen Objekten: **Funktionen**.

Definition 2.1.1 (Funktion/Abbildung)**.** Seien X, Y Mengen. Eine **Funktion** (oder **Abbildung**) f von X nach Y ist eine Zuordnungsvorschrift, die jedem Element $x \in X$ ein eindeutig bestimmtes Element aus Y – welches wir mit $f(x)$ bezeichnen – zuweist.

Wir nennen X den **Definitionsbereich** von X und Y den **Wertebereich** von f.

Beachten Sie unbedingt: Um eine Funktion konkret anzugeben, müssen Sie auf jeden Fall auch den Definitions- und den Wertebereich angeben. Funktionen erhalten nicht auf magische Weise von selbst einen Werteebereich,[1] sondern der Definitionsbereich der Funktion muss explizit angegeben werden, wenn man eine Funktion angibt. Ohne Angabe des Definitionsbereich kann man eine Funktion nicht wirklich verstehen.

Wenn man keine Lust hat, Sätze wie „Sei f eine Funktion von X nach Y“ jedes mal auszuschreiben, ist folgende Notation nützlich:

Notation 2.1.2. Seien X, Y Mengen. Jede der folgenden beiden Notationen wird synonym mit dem Satz „Sei f eine Funktion von X nach Y“ verwendet:

(a) Sei $f : X \to Y$.

(b) Sei $X \xrightarrow{f} Y$.

Verschiedene Arten um Funktionen zu beschreiben

Bis jetzt haben wir lediglich abstrakt gesagt, was man unter einer Funktion versteht. Um mit diesem Begriff arbeiten zu können, brauchen man natürlich Möglichkeiten, um eine Funktion explizit anzugeben. Es gibt verschiedene solche Möglichkeiten; einige wichtige stellen wir im folgenden vor:

Beispiele 2.1.3. Seien X, Y Mengen. Es folgen einige Möglichkeiten um eine konkrete Funktion von X nach Y zu spezifieren.

(a) Wenn X nur endlich viele Elemente hat, kann man eine Funktion $f : X \to Y$ angeben, indem man alle Elemente x von X aufzählt und für jedes dieser Elemente den Wert $f(x)$ konkret angibt – zum Beispiel in einer Tabelle.

Sei zum Beispiel $X = \{1, 2, 3, 4\}$ und $Y = \{-\frac{3}{2}, 0, \pi\}$. Wir definieren eine Funktion $f : X \to Y$ durch die folgende Wertetabelle, in der alle Elemente $x \in X$ aufgezählt sind:

x	1	2	3	4
$f(x)$	0	$-\frac{3}{2}$	0	π

(b) Manche Funktionen lassen sich mit Hilfe von Formeln darstellen. Wir können zum Beispiel eine Funktion $g : \mathbb{R} \to \mathbb{R}$ durch die Formel

$$g(x) = x^3 - 7 \qquad \text{für alle } x \in \mathbb{R}$$

[1] Auch, wenn in der Schule manchmal dieser Eindruck erweckt wird.

definieren.[2,3]

Anstatt „$g(x) = x^3 - 7$ für alle $x \in \mathbb{R}$“ zu schreiben, benutzt man in der Mathematik auch sehr häufig die Notation „$x \mapsto x^3 - 7$“.[4]

Wenn man eine Funktion sehr effizient definieren will, kann man die Notation für Definitions- und Wertebereich sowie die zugehörige Formel[5] auch direkt untereinander schreiben – zum Beispiel kann man eine Funkton h so folgendermaßen beschreiben:

$$\begin{aligned} h : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto 7x - 5. \end{aligned}$$

Übrigens können Funktionen natürlich auch kompliziertere Definitions- und Wertebereiche haben – betrachten Sie als Beispiel die Funktion

$$\begin{aligned} k : \mathbb{R}^2 &\to \mathbb{R}^3, \\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &\mapsto \begin{pmatrix} x_1 + x_2 \\ x_1 - x_2 \\ 2x_1 \end{pmatrix}. \end{aligned}$$

(c) Eine weitere nützliche Möglichkeit um manche Funktionen zu beschreiben ist die Verwendung einer *Fallunterscheidung*. Hier ist ein Beispiel: Es sei[6]

$$\begin{aligned} \ell : \mathbb{R} &\to \mathbb{R}, \\ \ell(z) &= \begin{cases} 2z & \text{falls } z \geq 0, \\ -1 & \text{falls } z < 0. \end{cases} \end{aligned}$$

Natürlich könnte man dasselbe genauso gut mit Hilfe des Pfeils $\mapsto$ zum Ausdruck bringen, indem man stattdessen schreibt: Es sei

$$\ell : \mathbb{R} \to \mathbb{R}$$

[2]Beachten Sie aber unbedingt, dass man nicht jede Funktion von $\mathbb{R}$ nach $\mathbb{R}$ mit solch einer einfachen Formel ausdrücken kann. Man kann sogar beweisen, dass es Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ gibt, die sich gar nicht mit Hilfe einer Formel darstellen lassen!

[3]Übrigens haben wir uns hier ein wenig am eigenen Schopf aus dem Sumpf gezogen: Eine Funktion auf diese Weise zu definieren, ist uns nur deshalb möglich, weil wir bereits einige andere Funktionen kennen und von ihnen hier sehr freigiebig Gebrauch machen: Addition und Multiplikation.
Über Addition, Multiplikation und ähnliche Funktionen werden wir in Abschnitt **??** noch ausgiebig diskutieren.

[4]Beachten Sie hier den vertikalen Strich am Beginn des Pfeils $\mapsto$. Der Pfeil $\to$, mit dem angegeben wird, von wo nach wo die Funktion abbildet, hat diesen Strich nicht.

[5]Sofern sich die Funktion durch eine Formel beschreiben lässt.

[6]In diesem Beispiel sehen Sie übrigens, dass man die Variable keineswegs x nennen muss – auch jede andere Variable ist in Ordnung.

$$z \mapsto \begin{cases} 2z & \text{falls } z \geq 0, \\ -1 & \text{falls } z < 0. \end{cases}$$

Übrigens ist die Spezifizierung einer Funktion mit Hilfe einer Tabelle, die wir in Beispiel (a) besprochen haben, auch nur eine Kurzschreibweise für eine Fallunterscheidung. Beispielsweise kann man die Funktion f aus Beispiel (a) auch folgendermaßen beschreiben:

$$f : \{1,2,3,4\} \to Y, \qquad x \mapsto \begin{cases} 0 & \text{falls } x = 1, \\ -\frac{3}{2} & \text{falls } x = 2, \\ 0 & \text{falls } x = 3, \\ \pi & \text{falls } x = 4. \end{cases}$$

In diesem Fall ist die Tabelle aber vielleicht etwas übersichtlicher.

Funktion, Argument und Funktionswert

In der Mathematik ist die folgende Terminologie üblich:

Konvention 2.1.4 (Argument und Funktionswert)**.** Seien X, Y Mengen und sei $f : X \to Y$. Für ein Element $x \in X$ betrachten wir die Notation „$f(x)$“: in dieser Notation heißt

- $\ldots x$ das **Argument**,
- und $f(x)$ der **Wert von f an dieser Stelle x**.[7]

Die folgende Bemerkung finden Sie auf den ersten Blick wahrscheinlich subtil[8], aber sie ist enorm wichtig um im Laufe der Vorlesung – und im Laufe Ihres restlichen Studiums – korrekt mit Funktionen umzugehen:

Bemerkung 2.1.5 (Funktion vs. Funktionswert)**.** Man muss auf jeden Fall eine *Funktion* von ihren *Funktionswerten* unterscheiden: Seien X, Y Mengen und sei $f : X \to Y$. Es ist *nicht* richtig zu sagen, „$f(x)$ ist eine Funktion“. Die Funktion heißt f, nicht $f(x)$. Mit $f(x)$ ist etwas anderes gemeint: Für ein Element $x \in X$ ist $f(x)$ – wie Sie der vorangehenden Vereinbarung entnehmen können – der Wert von f an der Stelle x. Es handelt sich bei $f(x)$ also um ein Element von Y, während es sich bei f um eine Zuordnung von X nach Y handelt.

Das lässt sich am besten mit Hilfe eines Beispiels veranschaulichen: Sei X die Menge aller Einwohner von Passau, die im Telefon verzeichnet sind, und sei Y die Menge aller in Passau vergebenen Telefonnummern. Dann ist das Telefonbuch von

[7] Oft sagt man hier anstelle von „Wert“ auch etwas länger „Funktionswert“.

[8] Und womöglich steht die Bemerkung auch der Art entgegen, wie Sie in der Schule über Funktionen gedacht oder gesprochen haben.

Passau schlicht und einfach diejenige Funktion f, die jeder Person $x \in X$ ihre Telefonnummer zuordnet. Hier sehen Sie den Unterscheid zwischen f und $f(x)$: Bei f handelt es sich um das gesamte Telefonbuch; bei $f(x)$ handelt es sich um eine einzelne Telefonnummer[9].

Hintereinanderausführung und Gleichheit von Funktionen

Wenn wir zwei Funktionen f und g gegeben haben und der Wertebereich von f mit dem Definitionsbereich von g übereinstimmt, dann können wir die beiden Funktionen zu einer neuen Funktion verknüpfen:

Definition 2.1.6 (Hintereinanderausführung)**.** Seien X, Y, Z Mengen und seien $f : X \to Y$ und $g : Y \to Z$. Dann definieren wir eine Funktion $g \circ f : X \to Z$ durch die Formel[10]

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

Die Funktion $g \circ f$ heißt die **Hintereinanderausführung** (oder **Komposition**) von f und g.

Wenn man anstelle der Notation $f : X \to Y$ und $g : Y \to Z$ die Notation $X \xrightarrow{f} Y$ und $Y \xrightarrow{g} Z$ verwenden[11], lässt sich die Komposition von $g \circ f$ besonders anschaulich in der Form

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

darstellen.

Wir wollen in Kürze das sogenannten *Assoziativgesetz* für die Hintereinanderausführung von Funktionen beweisen.[12] Damit wir dies sinnvoller Weise tun können, müssen wir uns aber zunächst einmal darauf einigen, wann wir zwei Funktionen als **gleich** ansehen.[13]

Definition 2.1.7 (Gleichheit von Funktionen)**.** Zwei Funktionen f und g heißen **gleich**, wenn die drei folgenden Aussagen wahr sind:

[9] Welche Telefonnummer das konkret ist, kann man natürlich nur wissen, wenn man weiß, welche Person gerade mit x gemeint ist.

[10] Beachten Sie hierbei unbedingt die Reihenfolge: Anschaulich gesprochen wird f zuerst ausgeführt und dann erst g – man schreibt in der Notation $g \circ f$ allerdings g nach links.
Der Grund für diese Konvention ist einfach: Man möchte in den beiden Ausdrücken $(g \circ f)(x)$ und $g\big(f(x)\big)$ die Funktionen f und g gerne in derselben Reihenfolge anschreiben.

[11] Die wir ebenfalls in Notation 2.1.2 eingeführt hatten.

[12] Ein Assoziativgesetz für die Addition und die Multiplikation reeller Zahlen kennen Sie bereits aus der Schule; und einige Assoziativgesetze in der Aussagenlogik haben Sie bereits in Proposition 1.2.12 gesehen. Auf dieser Grundlagen können Sie vielleicht jetzt schon erraten, was sich hinter dem Begriff „Assoziativgesetz für die Hintereinanderausführung von Funktionen“ verbirgt.

[13] Denken Sie an dieser Stelle zurück an die Einführung in die Mengentheorie in Abschnitt 1.3: Dort sind wir auch nicht einfach davon ausgegangen, dass schon irgendwie klar sein wird, wann zwei Mengen gleich sind, sondern haben in Definition 1.3.9 exakt festgelegt, wann zwei Mengen gleich heißen.

(I) Die Funktionen f und g haben denselben Definitionsbereich.

(II) Die Funktionen f und g haben denselben Wertebereich.

(III) Für jedes x aus dem Definitionsbereich von f und g gilt $f(x) = g(x)$.

Wir verwenden die Notation $f = g$ um auszudrücken, dass f und g gleich sind.

Nun kommen wir zum bereits angekündigten Assoziativegesetz:

Proposition 2.1.8 (Assoziativgesetz für die Hintereinanderausführung von Funktionen)**.** *Seien W, X, Y, Z Mengen und seien*

$$W \xrightarrow{f} X, \qquad X \xrightarrow{g} Y, \qquad Y \xrightarrow{h} Z$$

Funktionen. Dann gilt

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

Beweis. Laut Proposition 2.1.7 müssen wir folgende Aussagen zeigen:

Gleichheit der Definitionsbereiche und Gleichheit der Wertebereiche: Weil f von W nach X abbildet und $h \circ g$ von X nach Z, bildet $(h \circ g) \circ f$ von W nach Z ab.

Ebenso gilt: Weil $g \circ f$ von W nach Y abbildet und h von Y nach Z, bildet $h \circ (g \circ f)$ von W nach Z ab. Also haben die Funktionen $(h \circ g) \circ f$ und $h \circ (g \circ f)$ beide den Definitionsbereich W und den Wertebereich Z.

Gleichheit der Funktionswerte an allen Elementen des Definitonsbereichs: Wir müssen die Aussage

$$\forall w \in W: \qquad \big((h \circ g) \circ f\big)(w) = \big(h \circ (g \circ f)\big)(w)$$

Um dies zu zeigen, betrachten wir ein beliebiges, aber festes Element $w \in W$.[14] Für dieses Element w gilt zum einen

$$\big((h \circ g) \circ f\big)(w) \overset{\text{Def. 2.1.6}}{=} (h \circ g)\big(f(w)\big) \overset{\text{Def. 2.1.6}}{=} h\Big(g\big(f(w)\big)\Big),$$

und andererseits

$$\big(h \circ (g \circ f)\big)(w) \overset{\text{Def. 2.1.6}}{=} h\big((g \circ f)(w)\big) \overset{\text{Def. 2.1.6}}{=} h\Big(g\big(f(w)\big)\Big).$$

Also sind $\big((h \circ g) \circ f\big)(w)$ und $\big(h \circ (g \circ f)\big)(w)$ tatsächlich gleich. □

[14] Wichtig: Hier sehen Sie (nicht zum ersten mal in dieser Vorlesung) eine extrem wichtige Beweistechnik, die Sie in Ihrem Studium ständig benötigen werden: Wenn man eine Aussage für alle Elemente einer Menge – in der aktuellen Situation heißt sie W – zeigen will, dann betrachtet man hierzu ein einzelnes Element w der Menge; dieses Element fixiert man gedanklich für die Dauer des Beweises (damit man sicher ist, während des kompletten Beweises immer über dasselbe Element zu sprechen), aber man bestimmt *nicht* näher, um welches Element es sich konkret handelt. Dies wird mit der Floskel „Sei $w \in W$ beliebig, aber fest“ zu Beginn des Beweises zum Ausdruck gebracht; das Wort „beliebig“ ist hierbei also im Sinne von „nicht näher bestimmt“ gemeint. Hat man die gewünschte Aussage dann am Ende für dieses Element w bewiesen, so kann man sicher sein, dass die Aussage für alle Elemente von W stimmt – denn weil w ein nicht näher bestimmtes Element von W war, funktioniert der Beweis, den man angegeben hat, für jedes Element von W.

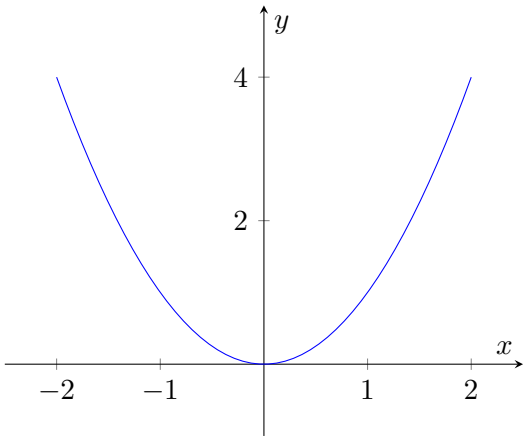

Abbildung 2.2.1: Graph der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$

2.2 Bildliche Darstellung von Funktionen

Es gibt viele verschiedene Möglichkeiten Funktionen graphisch darzustellen. Welche dieser Möglichkeiten sich gut eignet, hängt jeweils von der Funktion ab – und insbesondere von ihrem Definitions- und Wertebereich – ab. Im Folgenden besprechen wir einige Beispiele für solche graphischen Veranschaulichungen.

Beispiel 2.2.1 (Veranschaulichung durch Pfeile zwischen Mengen)**.** Betrachten Sie erneut die Funktion f aus Beispiel 2.1.3(a).

[In der Vorlesung wurde hier an der Tafel gezeigt, wie sich f mit Hilfe von Pfeilen zwischen zwei Mengen veranschaulichen lässt. Im Manuskript fehlt diese Skizze, da ich zeitlich nicht dazu gekommen bin, sie zu erstellen.]

Für die nächsten bildlichen Darstellungen von Funktionen benötigen wir den Begriff des *Funktionsgraphen*.

Definition 2.2.2 (Funktionsgraph)**.** Seien X und Y Mengen und sei $f\colon X \to Y$ eine Funktion. Die Teilmenge

$$\mathrm{Gr}(f) \coloneqq \big\{(x, f(x)) \mid\ x \in X\big\}$$

von $X \times Y$ heißt der **Funktionsgraph** oder kurz der **Graph** von f.

Beispiel 2.2.3 (Der Graph einer Funktion $\boldsymbol{f : \mathbb{R} \to \mathbb{R}}$)**.** Betrachten Sie die Funktion $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Ihr Graph

$$\mathrm{Gr}(f) = \big\{(x, x^2) \mid\ x \in \mathbb{R}\big\} \subseteq \mathbb{R}^2 = \big\{(x, y) \mid\ x, y \in \mathbb{R}\big\}$$

wird in Abbildung 2.2.1 gezeigt:

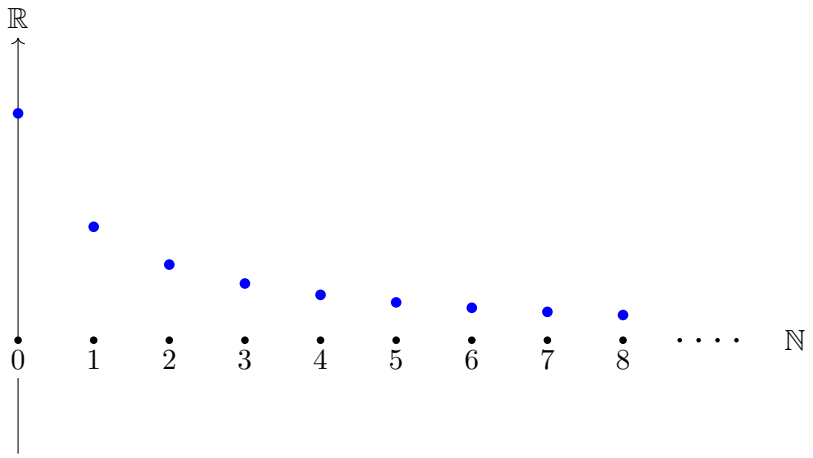

Abbildung 2.2.2: Graph der Funktion $f : \mathbb{N} \to \mathbb{R}$, $n \mapsto \frac{3}{n+1}$

Beispiel 2.2.4 (Der Graph einer Funktion $\boldsymbol{f : \mathbb{N} \to \mathbb{R}}$)**.** Lassen Sie uns die Funktion

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{R}, \\ n &\mapsto \frac{3}{n+1} \end{aligned}$$

betrachten. Ihren Funktionsgraphen

$$\mathrm{Gr}(f) = \left\{(n, \frac{3}{n+1}) \mid \ n \in \mathbb{N}\right\}$$

können Sie in Abbildung 2.2.2 sehen.

Beispiel 2.2.5 (Der Graph einer Funktion $\boldsymbol{f : \mathbb{R} \to \mathbb{R}^2}$)**.** Betrachten Sie die Funktion

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}^2, \\ x &\mapsto \begin{pmatrix} \cos(x) \\ \sin(x) \end{pmatrix}. \end{aligned}$$

Ihr Funktionsgraph

$$\mathrm{Gr}(f) = \left\{ \begin{pmatrix} x \\ \cos(X) \\ \sin(x) \end{pmatrix} \mid \ x \in \mathbb{R}^3 \right\} \subseteq \mathbb{R}^3$$

wird in Abbildung 2.2.3 gezeigt.

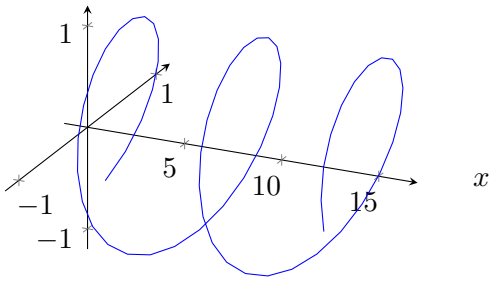

Abbildung 2.2.3: Graph der Funktion $f : \mathbb{R} \to \mathbb{R}^2$, $x \mapsto (\cos(x), \sin(x))$

Beispiel 2.2.6 (Der Graph einer Funktion $\boldsymbol{f : \mathbb{R}^2 \to \mathbb{R}}$ als Funktionsgebirge)**.** Lassen Sie uns die Funktion

$$\begin{aligned} f : \mathbb{R}^2 &\to \mathbb{R}, \\ (x_1, x_2) &\mapsto x_1^2 + x_2^2 \end{aligned}$$

betrachten. Ihren Funktionsgraphen

$$\mathrm{Gr}(f) = \left\{(x_1, x_2, x_1^2 + x_2^2) \mid \ (x_1, x_2) \in \mathbb{R}^2\right\} \subseteq \mathbb{R}^3$$

können Sie in Abbildung 2.2.4 sehen. Funktionengraphen von Funktionen $\mathbb{R}^2 \to \mathbb{R}$ bezeichnet man manchmal naheliegender Weise als **Funktionsgebirge**.

Beispiel 2.2.7 (Eine Funktion von $\mathbb{R}^2$ nach $\mathbb{R}^2$ als Vektorfeld)**.** Betrachten Sie die Funktion

$$\begin{aligned} f : \mathbb{R}^2 &\to \mathbb{R}^2, \\ x &\mapsto \mathbb{R}^2. \end{aligned}$$

Der Graph dieser Funktion ist eine Teilmenge von $\mathbb{R}^2 \times \mathbb{R}^2 = \mathbb{R}^4$, deshalb kann man ihn nicht in ein zwei- oder drei-dimensionales Bild zeichnen. Man kann die Funktion f aber stattdessen als ein sogenanntes *Vektorfeld* veranschaulichen. Damit nimmt man sich einige Punkte x des Definitionsbereichs $\mathbb{R}^2$ und zeichnet den Vektor $f(x)$ so im $\mathbb{R}^2$ ein, dass sein Fußpunkt in den Punkt x verschoben ist. Das können Sie in Abbildung 2.2.5 sehen.

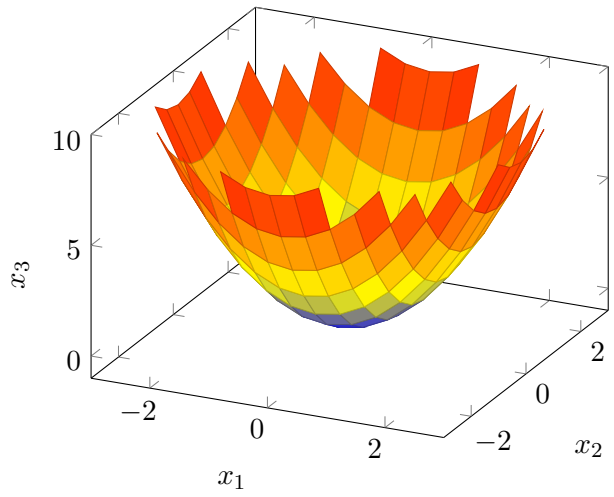

Abbildung 2.2.4: Graph der Funktion $\mathbb{R}^2 \to \mathbb{R}$, $(x_1, x_2) \mapsto x_1^2 + x_2^2$

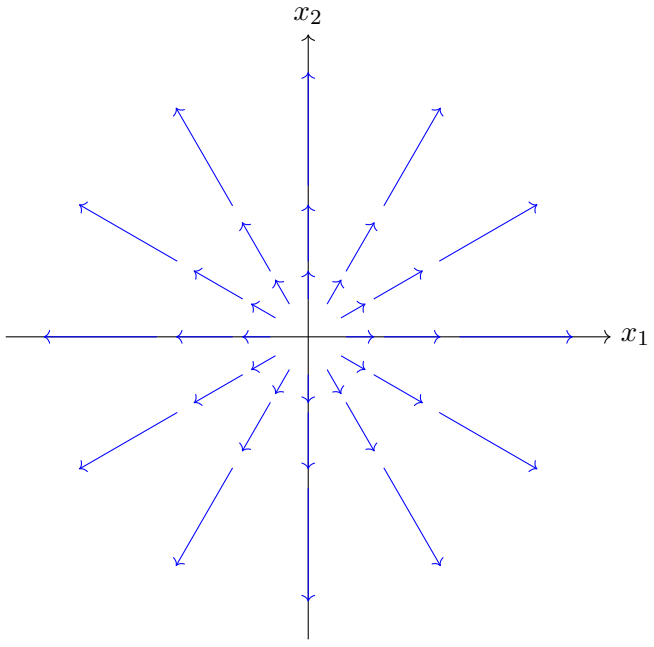

Abbildung 2.2.5: Bildliche Darstellung der Funktion $\mathbb{R}^2 \to \mathbb{R}^2$, $x \mapsto \frac{3}{4}x$ als Vektorfeld.

2.3 Eigenschaften von Funktionen: Injektivität, Surjektivität und Bijektivität

Im Umgang mit Funktionen gehören die folgenden drei Begriffe zum täglichen Handwerkszeug. Sie müssen deshalb schon jetzt lernen, den Umgang mit desen Begriffen zu beherrschen.

Definition 2.3.1 (Injektive, surjektive und bijektive Funktionen)**.** Seien X, Y Mengen und sei $f : X \to Y$.

(a) Die Funktion f heißt **injektiv**,[15] wenn für alle $x, \tilde{x} \in X$ gilt: Falls $x \neq \tilde{x}$ ist, dann ist auch $f(x) \neq f(\tilde{x})$.

(b) Die Funktion f heißt **surjektiv**, falls es für jedes $y \in Y$ ein $x \in X$ mit der Eigenschaft $f(x) = y$ gibt.

(c) Die Funktion f heißt **bijektiv**, falls sie sowohl injektiv als auch surjektiv ist.

Lassen Sie uns alle drei Teile der Definition noch eimal kurz und knapp und aussagenlogischer Notation darstellen: Für eine Funktion $f : X \to Y$ besagt obige Defintion:

(a) Es ist f genau dann injektiv, wenn folgendes gilt:

$$\forall x, \tilde{x} \in X : \quad x \neq \tilde{x} \quad \Rightarrow \quad f(x) \neq f(\tilde{x}).$$

(b) Es ist f genau dann surjektiv, wenn folgendes gilt:

$$\forall y \in Y \; \exists x \in X : \quad f(x) = y.$$

(c) Es ist f genau dann bijektiv, wenn folgendes gilt:

$$\forall y \in Y \; \exists! x \in X : \quad f(x) = y.$$

Beispiele 2.3.2. (a) Die Abbildung f aus Beispiel 2.1.3(a) ist nicht injektiv, denn es gilt $f(1) = f(3)$.

Die Abbildung

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 \end{aligned}$$

ist ebenfalls nicht injektiv, denn es ist z.B. $g(-1) = g(1)$.

[15] Manchmal sagt man anstelle von injektiv auch **ein-eindeutig**.

(b) Die Abbildung

$$k : \mathbb{R}^2 \to \mathbb{R}^3,$$
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2 \\ x_1 - x_2 \\ 2x_1 \end{pmatrix}.$$

aus Beispiel 2.1.3(b) ist injektiv.

Beweis. Seien $x, \tilde{x} \in \mathbb{R}^2$ beliebig, aber fest. Wir müssen die Implikation

$$x \neq \tilde{x} \quad \Rightarrow \quad k(x) \neq k(\tilde{x}) \tag{2.3.1}$$

zeigen. Hierzu verwenden wir eine aussagenlogisches Resultat, dass Sie in Aufgabe 2(a) auf Tutoriumsblatt 2 bewiesen haben: Wenn A und B Aussagen sind, dann ist die Implikation $A \Rightarrow B$ gleichbedeutend mit der Implikation $\neg B \Rightarrow \neg A$.

Anstatt die Implikation 2.3.1 zu beweisen, können wir also auch einfach die Implikation

$$k(x) = k(\tilde{x}) \quad \Rightarrow \quad x = \tilde{x}$$

zeigen, und genau dies tun wir nun.[16,17]

Sei also $k(x) = k(\tilde{x})$. Aufgrund der Definition von k gilt dann

$$\begin{pmatrix} x_1 + x_2 \\ x_1 - x_2 \\ 2x_1 \end{pmatrix} = \begin{pmatrix} \tilde{x}_1 + \tilde{x}_2 \\ \tilde{x}_1 - \tilde{x}_2 \\ 2\tilde{x}_1 \end{pmatrix}.$$

Wegen der Definition der Gleichheit von Tupeln (Definition 1.3.16(c)) folgt hieraus

$$\begin{aligned} & x_1 + x_2 = \tilde{x}_1 + \tilde{x}_2 \\ \wedge \quad & x_1 - x_2 = \tilde{x}_1 - \tilde{x}_2 \\ \wedge \quad & 2x_1 = 2\tilde{x}_1. \end{aligned}$$

Aus der dritten dieser Gleichungen erhalten wir $x_1 = \tilde{x}_1$, und wenn wir dann noch die erste der drei Gleichungen verwenden, folgt zudem $x_2 = \tilde{x}_2$.

Dies bedeutet – erneut wegen der Definition der Gleichheit von Tupeln –, dass $x = \tilde{x}$ ist. □

[16] Dies ist ein sogenannter Beweis per **Kontraposition** (ein Spezialfall des sogenannten Widerspruchsbeweises).

[17] Diese Vorgehensweise – also anzunehmen, dass $k(x) = k(\tilde{x})$ gilt, und daraus $x = \tilde{x}$ zu folgern, ist in vielen Fällen gut geeignet um Injektivität einer Funktion k zu beweisen.

(c) Die Abbildung f aus Beispiel 2.1.3(a) ist nicht surjektiv, denn es gibt z.B. kein $x \in \{1, 2, 3, 4\}$ mit der Eigenschaft $f(x) = 10$.

Die Abbildung

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto x^2 \end{aligned}$$

ist ebenfalls nicht surjektiv, denn es gibt kein $x \in \mathbb{R}$ mit $g(x) = -1$.

(d) Die Abbildung

$$\begin{aligned} h : \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto 2x + 1 \end{aligned}$$

ist bijektiv.

Beweis. Wir müssen Injektivität und Surjektivität zeigen.

Injektivität: Seien $x, \tilde{x} \in \mathbb{R}$ beliebig, aber fest. Wir führen den Beweis der Injektivität erneut per Kontraposition, d.h. wir zeigen die Implikation

$$h(x) = h(\tilde{x}) \quad \Rightarrow \quad x = \tilde{x}.$$

Sei also $h(x) = h(\tilde{x})$. Wegen der Definition von h gilt somit $2x + 1 = 2\tilde{x} + 1$. Indem wir auf beiden Seiten der Gleichung zuerst 1 subtrahieren und dann durch zwei teilen, folgt hieraus $x = \tilde{x}$.

Surjektivität: Wir müssen folgendes zeigen:

$$\forall y \in \mathbb{R}\ \exists x \in \mathbb{R} : \qquad h(x) = y.$$

Sei also $y \in \mathbb{R}$ beliebig, aber fest. Unsere Aufgabe ist es zu beweisen, dass ein $x \in \mathbb{R}$ existiert, welches die Gleichung $h(x) = y$ erfüllt. In der vorliegenden Situation ist dies sehr einfach, denn wir können ein solches x konkret angeben: Wir wählen $x = \frac{y-1}{2}$. Dann ist x tatsächlich ein Element von $\mathbb{R}$, und es gilt, wie gewünscht, $h(x) = 2x + 1 = y$. □

Lassen Sie uns nun zeigen, dass die Hintereinanderausführung zweier injektiver Funktionen wieder injektiv ist, und dass die Hintereinanderausführung zweier surjektiver Funktionen wieder surjektiv ist.

Proposition 2.3.3. *Seien X, Y, Z Mengen, und seien $f : X \to Y$ und $g : Y \to Z$.*

(a) *Wenn f und g beide injektiv sind, dann ist auch $g \circ f$ injektiv.*

(b) *Wenn f und g beide surjektiv sind, dann ist auch $g \circ f$ surjektiv.*

Beweis. (a) Seien f und g injektiv. Wir müssen zeigen, dass $g \circ f$ injektiv ist.

Seien dazu $x, \tilde{x} \in X$. Wie Sie nun bereits zweimal gesehen haben, genügt es die Implikation

$$(g \circ f)(x) = (g \circ f)(\tilde{x}) \quad \Rightarrow \quad x = \tilde{x}$$

zu zeigen. Also gelte nun $(g \circ f)(x) = (g \circ f)(\tilde{x})$. Laut Definition der Hintereinanderausführung von Funktionen ist dann

$$g\big(f(x)\big) = g\big(f(\tilde{x})\big).$$

Weil g injektiv ist, folgt hieraus $f(x) = f(\tilde{x})$. Und weil f injektiv ist, folgt hieraus wiederum $x = \tilde{x}$.

(b) Seien f und g surjektiv. Wir müssen die Aussage

$$\forall z \in Z \; \exists x \in X : \qquad (g \circ f)(x) = z$$

zeigen. Sei also $z \in Z$ beliebig, aber fest.

Weil g surjektiv ist, gibt es ein $y \in Y$ mit der Eigenschaft $g(y) = z$. Und weil auch f surjektiv ist, gibt es ein $x \in X$ mit der Eigenschaft $f(x) = y$. Für dieses x gilt somit

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

Also haben wir gezeigt, dass es tatsächlich ein $x \in X$ mit der Eigenschaft $(g \circ f)(x) = z$ gibt. □

Bijektive Funktionen sind deshalb besonders nützlich, weil man Sie umkehren kann:

Definition 2.3.4 (Umkehrfunktion)**.** Seien X, Y Mengen und sei $f : X \to Y$ eine bijektive Abbildung.[18]

Wir definieren eine Funktion $f^{-1} : Y \to X$, die jedem $y \in Y$ genau dasjenige $x \in X$ zuordnet, für welches $f(x) = y$ gilt. Die Funktion f^{-1} heißt die **Umkehrfunktion** (oder **Umkehrabbildung**) von f.

Man beachte: Die Definition der Umkehrabbildung f^{-1} besagt gerade, dass für jedes $y \in Y$ die Gleichung

$$f\big(f^{-1}(y)\big) = y$$

gilt. Bevor wir einige Eigenschaften der Umkehrfunktion beweisen, benötigen wir die folgende Terminologie:

[18] D.h., es gibt für jedes $y \in Y$ genau ein $x \in X$ mit der Eigenschaft $f(x) = y$.

Definition 2.3.5 (Identische Funktion)**.** Sei X eine Menge. Die Abbildung

$$\begin{aligned} \mathrm{id}_X : X &\to X, \\ x &\mapsto x \end{aligned}$$

heißt die **identische Abbildung** oder die **Identität** auf X.

Wenn die Menge X aus dem Kontext klar ist, lassen wir das X im Index manchmal auch weg und schreiben einfach nur id anstelle von id_X.

Wenn wir die Identität mit einer anderen Funktion verknüpfen, dann erhalten wir diesselbe Funktion. Genauer: Wenn $f : X \to Y$ eine Funktion zwischen zwei Mengen X, Y ist, dann gilt

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

Dies kann man sich leicht mit Hilfe der Definition der Identität und der Definition der Gleichheit von Funktionen überlegen.[19]

Proposition 2.3.6 (Eigenschaften der Umkehrfunktion)**.** *Seien X, Y, Z Mengen, und seien $f : X \to Y$ und $g : Y \to Z$ zwei bijektive Funktionen.*

(a) *Für alle $x \in X$ und alle $y \in Y$ gilt*

$$f^{-1}\big(f(x)\big) = x \qquad \textit{und} \qquad f\big(f^{-1}(y)\big) = y;$$

d.h. etwas kürzer ausgedrückt:

$$f^{-1} \circ f = \mathrm{id}_X \qquad \textit{und} \qquad f \circ f^{-1} = \mathrm{id}_Y .$$

(b) *Die Umkehrabbildung $f^{-1} : Y \to X$ ist ebenfalls bijektiv, und es gilt*

$$(f^{-1})^{-1} = f.$$

(c) *Die Hintereinanderausführung $g \circ f$ ist ebenfalls bijektiv, und es gilt*

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

Beweis. (a) Die Eigenschaft

$$\forall y \in Y : \qquad f\big(f^{-1}(y)\big) = y$$

ist exakt die Eigenschaft, durch die wir die Umkehrfunktion definiert haben (siehe Definition 2.3.4 und die Erläuterung direkt nach der Definition).

[19] Erinnern Sie sich daran, was schon in einer vorherigen Fußnote stand: Das Wort „leicht“ ist hier als Zielmarke zu verstehen, und die Formulierung „Das kann man sich leicht überlegen“ bedeutet nicht, dass Sie das ohne weitere Überlegung glauben dürfen, sondern Sie bedeutet, dass Sie sich das jetzt noch einmal selbst im Detail überlegen müssen um zu sehen, dass es wirklich direkt aus den Definitionen folgt.

Wir müssen noch die zweite Eigenschaft zeigen. Sei also $x \in X$ beliebig, aber fest. Wir setzen $y := f(x)$. Für dieses y gilt aufgrund der soeben besprochenen Eigenschaft die Gleichheit $f\big(f^{-1}(y)\big) = y$, also

$$f\Big(f^{-1}\big(f(x)\big)\Big) = f(x).$$

Weil f injektiv ist, folgt daraus die Gleichheit

$$f^{-1}\big(f(x)\big) = x.$$

Wenn wir die Definition der Gleichheit von Funktionen (Definition 2.1.7) verwenden, können wir aus den bisher gezeigten Eigenschaften sofort folgern, dass

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{und} \qquad f \circ f^{-1} = \mathrm{id}_Y\,.$$

gilt.[20]

(b) *Injektivität:* Seien $y, \tilde{y} \in Y$ und sei $f^{-1}(y) = f^{-1}(\tilde{y})$. Dann ist

$$f\big(f^{-1}(y)\big) = f\big(f^{-1}(\tilde{y})\big).$$

Wie bereits in (a) festgestellt, ist die linke Seite dieser Gleichung gleich y und die rechte Seite gleich $\tilde{y}$. Es folgt also $y = \tilde{y}$.

Surjektivität: Sei $x \in X$. Wir müssen zeigen, dass ein $y \in Y$ existiert, für welches $f^{-1}(y) = x$ gilt. Hierzu wählen wür einfach $y = f(x)$. Für dieses y gilt tatsächlich

$$f^{-1}(y) = f^{-1}\big(f(x)\big) = x,$$

wobei die letzte Gleichheit aus (a) folgt.

[20] **Achtung:** Wenn in einer Vorlesung in einem Beweis gesagt wird, dass etwas „sofort folgt“, dann bedeutet dies lediglich, dass man die behauptete Aussage ohne großen Aufwand aus dem folgern kann, was soeben gesagt wurde. Das bedeutet aber nicht automatisch, dass Ihnen dies auch wirklich klar ist. Wann immer Sie eine Aussage von der Form „nun folgt sofort“ (oder eine ähnliche Formulierung wie „jetzt folgt leicht“) lesen, müssen Sie also noch einmal nachprüfen, ob Sie diese Folgerung wirklich bis ins Detail begründen können. Dies tun Sie am besten auf einem Blatt Papier (oder einem Tablet).

Nehmen Sie sich also sogleich einen Stift und versuchen Sie extrem detailliert aufzuschreiben, weshalb die Gleichungen $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$ an dieser Stelle im Beweis wirklich folgen. Beachten Sie dabei: Sie können dies natürlich nur dann korrekt begründen, wenn Sie verwenden, wie die Gleichheit von Funktionen definiert ist. Ihre Begründung kann also nur funktionieren, wenn Sie Definition 2.1.7 zu Rate ziehen.

Übrigens: Es besteht kein Grund zur Frustration, falls Sie für das Ausarbeiten der Details länger brauchen, als Sie aufgrund des Wortes „sofort“ erwarten würden: Was eine Person mit einiger Erfahrung innerhalb von Sekunden sehen kann, kann jemand ohne Erfahrung manchmal erst nach einer viertel oder halben Stunde sehen. Fassen Sie den hier verwendeten Begriff „sofort“ deshalb als Zielmarke auf: Sie müssen sich solche „einfachen“ Details solange ausführlich und mit viel Zeitaufwand überlegen, bis Sie soviel Übung, Verständnis und Erfahrung gesammelt haben, dass Sie solche Details selbst auch sofort verstehen.

Gleichheit $(f^{-1})^{-1} = f$*:* Hier zu müssen wir laut Definition 2.1.7 zeigen, dass beiden Funktionen f und $(f^{-1})^{-1}$ denselben Definitions- und Wertebereich haben, und dass sie an alle Elementen des Wertebereichs denselben Werte annehmen.

Weil f von X nach Y abbildet, bildet f^{-1} laut Definition der Umkehrfunktion von Y nach X ab. Erneut aufgrund der Definition der Umkehrfunktion folgt hieraus, dass $(f^{-1})^{-1}$ von X nach Y abbildet. Also haben beide Funktionen f und $(f^{-1})^{-1}$ den Definitionsbereich X und den Wertebereich Y.

Nun müssen wir noch zeigen, dass für alle $x \in X$ die Gleichheit $f(x) = (f^{-1})^{-1}(x)$ gilt. Sei also $x \in X$ beliebig, aber fest. Der Übersicht halber ist es nützlich, im folgenden die Notation $h := f^{-1}$ zu verwenden. Somit ist h eine bijektive Abbildung von Y nach X, und unsere Aufgabe ist es, $f(x) = h^{-1}(x)$ zu zeigen.

Indem wir die rechtsstehende Formel aus Teil (a) anwenden – allerdings nicht auf die Funktion $f : X \to Y$, sondern auf die Funktion $h : Y \to X$ – erhalten wir die Formel

$$h\big(h^{-1}(x)\big) = x, \qquad \text{d.h.} \qquad f^{-1}\big(h^{-1}(x)\big) = x.$$

Jetzt wenden wir auf letztgenannte Gleichheit noch die Funktion f an, und erhalten somit

$$f\Big(f^{-1}\big(h^{-1}(x)\big)\Big) = f(x).$$

Die linke Seite dieser Formel ist aber – erneut wegen der rechtsstehenden Formel in Teil (a) (die wir aber dieses Mal auf die Funktion $f : X \to Y$, und auf das Element $y := h^{-1}(x) \in Y$ anwenden) – gleich $h^{-1}(x)$. Somit haben wir, wie gewünscht, $h^{-1}(x) = f(x)$ gezeigt.

(c) Diesen Beweis lagern wir in die Übungen aus. □

2.4 Bilder und Urbilder

Definition 2.4.1 (Bild und Urbild)**.** Seien X, Y Mengen und sei $f : X \to Y$.

(a) Für eine Menge $A \subseteq X$ nennt man

$$f(A) := \{f(a) \mid\ a \in A\} = \{y \in Y \mid\ \exists a \in A :\ y = f(a)\}$$

das **Bild von A unter f**.

Das Bild von X unter f – also die Menge $f(X)$ – bezeichnet man manchmal auch einfach als das **Bild von f**.

(b) Für eine Menge $B \subseteq Y$ nennt man

$$f^{-1}(B) := \{x \in X \mid\ f(x) \in B\}$$

das **Urbild von B unter f**.

Beispiele 2.4.2. (a) Sei $X = \{1, 2, 3, 4\}$ und $Y = \{3, 4, 5, 6\}$. Wir definieren $f : X \to Y$ durch die Tabelle

x	1	2	3	4
$f(x)$	6	3	6	4.

Dann gilt zum Beispiel

$$f(\emptyset) = \emptyset, \quad f(\{1\}) = (\{f\}), \quad f(\{1, 2\}) = \{3, 6\},$$
$$f(\{1, 2, 3\}) = \{3, 6\}, \quad f(\{1, 2, 3, 4\}) = \{3, 4, 6\}.$$

Zudem gilt zum Beispiel

$$f^{-1}(\emptyset) = \emptyset, \quad f^{-1}(\{5\}) = \emptyset, \quad f^{-1}(\{3\}) = \{2\},$$
$$f^{-1}(\{6\}) = \{1, 3\}, \quad f^{-1}(\{5, 6\}) = \{1, 3\}.$$

(b) Sei $g : \mathbb{R} \to \mathbb{R}$ gegeben durch $g(x) = x^2$ für alle $x \in \mathbb{R}$. Dann gilt zum Beispiel

$$g(\mathbb{R}) = [0, \infty), \quad g([-1, 1]) = g([0, 1]) = [0, 1], \quad q([2, 3]) = [4, 9],$$

sowie

$$g^{-1}((0, 4]) = [-2, 0) \cup (0, 2], \quad g^{-1}(\{9\}) = \{-3, 3\}, \quad g^{-1}([-1, 0]) = \{0\}.$$

Aus der Definition der Begriffe Bild und Urbild folgt sofort die folgende Proposition:

Proposition 2.4.3. *Seien X, Y Mengen und sei $f : X \to Y$*

(a) *Die Abbildung f ist genau dann injektiv, wenn für jedes $y \in Y$ das Urbild $f^{-1}(\{y\})$ höchstens ein Element hat.*

(b) *Die Abbildung f ist surjektiv genau dann, wenn ihr Bild $f(X)$ gleich Y ist, genau dann, wenn für jedes $y \in Y$ das Urbild $f^{-1}(\{y\})$ mindestens ein Element hat.*

Bemerkung 2.4.4. Sei $f : X \to Y$ eine Abbildung von einer Menge X in eine Menge Y.

Beachten Sie unbedingt, dass das Urbild $f^{-1}(B)$ einer Menge $B \subseteq Y$ auch dann definiert ist, wenn f nicht bijektiv ist (und f somit keine Umkehrfunktion besitzt).

Zur Unterscheidung der Notationen für Urbild und Umkehrfunktion muss man den Kontext verwenden:

- Wenn $y \in Y$ ist, ist mit $f^{-1}(y)$ die Umkehrfunktion f, ausgewertet an der Stelle y, gemeint. Diese Notation ergibt somit nur Sinn, wenn f bijektiv ist.
- Wenn aber $B \subseteq Y$ ist, ist mit $f^{-1}(B)$ das Urbild von B unter f gemeint. Diese Notation ergibt immer Sinn, egal ob f bijektiv ist.

Sie sollten sich nun die folgenden beiden Fragen stellen um zu überprüfen, ob Sie das richtig verstanden haben:

- Wenn $y \in Y$ ist – was ist dann mit $f^{-1}(\{y\})$ gemeint?
- Sei $B \subseteq Y$ und sei außerdem f bijektiv ist. Oben haben wir gesagt, dass mit $f^{-1}(B)$ tatsächlich das Urbild von B unter f gemeint ist. Aber da $f^{-1} : Y \to X$ ja auch die Umkehrfunktion von f bezeichnet, könnte mit der Notation $f^{-1}(B)$ ja auch das Bild von B unter der Funktion f^{-1} gemeint sein – woher weiß man nun, welches von beiden wirklich gemeint ist?

2.5 Mächtigkeit von Mengen

Definition 2.5.1 (Endlichkeit und Mächtigkeit)**.** Eine Menge X heißt **endlich**, falls es ein $n \in \mathbb{N}$ und eine bijektive Abbildung $X \to \mathbb{N}_{\leq n-1} \coloneqq \{k \in \mathbb{N} \mid \ k \leq n-1\}$ gibt. In diesem Fall heißt n die **Mächtigkeit** oder **Kardinalität** von X.[21]

Die Mächtigkeit einer endlichen Menge X ist also eine natürliche Zahl. Wir notieren[22] sie mit dem Symbol $\#X$ oder $\#(X)$.

Proposition 2.5.2. *Sei X, Y endlich Mengen. Es gilt $\#X = \#Y$ genau dann, wenn es eine bijektive Abbildung $X \to Y$ gibt.*

Beweis. "⇒" Sei $n \coloneqq \#X = \#Y \in \mathbb{N}$. Dann gibt es laut Definition 2.5.1 eine bijektive Abbildung $f : X \to \mathbb{N}_{\leq n-1}$ und eine bijektive Abbildung $g : Y \to \mathbb{N}_{\leq n-1}$. Laut Proposition 2.3.6(b) ist die Umkehrabbildung $g^{-1} : \mathbb{N}_{\leq n-1} \to Y$ ebenfalls bijektiv und laut Proposition 2.3.6(c) ist somit die Hintereinanderausführung

$$g^{-1} \circ f : X \to Y$$

ebenfalls bijektiv. Also gibt es eine bijektive Abbildung von X nach Y.

"⇐" Es $h : X \to Y$ eine bijektive Abbildung und sei $n \coloneqq \#X \in \mathbb{N}$. Laut Definition 2.5.1 gibt es eine bijektive Abbildung $f : X \to \mathbb{N}_{\leq n-1}$. Laut Proposition 2.3.6(b) ist $h^{-1} \colon Y \to X$ bijektiv und laut Proposition 2.3.6(c) ist somit auch $f \circ h^{-1} \colon Y \to \mathbb{N}_{\leq n-1}$ bijektiv. Somit gilt laut Definition 2.5.1, dass $\#Y = n$ ist, das heißt, wird haben $\#X = \#Y$ gezeigt. □

Definition 2.5.3 (Gleichmächtigkeit)**.** Seien X, Y Mengen. Die Menge X heißt **gleichmächtig** zu Y, wenn eine bijektive Abbildung $f : X \to Y$ existiert.

Wir beweisen einige Eigenschaften des Konzeptes „Gleichmächtigkeit":

Proposition 2.5.4 (Eigenschaften von Gleichmächtigkeit)**.** *Seien X, Y, Z Mengen. Es gelten folgende Eigenschaften des Gleichmächtigkeits-Begriffs:*

[21] Man kann auch für unendliche Mengen einen Kardinalitätsbegriff definieren. Dieser ist aber subtiler und abstrakter, weshalb wir uns an dieser Stelle der Vorlesung nicht weiter damit beschäftigen.

[22] Häufig wird anstelle des Symbols $\#X$ auch das Symbol $|X|$ für die Mächtigkeit verwendet.

(a) Reflexivität: *Die Menge X ist gleichmächtig zu sich selbst.*

(b) Symmetrie: *Wenn X gleichmächtig zu Y ist, dann ist Y auch gleichmächtig zu X.*

(c) Transitivität: *Wenn X gleichmächtig zu Y ist und Y gleichmächtig zu Z ist, dann ist X ebenfalls gleichmächtig zu Z.*

Beweis. (a) Die identische Abbildung $\mathrm{id}_X : X \to X$ ist bijektiv[23] , also existiert eine bijektive Abbildung $X \to X$.

(b) Sei X gleichmächtig zu Y. Dann gibt es eine bijektive Abbildung $f : X \to Y$. Laut Proposition 2.3.6(b) ist auch $f^{-1} : Y \to X$ bijektiv. Somit gibt es eine bijektive Abbildung $Y \to X$, d.h., Y ist gleichmächtig zu X.

(c) Sei X gleichmächtig zu Y und Y gleichmächtig zu Z. Dann gibt es eine bijektive Abbildung $f : X \to Y$ und eine bijektive Abbildung $g : Y \to Z$. Laut Proposition 2.3.6(c) ist die Hintereinanderausführung $g \circ f : X \to Z$ ebenfalls bijektiv. Somit gibt es eine bijektive Abbildung von X nach Z, d.h. X ist gleichmächtig zu Z. □

Nun kommen wir zu einer Sache, die viele Studierende am Anfang überrascht: Wir sehen uns an, zwischen welchen unendlichen Mengen es im bijektive Abbildungen gibt – d.h., welche unendlichen Mengen gleichmächtig sind (und welche nicht).

Definition 2.5.5 (Abzählbare und überabzählbare Mengen)**.** Sei X eine Menge.

(a) Die Menge X heißt **unendlich**, falls sie nicht endlich ist.

(b) Die Menge X heißt **abzählbar unendlich**, falls sie gleichmächtig zu $\mathbb{N}$ ist.

(c) Die Menge X heißt **abzählbar**, falls sie endlich oder abzählbar unendlich ist.

(d) Die Menge X heißt **überabzählbar**, falls sie nicht abzählbar ist.[24]

Die folgende Proposition bestimmt für einige interessante Mengen, ob Sie abzählbar sind:

Proposition 2.5.6 (Einige abzählbare und überabzählbare Mengen)**.** (a) *Die Menge $\mathbb{N}^*$ ist abzählbar unendlich.*

(b) *Die Menge $\mathbb{Z}$ ist abzählbar unendlich.*

(c) *Die Menge $\mathbb{N}^2$ ist abzählbar unendlich.*

(d) *Wenn X und Y abzählbar unendliche Mengen sind, dann ist auch $X \times Y$ abzählbar unendlich.*

[23] Warum eigentlich?

[24] Anders ausgerückt: Falls sie unendlich, aber nicht abzählbar unendlich ist.

Beweis. (a) Die Abbildung

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}^*, \\ n &\mapsto n - 1 \end{aligned}$$

ist bijektiv.[25] Somit ist $\mathbb{N}^*$ laut Definition 2.5.3 gleichmächtig zu $\mathbb{N}$.

(b) Lassen Sie uns die Funktion

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{Z}, \\ n &\mapsto \begin{cases} \frac{n+1}{2} & \text{falls } n \text{ ungerade ist,} \\ -\frac{n}{2} & \text{falls } n \text{ gerade ist.} \end{cases} \end{aligned}$$

Diese ist bijektiv.[26] Somit ist $\mathbb{Z}$ gleichmächtig zu $\mathbb{N}$.

(c) Das kann man mit einer Diagonalabzählung beweisen.

... Details und Bild werde noch hinzugefügt. ...

(d) ... □

Theorem 2.5.7 (Cantor–Bernstein–Schröder)**.** *Seien X, Y Mengen. Wenn es eine injektive Funktion $f\colon X \to Y$ und eine injektive Funktion $g\colon X \to Y$ gibt, dann gibt es eine bijektive Funktion $h\colon X \to Y$ (und somit sind X und Y gleichmächtig).*

Beweis. Wir konstruieren Teilmengen $C_0, C_1, C_2, \ldots$ von X durch folgendes Vorgehen: Wir setzen

$$\begin{aligned} C_0 &\coloneqq X \setminus g(Y), \\ C_1 &\coloneqq g\big(f(C_0)\big), \\ C_2 &\coloneqq g\big(f(C_1)\big), \\ &\text{und so weiter.} \end{aligned}$$

Allgemein ausgedrückt bedeutet das also: Wenn wir für ein $n \in \mathbb{N}$ die Menge C_n definiert haben, dann definieren wir als nächstes die Menge C_{n+1} als $C_{n+1} \coloneqq g\big(f(C_n)\big)$.[27] Außerdem setzen wir $C \coloneqq \bigcup_{n\in\mathbb{N}} C_n \subseteq X$.

Nun definieren wir eine Funktion $h\colon X \to Y$ folgendermaßen: Wir jedes $x \in X$ führen wir eine Fallunterscheidung durch: Falls x in C liegt, definieren wir $h(x) = f(x)$. Falls x hingegen nicht in C liegt, dann liegt x erst recht nicht in C_0 und somit liegt x insbesondere in $g(Y)$. Wegen der Injektivität von g gibt es also genau ein $y \in Y$ mit der Eigenschaft $x = g(y)$ und wir definieren $h(x)$ als eben dieses y.

Lassen Sie uns folgende Beobachtung machen:

$(*)$ Für ein beliebiges Element $x \in C$ und ein beliebiges Element $\tilde{x} \in X \setminus C$ gilt stets $h(x) \neq h(\tilde{x})$.

[25] Warum?

[26] Warum?

[27] Ein solches Vorgehen bezeichnet man als **Rekursion**. Darauf werden in Abschnitt 3.1 noch ausführlicher zu sprechen kommen.

Das kann man mit einem sogenannten **Widerspruchsbeweis** sehen:[28] Wir nehmen dazu an, dass $h(x) = h(\tilde{x})$ und führen dies nun zu einem Widerspruch. Wegen $\tilde{x} \in C$ gilt $\tilde{x} = g(h(\tilde{x})) = g(h(x)) = g(f(x))$, wobei die letzte Gleichheit aus $x \in C$ folgt. Wegen der Definition von C gibt ein $n \in \mathbb{N}$ mit $x \in C_n$. Somit gilt $f(x) \in f(C_n)$ und folglich $\tilde{x} = g(f(x)) \in g\big(f(C_n)\big) = C_{n+1} \subseteq C$. Das ist ein Widerspruch, da wir $\tilde{x} \notin C$ vorausgesetzt hatten.

Wir zeigen nun, dass h bijektiv ist:

Injektivität von h: Seien $x_1, x_2 \in X$ mit $h(x_1) = h(x_2)$. Wir unterscheiden die folgenden beiden Fälle:

- Erster Fall: Es gilt $x_1 \in C$.

  Wegen $(*)$ gilt dann auch $x_2 \in C$. Somit ist $f(x_1) = h(x_1) = h(x_2) = f(x_2)$. Weil f injektiv ist, folgt $x_1 = x_2$.

- Zweiter Fall: Es gilt $x_1 \in X \setminus C$.

  Wegen $(*)$ gilt dann auch $x_2 \in X \setminus C$. Somit ist $x_1 = g(h(x_1)) = g(h(x_2)) = x_2$.

Also ist h wie behauptet injektiv.

Surjektivität von h: Sei $y \in Y$ beliebig. Auch hier unterscheiden wir wieder zwei Fälle:

- Erster Fall: Es gilt $g(y) \in X \setminus C$.

  In diesem Fall definieren wir $x := g(y)$ und erhalten wegen $x \in X \setminus C$ die Gleichheit $h(x) = y$.

- Zweiter Fall: Es gilt $g(y) \in C$.

  Dann gibt es ein $n \in \mathbb{N}$ mit $g(y) \in C_n$. Wegen der Definition von C_0 kann nicht $g(y) \in C_0$ gelten, also ist $n \geq 1$ und somit $C_n = g\big(f(C_{n-1})\big)$. Also gibt es ein $x \in C_{n-1} \subseteq X$ derart, dass $g(y) = g(f(x))$ gilt. Wegen der Injektivität von g folgt daraus $y = f(x)$.

Somit ist auch die Surjektivität von h gezeigt. □

Korollar 2.5.8 (Cantor–Bernstein–Schröder umformuliert)**.** *Seien X, Y Mengen. Wenn es eine injektive Funktion $X \to Y$ und eine surjektive Funktion $X \to Y$ gibt, dann gibt es eine bijektive Funktion $X \to Y$ (und somit sind X und Y gleichmächtig).*

Beweis. Wegen Theorem 2.5.7 müssen wir nur zeigen, dass es eine injektive Funktion $g : Y \to X$ gibt. Laut Voraussetzung des Korollars gibt es eine surjektive Funktion $\tilde{g} : X \to Y$. Deshalb gibt es laut Aufgabe 2(b) auf Hausaufgabenblatt 5 eine Funktion $g : Y \to X$, für die $\tilde{g} \circ g = \mathrm{id}_Y$ gilt. Aus Teil (a) derselben Aufgabe folgt, dass g injektiv ist. □

[28] Unter einem Widerspruchsbeweis versteht man folgendes: Für zwei Aussagen A und B beweist man die Implikation $A \Rightarrow B$, indem man annimmt, dass A wahr ist und B falsch ist und daraus eine falsche Aussage herleitet.

Proposition 2.5.9 (Die rationalen Zahlen sind abzählbar)**.** *Die Menge $\mathbb{Q}$ ist abzählbar unendlich.*

Beweis. Es Abbildung $f : \mathbb{N} \to \mathbb{Q}$, $n \mapsto n$ ist injektiv. Außerdem ist die Abbildung $g_2 : \mathbb{Z} \times \mathbb{N}^* \to \mathbb{Q}$, $(z, n) \mapsto \frac{z}{n}$ surjektiv und laut Proposition (d) gibt es eine bijektive Abbildung $g_1 : \mathbb{N} \to \mathbb{Z} \times \mathbb{N}^*$. Damit ist die Abbildung $g_2 \circ g_1 : \mathbb{N} \to \mathbb{Q}$ laut Proposition 2.3.3(b) surjektiv, also folgt aus Korollar 2.5.8, dass $\mathbb{N}$ und $\mathbb{Q}$ gleichmächtig sind. □

Wenn L eine unendliche Teilmenge von $\mathbb{N}$ ist, kann man seine Elemente der Reihe nach abzählen und erhält somit eine bijektive Abbildung $\mathbb{N} \to L$ – d.h., L ist dann abzählbar unendlich. Wenn L eine endliche Teilmenge von $\mathbb{N}$ ist, dann ist L ebenfalls abzählbar. Somit gilt also die folgende Proposition:

Proposition 2.5.10 (Teilmengen von $\mathbb{N}$ sind abzählbar)**.** *Sei $L \subseteq \mathbb{N}$. Dann ist L abzählbar.*

Proposition 2.5.11 (Teilmengen abzählbarer Mengen sind abzählbar)**.** *Sei M eine abzählbare Menge und sei $L \subseteq M$. Dann ist auch L abzählbar.*

Beweis. □

Definition 2.5.12 (Potenzmenge)**.** Sei X eine Menge. Die Menge

$$\mathcal{P}(X) \coloneqq \Big\{ M \mid \ M \subseteq X \Big\},$$

das heißt die Menge, deren Elemente alle Teilmengen von X sind, nennt man die **Potenzmenge** von X.[29]

Beispiele 2.5.13 (Einige Beispiele für Potenzmengen)**.**

(a) Es gilt $\mathcal{P}(\emptyset) = \{\emptyset\}$.

(b) Es gilt $\mathcal{P}\big(\{1\}\big) = \Big\{\emptyset, \{1\}\Big\}$.

(c) Es gilt $\mathcal{P}\big(\{1,2\}\big) = \Big\{\emptyset, \{1\}, \{2\}, \{1,2\}\Big\}$.

(d) Es gilt $\mathcal{P}\big(\{1,2,3\}\big) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$.

Theorem 2.5.14 (Eine Menge ist kleiner als Ihre Potenzmenge)**.** *Sie X eine Menge. Dann gibt es keine surjektive Funktion $f\colon X \to \mathcal{P}(X)$.*

[29] Manchmal findet man auch die Notation 2^X für die Potenzmenge von X.

Beweis. Wir nehmen widerspruchshalber an, dass es eine surjektive Funktion $f : X \to \mathcal{P}(X)$ gibt. Lassen Sie uns nun die Menge

$$M \coloneqq \{x \in X \mid \ x \notin f(x)\} \in \mathcal{P}(X)$$

betrachten. Da f surjektiv ist, gibt es ein $x_0 \in X$ mit $f(x_0) = M$. Nun gilt entweder $x_0 \notin f(x_0)$ oder $x_0 \in f(x_0)$. Wir zeigen, dass in beiden Fällen ein Widerspruch auftritt:

- *Erster Fall:* $x_0 \notin f(x_0)$. In diesem Fall gilt laut Definition von M, dass $x_0 \in M$ ist. Wegen $M = f(x_0)$ kann das nicht sein.
- *Zweiter Fall:* $x_0 \in f(x_0)$.

  In diesem Fall gilt laut Definition von M, dass $x_0 \notin M$ ist. Wegen $M = f(x_0)$ kann das nicht sein.

Also führt die Annahme, dass es eine surjektive Funktion $f : X \to \mathcal{P}(X)$ gibt, zu einem Widerspruch, das heißt, es gibt keine solche Funktion. □

Korollar 2.5.15 (ℕ hat überabzählbar viele Teilmengen)**.** *Die Menge $\mathcal{P}(\mathbb{N})$ ist überabzählbar.*

Beweis. Die Menge $\mathcal{P}(\mathbb{N})$ ist unendlich.[30] Außerdem folgt aus Theorem 2.5.14, dass es keine surjektive Funktion $\mathbb{N} \to \mathcal{P}(\mathbb{N})$ gibt. Insbesondere gibt es also keine bijektive Funktion $\mathbb{N} \to \mathcal{P}(\mathbb{N})$, d.h., $\mathcal{P}(\mathbb{N})$ ist nicht abzählbar unendlich. □

[30] Warum?

Kapitel 3

Die natürlichen Zahlen und vollständige Induktion

Einstiegsfragen. (a) Sei n eine natürliche Zahl. Kennen Sie eine effiziente mathematische Notation für „die Summe der ersten n ungeraden natürlichen Zahlen“?

(b) A propos: Welcher Wert kommt eigentlich heraus, wenn man die Summe der ersten n ungeraden natürlichen Zahlen berechnet?

(c) Ein Gedankenspiel aus dem Märchenland: In den nächsten Semesterferien haben Sie bei einer guten Fee einen Wunsch frei, und Sie wünschen sich, dass immer und stets, egal was auch passiert, der erste Tag der Vorlesungszeit lieber noch ein Ferientag sei.

Die gute Fee erfüllt freilich Ihren Wunsch (sonst wäre sie ja keine gute Fee). Wann gehen Sie das nächste mal zur Vorlesung?

(d) Wie viele Teilmengen hat die Menge $\{1, 2, \ldots, 10\}$?

(e) Sechs Leute sitzen beim Bier. Bevor getrunken wird, stößt jede Person einmal separat mit jeder anderen an. Wie oft klirren die Gläser?

Und was hat das mit der Fußballbundesliga zu tun?

3.1 Folgen und Rekursion

Sie X eine Menge. Wie Sie bereits wissen, kann man zwei Elemente x_1, x_2 von X zu einem Tupel $(x_1, x_2) \in X^2$ zusammenfassen. Ebenso kann man drei Elemente $x_1, x_2, x_3 \in X$ zu einem Tupel $(x_1, x_2, x_3) \in X^3$ zusammenfassen, und so weiter. Es es naheliegend, dass man auch abzählbar viele Elemente

$$x_0, x_1, x_2, \cdots \in X$$

zu einer Art „Tupel“ zusammenfassen möchte. Das tun kann man mit dem Begriff der **Folge** tun:

Definition 3.1.1 (Folgen)**.** Sei X eine Menge. Eine Funktion $x : \mathbb{N} \to X$ bezeichnet man auch als eine **Folge** in X. Für $n \in \mathbb{N}$ schreibt man anstelle von $x(n)$ häufig auch x_n und oft notiert man die Folge x als $(x_n)_{n\in\mathbb{N}}$.

Den Definitionsbereich $\mathbb{N}$ der Folge bezeichnet man in dieser Schreibweise als die **Indexmenge** der Folge. Für jedes $n \in \mathbb{N}$ heißt das Elemente $x_n = x(n) \in X$ das n-te **Folgenglied** der Folge.

Analog kann man auch Folgen betrachten, deren Indexmenge $\mathbb{N}^*$ ist – also Objekte der Form $(x_n)_{n\in\mathbb{N}^*}$.

Anschaulich lässt sich eine Folge notationell andeuten, indem man die ersten paar Folgenglieder auflistet, das heißt, indem man zum Beispiel schreibt

$$(x_n)_{n\in\mathbb{N}} = (x_0, x_1, x_2, x_3, \dots).$$

Beispiele 3.1.2 (Einige Beispiele für Folgen)**.** (a) Für jedes $n \in \mathbb{N}$ sei $x_n = 2n$. Dann besteht die Folge

$$(x_n)_{n\in\mathbb{N}} = (2n)_{n\in\mathbb{N}} = (0, 2, 4, 6, \dots)$$

aus den geraden natürlichen Zahlen.

(b) Für jedes $n \in \mathbb{N}^*$ sei y_n den n-te ungerade natürliche Zahl, d.h., es sei $y_n = 2n - 1$ für jedes $n \in \mathbb{N}$. Dann ist also

$$(y_n)_{n\in\mathbb{N}} = (2n - 1)_{n\in\mathbb{N}} = (1, 3, 5, 7, \dots).$$

(c) Für jedes $n \in \mathbb{N}^*$ sei p_n die n-te Primzahl. Dann ist

$$(p_n)_{n\in\mathbb{N}} = (2, 3, 5, 7, 11, 13, \dots).$$

Übrigens: An diesem Beispiel können Sie ein Problem der Pünktchen-Schreibweise für Folgen erkennen: Sie ist etwas ungenau. Hätten wir nicht genau gesagt, dass p_n die n-te Primzahl sein soll, sondern lediglich die Pünktchenschreibweise angegeben, so wäre nicht wirklich klar gewesen, ob das nächste Folgenglied nach der 13 tatsächlich die Zahl 17 oder vielleicht doch eher die Zahl 15 – oder vielleicht doch eine ganze andere Zahl – ist.

In den vorangehenden Beispielen haben Sie bereits zwei Möglichkeiten gesehen um die Glieder einer Folge exakt zu beschreiben: Man kann dies – zumindest für manche Folgen – jedes Folgenglied mit Hilfe einer Formel oder mit Hilfe von Worten beschreiben.

Es gibt noch eine weitere sehr nützliche Möglichkeit um alle Glieder einer Folge festzulegen: die **Rekursion**. Dabei legt man das führende Glied der Folge fest – wenn die Indexmenge gleich $\mathbb{N}$ ist also das 0-te Folgenglied – und beschreibt außerdem, wie man aus jedem Folgenglied das nachfolgende Folgenglied erhält.

Das lässt sich am besten an einige Beispiele verstehen:

Beispiele 3.1.3 (Einige Beispiele für rekursive definierte Folgen)**.** (a) Wir definieren eine Folgen $(s_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ durch $a_0 \coloneqq \frac{7}{4}$ und $s_{n+1} \coloneqq 2s_n - 1$ für jedes $n \in \mathbb{N}$.

Zum Beispiel die ersten fünf Folgenglieder sind dann also

$$s_0 = \frac{7}{4}, \quad s_1 = \frac{5}{2}, \quad s_2 = 4, \quad s_3 = 7, \quad s_4 = 13.$$

(b) Wir definieren eine Folge $(n!)_{n\in\mathbb{N}_0}$ durch $0! \coloneqq 1$ und $(n+1)! \coloneqq n! \cdot (n+1)$ for jedes $n \in \mathbb{N}$. Man spricht die Zahl $n!$ aus als „n Fakultät“.[1]

Sie können sich leicht überlegen, dass für jedes n die Formel $n! = 1 \cdot 2 \cdots (n-1) \cdot n$ gilt.

(c) Am Anfang des Beweises des Theorems 2.5.7 von Cantor–Bernstein–Schröder hatten wir eine Folgen $(C_n)_{n\in\mathbb{N}}$ von Teilmengen von X – das heißt also eine Folge in $\mathcal{P}(X)$ – rekursiv definiert durch den Rekursionsbeginn $C_0 \coloneqq X \setminus g(Y)$ und die Rekursionsvorschrift $C_{n+1} \coloneqq g\big(f(C_n)\big)$.

(d) Man kann Folgen auch rekursive definieren, indem man zum Beispiel die ersten beiden Folgenglieder festlegt und zudem angibt, wie man aus zwei aufeinander folgenden Folgenglieder das nächste erhält.

Seien zum Beispiel $f_0 \coloneqq 0$ und $f_1 \coloneqq 1$ und für jedes $n \in \mathbb{N}$ sei $f_{n+2} = f_{n+1} + f_n$. Die Folge $(f_n)_{n\in\mathbb{N}}$ nennt man die **Fibonacci-Folge**. Ihre ersten Glieder sind

$$f_0 = 0, \quad f_1 = 1, \quad f_2 = 1, \quad f_3 = 2, \quad f_4 = 3,$$
$$f_5 = 5, \quad f_6 = 8, \quad f_7 = 13, \quad f_8 = 21, \quad \ldots$$

Zum Abschluss dieses Abschnitts definieren wir noch eine sehr nützliche Schreibweise für Summen und Produkte von Zahlen:

Definition 3.1.4 (Summen- und Produkt-Schreibweise)**.** Seien $m, n \in \mathbb{Z}$ mit $m \leq n$ und seien $a_m, a_{m+1}, \ldots, a_{n-1}, a_n \in \mathbb{R}$. Wir definieren

$$\sum_{k=m}^{n} a_k \coloneqq a_m + a_{m+1} + \cdots + a_{n-1} + a_n$$

und

$$\prod_{k=m}^{n} a_k \coloneqq a_m \cdot a_{m+1} \cdot \cdots \cdot a_{n-1} \cdot a_n.$$

Hierbei ist k der sogenannte **Laufindex**.[2] Die Wahl der Variablen k für den Laufindex spielt keine Rolle – man kann stattdessen auch jedes andere Variable verwenden, die im gegebenen Kontext noch nicht mit einer anderen Bedeutung belegt ist.

[1] Auf Englisch „n factorial“.

[2] In der Summe $\sum_{k=m}^{n} a_k$ nennt man den Laufindex manchmal auch **Summationsindex**.

Der Zusammenhang der Summen- und Produktnotation mit dem Thema dieses Abschnitts ist folgendermaßen: Wenn man bei der Definition der beiden Notationen noch etwas genauer sein und die Pünktchen vermeiden will, so kann man sie rekursiv definieren: Hat man zum Beispiel eine Folge $(a_k)_{k\in\mathbb{N}}$ gegeben, so kann man für jedes $n \in \mathbb{N}$ die Summe $\sum_{k=0}^{n} a_k$ rekursiv definieren durch

$$\sum_{k=0}^{0} a_k := a_0,$$
$$\sum_{k=0}^{n+1} a_k := a_{n+1} + \sum_{k=0}^{n} a_k \quad \text{für alle } n \in \mathbb{N}.$$

Beispiele 3.1.5 (Einige Beispiele für Summen und Produkte)**.** (a) Für jedes $n \in \mathbb{N}^*$ kann man $n!$ schreiben als $n! = \prod_{k=1}^{n} k$.

(b) Für jedes $n \in \mathbb{N}$ ist $\sum_{k=0}^{n} = 0 + 1 + 2 + \cdots + (n-1) + n$.

(c) Für jedes $n \in \mathbb{N}^*$ ist $\sum_{k=1}^{n}(2k-1) = 1 + 3 + \cdots + (2n-1)$ gleich die Summe der ersten n ungeraden Zahlen.

(d) Für jedes $n \in \mathbb{N}^*$ ist $\prod_{k=1}^{n} 2 = 2 \cdot \cdots \cdot 2 = 2^n$.

3.2 Induktion

Die natürlichen Zahlen haben eine sehr nützliche Eigenschaft, die Teil der Definition der natürlichen Zahlen sind und die wir deshalb im folgenden in einer Definition auflisten.

Definition 3.2.1 (Prinzip der vollständigen Induktion)**.** Für jedes $n \in \mathbb{N}$ sei eine Aussage $A(n)$ gegeben. Falls $A(0)$ gilt und zudem die Aussage

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

gilt, dann gilt $A(n)$ für alle $n \in \mathbb{N}$.

Wenn wir also eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ beweisen wollen, dann genügt es zu zeigen, dass $A(0)$ gilt[3] und dass für jedes $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$ gilt.[4] Man muss übrigens nicht unbedingt bei 0 anfangen: Sie können zum Beispiel auch die ersten drei Aussagen $A(0)$, $A(1)$ und $A(2)$ direkt überprüfen und müssen dann die Implikation $A(n) \Rightarrow A(n+1)$ nur für alle $n \geq 2$ zeigen.

Lassen Sie uns das an einigen Beispielen zeigen.

[3] Das zu zeigen, bezeichnet man auch als **Induktionsanfang**.
[4] Das zu zeigen bezeichnet man auch als **Induktionsschritt**.

Beispiel 3.2.2 (Gaußsche Summenformel)**.** Für jedes $n \in \mathbb{N}$ gilt die Formel

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

Beweis. Wir beweisen die Aussage mit Hilfe des Prinzips der vollständigen Induktion. Für jedes $n \in \mathbb{N}$ bezeichne $A(n)$ die Aussage „Es gilt $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$“.

Dann ist $A(0)$ wahr, denn es ist $\sum_{k=0}^{0} k = 0 = \frac{0\cdot(0+1)}{2}$.

Als nächstes zeigen wir, dass für jedes $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$ gilt. Sei dazu $n \in \mathbb{N}$ beliebig und sei $A(n)$ wahr. Dann ist

$$\begin{aligned}\sum_{k=0}^{n+1} k &= \sum_{k=0}^{n} k \;+\; n+1 \overset{A(n)}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} = \frac{((n+1)(n+1)}{2} = \frac{(n+1)\big((n+1)+1\big)}{2}.\end{aligned}$$

Also ist $A(n+1)$ wahr.

Somit haben wir die Implikation $A(n) \Rightarrow A(n+1)$ für jedes $n \in \mathbb{N}$ gezeigt. Aufgrund des Prinzips der vollständigen Induktion aus Definition 3.2.1 ist somit $A(n)$ für jedes $n \in \mathbb{N}$ wahr. □

Folgendes Resultat zeigt, dass man bei Induktionsbeweisen nicht unbedingt bei 0 beginnen muss:

Lemma 3.2.3 (Induktion ab einer beliebigen Zahl)**.** *Sei $n_1 \in \mathbb{Z}$ und für jedes $n \in \mathbb{Z}$ sei eine Aussage $A(n)$ gegeben. Falls $A(n_1)$ gilt und zudem die Aussage*

$$\forall n \in \mathbb{Z} \text{ mit } n \geq n_1 : \big(A(n) \Rightarrow A(n+1)\big)$$

gilt, dann gilt $A(n)$ für alle $n \in \mathbb{Z}$ mit $n \geq n_1$.

Beweis. Bezeichne für jedes $n \in \mathbb{N}$ mit $B(n)$ die Aussage $A(n+n_1)$. Weil $A(n_1)$ wahr ist, ist $B(0)$ wahr. Für jedes $n \in \mathbb{N}$ gilt außerdem $n + n_1 \geq n_1$ und somit gilt Voraussetzung die Implikation $A(n+n_1) \Rightarrow A(n+n_1+1)$; also gilt die Implikation $B(n) \Rightarrow B(n+1)$. Laut Definition 3.2.1 ist somit $B(n)$ für alle $n \in \mathbb{N}$ wahr. Also gilt $A(n+n_1)$ für alle $n \in \mathbb{N}$ und somit gilt $A(n)$ für alle $n \in \mathbb{Z}$ mit $n \geq n_1$ □

Theorem 3.2.4 (Starke Induktion)**.** *Seien $n_0, n_1 \in \mathbb{Z}$ mit $n_0 \leq n_1$ und für jede Zahl $n \in \mathbb{Z}$ mit $n \geq n_0$ sei eine Aussage $A(n)$ gegeben. Falls $A(n_0), \ldots, A(n_1)$ wahr sind und falls für alle $n \geq n_1$ die Implikation*

$$\Big(A(n_0) \wedge \cdots \wedge A(n)\Big) \Rightarrow A(n+1)$$

gilt, dann ist $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ wahr.

Beweis. Für jedes $n \in \mathbb{N}$ mit $n \geq n_1$ kürzen wir die Aussage $A(n_0), \ldots, A(n)$ mit $B(n)$ ab. Laut Voraussetzung ist $B(n_1)$ wahr. Außerdem gilt für jedes $n \in \mathbb{Z}$ mit $n \geq n_1$ die Implikation $B(n) \Rightarrow B(n+1)$: Wenn nämlich $B(n)$ wahr ist, dann sind $A(n_0), \ldots, A(n)$ wahr; somit ist nach Voraussetzung auch $A(n+1)$ wahr und somit ist $B(n+1)$ wahr.

Laut Lemma 3.2.3 ist somit $B(n)$ für alle $n \in \mathbb{Z}$ mit $n \geq n_1$ wahr. Folglich ist $A(n)$ für alle $n \in \mathbb{Z}$ mit $n \geq n_0$ wahr. □

Beispiel 3.2.5 (Fibonacci-Zahlen)**.** Sei $\varphi_+ \coloneqq \frac{1+\sqrt{5}}{2}$ und $\varphi_- \coloneqq \frac{1-\sqrt{5}}{2}$ (übrigens wird die Zahl $\frac{1+\sqrt{5}}{2}$ oft als der **Goldene Schnitt** bezeichnet). Für die Fibonacci-Folge (f_n) gilt die Formel

$$f_n = \frac{\varphi_+^n - \varphi_-^n}{\varphi_+ - \varphi_-}$$

für alle $n \in \mathbb{N}$.

Beweis. Zunächst beobachten wir, dass für die beiden Zahlen φ_+ und φ_- die Formeln $\varphi_+^2 = \varphi_+ + 1$ und $\varphi_-^2 = \varphi_- + 1$ gelten.

Nun beweisen wir die behauptete Aussage per starker Induktion über n. Für jedes $n \in \mathbb{N}$ bezeichne $A(n)$ die Aussage „Es gilt $f_n = \frac{\varphi_+^n - \varphi_-^n}{\varphi_+ - \varphi_-}$." Wir wollen Theorem 3.2.4 mit $n_0 = 0$ und $n_1 = 1$ anwenden.

Die Aussage $A(0)$ ist wahr, denn es ist

$$\frac{\varphi_+^0 - \varphi_-^0}{\varphi_+ - \varphi_-} = \frac{1-1}{\varphi_+ - \varphi_-} = 0 = f_0.$$

Außerdem ist $A(1)$ wahr, denn es ist

$$\frac{\varphi_+^1 - \varphi_-^1}{\varphi_+ - \varphi_-} = 1 = f_1.$$

Nun zeigen wir, dass für alle $n \in \mathbb{N}$ mit $n \geq 1$ die Implikation $\Big(A(0) \wedge A(1) \wedge \cdots \wedge A(n)\Big) \Rightarrow A(n+1)$ gilt. Sei dazu $n \in \mathbb{N}$ beliebig. Wir nehmen an, dass $A(n)$ war ist. Dann folgt

$$\begin{aligned} f_{n+1} = f_n + f_{n-1} &\overset{A(n-1) \text{ und } A(n) \text{ sind wahr}}{=} \frac{\varphi_+^n - \varphi_-^n}{\varphi_+ - \varphi_-} + \frac{\varphi_+^{n-1} - \varphi_-^{n-1}}{\varphi_+ - \varphi_-} \\ &= \frac{\varphi_+^{n-1}(\varphi_+ + 1) - \varphi_-^{n-1}(\varphi_- + 1)}{\varphi_+ - \varphi_-} = \frac{\varphi_+^{n+1} - \varphi_-^{n+1}}{\varphi_+ - \varphi_-}, \end{aligned}$$

wobei die letzte Gleichheit wegen der beiden Gleichheiten im ersten Absatz des Beweises gilt. Also haben wir gezeigt, dass $A(n+1)$ wahr ist.

Laut Theorem 3.2.4 ist also $A(n)$ für alle $n \geq n_0 = 0$ wahr. □

3.3 Primzahlen

In diesem kurzen Abschnitt wollen wir das Induktionsverfahren aus Theorem 3.2.4 benutzen um die Existenz von Primfaktorzerlegungen natürlicher Zahlen zu beweisen. Dazu wiederholen wir zunächst noch einmal, was genau eine Primzahl ist:

Definition 3.3.1 (Primzahlen)**.** Eine Zahl $p \in \mathbb{N}^*$ heißt prim, falls sie ungleich 1 ist und nur durch 1 und sich selbst teilbar ist.

Lassen Sie uns nun beweisen, dass man jede natürliche Zahl ab 2 in Primfaktoren zerlegen kann.[5]

Theorem 3.3.2 (Existenz der Primfaktorzerlegung)**.** *Sei $n \in \mathbb{N}^*$ und $n \neq 1$. Dann besitzt n eine Primfaktorzerlegung, das heißt, es gibt es ein $m \in \mathbb{N}^*$ und Primzahlen $p_1, \ldots, p_m \in \mathbb{N}^*$ derart, dass $n = p_1 \cdot p_2 \cdot \cdots \cdot p_m$ gilt.*

Beweis. Für jedes $n \in \mathbb{N}$ mit $n \geq 2$ sei $A(n)$ die Aussage „Die Zahl n besitzt eine Primfaktorzerlegung.“ Wir wenden Theorem 3.2.4 für $n_0 = n_1 = 2$ an.

Die Aussage $A(2)$ stimmt, weil 2 seine eigene Primfaktorzerlegung ist – das heißt wir können 2 schreiben als $2 = p_1 \cdot \cdots \cdot p_m$ mit $m = 1$ und $p_1 = 2$. Wir zeigen nun, dass für alle $n \in \mathbb{N}$ mit $n \geq 2$ die Aussage $\Big(A(2) \wedge \cdots \wedge A(n)\Big) \Rightarrow A(n+1)$ stimmt.

Sei dazu $n \in \mathbb{N}$ mit $n \geq 2$ beliebig und seien $A(2), \ldots, A(n)$ wahr. Wir unterscheiden zwei Fälle:

- *Erster Fall:* Die Zahl $n+1$ ist eine Primzahl.

  In diesem Fall ist $n+1$ ihre eigene Primfaktorzerlegung, also ist $A(n+1)$ wahr.

- *Zweiter Fall:* Die Zahl $n+1$ ist keine Primzahl.

  In diesem Fall können wir $n+1$ schreiben als $n+1 = bc$ für zwei Zahlen $bc \in \{2, \ldots, n\}$. Weil $A(2), \ldots, A(n)$ wahr sind, sind insbesondere $A(b)$ und $A(c)$ wahr. Somit können wir b und c als Produkt von Primzahlen schreiben und somit ist auch $n+1 = bc$ ein Produkt von Primzahlen. Also ist $A(n+1)$ wahr.

In jedem Fall ist also $A(n+1)$ wahr. Laut Theorem 3.2.4 gilt also $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq 2$. □

Die Primfaktorzerlegung existiert nicht nur, sondern sie ist auch eindeutig:

[5] Genau genommen kann man auch die Zahl 1 als ein Produkt von Primzahlen schreiben – nämlich als ein sogenanntes leeres Produkt. Auf diesen Begriff kommen wir später im Verlauf der Vorlesung noch einmal genauer zurück.

Theorem 3.3.3 (Eindeutigkeit der Primfaktorzerlegung)**.** *Sei $n \in \mathbb{N}^*$ mit $n \neq 1$. Die Primzahlen $p_1, \ldots, p_m$ aus Theorem 3.3.2, die $n = p_1 \cdot p_2 \cdot \cdots \cdot p_m$ erfüllen, sind bis auf Ihre Reihenfolge eindeutig bestimmt.*[6]

Den Beweis des Theorems verschieben wir auf später in der Vorlesung, wenn wir einige Hilfsresultate über Teilbarkeit von ganzen Zahlen bewiesen haben. Sie finden den Beweis am Ende von Abschnitt 4.5. In der Zwischenzeit dürfen Sie das Theorem aber bereits für Übungsaufgaben verwenden.

3.4 Binomialkoeffizienten

In diesem Abschnitt besprechen wir ein Konzept, dass im mathematische Teilgebiet *Kombinatorik* – das ist das Gebiet, dass sich mit dem Zählen von Objekten beschäftigt – sehr nützlich ist, nämlich die sogenannten *Binomialkoeffizienten*.

Definition 3.4.1 (Binomialkoeffizient)**.** Für alle $n, k \in \mathbb{N}$ definieren wir

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{falls } k \leq n, \\ 0 & \text{falls } k > n. \end{cases}$$

In der Vorlesung *Analyis 1* werden Sie sehen, dass man Binomialkoeffizienten $\binom{n}{k}$ sogar sinnvoll definieren kann, wenn $k \in \mathbb{N}$ und $n \in \mathbb{R}$ ist (oder noch allgemeiner, wenn n eine komplexe Zahl ist). Im Moment begnügen wir uns aber mit dem Fall $n \in \mathbb{N}$ – dieser ist bereits sehr interessant, wie Sie im folgenden sehen werden.

Lassen Sie uns einige grundlegende Eigenschaften von Binomialkoeffizienten zeigen:

Proposition 3.4.2 (Eigenschaften von Binomialkoeffizienten)**.** *Seien $n, k \in \mathbb{N}$.*

(a) *Es gilt $\binom{n}{0} = \binom{n}{n} = 1$.*

(b) *Es gilt $\binom{n}{1} = n$.*

(c) *Falls $k \leq n$ ist, gilt $\binom{n}{k} = \binom{n}{n-k}$.*

(d) *Es gilt $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.*

(e) *Es gilt $\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}$.*

Beweis. (a) Laut Definition 3.4.1 gilt $\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1$ und $\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1$, da $0! = 1$ ist.

[6] Beachte Sie, dass manche der Primzahlen $p_1, \ldots, p_m$ gleich sein können. Wenn wir sagen, dass $p_1, \ldots, p_m$ bis auf Reihenfolge eindeutig bestimmt sind, so beinhaltet das auch die Aussage, das m eindeutig bestimmt ist und dass eindeutig bestimmt ist, wie oft jede Primzahl innerhalb der Zahlen $p_1, \ldots, p_m$ vorkommt.

(b) Falls $n = 0$ ist, sind beide Seite der behaupteten Gleichheit gleich 0. Falls $n \geq 1$ ist, gilt $\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$.

(c) Wegen $0 \leq k \leq n$ ist auch $0 \leq n - k \leq n$ und somit gilt laut Definition 3.4.1 $\binom{n}{n-k} = \frac{n!}{(n-k)!\big(n-(n-k)\big)!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$.

(d) Um zu wissen, in welchem der beiden Fälle in Definition 3.4.1 wir jeweils sind, unterscheiden wir folgende Fälle:

- *Erster Fall: $k > n$.*

  In diesem Fall ist auch $k + 1 > n$ und $k + 1 > n + 1$, also gilt $\binom{n}{k} + \binom{n}{k+1} = 0 + 0 = 0 = \binom{n+1}{k+1}$.

- *Zweiter Fall: $k = k$.*

  In diesem Fall ist auch $k + 1 = n + 1$, aber $k + 1 > n$, also gilt $\binom{n}{k} + \binom{n}{k+1} = 1 + 0 = 1 = \binom{n+1}{k+1}$, wobei wir den bereits bewiesenen Teil (a) der Proposition verwendet haben.

- *Dritter Fall: $k < n$.*

  In diesem Fall $k + 1 < n + 1$ und $k + 1 \leq n$, also gilt

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

(e) Wir beweisen die Behauptung per Induktion über n. Dazu halten wir $k \in \mathbb{N}$ fest und bezeichnen für jedes $n \in \mathbb{N}$ mit $A(n)$ die Aussage „Es gilt $\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}$“.

Die Aussage $A(0)$ ist wahr, denn es gilt $\sum_{m=0}^{0} \binom{m}{k} = \binom{0}{k} = \binom{1}{k+1} = \binom{0+1}{k+1}$; dass die zweite dieser Gleichheiten gilt, kann man sehen, indem man die beiden Fälle $k = 0$ und $k \geq 1$ unterscheidet.

Nun zeigen wir für jedes $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$. Sei dazu $n \in \mathbb{N}$ beliebig und sei $A(n)$ wahr. Dann gilt

$$\begin{aligned}\sum_{m=0}^{n+1} \binom{m}{k} = \sum_{m=0}^{n} \binom{m}{k} + \binom{n+1}{k} &\overset{A(n)}{=} \binom{n+1}{k+1} + \binom{n+1}{k} \\ &\overset{\text{(d)}}{=} \binom{n+2}{k+1} = \binom{(n+1)+1}{k+1}.\end{aligned}$$

Also ist $A(n+1)$ wahr.

Aufgrund des Prinzips der vollständigen Induktion (Definition 3.4.1) folgt somit, dass $A(n)$ für alle $n \in \mathbb{N}$ wahr ist. □

Mehrere Eigenschaften, die wir in Proposition 3.4.2 bewiesen haben, kann man veranschaulichen, indem man einige der Binomialkoeffizienten $\binom{n}{k}$ in eine Tabelle einträgt:

$\binom{n}{k}$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
$n=0$	1	0	0	0	0	0	0	0	0
$n=1$	1	1	0	0	0	0	0	0	0
$n=2$	1	2	1	0	0	0	0	0	0
$n=3$	1	3	3	1	0	0	0	0	0
$n=4$	1	4	6	4	1	0	0	0	0
$n=5$	1	5	10	10	5	1	0	0	0
$n=6$	1	6	15	20	15	6	1	0	0
$n=7$	1	7	21	35	35	21	7	1	0
$n=8$	1	8	28	56	70	56	28	8	1

Dass die Einträge oberhalb der Diagonalen gleich 0 sind, folgt direkt aus Definition 3.4.1. In der Tabelle finden sich außerdem viele Aussagen von Proposition 3.4.2 wieder:

- Dass in der Spalte mit $k = 0$ und sowie auf der Diagonalen überall die 1 steht, folgt aus Proposition 3.4.2(a).
- Die Einträge in der Spalte $k = 1$ sind genau so, wie Proposition 3.4.2(b) es besagt.
- In jeder Zeile der Tabelle können Sie von $k = 0$ bis $k = n$ eine Symmetrie der Binomialkoeffizienten sehen: Die Zahlen bis zur Mitte wiederholen sich anschließend in umgekehrter Reihenfolge wieder. Das ist genau die Aussage von Proposition 3.4.2(c).
- Proposition 3.4.2(d) besagt folgendes: Wenn man zwei nebeneinander stehende Einträge in der Tabelle addiert, dann erhält man die Zahl, die unter dem rechten der beiden Einträge steht.

  Mit dieser Beobachtung kann man übrigens alle Einträge der Tabelle rekursive berechnen ohne die explizite Formel aus Definition 3.4.1 zu verwenden: Man trägt zuerst die Nullen ein sowie die Einsen in der Spalte ganz links und auf der Diagonalen. Anschließend geht man die nächste Spalte (für $k = 1$ von oben nach unten durch – man kann alle ihre Einträge bis zu einem gewünschte n durch Addition berechnen. Dann macht man dasselbe für die Spalte $k = 2$ und so weiter.
- Proposition 3.4.2(d) besagt folgendes: Wenn man in einer Spalte der Tabelle von oben an alle Zahlen bis einer Zeile mit der Nummer n addiert, dann erhält man den Eintrag, der rechts davon in der Zeile $n + 1$ steht.

Den Teil der Tabelle, in dem keine Nullen stehen (also den Teil auf und unterhalb der Diagonalen) bezeichnet man als **Pascalsches Dreieck**. Um die Symmetrie

innerhalb der Zeilen deutlicher hervorzuheben, ist es üblich jede neue Zeile um einen halben Eintrag nach links zu versetzen. Das Pascalsche Dreieck sieht dann folgendermaßen aus:

$\binom{n}{k}$																	
$n=0$								1									
$n=1$							1		1								
$n=2$						1		2		1							
$n=3$					1		3		3		1						
$n=4$				1		4		6		4		1					
$n=5$			1		5		10		10		5		1				
$n=6$		1		6		15		20		15		6		1			
$n=7$	1		7		21		35		35		21		7		1		
$n=8$	1		8		28		56		70		56		28		8		1

Hierbei läuft k in der n-ten Zeile von 0 bis n, das heißt in der n-ten Zeilen sind die Binomialkoeffizienten $\binom{n}{0}$ bis $\binom{n}{n}$ eingetragen. In dieser Schreibweise besagt Proposition 3.4.2(d), dass in die Summe zweier nebeneinander stehenden Einträge jeweils den Wert ergibt, der in der Mitte unter diesen beiden Einträgen steht.

Weil man das Pascalsche Dreieck der Reihe nach Ausfüßllen kann, indem man zwei vorangehende Zahlen addiert und weil man dabei mit den Zahlen 1 beginnt, erhält man sofort die folgende Konsequenz:

Korollar 3.4.3 (Binomialkoeffizienten sind ganzzahlig)**.** *Für alle natürlichen Zahlen n, k gilt $\binom{n}{k} \in \mathbb{N}$.*

Das Korollar ist deshalb bemerkenswert, weil die Ganzzahligkeit der Binomialkoeffizienten nicht unmittelbar aus Definition 3.4.1 ersichtlich ist.

Bemerkung 3.4.4 (Gaußsche Summenformel, nochmal)**.** Die Summenformel für Binomialkoeffizienten in Proposition 3.4.2(e) enthält die Gaußsche Summenformel aus Beispiel 3.2.2 als Spezialfall: Für jedes $n \in \mathbb{N}$ gilt nämlich

$$\sum_{m=0}^{n} m = \sum_{m=0}^{n} \binom{m}{1} = \binom{n+1}{2},$$

wobei die erste Gleichheit laut Proposition 3.4.2(b) gilt und die zweite Gleichheit aus Proposition 3.4.2(e) für $k = 1$ folgt. Für $n = 0$ ist $\binom{n+1}{2} = 0 = \frac{n(n+1)}{2}$ und für $n \geq 1$ ist

$$\binom{n+1}{2} = \frac{(n+1)!}{2!(n-1)!} = \frac{n(n+1)}{2},$$

also erhält man auch so die Gaußsche Summenformel.

Ein Grund, weshalb Binomialkoeffizienten nützlich sind, ist, dass man mit ihrer Hilfe zählen kann, wieviele Teilmenge einer bestimmten Kardinalität eine gegebene Menge besitzt:

Theorem 3.4.5. *Seien $n, k \in \mathbb{N}$. Jede Menge mit n Elementen besitzt genau $\binom{n}{k}$ Teilmengen mit k Elementen.*

Beweis. Wir zeigen die Behauptung per Induktion über n. Für jedes $n \in \mathbb{N}$ bezeichnen wir mit $A(n)$ die Aussage „Für jedes $k \in \mathbb{N}$ gilt: Jede Menge mit n Elementen besitzt genau $\binom{n}{k}$ Teilmengen mit k Elementen“.

Wir beobachten zunächst, dass $A(0)$ wahr ist. Sei nämlich X eine Menge mit 0 Elementen und sei $k \in \mathbb{N}$. Dann ist $X = \emptyset$. Wenn $k = 0$ ist, besitzt X genau 1 Teilmenge mit k Elementen – nämlich die Menge $\emptyset$ – und zugleich gilt $\binom{0}{k} = \binom{0}{0} = 1$. Wenn $k \geq 1$ ist, besitzt X genau 0 Teilmengen mit k Elementen und zugleich gilt $\binom{0}{k} = 0$. Also ist $A(0)$ tatsächlich wahr.

Nun zeigen wir für jedes $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$. Sei dazu $n \in \mathbb{N}$ beliebig und sei $A(n)$ wahr. Wir müssen $A(n+1)$ beweisen. Sei also X eine Menge mit $n+1$ Elementen und sei $k \in \mathbb{N}$.

Der Fall $k = 0$ ist leicht: Wenn $k = 0$ ist, gilt $\binom{n+1}{k} = 1$ und zugleich besitzt X genau eine Teilmenge mit k Elementen (nämlich $\emptyset$).

Sei nun also $k \geq 1$. Wir nummerieren die Elementen von X durch als $x_1, \ldots, x_{n+1}$. Die k-elementigen Teilmengen von X, die x_{n+1} nicht enthalten, sind genau die k-elementigen Teilmengen von $\{x_1, \ldots, x_n\}$ – davon gibt es wegen der Gültigkeit von $A(n)$ genau $\binom{n}{k}$ Stück. Abgesehen davon gibt es noch diejenigen k-elementigen Teilmengen von X; die x_{n+1} enthalten. Davon gibt es genauso viele, wie es $k-1$-elementige Teilmengen von $\{x_1, \ldots, x_n\}$ gibt – also $\binom{n}{k-1}$ aufgrund der Gültigkeit von $A(n)$. Insgesamt besitzt X also $\binom{n}{k-1} + \binom{n}{k}$ Teilmengen mit k Elementen. laut Proposition 3.4.2(d) ist diese Summe gleich $\binom{n+1}{k}$. Damit ist $A(n+1)$ bewiesen.

Wegen des Prinzips der vollständigen Induktion (Definition 3.2.1) ist also $A(n)$ für jedes $n \in \mathbb{N}$ wahr. □

Auch an dieser Stelle ist es nochmals interessant, auf den Zusammenhang zwischen Binomialkoeffizienten und der Gaußschen Summenformel zurückzukommen. Wir tun das in folgendem Beispiel:

Beispiel 3.4.6 (Anstoßen)**.** Nach einer anstrengenden Mathe-Vorlesung am Freitag gehen Sie gemeinsam etwas trinken. Sie sind insgesamt $n \geq 2$ Personen; jede und jeder hält eine Flasche in der Hand. Bevor Sie zu trinken beginnen, stößt jede Person mit jeder anderen einmal an. Wieviele Zusammenstöße von Flaschen gibt es?

Lassen Sie uns zwei verschiedene Möglichkeiten diskutieren um die Anzahl der Zusammenstöße zu berechnen:

- *1. Möglichkeit:* Die erste Person aus Ihrer Gruppe stößt mit allen anderen $n-1$ Personen an. Die zweite Person muss dann noch mit $n-2$ verbleibenden Personen anstoßen. Die dritte Person muss noch mit $n-3$ Personen anstoßen, und so weiter. Die vorletzte Person muss noch mit einer Person anstoßen, und die letzte Person mit gar niemandem mehr. Die Gesamtzahl der Anstöße ist

also

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

wobei die zweite Gleichheit die Gaußsche Summenformel ist.

- *2. Möglichkeit:* Wir stellen uns alle n Personen gemeinsam in einer Menge vor. Für jeden Anstoß benötigt man jeweils genau 2 Personen aus dieser Menge. Also ist die Anzahl der Anstöße gleich der Anzahl der 2-elementigen Teilmengen der Menge. Laut Theorem 3.4.5 sind das genau $\binom{n}{2}$ Stück. Es ist

$$\binom{n}{2}=\frac{n!}{2!(n-2)!}=\frac{n(n-1)}{2},$$

also kommen wir – natürlich – auf dasselbe Ergebnis wie mit Möglichkeit 1.

Ein zweiter Grund, weshalb Binomialkoeffizienten sehr hilfreich sind, ist folgender: Sie erinnern sich aus der Schule gewiss an die binomische Formel

$$(a+b)^2=a^2+2ab+b^2,$$

die für alle Zahlen $a,b\in\mathbb{R}$ gilt; dass die Formel stimmt, sieht man leicht, indem man den Ausdruck $(a+b)^2=(a+b)(a+b)$ einfach ausmultipliziert und zusammenfasst. Was Sie in der Schule vielleicht nicht gesehen haben, ist, dass man eine ähnliche Formel auch für die dritte Potenz herleiten kann: Durch Ausmultiplizieren und zusammenfassen können Sie sich leicht vergewissern, dass für alle $a,b\in\mathbb{R}$ die Formel

$$(a+b)^3=a^3+3a^2b+3ab^2+b^3$$

gilt. Wie sieht es aber mit höheren Potenzen $(a+b)^n$ aus? Das folgende Resultat gibt die Antwort. Um das Resultat richtig zu lesen, muss man sich daran erinnern, dass $x^0=1$ für jedes reelle Zahl x ist.[7]

Theorem 3.4.7 (Binomischer Lehrsatz)**.** *Seien $a,b\in\mathbb{R}$ und sei $n\in\mathbb{N}$. Dann gilt*

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

Beweis. Den Beweis kann man zum Beispiel per Induktion über n führen. Wir lagern ihn in die Übungen aus. □

[7] Insbesondere ist auch 0^0 als 1 definiert.

Es ist für die Intuition sehr hilfreich, wenn man den binomische Lehrsatz für die ersten paar natürlichen Zahlen n einmal ganz ausschreibt. Man erhält

$$\begin{aligned}
(a+b)^0 &= 1 \cdot a^0 b^0 \\
&= 1, \\
(a+b)^1 &= 1 \cdot a^1 b^0 + 1 \cdot a^0 b^1 \\
&= a + b, \\
(a+b)^2 &= 1 \cdot a^2 b^0 + 2 \cdot a^1 b^1 + 1 \cdot a^0 b^2 \\
&= a^2 + 2ab + b^2, \\
(a+b)^3 &= 1 \cdot a^3 b^0 + 3 \cdot a^2 b^1 + 3 \cdot a^1 b^2 + 1 \cdot a^0 b^3 \\
&= a^3 + 3a^2 b + 3ab^2 + b^3, \\
(a+b)^4 &= 1 \cdot a^4 b^0 + 4 \cdot a^3 b^1 + 6 \cdot a^2 b^2 + 4a^4 b^1 + 1 \cdot a^0 b^4 \\
&= a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4.
\end{aligned}$$

Wenn man die Formeln mit den Zeilen im Pascalschen Dreieck vergleicht, kann kann man sehr gut die Binomialkoeffizienten wiedererkennen.

Mit Hilfe der beiden vorangehenden Theoreme kann man zählen, wie viele Teilmengen eine endliche Menge besitzt.

Korollar 3.4.8 (Kardinalität der Potenzmenge)**.** *Sei $n \in \mathbb{N}$. Eine Menge mit n Elementen besitzt genau 2^n Teilmengen.*[8]

Beweis. Sei X eine Menge mit n Elementen. Laut Theorem 3.4.5 besitzt X genau $\binom{n}{0}$ Teilmengen der Kardinalität 0, genau $\binom{n}{1}$ Teilmengen der Kardinalität 1, ..., und genau $\binom{n}{n}$ Teilmengen der Kardinalität n. Insgesamt besitzt X also

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

Teilmengen. Diese Summe kann man schreiben als

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n = 2^n,$$

wobei die zweite Gleichheit aus dem binomischen Lehrsatz (Theorem 3.4.7) folgt. □

Man kann übrigens auch einen anderen Beweis von Korollar 3.4.8 geben, der ohne die beiden Theoreme 3.4.5 und 3.4.7 auskommt. Wir führen ihn hier im Manuskript auf, falls Sie Lust haben, ihn zu lesen (in der Vorlesung wird dieser Beweis aber aus Zeitgründen nicht besprochen):

[8] Anders ausgedrückt: Für jede endliche Menge X gilt $\#\mathcal{P}(X) = 2^{\#X}$. Das ist übrigens eine Motivation dafür, dass manche Leute für die Potenzmenge einer Menge X die Notation 2^X anstelle der Notation $\mathcal{P}(X)$ verwenden; mit dieser alternativen Notation gilt also $\#(2^X) = 2^{\#X}$.

Alternativer Beweis von Korollar 3.4.8. Sei X eine Menge mit n Elementen. Für jede Teilmenge $M \subseteq X$ sei die Funktion $\mathbb{1}_M : X \to \{0,1\}$ gegeben durch[9]

$$\mathbb{1}_M(x) = \begin{cases} 1, & \text{falls } x \in M, \\ 0, & \text{falls } x \notin M. \end{cases}$$

Nun sei $\mathcal{F}$ die Menge aller Funktionen von X nach $\{0,1\}$. Dann besitzt $\mathcal{F}$ genau 2^n Elemente.

Zugleich kann man nachprüfen, dass die Abbildung

$$\begin{aligned} \varphi : \mathcal{P}(X) &\to \mathcal{F}, \\ M &\mapsto \mathbb{1}_M \end{aligned}$$

bijektiv ist (das haben Sie im Detail in einem Großtutorium gesehen). Also besitzen $\mathcal{P}(X)$ und $\mathcal{F}$ gleich viele Elemente, das heißt, auch $\mathcal{P}(X)$ besitzt 2^n Elemente. □

3.5 Ergänzung: Die Peano-Axiome

Wir haben in dieser Vorlesung nicht sauber definiert, was die natürlichen Zahlen sind. Lediglich die Tatsache, dass das Prinzip der vollständigen Induktion Teil ihrer Definition ist, wurde in Abschnitt 3.2 erwähnt. Um genauer zu verstehen, was die natürlichen Zahlen eigentlich sind, kann man sie mit Hilfe der sogenannten **Peano-Axiome** beschrieben. Details dazu finden Sie beispielsweise in [For15, Kapitel 1].

[9] Man bezeichnet die Funktion $\mathbb{1}_M$ auch als die **Indikatorfunktion** der Menge M.

Kapitel 4

Algebraische Strukturen

Einstiegsfragen. (a) Erinnern Sie sich, was das Assoziativgesetz für die Addition reeller Zahlen besagt?

Kennen Sie noch weitere Rechenoperationen, die ebenfalls assoziativ sind? Kennen Sie auch Rechenoperationen, die nicht assoziativ sind?

(b) Wenn Sie zu einer gegebenen reellen Zahl r die Zahl 5 addieren – wie können Sie das wieder rückgängig machen?

Wenn Sie eine gegebene reelle Zahl r mit π multiplizieren – wie können Sie das wieder rückgängig machen?

Wenn Sie ein Blatt Papier auf Ihrem Tisch um 35 Grad gegen den Uhrzeigersinn drehen – wie können Sie das wieder rückgängig machen?

Was haben die vorangehenden drei Fragen miteinander zu tun?

(c) Was halten Sie von der Aussage $1 + 1 = 0$?

(d) Auf G.15 gibt es zwischen Treppenhaus und Büros zwei Glastüren. Wenn ich mit einer anderen Person aus dem Aufzug steige, halte ich manchmal die erste Türe auf; die andere Person revanchiert sich, in dem sie mir die zweite Türe aufhält. Wenn nun aber drei Personen aus dem Aufzug steigen. . . ?

4.1 Assoziative Verknüpfungen und Halbgruppen

Halbgruppen

In diesem Abschnitt werden wir über sogenannte **assoziative binäre Verknüpfungen** sprechen. Um dies effizient tun zu können, besprechen wir zunächst kurz verschiedene Notationen für Funktionen, die wir bisher noch nicht explizit diskutiert haben.

Wenn X and Y Mengen sind und $f : X \to Y$ eine Funktion ist, so wissen Sie bereits, dass man den Funktionswert von f an einem Element $x \in X$ üblicherweise

mit $f(x)$ bezeichnet. Es gibt aber auch noch andere mögliche Notationen für eine Funktion:

Bemerkungen 4.1.1 (Postfix- und Infix-Notation für Funktionen)**.** (a) Für jede natürliche Zahl $n \in \mathbb{N}^*$ nennt man das Produkt aller Zahlen von 1 bis n die **Fakultät** von n. Man bezeichnet sie überlicherweise mit dem Symbol $n!$. Außerdem erweist es sich als nützlich, auch die Fakultät von 0 zu definieren, und zwar als 1 (d.h., $0! = 1$ per Definition).

Wie Sie sehen, ist die Fakultät eine Abbildung, nämlich die Abbildung

$$\begin{aligned} \mathbb{N} &\to \mathbb{N}^*, \\ n &\mapsto n!, \end{aligned}$$

wobei $n!$ definiert ist wie oben beschrieben.

Wenn man zur Notation einer Abbildung ein Symbol benutzt und dieser aber *hinter* das Argument setzt, so bezeichnet man dies als **Postfix-Notation** für diese Funktion.

(b) Eine der wichtigsten Abbildungen, die Sie kennen, ist die Addition reeller Zahlen. Es handelt sich dabei um eine Abbildung von $\mathbb{R}^2$ nach $\mathbb{R}$ (denn die Abbildung nimmt sich ein Tupel aus zwei reellen Zahlen und weist diesem Tupel die Summe der beiden Zahlen zu).

Das Symbol für diese Abbildung, nämlich „+“, schreibt man aber üblicherweise *zwischen* den beiden Zahlen, die man addiert. Dies bezeichnet man als **Infix-Notation**.

Neben der Addition reeller Zahlen gibt es noch viele weitere Funktionen, die je zwei Elementen aus einer gegebenen Menge X ein weiteres Element aus X zuweisen. Für solche Abbildung verwendet man oft die folgende recht intuitive Terminologie:

Sei X eine Menge. Eine **binäre**[1] Verknüpfung auf X ist eine Abbildung von X^2 nach X. Genau wie die Addition reeller Zahlen notiert man auch andere binäre Verknüpfungen häufig[2] mit Hilfe der Infix-Notation.

Besonders interessant sind binäre Verknüpfungen, die **assoziativ** sind:

Definition 4.1.2 (Halbgruppe)**.** (a) Unter einer **Halbgruppe** versteht man ein Tupel $(X, \circ)$, bestehend aus einer Menge X und einer Abbildung[3] $\circ$, die folgende Eigenschaften erfüllt:

(HG0) *Binäre Verknüpfung auf X:* Es gilt $\circ : X^2 \to X$.

(HG1) *Assoziativgesetz*:

$$\forall a, b, c \in X : \quad (a \circ b) \circ c = a \circ (b \circ c).$$

[1] Oder auch: **zweistellige**.

[2] Aber nicht immer.

[3] Die man üblicherweise mit Infix-Notation notiert, d.h. also, man schreibt für $a, b \in X$ lieber $a \circ b$ anstelle von $\circ(a, b)$.

(b) Eine Halbgruppe $(X, \circ)$ heißt **kommutativ**[4], falls sie das sogenannte **Kommutativgesetz** erfüllt:

$$\forall a, b \in X : \quad a \circ b = b \circ a.$$

Einige Beispiele für Halbgruppen kann man sofort erhalten, wenn man die Addition und Multiplikation reeller Zahlen verwendet; es gibt aber noch viele weitere Beispiele für Halbgruppen. Dies ist gerade der Reiz bei dieser Begriffsbildung: Mit de axiomatischen Definition einer Halbgruppe erfasst man zahlreiche verschiedene mathematische Objekte auf einmal – und alles, was man für allgemeine Halbgruppen beweist, stimmt somit automatisch für jedes Objekt, das eine Halbgruppe ist.

Lassen Sie uns zunächst einige einfache Beispiele von Halbgruppen aufzählen:[5]

Beispiele 4.1.3. (a) Es sind $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ Halbgruppen (wobei $+$ die übliche Addition und $\cdot$ die übliche Multiplikation bezeichnet).

(b) Ebenso sind $(\mathbb{N}^*, +)$ und $(\mathbb{N}^*, \cdot)$ Halbgruppen.

(c) Es ist $(\mathbb{N} \cup \{-1\}, +)$ keine Halbgruppe, denn $+$ ist keine binäre Verknüpfung auf der Menge $\mathbb{N} \cup \{-1\}$ (weil nämlich $(-1) + (-1) = -2 \notin \mathbb{N} \cup \{-1\}$ ist).

(d) Sei $\star : \mathbb{R}^2 \to \mathbb{R}$ durch $a \star b = a^2 b$ für alle $(a, b) \in \mathbb{R}^2$ gegeben. Dann ist $(\mathbb{R}, \star)$ keine Halbgruppe, weil die binäre Verknüpfung $\star$ nicht assoziativ ist.

(e) Es ist $\big(\{-1, 0, 1\}, \cdot\big)$ eine Halbgruppe (wobei $\cdot$ hier wieder die übliche Multiplikation bezeichnet).

Ein etwas interessanteres Beispiel ist das folgende.

Beispiel 4.1.4. Sei X eine Menge und bezeichne $\mathrm{Abb}(X; X)$ die Menge aller Abbildungen von X nach X. Außerdem bezeichnen wir mit $\circ$ die Hintereinanderausführung von Abbildungen.[6] Dann ist $(\mathrm{Abb}(X; X), \circ)$ eine Halbgruppe.

[4] Oder auch: **Abelsch** – benannt nach dem norwegischen Mathematiker Niels Henrik Abel (1802 in Frindöe, Norwegen, – 1829 in Froland, Norwegen).

[5] In den Übungen werden Sie noch weitere kennenlernen.

[6] Beachten Sie, dass man hier unbedingt dazu sagen muss, was gemeint ist: In Definition **??** haben wir mit $\circ$ tatsächlich die Hintereinanderausführung von Funktionen bezeichnet. In Definition 4.1.2 haben wir mit $\circ$ hingegen eine allgemeine binäre Verknüpfung bezeichnet.
Sie erkennen hier bereits eine Sache, die Ihnen bereits im Laufe Ihres ersten Semesters noch öfter begegnen wird: Viele Symbole in der Mathematik sind mit verschiedenen Bedeutungen „überladen“ (*überladen* ist übrigens tatsächlich ein technischer Begriff aus der Informatik, um solch einen Sachverhalt zu beschreiben). Man muss dann aus dem Kontext erkennen, was gemeint ist. Falls die Chance einer Unklarheit besteht, muss man explizit dazusagen, was mit einem Symbol gemeint ist. Auf den ersten Blick mag das so wirken, als wäre es unnötig fehleranfällig und schwer zu durchschauen. Aber im Laufe des Semesters werden wir noch viele weitere binäre Verknüpfungen diskutieren, und dann werden Sie die notationelle Einfachheit, die dadurch entsteht, verschiedene Dinge mit demselben Symbol zu bezeichnen, schnell zu schätzen lernen. (Ganz generell ist es übrigens eine große Kunst, mathematische Notation genauso schlank zu halten, dass man sie effizient benutzen kann, dass es aber zugleich nicht ständig zu Missverständnissen kommt.)

Beweis. Lassen Sie uns überprüfen, dass $(\mathrm{Abb}(X;X),\circ)$ die beiden Axiome aus Definition 4.1.2(a) erfüllt:

- (HG0): Für zwei Funktionen $f,g \in \mathrm{Abb}(X;X)$ ist auch $f\circ g \in \mathrm{Abb}(X;X)$, also ist $\circ$ tatsächlich eine binäre Verknüpfung auf $\mathrm{Abb}(X;X)$.[7]
- (HG1): Die Assoziativität dieser Verknüpfung haben wir bereits in Proposition 2.1.8 bewiesen. □

Die Halbgruppe $(\mathrm{Abb}(X;X),\circ)$ ist im Allgemeinen nicht kommutativ. Um das zu erkennen, können Sie zum Beispiel die Menge $X=\{1,2\}$ betrachten und sich zwei Funktionen $f,g\in\mathrm{Abb}(X;X)$ überlegen, für die

$$f\circ g \neq g\circ f$$

gilt.[8]

Neutrale Elemente

In manchen Halbgruppen gibt es Elemente, die keinerlei Wirkung haben, wenn man Sie mit anderen Elemente verknüpft. Dieses Verhalten präzisieren wir in der folgenden Begriffsbildung:

Definition 4.1.5 (Neutrales Element)**.** Sei $(X,\circ)$ eine Halbgruppe. Ein Element $e\in X$ heißt **neutrales Element** der Halbgruppe, falls

$$\forall a\in X:\quad a\circ e = a = e\circ a$$

gilt.[9]

Lassen Sie uns dieses Konzept zuerst anhand einiger Beispiele veranschaulichen:

Beispiele 4.1.6. (a) Die Halbgruppe $(\mathbb{N}^*,+)$ besitzt kein neutrales Element. Die Halbgruppe $(\mathbb{N}^*,\cdot)$ hingegen besitzt ein neutrales Element, nämlich die Zahl 1.

(b) Die Halbgruppe $\big(\{-1,0,1\},\cdot\big)$ besitzt ein neutrales Element, nämlich die Zahl 1.

(c) Sei X eine Menge. Die Halbgruppe $\big(\mathrm{Abb}(X;X),\circ\big)$ (wobei $\circ$ die Hintereinanderausführung bezeichnet) besitzt ein neutrales Element, nämlich id_X.

Jede Halbgruppe in den oben stehenden Beispiel besitzt ein oder kein neutrales Element. Das liegt nicht an den speziellen Beispielen, die wir uns bisher angesehen haben, sondern ist in allen Halbgruppen so:

[7] Machen Sie sich bitte unbedingt klar, dass hier etwas „Wildes“ passiert: Der Satz vor dieser Fußnote besagt, dass $\circ$ eine Abbildung von $\big(\mathrm{Abb}(X;X)\big)^2 \to \mathrm{Abb}(X;X)$ ist – d.h., wir betrachten hier gerade eine Abbildung, die Tupel aus Abbildungen auf Abbildungen abbildet.

[8] Und das sollten Sie auch tatsächlich tun!

[9] Eine Halbgruppe, in der ein neutrales Element existiert, wird auch als **Monoid** bezeichnet.

Proposition 4.1.7 (Eindeutigkeit des neutralen Elements)**.** *Sei* $(X, \circ)$ *eine Halbgruppe. Dann gibt es höchstens ein neutrales Element in* X*.*

Beweis. Seien $e_1, e_2 \in X$ neutrale Elemente. Dann gilt

$$e_2 = e_1 \circ e_2 = e_1;$$

hierbei gilt die erste Gleichheit, weil e_1 ein neutrales Element ist, und die zweite Gleichheit gilt, weil e_2 ein neutrales Element ist.[10] □

4.2 Gruppen

Inverse Elemente und Gruppen

Nun geht's zur Sache: Wir betrachten jetzt Halbgruppen, in denen es nicht nur ein neutrales Element gibt, sondern auch noch sogenannte **inverse Elemente**:

Definition 4.2.1 (Gruppe)**.** Eine **Gruppe** ist ein Tupel $(G, \circ)$, wobei G eine Menge und $\circ$ eine Abbildung ist, und folgende Eigenschaften erfüllt sind:

(G0) *Binäre Verknüpfung auf* G*:* Es gilt $\circ\colon G^2 \to G$.

(G1) *Assoziativität:* Die binäre Verknüpfung $\circ$ erfüllt das Assoziativgesetz.[11]

(G2) *Existenz eines neutralen Elementes:* Es gibt ein neutrales Element e in der Halbgruppe $(G, \circ)$.[12]

(G3) *Existenz inverser Elemente:* Es gilt

$$\forall a \in G \ \exists b \in G: \quad a \circ b = e.$$

Wenn $a \in G$ ist, dann nennt man ein Element $b \in G$ mit der Eigenschaft $a \circ b$ ein **rechtsinverses Element von** $\boldsymbol{a}$.

Jede Gruppe ist natürlich auch eine Halbgruppe. Entsprechend ist der Begriff **kommutativ**, den wir für Halbgruppen in Definition 4.1.2(b) eingeführt haben, auch für Gruppen definiert.[13]

Bevor wir Beispiele diskutieren, beweisen wir zunächst einige allgemeine Aussagen über Gruppen:

[10] Hier sehen Sie eine allgemeine Beweistechnik um Eindeutigkeit zu zeigen: Wenn man beweisen will, dass es von einem bestimmten Typ von Objekt nur eines (oder höchstens eines) gibt, dann nimmt man sich zwei solcher Objekte (die man mit verschiedenen Variablen bezeichnet, von denen man aber nicht voraussetzt, dass sie verschieden sein müssen). Daraufhin beweist man dann, dass diese beiden Objekte unter den gegebenen Voraussetzungen automatisch gleich sind. Damit hat man dann gezeigt, dass es in Wirklichkeit höchstens ein solches Objekt geben kann.

[11] D.h. anders ausgedrückt: $(G, \circ)$ ist eine Halbgruppe.

[12] Beachten Sie, dass das neutrale Element dann wegen Proposition 4.1.7 eindeutig bestimmt ist.

[13] D.h., eine Gruppe heißt **kommutativ**, wenn $a \circ b = b \circ a$ for alle $a, b \in G$ gilt.

Proposition 4.2.2 (Eigenschaften von rechtsinversen Elementen in Gruppen)**.** *Sei $(G, \circ)$ eine Gruppe, und bezeichne e ihr neutrales Element.*

(a) *Sei $a \in G$ und sei $b \in G$ ein rechtsinverses Element von a. Dann ist b auch **linksinvers** zu a, d.h. es gilt $b \circ a = e$.*

(b) *Jedes Element in G besitzt genau ein rechtsinverses Element in G, d.h., es gilt*

$$\forall a \in G \ \exists! b \in G : \quad a \circ b = e.$$

Beweis. (a) Sei $a \in G$ und sei $b \in G$ rechtsinvers zu a. Laut Axiom (G3) in der Definition einer Gruppe besitzt jedes Element der Gruppe ein rechtsinverses Element – also besitzt auch b ein rechtsinverses Element in G, nennen wir es c. Es gilt

$$a = a \circ e = a \circ (b \circ c) = (a \circ b) \circ c = e \circ c = c,$$

und somit

$$b \circ a = b \circ c = e.$$

Dies beweist, dass b tatsächlich linksinvers zu a ist.

(b) Sei $a \in G$ beliebig, aber fest. Laut Axiom (G3) in der Definition einer Gruppe besitzt a ein rechtsinverses Element $b \in G$, also müssen wir nur die Eindeutigkeit zeigen.

Sei also $\hat{b} \in G$ ebenfalls ein rechtsinverses Element von a. Es gilt

$$b = b \circ e = b \circ (a \circ \hat{b}) = (b \circ a) \circ \hat{b} = e \circ \hat{b} = \hat{b};$$

für die vorletzte Gleichheit haben wir die bereits bewiesene Aussage (a) benutzt. □

Laut der vorangehenden Proposition hat jedes Element a einer Gruppe also nur ein rechtsinverses Element – deshalb ist es sinnvoll, vom *dem* rechtsinversen Element von a zu sprechen. Zudem ist das rechtsinverse Element von a immer auch automatisch linksinvers zu a – deshalb ist es sinnvoll, das rechtsinverse Element von a einfach das **inverse Element von a** zu nennen. Es ist üblich die folgende Notation für das inverse Element zu verwenden:

Notation 4.2.3. Sei $(G, \circ)$ eine Gruppe und sei $a \in G$. Das rechtsinverse Element von a (das laut Proposition 4.2.2 eindeutig bestimmt ist und zugleich auch linksinvers zu a ist) wird mit a^{-1} notiert.

In vielen Fällen wird die binäre Verknüpfung einer Gruppe nicht mit dem Symbol $\circ$ bezeichnet, sondern mit dem Symbol $+$.[14] Dies ist zum Beispiel bei der Gruppe $(\mathbb{R}, +)$ der Fall, wobei $+$ hier die übliche Addition auf den reellen Zahlen beschreibt.

Wenn die Gruppenverknüpfung als $+$ geschrieben wird, bezeichnet man das inverse Element eines Elementes a aus der Gruppe üblicherweise nicht mit a^{-1}, sondern mit $-a$.

[14] Allerdings wird ein Plus meist nur dann zur Notation einer Gruppenverknüpfung verwendet, wenn die Gruppe kommutativ ist.

Wir werden von nun an häufig von der Terminologie Gebrauch machen, die direkt vor der vorangehenden Notation eingeführt wurde und a^{-1} somit als inverses Element von a bezeichnen. Es folgen einige Eigenschaften inverser Elemente:

Proposition 4.2.4 (Eigenschaften inverser Elemente)**.** *Sei $(G, \circ)$ eine Gruppe, und bezeichne e das neutrale Element der Gruppe.*

(a) *Es gilt $e^{-1} = e$.*

(b) *Für jedes $a \in G$ gilt $(a^{-1})^{-1} = a$.*

(c) *Für alle $a_1, a_2 \in G$ gilt $(a_1 \circ a_2)^{-1} = a_2^{-1} \circ a_1^{-1}$.*

Beweis. (a) Die Behauptung besagt nichts weiter, als dass e das rechtsinverse Element von e ist. Und dass dies wirklich stimmt, folgt aus der Gleichung $e \circ e = e$ (welche wiederum wahr ist, weil e das neutrale Element der Gruppe ist).

(b) Laut Proposition 4.2.2(a) gilt $a^{-1} \circ a = e$. Wenn wir nun diese Gleichung von links mit $(a^{-1})^{-1}$ verknüpfen, dann folgt

$$(a^{-1})^{-1} \circ a^{-1} \circ a = (a^{-1})^{-1} \circ e,$$

und somit $e \circ a = (a^{-1})^{-1}$. Das Element auf der linken Seite dieser Gleichung ist gleich a, womit die Behauptung gezeigt ist.

(c) Weil $(a_1 \circ a_2)^{-1}$ per Definition dieser Notation rechtsinvers zu $a_1 \circ a_2$ ist, gilt

$$a_1 \circ a_2 \circ (a_1 \circ a_2)^{-1} = e.$$

Wir benutzen nun erneut, dass rechtsinverse Elemente laut Proposition 4.2.2(a) auch linksinvers sind: Durch Verknüpfen der zuletzt angeschriebenen Gleichung von links mit a_1^{-1} erhält man

$$a_2 \circ (a_1 \circ a_2)^{-1} = a_1^{-1}.$$

Diese Gleichung verknüpfen wir nun noch von links mit a_2^{-1} und erhalten somit

$$(a_1 \circ a_2)^{-1} = a_2^{-1} \circ a_1^{-1}.$$

Dies ist gerade die Behauptung. □

Nun diskutieren wir wie angekündigt einige Beispiele.

Beispiele 4.2.5. (a) Sowohl $(\mathbb{Z}, +)$ als auch $(\mathbb{R}, +)$ ist eine Gruppe, und die Zahl 0 ist jeweils das neutrale Element. Außerdem ist für jedes Element a von $\mathbb{Z}$ bzw. $\mathbb{R}$ die Zahl $-a$ das inverse Element.

(b) Es ist $(\mathbb{R}, \cdot)$ eine Halbgruppe mit neutralem Element 1, aber keine Gruppe – denn das Element 0 hat kein rechtsinverses Element (wäre nämlich eine Zahl $r \in \mathbb{R}$ rechtsinvers zu 0, so würde $1 = 0 \cdot r = 0$ gelten).

(c) Sei $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$.[15] Im Gegensatz zum vorangehenden Beispiel ist $(\mathbb{R}^*, \cdot)$ eine Gruppe.

In den Übungen werden Sie noch einige deutlich überraschendere Beispiele für Gruppen kennenlernen. Sehr interessante Beispiele für Gruppen sind zudem sogenannten die Permutationsgruppen – diese besprechen wir kurz am Ende dieses Abschnitts.

Untergruppen

Ein wichtiges Konzept in der Mathematik besteht darin, aus gegebenen Objekten neue Objekte mit ähnlichen Eigenschaften zu bauen. Eine erste Demonstration dieses Konzeptes folgt nun anhand des Begriffs der **Untergruppe**.

Definition 4.2.6 (Untergruppe)**.** Sei $(G, \circ)$ eine Gruppe, und bezeichne e das neutrale Element von G. Eine **Untergruppe** von $(G, \circ)$ ist eine Teilmenge $U \subseteq G$, die die folgenden Eigenschaften erfüllt:

(UG1) Es ist $e \in U$.

(UG2) Abgeschlossenheit bzgl. der Gruppenvernüpfung:

$$\forall u_1, u_2 \in U : \quad u_1 \circ u_2 \in U.$$

(UG3) Abgeschlossenheit bzgl. der Bildung von Inversen:

$$\forall u \in U : \quad u^{-1} \in U.$$

Proposition 4.2.7. *Sie $(G, \circ)$ eine Gruppe, und sei $U \subseteq G$ eine Untergruppe. Dann ist $(U, \circ)$ selbst eine Gruppe.*

Bevor wir die Proposition beweisen, ist es sinnvoll folgenden Punkt zu besprechen: In der Formulierung der Proposition waren wir genau genommen etwas unpräzise in der Notation. Weil $(G, \circ)$ eine Gruppe ist, wissen wir ja, dass $\circ$ eine Abbildung von G^2 nach G ist. Somit kann aber $(U, \circ)$ genau genommen gar keine Gruppe sein, denn damit dies überhaupt möglich ist, müsste ja $\circ$ eine Abbildung von U^2 nach U sein (und nicht von G^2 nach G).

Was hier vor sich geht, ist folgendes: Genau genommen meint man, wenn man von der Gruppe $(U, \circ)$ spricht, mit $\circ$ nicht exakt diesselbe Abbildung wie in $(G, \circ)$ – sondern man meint die sogenannte **Einschränkung** von $\circ$ auf U^2 (d.h., man wendet $\circ$ nun nicht mehr auf Elemente a und b aus G an, sondern nur noch auf Elemente auf U). Aus Axiom (UG2) in der Definition einer Untergruppe folgt, dass man somit

[15] Diese Notation ist sehr üblich und wir werden sie in der Vorlesung von nun an durchgehend verwenden.

eine Abbildung enthält, deren Werte alle in U liegen – also tatsächlich ein binäre Verknüpfung auf U.[16]

Beweis von Proposition 4.2.7. Wir müssen nachweisen, dass $(U, \circ)$ die Axiome aus der Definition einer Gruppe erfüllt:

- (G0): Dies folgt, wie bereits vor dem Beweis diskutiert, aus Untergruppen-Axiom (UG2).
- (G1): Weil $(G, \circ)$ eine Gruppe ist, gilt dass Assoziativgesetz

  $$(a \circ b) \circ c = a \circ (b \circ c)$$

  für alle $a, b, c \in G$. Also gilt es insbesondere für alle $a, b, c \in U$.
- (G2): Bezeichne e das neutrale Element von G. Laut Untergruppen-Axiom (UG1) ist $e \in U$, und offensichtlich ist e auch in $(U, \circ)$ neutrales Element.
- (G3): Sei $u \in U$. Das inverse Element u^{-1} von u in der Gruppe $(G, \circ)$ ist laut Untergruppen-Axiom (UG3) ein Element von U. Somit besitzt u ein inverses – und somit insbesondere rechts-inverses – Element in U. □

Aufgrund von Proposition 4.2.7 ist das Konzept der Untergruppen sehr nützlich, um aus einer Gruppe neue, „kleinere“ Gruppen zu erhalten.

Wir schließen diesen Abschnitt mit folgenden Beispielen:

Beispiele 4.2.8. (a) Das Intervall $(0, \infty) \coloneqq \{x \in \mathbb{R} \mid \ x > 0\}$ ist eine Untergruppe von $(\mathbb{R}^*, \cdot)$. Dies kann man leicht nachrechen, indem man die Untergruppenaxiome überprüft:

(UG1) Das neutrale Elemente der Gruppe $(\mathbb{R}^*, \cdot)$ ist die Zahl 1. Es gilt $1 \in (0, \infty)$.

(UG2) Für zwei Elemente $u_1, u_2 \in (0, \infty)$ gilt $u_1 \cdot u_2 > 0$, also $u_1 \cdot u_2 \in (0, \infty)$.

(UG3) Für jedes $u \in (0, \infty)$ ist das das inverse Element u^{-1} gleich $1/u$. Also ist $u^{-1} = 1/u > 0$ und somit $u^{-1} \in (0, \infty)$.

(b) Das Intervall $[1, \infty) \coloneqq \{x \in \mathbb{R} \mid \ x \geq 1\}$ ist keine Untergruppe von $(\mathbb{R}^*, \cdot)$, denn zum Beispiel ist das inverse Element von 2 – also die Zahl $\frac{1}{2}$ – kein Element von $[1, \infty)$. Somit ist die Bedingung (UG3) nicht erfüllt.

[16] Für Einschränkungen von Abbildungen gibt es eigentlich eine spezielle Notation, die Sie auch schon in den Übungen (in Aufgabe 1(b) auf Hausaufgabenblatt 3) kennengelernt haben. Wenn man dieser Notation folgt, muss man der Genauigkeit halber eigentlich sagen, „$(U, \circ|_{U \times U})$ ist eine Gruppe“, anstelle von „$(U, \circ)$ ist eine Gruppe“. Die Erfahrung zeigt aber, dass diese genauere Notation beim Behandeln von Untergruppen keinen Mehrwert bringt, und lediglich die Notation verkomplizieren würde. Deshalb ist man hier meist etwas ungenau und spricht stattdessen einfach von der Gruppe $(U, \circ)$. In anderen Kontexten (wenn es nicht gerade um Untergruppen oder ähnliche Strukturen geht) ist es aber wichtig, dass man es notational deutlich zum Ausdruck bringt, wenn eine Funktion auf eine Teilmenge ihres Definitionsbereichs eingeschränkt wird.

4.3 Permutationen

Hier ist eine weitere Klasse von Gruppen:

Beispiel 4.3.1. Sei X eine Menge. Es bezeichne $\mathcal{S}(X)$ die Menge aller bijektiven Abbildungen von X nach X,[17] und bezeichne $\circ$ die Hintereinanderausführung von Funktionen aus $\mathcal{S}(X)$.

Dann ist $(\mathcal{S}(X), \circ)$ eine Gruppe, und für jedes $f \in \mathcal{S}(X)$ ist die Umkehrfunktion von f zugleich das inverse Elemente von f in der Gruppe $(\mathcal{S}(X), \circ)$.[18]

Man bezeichnet sie als **symmetrische Gruppe** auf X.

Beweis. Lassen Sie uns überprüfen, dass $(\mathcal{S}(X), \circ)$ die Axiome einer Gruppe erfüllt:

- (G0): Wenn wir nur Funktionen aus $\mathcal{S}(X)$ verknüpfen, dann bildet $\circ$ tatsächlich von $\mathcal{S}(X) \times \mathcal{S}(X)$ nach $\mathcal{S}(X)$ ab, denn für $f, g \in \mathcal{S}(X)$ ist $f \circ g$ ebenfalls eine Abbildung von X nach X, und laut Proposition 2.3.6(c) auch bijektiv.
- (G1): Die Hintereinanderausführung von Funktionen ist laut Proposition 2.1.8 assoziativ.
- (G2): Die Identität id_X ist ein Element von $\mathcal{S}(X)$ und es gilt

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

  für jedes $f \in \mathcal{S}(X)$. Somit ist id_X neutrales Element in $(\mathcal{S}(X), \circ)$.
- (G3): Sei $f \in \mathcal{S}(X)$. Dann besitzt f aufgrund seiner Bijektivität eine Umkehrfunktion f^{-1}. Diese bildet ebenfalls von X nach X ab, und ist laut Proposition **????** ebenfalls bijektiv. Außerdem ist sie laut Proposition **????** rechts-invers zu f (womit auch gleich die letzte Behauptung im Beispiel bewiesen ist). □

Das vorangehende Beispiel ist besonders wichtig, wenn X eine endliche Menge ist.

Beispiel 4.3.2. Sei $n \in \mathbb{N}^*$. Dann notiert man die symmetrische Gruppe auf der Menge $\{1, \ldots, n\}$ – also die Gruppe $\mathcal{S}\big(\{1, \ldots, n\}\big)$ – oft kurz als $\mathcal{S}_n$ und bezeichnet sie auch als **symmetrische Gruppe auf n Elementen.** Die Elemente von $\mathcal{S}_n$ nennt man **Permutationen auf n Elementen**.

Jedes Element von $\mathcal{S}_n$ – d.h. jede Permutation von n Elementen – ist also eine bijektive Abbildungen von $\{1, \ldots, n\}$ nach $\{1, \ldots, n\}$. Wie Sie bereits aus Beispiel **????**

[17] D.h., $\mathcal{S}(X)$ ist eine Teilmenge von $\mathrm{Abb}(X; X)$.

[18] Beachten Sie, dass wir die Notation „hoch -1“ in zwei verschiedenen Kontexten eingeführt haben: Laut Definition **??** wird sie für die Umkehrfunktion benutzt, und laut Notation 4.2.3 wird sie zur Bezeichnung von inversen Elementen in einer Gruppe benutzt. Wenn f ein Element der symmetrischen Gruppe $\mathcal{S}(X)$ ist, ist auf den ersten Blick nicht klar, welche der beiden Bedeutungen mit der Notation f^{-1} gemeint ist. Es ist deshalb wichtig, dass Sie sich an der Stelle überlegen, weshalb die beiden Notation in diesem Fall dasgleiche bedeuten (und somit an dieser Stelle kein Notationskonflikt auftritt).

wissen, kann man Funktionen, deren Definitionsbereich endlich ist, in Tabellenform angeben. Bei Permutationen ist dies sehr üblich und äußerst nützlich.

Hierbei sind die folgenden Konventionen üblich: Man schreibt die komplette Tabelle innerhalb von geschweiften Klammern auf, und man lässt oft sämtliche Trennstriche zwischen Zeilen und Spalten der Tabelle weg. Außerdem ist man meist sogar so dreist, die Tabelle selbst einfach als die entsprechende Funktion aufzufassen. Somit ist also die Permutation

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

zum Beispiel ein Element aus $\mathcal{S}_4$. Für dieses σ gilt

$$\sigma(1) = 3, \qquad \sigma(2) = 1, \qquad \sigma(3) = 2, \qquad \sigma(4) = 4.$$

Das neutrale Element von $\mathcal{S}_3$ – also die Funktion $\mathrm{id}_{\{1,2,3\}}$ – lässt sich in dieser Notation schreiben als

$$\mathrm{id}_{\{1,2,3\}} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Im folgenden und letzten Beispiel dieses Abschnitts zeigen wir, wie man die Hintereinanderausführung von Permutationen konkret berechnen kann:

Beispiel 4.3.3. Betrachten Sie die folgenden drei Permutationen aus $\mathcal{S}_4$:

$$\sigma_1 \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \qquad \sigma_2 \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \sigma_3 \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Es gilt

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

und

$$\sigma_3 \circ \sigma_2 \circ \sigma_1 = \sigma_3 \circ (\sigma_2 \circ \sigma_1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Durch Permutationen lässt sich sehr gut die Umordnung von Objekten beschreiben, die in einer bestimmten Reihenfolge aufgestellt sind. Dies demonstrieren wir anschaulich in der Vorlesung (mit ganz konkreten Gegenständen, sodass sich die Demonstration nur schwer schriftlich darstellen lässt – deshalb wird sie hier im Manuskript nicht beschrieben).

Besonders einfache Permutationen sind sogenannte **Tranpositionen**:

Definition 4.3.4 (Transposition)**.** Sei $n \in \mathbb{N}^*$. Eine Permutation $\sigma \in \mathcal{S}_n$ bezeichnet man als eine **Transposition**, falls σ genau zwei Elemente von $\{1, \ldots, n\}$ vertauscht und alle anderen Elemente von $\{1, \ldots, n\}$ unverändert lässt.

Beachten Sie: Für jedes Transposition $\tau \in \mathcal{S}_n$ gilt $\tau \circ \tau = \mathrm{id}$ und somit $\tau^{-1} = \tau$.[19]

Proposition 4.3.5 (Permutationen sind Hintereinanderausführungen von Transpositionen)**.** *Sei $n \in \mathbb{N}$ mit $n \geq 2$. Jede Proposition $\sigma \in \mathcal{S}_n$, die nicht die Identität ist, lässt sich als Komposition von Transpositionen schreiben.*

Beweis. Sie $\sigma \in \mathcal{S}_n$ und $\sigma \neq \mathrm{id}$.

Sei $\tau_1 \in \mathcal{S}_n$ diejenige Permutation, die 1 mit $\sigma(1)$ vertauscht; dann ist τ_1 entweder eine Transposition oder die Identität. Wir definieren $\rho_1 \coloneqq \tau_1 \circ \sigma$. Die Permutation ρ_1 erfüllt $\rho_1(1) = 1$ und wegen $\tau_1 \circ \tau_1 = \mathrm{id}$ gilt.

$$\sigma = \tau_1 \circ \rho_1.$$

Nun sei $\tau_2 \in \mathcal{S}_n$ diejenige Permutation, die 2 mit $\rho_1(2)$ vertauscht; dann ist τ_2 entweder eine Transposition oder die Identität. Weil $\rho_1(1) = 1$ ist, gilt wegen der Injektivität von ρ_1, dass $\rho_1(2) \geq 2$ ist; also lässt τ_2 die Zahl 1 unverändert. Ähnlich wie zuvor definieren wir jetzt $\rho_2 \coloneqq \tau_2 \circ \rho_1$; dann gilt $\rho_2(1) = 1$ und $\rho_2(2) = 2$ sowie

$$\sigma = \tau_1 \circ \rho_1 = \tau_1 \circ \tau_2 \circ \rho_2.$$

Dieses fahren führen wir weiter fort; damit erhalten wir Permutationen $\tau_1, \ldots, \tau_{n-1} \in \mathcal{S}_n$, von denen jede jeweils die Identität oder eine Transposition ist, sowie eine Permutation $\rho_{n-1} \in \mathcal{S}_n$, die $\rho_{n-1}(k) = k$ für alle $k \in \{1, \ldots, n-1\}$ erfüllt und für die

$$\sigma = \tau_1 \circ \cdots \circ \tau_{n-1} \circ \rho_{n-1}$$

gilt. Wegen der Bijektivität von ρ_{n-1} ist auch $\rho_{n-1}(n) = n$, das heißt $\rho_{n-1} = \mathrm{id}$. Also haben wir σ als Komposition von Permutationen geschrieben, von denen jede jeweils die Identität oder eine Transposition ist. Diejenigen Transpositionen, die gleich der Identität sind, können wir in der Komposition einfach weglassen. Damit ist die Behauptung bewiesen. □

Lassen Sie uns das Zerlegen von Permutationen in Transpositionen an einem Beispiel veranschaulichen:

Beispiel 4.3.6 (Zerlegen einer Permutation in Transpositionen)**.** Betrachten Sie die Transposition

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in \mathcal{S}_4.$$

Folgt man der Prozedur aus dem Beweis von Proposition 4.3.5, so erhält man $\sigma = \tau_1 \circ \tau_2 \circ \tau_3$ mit

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

[19] Können Sie ein Beispiel einer Permutation angeben, die diese Eigenschaft nicht erfüllt?

Zum Schluss besprechen wir noch das sogenannte **Vorzeichen** von Permutationen. Dieses Konzept benutzt man zum Beispiel in der Linearen Algebra um die sogenannte **Leibnizformel** für Determinanten aufzuschreiben.

Theorem 4.3.7. *Sei $n \in \mathbb{N}^*$. Dann gibt es genau eine Abbildung* $\operatorname{sgn} : \mathcal{S}_n \to \{-1, 1\}$*, die die folgenden beiden Eigenschaften erfüllt:*

(I) *Für alle $\sigma, \rho \in \mathcal{S}_n$ gilt* $\operatorname{sgn}(\sigma \circ \rho) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\rho)$.

(II) *Für jede Transposition $\tau \in \mathcal{S}_n$ gilt* $\operatorname{sgn}(\tau) = -1$.

Beweis. Existenz:

Für den Beweis[20] schauen wir uns sogenannte **gerichtete vollständige Graphen** mit den Eckpunkten $1, \ldots, n$ an:[21] Damit meinen wir, dass wir n Punkte mit den den Nummer $1, \ldots, n$ aufzeichnen, und jeden der Punkte mit einer Linie mit jedem anderen Punkt verbinden; das nennt man einen **vollständigen Graphen** und die Verbindungslinien bezeichnet man als **Kanten**. Jeder der Kanten geben wir eine Richtung, in dem wir einen Pfeil von einem der Endpunkte zum anderen zeichnen; das Ergebnis nennt man einen **gerichteten Graphen** und weil jeder Punkt mit jedem verbunden ist, spricht man von einem **gerichteten vollständigen Graphen**.

Sei $\mathcal{G}$ die Menge aller gerichteten vollständigen Graphen, die man so erhalten kann.[22] Wir unterteilen $\mathcal{G}$ nun in verschiedene „Teams“: Zwei Graphen $G_1, G_2 \in \mathcal{G}$ kommen ins selbe Team, wenn man G_2 aus G_1 erhalten kann, indem man für eine gerade Anzahl an Kanten die Richtung umdreht.[23]

Wir beobachten nun, dass man auf diese Weise genau zwei Teams erhält. Um das zu sehen, nehmen wir uns irgendeinen beliebigen Graphen $G_1 \in \mathcal{G}$ und einen weiteren Graphen $G_2 \in \mathcal{G}$, den man aus G_1 erhält, in dem man genau eine Kante umdreht. Für jedes $G \in \mathcal{G}$ gibt es dann genau zwei Möglichkeiten:

- Entweder G ist im selben Team wie G_1. Dann erhält man G_1 aus G, indem man eine gerade Anzahl an Kanten umdreht.

[20] Die Idee des folgenden Beweises habe ich in dem MathOverflow-Post mit dem Link `mathoverflow.net/a/417732/102946` gefunden. Der Beweis wird hier mit vereinfachter Terminologie und mehr Details dargestellt. In den meisten Büchern ist die Vorgehensweise deutlich anders.

[21] Wichtig: Der Begriff das **Graphen**, wie wir ihn hier verwenden, stammt aus der sogenannten **Graphentheorie** und hat nichts mit dem Begriff des **Funktionsgraphen** zu tun.

[22] Weil jeder solche Graph genau $\frac{n(n-1)}{2}$ Kanten besitzt (Gaußsche Summenformel!) und es für jede Kante genau zwei Möglichkeiten gibt, die Richtung zu wählen, besteht $\mathcal{G}$ aus insgesamt $2^{\frac{n(n-1)}{2}}$ verschiedenen gerichteten vollständigen Graphen. Diese Beobachtung benötigen wir zwar im Beweis nicht, aber sie ist nützlich um sich vor Augen zu führen, wie $\mathcal{G}$ genau aussieht.

[23] Beachten Sie, dass die tatsächlich eine vernünftige Möglichkeit ist, um $\mathcal{G}$ in „Teams“ aufzuteilen: Jeder Graph $G \in \mathcal{G}$ ist auf diese Weise mit sich selbst im Team (was man ja erwarten würde, wenn man von „Teams“ sprechen will). Die Beziehung zwischen G_1 und G_2 ist außerdem symmetrisch. Und wenn G_1 mit G_2 im Team ist und G_2 mit G_3 im Team ist, dann ist auch G_1 mit G_3 im Team.

Über diese Eigenschaften der „Teambildung“ werden wir später noch etwas genauer und formaler sprechen, wenn wir in Abschnitt 6.2 **Äquivalenzrelationen** behandeln.

- Oder G ist nicht im selben Team wie G_1. Dann erhält man G_1 aus G, indem man eine ungerade Anzahl an Kanten umdreht. Indem man nochmals eine weitere Kante umdreht, erhält man dann G_2 aus G – somit ist G im selben Team wie G_2.

Jeder Graph $G \in \mathcal{G}$ ist also entweder im Team wie G_1 oder im selben Team wie G_2. Damit gibt es in der Tat nur zwei Teams.

Nun betrachten wir eine Permutation $\sigma \in \mathcal{S}_n$. Wir definieren eine Abbildung $\hat{\sigma} : \mathcal{G} \to \mathcal{G}$ folgendermaßen: Für jedes $G \in \mathcal{G}$ sei $\hat{\sigma}(G) \in \mathcal{G}$ derjenige Graph, der aus G folgendermaßen entsteht: man sieht sich an, wie σ die Eckpunkte von G vertauschen würde (lässt die Eckpunkte aber in Wirklichkeit fest) und bewegt die Kanten mit ihren Eckpunkten mit.

Für jedes $\sigma \in \mathcal{G}$ beweisen wir nun folgende Aussage:

$(*)$ Wenn es ein $G_0 \in \mathcal{G}$ gibt, das im selben Team ist wie $\hat{\sigma}(G_0)$, dann liegt jedes $G \in \mathcal{G}$ im selben Team wie $\hat{\sigma}(G)$.

Liege also $G_0 \in \mathcal{G}$ im selben Team wie $\hat{\sigma}(G_0)$. Sei j die Anzahl der Kanten von G_0, die man umdrehen muss, um $\hat{\sigma}(G_0)$ zu erhalten. Dann ist j eine gerade Zahl. Sei $G \in \mathcal{G}$. Stellen Sie sich über denjenigen Kanten von G_0, die man umdrehen muss um G zu erhalten, ein Minuszeichen vor; es sei k die Anzahl dieser Minuszeichen. Um $\hat{\sigma}(G)$ zu erhalten, muss man zuerst alle Kanten von G_0, über denen ein Minus steht, umdrehen (um G zu erhalten) und dann $\hat{\sigma}$ anwenden. Genauso gut kann man aber auch zuerst $\hat{\sigma}$ auf G_0 anwenden, dabei alle Minuszeichen mit bewegen und erst hinterher alle Kanten mit Minuszeichen umdrehen; auch so erhält man $\hat{\sigma}(G)$. Das heißt, um $\hat{\sigma}(G)$ aus G_0 zu erhalten, muss man insgesamt $j + k$ Kanten umdrehen. Nun gibt es zwei Möglichkeiten:

- *Erster Fall:* G ist im selben Team wie G_0.

  Dann ist k gerade, also ist $j + k$ gerade, also ist $\hat{\sigma}(G)$ im selben Team wie G_0 und somit im selben Team wie G.

- *Zweiter Fall:* G ist im anderen Team wie G_0.

  Dann ist k ungerade, also ist $j + k$ ungerade, also ist $\hat{\sigma}(G)$ nicht im anderen Team wie G_0. Somit ist $\hat{\sigma}(G)$ im selben Team wie G.

Damit ist die Aussage $(*)$ bewiesen.

Also gibt es für jedes $\sigma \in \mathcal{S}_n$ nur zwei Möglichkeiten: Entweder $\hat{\sigma}$ belässt jedes $G \in \mathcal{G}$ in seinem eigenen Team oder es tauscht die beiden Teams durch. Im ersten Fall definieren wir $\operatorname{sgn}(\sigma) := 1$ und im zweiten Fall definieren wir $\operatorname{sgn}(\sigma) := -1$.

Die Eigenschaft (I) kann man jetzt sofort überprüft, indem man sich ansieht, ob σ und ρ jeweils alle $G \in \mathcal{G}$ in ihrem Team belassen oder die Teams durch tauschen und dabei alle vier möglichen Fälle unterscheidet.

Als nächstes zeigen wir die Eigenschaft (II): Wir tun dies im Folgenden für die Transposition τ, die die Elemente 1 und 2 vertauscht; für alle anderen Transpositionen geht der Beweis genauso.

Wir betrachten dazu den Graphen $G \in \mathcal{G}$, dessen Kanten folgendermaßen gerichtet sind: Alle Kanten, die eine der Ecken $3, \ldots, n$ mit 1 verbinden, zeigen zu 1; und alle Kanten, die eine der Ecken $3, \ldots, n$ mit 2 verbinden, zeigen zu 2; außerdem zeigt die Kanten, die 1 mit 2 verbindet, von 1 nach 2. Im Graphen $\hat{\tau}(G)$ zeigt die Kante, die 1 und 2 verbindet, von 2 nach 1. Jede andere Kanten von $\hat{\tau}(G)$ zeigt in dieselbe Richtung wie die entsprechenden Kanten von G. Also sind G und $\hat{\tau}(G)$ nicht im selben Team, das heißt es ist $\operatorname{sgn}(\tau) = -1$.

Eindeutigkeit: Die Eindeutigkeit einer Abbildung, die die Eigenschaften (I) und (II) erfüllt, folgt daraus, dass sich jede Permutation aus Hintereinanderausführung von Transpositionen schreiben lässt (Proposition 4.3.5). □

Definition 4.3.8 (Vorzeichen einer Permutation)**.** Für $n \geq 2$ sei $\operatorname{sgn} : \mathcal{S}_n \to \{-1, 1\}$ die Abbildung aus Theorem 4.3.7 und für $n = 1$ sei $\operatorname{sgn} : \mathcal{S}_n = \mathcal{S}_1 \to \{-1, 1\}$ die Abbildung, die durch $\operatorname{sgn}(\mathrm{id}) = 1$ gegeben ist.

Für jedes $\sigma \in \mathcal{S}_n$ nennt man $\operatorname{sgn} \sigma$ das **Vorzeichen** oder **Signum** von σ.

Wie vor Theorem 4.3.7 erwähnt, taucht das Vorzeichen von Permutationen zum Beispiel in der Linearen Algebra auf, wenn man Determinanten von Matrizen behandelt. Damit Sie schon jetzt sehen können, dass das Vorzeichen von Permutationen auch in anderen Kontexten nützlich sein kann, besprechen wir nun eine Anwendung auf das sogenannte **Fünfzehnerspiel**:

Beispiel 4.3.9 (Fünfzehnerspiel)**.**

4.4 Teilen mit Rest

Definition 4.4.1 (Teilen mit Rest)**.** Für alle $z \in \mathbb{Z}$ and alle $n \in \mathbb{N}^*$ ist der **Rest von z geteilt durch n** diejenige Zahl $r \in \{0, 1, \ldots, n-1\}$, für die $z - r$ durch n teilbar ist – das heißt, für dies es ein $\ell \in \mathbb{Z}$ gibt, welches $n\ell = z - r$ erfüllt.

Wir verwenden für r die Notation $\operatorname{Rest}(z, n)$.[24]

Lemma 4.4.2 (Teilen mit Rest für Summen und Produkte)**.** *Sei $k \in \mathbb{N}^*$ und $z_1, z_2, \ldots, z_k \in \mathbb{Z}$ sowie $n \in \mathbb{N}^*$.*

(a) *Es gilt*

$$\operatorname{Rest}\Big(\operatorname{Rest}(z_1, n) + \cdots + \operatorname{Rest}(z_k, n)\,,\, n\Big) = \operatorname{Rest}(z_1 + \cdots + z_k, n).$$

(b) *Es gilt*

$$\operatorname{Rest}\Big(\operatorname{Rest}(z_1, n) \cdot \ldots \cdot \operatorname{Rest}(z_k, n)\,,\, n\Big) = \operatorname{Rest}(z_1 \cdot \ldots \cdot z_k, n).$$

[24] Beachten Sie aber, dass diese Notation nicht sehr üblich ist; wir verwenden Sie auch lediglich in diesem Abschnitt. Sobald wir später Äquivalenzrelationen und Quotientenräume besprochen haben, werden Sie sehen, dass man Teilen mit Rest auch auf eine effizientere Weise ausdrücken kann.

Beweis. (a) Für $k = 1$ ist die Behauptung klar; als nächstes zeigen wir sie für $k = 2$. Zur einfacheren Notation verwenden wir die Abkürzungen $r_1 = \text{Rest}(z_1, n)$ und $r_2 = \text{Rest}(z_2, n)$ sowie $r_s = \text{Rest}(z_1 + z_2, n)$. Laut Definition 4.4.1 liegen die drei Zahlen r_1, r_2, r_s in $\{0, \ldots, n-1\}$ und die drei Zahlen $z_1 - r_1$ und $z_2 - r_2$ sowie $z_1 + z_2 - r_s$ sind durch n teilbar. Wegen

$$r_1 + r_2 - r_s = (r_1 - z_1) + (r_2 - z_2) + (z_1 + z_2 - r_s)$$

folgt, dass $r_1 + r_2 - r_s$ ebenfalls durch n teilbar ist. Wegen $r_s \in \{0, \ldots, n-1\}$ folgt somit $\text{Rest}(r_1 + r_2, n) = r_s$.

Für alle weiteren k zeigen wir die Behauptung nun per Induktion über k: Für jedes ganzzahlige k mit $k \geq 2$ bezeichne $A(k)$ die Aussage

...

...

(b) Für $k = 1$ ist die Behauptung offensichtlich; wir zeigen die Behauptung als nächstes für $k = 2$. Wie zuvor verwenden wir die Abkürzungen $r_1 = \text{Rest}(z_1, n)$ und $r_2 = \text{Rest}(z_2, n)$; außerdem kürzen wir $r_p = \text{Rest}(z_1 z_2)$ ab. Dann sind $r_1, r_2, r_p \in \{0, \ldots, n-1\}$ und die Zahlen $z_1 - r_1$, $z_2 - r_2$ und $z_1 z_2 - r_p$ sind durch n teilbar. Es gilt

$$\begin{aligned} r_1 r_2 - r_p &= (r_1 - z_1 + z_1) r_2 - r_p \\ &= (r_1 - z_1) r_2 + z_1 (r_2 - z_2 + z_2) - r_p \\ &= (r_1 - z_1) r_2 + z_1 (r_2 - z_2) + (z_1 z_2 - r_p), \end{aligned}$$

also ist auch $r_1 r_2 - r_p$ durch n teilbar. Wegen $r_p \in \{0, \ldots, n-1\}$ gilt somit $\text{Rest}(r_1 r_2, n) = r_p$.

Wie bei Teil (a) des Beweises folgt die Behauptung für alle weiteren k nun per Induktion über k. □

Auf Hausaufgabenblatt 9 beweisen Sie in Aufgabe 4(a) die folgende Aussage. Hierfür ist Lemma 4.4.2(a) sehr nützlich.

Proposition 4.4.3 (Die Gruppe $\mathbb{Z}_n$)**.** *Sei $n \in \mathbb{N}^*$ und setze $\mathbb{Z}_n \coloneqq \{0, \ldots, n-1\}$. Definieren $\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ durch*

$$a \oplus b \coloneqq \text{Rest}(a + b, n)$$

für alle $a, b \in \mathbb{Z}_n$. Dann ist $(\mathbb{Z}_n, \oplus)$ eine kommutative Gruppe.[25]

Beispiele 4.4.4 (Einige Beispiele für die Addition in $\mathbb{Z}_n$)**.**

(a) In $\mathbb{Z}_2$ gilt $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ und $1 \oplus 1 = 0$.

(b) In $\mathbb{Z}_3$ gilt zum Beispiel $1 \oplus 1 = 2$, $1 \oplus 2 = 0$ und $2 \oplus 2 = 1$.

[25] Später werden wir anstelle von $\oplus$ einfach das Symbol $+$ für die Verknüpfung in dieser Gruppe benutzen. Man muss dann anhand des Kontexts entscheiden, ob mit $+$ die übliche Addition natürlicher Zahlen oder die Addition in $\mathbb{Z}_n$ gemeint ist.

4.5 Körper

Wie Sie bereits wissen, ist eine Gruppe eine Menge zusammen mit einer binären Verknüpfung, welche bestimmte Eigenschaften erfüllt. Wenn Sie nun aber z.B. die reellen Zahlen betrachten, dann kennen Sie auf dieser Menge ja zwei Verknüpfungen mit interessanten Eigenschaften: Die Addition und die Multiplikation. Zudem hängen beide Verknüpfungen auch noch mittels des Distributivgesetzes zusammen.

Es gibt aber noch weitere Mengen, auf denen binäre Verknüpfungen mit ähnlichen Eigenschaften definiert sind. Um all diese zugleich behandeln zu können, führt man den folgenden Begriff ein:

Definition 4.5.1 (Körper)**.** Ein Körper ist ein Tupel $(\mathbb{K}, +, \cdot)$, wobei $\mathbb{K}$ eine Menge ist, und $+$ und $\cdot$ Abbildungen sind[26], welche die folgenden Eigenschaften erfüllen:[27]

(K0) *Binäre Verknüpfungen auf* $\mathbb{K}$*:* Es gilt $+ : \mathbb{K}^2 \to \mathbb{K}$ und $\cdot : \mathbb{K}^2 \to \mathbb{K}$.

(K1) *Axiome der Addition:*
Es ist $(\mathbb{K}, +)$ eine kommutative Gruppe.

Das neutrale Element dieser Gruppe bezeichnet man mit 0. Außerdem verwendet man für jedes $\alpha \in \mathbb{K}$ die Notation $-\alpha$ um das inverse Elemente von α in der Gruppe $(\mathbb{K}, +)$ zu bezeichnen.

(K2) *Axiome der Multiplikation, Teil 1:* Es ist $(\mathbb{K}, \cdot)$ eine kommutative Halbgruppe, die ein neutrales Element besitzt.[28] Das neutrale Element bezeichnen wir mit 1.

(K3) *Axiome der Multiplikation, Teil 2:* Für jedes $\alpha \in \mathbb{K} \setminus \{0\}$ existiert ein $\beta \in \mathbb{K}$ mit der Eigenschaft $\alpha \cdot \beta = 1$.
Wir verwenden die Notation $\mathbb{K}^* \coloneqq \mathbb{K} \setminus \{0\}$.

(K4) *Distributivgesetz:* Für alle $\alpha, \beta, \lambda \in \mathbb{K}$ gilt: $(\alpha + \beta) \cdot \lambda = \alpha \cdot \lambda + \beta \cdot \lambda$.

(K5) *Nicht-Trivialität des multiplikativ neutralen Elements:* Es ist $1 \neq 0$.

Aus den Körperaxiomen folgen einige einfache, aber nützliche Konsequenzen, die im folgenden aufgezählt werden:

Proposition 4.5.2 (Rechenregeln in Körpern)**.** *Sei* $(\mathbb{K}, +, \cdot)$ *ein Körper.*

(a) *Für alle* $\alpha, \beta \in \mathbb{K}$ *gilt:*

$$\alpha \cdot \beta = 0 \qquad \Leftrightarrow \qquad \alpha = 0 \quad \vee \quad \beta = 0.$$

[26] Die wir mit Infix-Notation verwenden werden.

[27] Die Verknüpfung $+$ bezeichnet man üblicherweise als **Addition** und die Verknüpfung $\cdot$ als **Multiplikation**.

[28] Beachten Sie, dass das neutrale Element laut Proposition 4.1.7 automatisch eindeutig bestimmt ist.

(b) *Für alle* $\alpha, \beta \in \mathbb{K}$ *gilt*

$$(-1) \cdot \beta = -\beta, \quad (-\alpha) \cdot \beta = -(\alpha \cdot \beta), \quad \textit{und} \quad (-\alpha) \cdot (-\beta) = \alpha \cdot \beta.$$

(c) *Für alle* $\alpha, \beta \in \mathbb{K}$ *gilt*

$$-(\alpha + \beta) = (-\alpha) + (-\beta).$$

(d) *Für jedes* $\alpha \in \mathbb{K}^*$ *gibt es genau ein* $\beta \in \mathbb{K}$ *mit der Eigenschaft* $\alpha \cdot \beta = 1$. *Außerdem ist dieses* β *nicht* 0*, d.h. ein Element von* $\mathbb{K}^*$.

(e) *Es ist* $(\mathbb{K}^*, \cdot)$ *eine kommutative Gruppe.*

Beweis. (a) Seien $\alpha, \beta \in \mathbb{K}$.

"$\Leftarrow$" Wir nehmen zuerst an, dass $\alpha = 0$ gilt, und wir müssen $0 \cdot \beta = 0$ zeigen.

Hierzu verwenden wir das Distributivgesetz: Es gilt

$$0 \cdot \beta = (0 + 0) \cdot \beta = 0 \cdot \beta + 0 \cdot \beta.$$

Indem wir dass additiv inverse Elemente von $0 \cdot \beta$ auf beiden Seiten der Gleichung addieren, erhalten wir hieraus wie behauptet $0 = 0 \cdot \beta$.

Wenn stattdessen $\beta = 0$ ist, dann folgt mithilfe der Kommutativität von $\cdot$ und der bereits gezeigten Eigenschaft, dass $\alpha \cdot 0 = 0 \cdot \alpha = 0$ gilt.

"$\Rightarrow$" Sei nun $\alpha \cdot \beta = 0$. Wir nehmen widerspruchshalber an, dass $\alpha \neq 0$ und $\beta \neq 0$ gilt. Dann gibt es laut Körperaxiomen Elemente $\tilde{\alpha}, \tilde{\beta} \in \mathbb{K}$ mit der Eigenschaft $\alpha\tilde{\alpha} = 1$ und $\beta\tilde{\beta} = 1$. Hieraus folgt

$$0 = \tilde{\alpha} \cdot 0 \cdot \tilde{\beta} = \tilde{\alpha} \cdot \alpha \cdot \beta \cdot \tilde{\beta} = 1 \cdot 1 = 1,$$

wobei wir für die erste Gleichheit die bereits gezeigte Implikation verwenden haben. Die Gleichheit $0 = 1$ ist aber ein Widerspruch zu den Körperaxiomen.

(b) Sei $\beta \in \mathbb{K}$. Wir zeigen zunächst, dass $(-1) \cdot \beta = -\beta$ gilt:

Mithilfe des Distributivgesetzes erhalten wir

$$\beta + (-1) \cdot \beta = 1 \cdot \beta + (-1) \cdot \beta = \big(1 + (-1)\big) \cdot \beta = 0 \cdot \beta = 0,$$

wobei wir für die letzte Gleichheit Aussage (a) benutzt haben. Indem wir nun auf beiden Seiten $-\beta$ addieren, folgt wie behauptet $(-1) \cdot \beta = -\beta$.

Die zweite Gleichheit in (b) folgt durch Umklammern aus der ersten.

Um die dritte Gleichheit zu zeigen, beobachten wir zuerst, dass aus der ersten Gleichheit die Eigenschaft

$$(-1) \cdot (-1) = -(-1) = 1$$

folgt. Für $\alpha, \beta \in \mathbb{K}$ folgt hieraus durch geeignetes Umklammern sofort die behauptete Gleichheit $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$

(c) Dies folgt aus der ersten Gleichheit in (b) und dem Distributivgesetz.

(d) Sei $\alpha \in \mathbb{K}^*$. Wir wissen bereits aus den Körperaxiomen, dass es ein $\beta \in \mathbb{K}$ mit der Eigenschaft $\alpha \cdot \beta = 1$ gibt. Wir müssen aber die Eindeutigkeit beweisen.

Seien also $\beta_1, \beta_2 \in \mathbb{K}$ derart, dass $\alpha \cdot \beta_1 = 1$ und $\alpha \cdot \beta_2 = 1$ gilt. Dann folgt

$$0 = \alpha \cdot \beta_1 + \big(-(\alpha \cdot \beta_2)\big) = \alpha \cdot \beta_1 + \alpha \cdot (-\beta_2) = \alpha \cdot \big(\beta_1 + (-\beta_2)\big).$$

Weil α nach Voraussetzung nicht 0 ist, folgt aus (a), dass $\beta_1 + (-\beta_2) = 0$ gilt. Durch Addition von β_2 auf beiden Seiten dieser Gleichung erhalten wir $\beta_1 = \beta_2$. Damit ist die Eindeutigkeit beweisen.

Dass das Element $\beta \in \mathbb{K}$, welches $\alpha \cdot \beta = 1$ erfüllt, nicht 0 sein kann (und somit in $\mathbb{K}^*$ liegt), folgt wegen $1 \neq 0$ aus (a).

(e) Dies folgt unmittelbar aus den Körperaxiomen und Aussage (d). □

In Körpern sind einige notationelle Konventionen üblich, die im folgenden aufgezählt werden:

Notation 4.5.3 (Übliche Notationen in Körpern)**.** Sei $(\mathbb{K}, +, \cdot)$ ein Körper

(a) Für zwei Elemente α, β verwendet man meist die Abkürzung $\alpha - \beta \coloneqq \alpha + (-\beta)$.

(b) Für jedes $\alpha \in \mathbb{K}^*$ notiert man das inverse Element von α in der Gruppe $(\mathbb{K}^*, \cdot)$ (d.h. das eindeutig bestimmte Element $\beta \in \mathbb{K}$ mit der Eigenschaft $\alpha \cdot \beta = 1$), wie in Gruppen üblich, als α^{-1}.

(c) Für alle $\alpha \in \mathbb{K}^*$ und alle $\beta \in \mathbb{K}$ folgt aus den Körperaxiomen und den bereits gezeigten Eigenschaften, dass es genau ein Element $x \in \mathbb{K}$ mit der Eigenschaft $\alpha \cdot x = \beta$ gibt. Dieses Element x bezeichent man üblicherweise mit der Notation $\frac{\beta}{\alpha}$.[29]

Zugleich kann man sofort nachrechen, dass $x = \alpha^{-1} \cdot \beta$ ist. D.h. $\frac{\beta}{\alpha}$ ist eine Kurzschreibweise für $\alpha^{-1} \cdot \beta$. Insbesondere ist somit $\frac{1}{\alpha} = \alpha^{-1}$.

Wir sprechen kurz einige klassische Beispiele an:

Beispiele 4.5.4. (a) Es ist $(\mathbb{R}, +, \cdot)$ ein Körper (wobei + und $\cdot$ die übliche Addition und Multiplikation von reellen Zahlen bezeichen).

(b) Es ist auch $(\mathbb{Q}, +, \cdot)$ ein Körper (wobei + und $\cdot$ ebenfalls die übliche Addition und Multiplikation bezeichnen).

(c) Es ist $(\mathbb{Z}, +, \cdot)$ (ebenfalls mit üblicher Addition und Multiplikation) *kein* Körper, denn beispielsweise gibt es für das Element $\alpha \coloneqq 2 \in \mathbb{Z}$ keine $\beta \in \mathbb{Z}$ mit der Eigenschaft $\alpha \cdot \beta = 1$.

[29] Manchmal schreibt man auch β/α anstelle von $\frac{\beta}{\alpha}$. Äußerst unüblich ist hingegen die Verwendung eines Doppelpunktes zur Notation einer Division.

Körper sind also Verallgemeinerungen der Ihnen bereits bekannten Strukturen $\mathbb{R}$ bzw. $\mathbb{Q}$. Die Körperaxiome zusammen mit Proposition 4.5.2 und Notation 4.5.2 zeigen, dass Sie in allgemeinen Körpern im Grunde genauso rechnen dürfen, wie Sie es mit rationalen oder reellen Zahlen gewohnt sind.

Es gibt allerdings einen entscheidenden Unterschied: Zwei reelle Zahlen kann man immer der Größe nach vergleichen (und selbiges gilt für zwei Zahlen aus $\mathbb{Q}$). Dies ist für Elemente beliebiger Körper hingegen nicht richtig: Beachten Sie, dass wir in den Körperaxiomen nirgends gefordert haben, dass es eine Möglichkeit gibt, für zwei Elemente eines Körpers zu bestimmen, welches „größer“ ist. Wir haben noch nicht einmal definiert, was „größer“ in einem beliebigen Körper überhaupt heißen soll.

Nun besprechen wir eine Klasse von Körpern, die sich etwas anders verhalten als die reellen oder die rationalen Zahlen: Körper mit endlichen vielen Elementen.

Um solche Körper zu konstruieren, brauchen wir zuerst einige Hilfsresultate.

Definition 4.5.5 (Teilerfremde ganze Zahlen)**.** Zwei Zahlen $z_1, z_2 \in \mathbb{Z}$ heißen **teilerfremd**, falls es keine Zahl $n \in \mathbb{N}^* \setminus \{1\}$ gibt, die sowohl z_1 als auch z_2 teilt.

Ein sehr nützliches Resultat über teilerfremde Zahlen ist das folgende Lemma.

Lemma 4.5.6 (Lemma von Bézout)**.** *Seien $z_1, z_2 \in \mathbb{Z}$ teilerfremd. Dann gibt es Zahlen $a_1, a_2 \in \mathbb{Z}$ derart, dass $a_1 z_1 + a_2 z_2 = 1$ gilt.*

Beweis. Wir können ohne Einschränkung annehmen, dass $z_1, z_2 \in \mathbb{N}$ gilt.[30] Wir zeigen die Behauptung per Induktion. Für jedes $n \in \mathbb{N}^*$ bezeichne $A(n)$ die folgende Aussage: „Für alle teilfremden Zahlen $z_1, z_2 \in \mathbb{N}$ mit $z_1 \leq n$ und $z_2 \leq n$ gibt es Zahlen $a_1, a_2 \in \mathbb{Z}$ mit $a_1 z_1 + a_2 z_2 = 1$.“

Dann ist $A(0)$ wahr, denn es gibt keine teilerfremden Zahlen $z_1, z_2 \in \mathbb{N}$ mit $z_1 \leq 0$ und $z_2 \leq 0$. Wir zeigen nun für jedes $n \in \mathbb{N}$, dass die Aussage $A(n)$ die Aussage $A(n+1)$ impliziert. Sei dazu $n \in \mathbb{N}$ beliebig und sei $A(n)$ wahr. Seien $z_1, z_2 \in \mathbb{Z}$ teilerfremd mit $z_1 \leq n+1$ und $z_2 \leq n+1$. Wenn $z_1 = z_2$ ist, gilt wegen der Teilerfremdheit $z_1 = z_2 = 1$ und dann ist die Behauptung klar. Also sei $z_1 \neq z_2$.

Wenn eine der Zahlen z_1, z_2 gleich 0 ist, ist die andere wegen der Teilerfremdheit gleich 1 und somit folgt ebenfalls die Behauptung. Also seien beiden Zahlen ungleich 0. Ohne Einschränkung sei dann z_2 die größere der beiden Zahlen (ansonsten vertauschen wir die Bezeichnungen von z_1 und z_2). Dann ist also $z_1 \leq n$.

Wir setzen $r \coloneqq \mathrm{Rest}(z_2, z_1) \in \{0, \ldots, z_1 - 1\} \subseteq \{0, \ldots, n-1\}$. Dann gibt es ein $c \in \mathbb{N}$ mit $z_2 = c z_1 + r$. Weil z_1 und z_2 teilerfremd sind, sind auch z_1 und r teilerfremd. Da $z_1, r \leq n$ gilt und $A(n)$ wahr ist, gibt es Zahlen $a, b \in \mathbb{Z}$ mit

$$1 = a z_1 + b r = a z_1 + b(z_2 - c z_1) = (a - bc) z_1 + b z_2.$$

Damit ist $A(n+1)$ bewiesen. Per Induktion ist somit $A(n)$ für alle $n \in \mathbb{N}$ wahr. □

[30] Warum?

Übrigens kann man Lemma 4.5.6 noch etwas verallgemeinern: Für alle Zahlen $z_1, z_2 \in \mathbb{Z}$ gibt es Zahlen $a_1, a_2 \in \mathbb{Z}$ derart, dass $a_1 z_1 + a_2 z_2$ gleich dem größten gemeinsamen Teiler von z_1 und z_2 ist (und üblicherweise wird diese allgemeinere Aussage als das Lemma von Bézout bezeichnet). Für unsere Zwecke im Folgenden genügt aber die Aussage aus Lemma 4.5.6.

Lemma 4.5.7 (Teilbarkeit durch Primzahlen)**.** *Seien $a, b \in \mathbb{N}$ und sei $p \in \mathbb{N}^*$ eine Primzahl. Wenn ab durch p teilbar ist, dann ist a oder b durch p teilbar.*[31]

Beweis. Sei ab durch p teilbar und sei a nicht durch p teilbar. Wir müssen zeigen, dass b durch p teilbar ist.

Da p Prim ist, besitzt es in $\mathbb{N}^* \setminus \{1\}$ nur den Teiler p. Dieser ist aber, wie soeben vorausgesetzt, kein Teiler von a, also sind a und p teilerfremd. Aufgrund des Lemmas 4.5.6 von Bézout gibt es deshalb ganze Zahlen c, d mit $1 = ca + dp$. Somit folgt $b = abc + bdp$. Weil ab durch p teilbar ist und p durch p teilbar ist, ist also auch b durch p teilbar. □

Nun können wir endliche Körper mit der Kardinalität von Primzahlen konstruieren. Beachten Sie, dass Sie die Verknüpfung $\oplus$ in folgendem Theorem bereits aus Proposition 4.4.3 kennen.

Theorem 4.5.8 (Die Körper $\mathbb{Z}_p$)**.** *Sei $p \in \mathbb{N}^*$ eine Primzahl. Wir definieren zwei Verknüpfungen $\oplus$ und $\odot$ auf der Menge $\mathbb{Z}_p = \{0, \ldots, p-1\}$ durch*

$$\begin{aligned} a \oplus b &\coloneqq \mathrm{Rest}(a + b, p), \\ a \odot b &\coloneqq \mathrm{Rest}(a \cdot b, p) \end{aligned}$$

für alle $a, b \in \mathbb{Z}_p$. Dann ist $(\mathbb{Z}_p, \oplus, \odot)$ ein Körper.

Beweis. Wir überprüfen, dass alle Körperaxiome erfüllt sind.

(K0) Das folgt direkt aus der Definitions des Teilens mit Rest.

(K1) Das ist die Aussage von Proposition 4.4.3.

(K2) Wir beweisen dass Assoziativgesetz. Seien $a, b, c \in \mathbb{Z}_p$. Dann folgt

$$\begin{aligned} a \odot (b \odot c) &= \mathrm{Rest}\Big(\mathrm{Rest}(a, p) \cdot \mathrm{Rest}(b \cdot c, p),\, p\Big) \\ &= \mathrm{Rest}(a \cdot (b \cdot c), p) = \mathrm{Rest}((a \cdot b) \cdot c, p) \\ &= \mathrm{Rest}\Big(\mathrm{Rest}(a \cdot b, p) \cdot \mathrm{Rest}(c, p),\, p\Big) = (a \odot b) \odot c. \end{aligned}$$

[31] Hinweis: Die Aussage von Lemma 4.5.7 finden Sie auch in Aufgabe 5 auf Hausaufgabenblatt 8. Im Lösungsvorschlag für dieses Hausaufgabenblatt wird aber die Eindeutigkeit der Primfaktorzerlegung – das heißt Theorem 3.3.3 – verwendet. Am Ende dieses Abschnitts werden Sie allerdings sehen, dass wir zum Beweis dieses Theorems (den wir bislang aufgeschoben hatten), gerade Lemma 4.5.7 verwenden. Die Argumentation würde sich somit im Kreis drehen und wir hätten somit weder das Lemma nach das Theorem bewiesen. Deshalb geben wir hier einen anderen Beweis von Lemma 4.5.7 an, der die Eindeutigkeit der Primfaktorzerlegung nicht verwendet.

Hierbei folgen die erste und die letzte Gleichheit aus der Definition von $\odot$ und aus den Gleichheiten $\mathrm{Rest}(a,p) = a$ und $\mathrm{Rest}(c,p) = c$; die zweite und die vorletzte Gleichheit folgende aus Lemma 4.4.2(a); und die Gleichheit in der Mitte folgt aus dem Assoziativgesetzt für die Multiplikation auf $\mathbb{Z}$.

Die Kommutativität von $\odot$ folgt direkt aus der Definition und aus der Kommutativität der Multiplikation auf $\mathbb{Z}$.

Außerdem ist das Elemente $1 \in \mathbb{Z}_p$ neutral bezüglich $\odot$, denn für jedes $a \in \mathbb{Z}_p$ gilt

$$a \odot 1 = \mathrm{Rest}(a \cdot 1, p) = a$$

wegen $a \cdot 1 = a \in \{0, \ldots, p-1\}$.[32]

(K3) Dies ist die einzige Stelle, an der wir benutzen, dass p prim ist. Sei $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, \ldots, p-1\}$. Wir betrachten die Abbildung $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $b \mapsto a \odot b$.

Lassen Sie uns zeigen, dass f injektiv ist: Für $b_1, b_2 \in \mathbb{Z}_p$ mit $f(b_1) = f(b_1)$ gilt $a \odot b_1 = a \odot b_2$; ohne Einschränkung sei dabei $b_2 \geq b_1$. Nach Definition von $\odot$ sind $ab_1 - a \odot b_1$ und $ab_2 - a \odot b_2$ durch p teilbar. Durch Subtraktion der ersten von der zweiten Gleichung folgt wegen $a \odot b_1 = a \odot b_2$, dass auch $ab_2 - ab_1 = a(b_2 - b_1)$ durch p teilbar ist. Da p prim ist, folgt aus Lemma 4.5.7, dass a oder $b_2 - b_1$ durch p teilbar ist. Wegen $a \in \{1, \ldots, p-1\}$ ist a nicht durch p teilbar, also ist $b_2 - b_1$ durch p teilbar. Es gilt aber $b_2 - b_1 \in \{0, \ldots, p-1\}$ und somit $b_2 - b_1 = 0$. Damit ist $b_1 = b_2$ gezeigt, das heißt, f ist in der Tat injektiv.

Da f von einer endlichen Menge in dieselbe Menge abbildet, impliziert die Injektivität von f, dass f auch surjektiv ist. Also gibt es ein $b \in \mathbb{Z}_p$ mit $f(b) = 1$. Aus der Definition von f folgt $a \odot b = 1$.

(K4) Den Beweis des Distributivgesetzes stellen wir als Übungsaufgabe.

(K5) In der Übungsaufgabe, in der Sie Proposition 4.4.3 bewiesen haben, haben Sie gesehen, dass $0 \in \mathbb{Z}_p$ das neutrale Elemente bezüglich $\oplus$ ist. Außerdem haben wir beim Beweis von (K2) gesehen, dass $1 \in \mathbb{Z}_p$ das neutrale Elemente bezüglich $\odot$ ist. Da diese beiden Elemente von $\mathbb{Z}_p$ verschieden sind, ist (K5) bewiesen. □

Es gibt übrigens nach andere Körper mit nur endlich vielen Elementen. Sie zu konstruieren ist etwas schwieriger;[33] Sie können das zum Beispiel in Algebra-Vorlesungen lernen. Man kann übrigens zeigen, dass die Kardinalität jedes endlichen Körpers eine Primzahlpotenz ist, aber das besprechen wir an dieser Stelle nicht weiter.

Bemerkungen 4.5.9 (Notation endlicher Körper)**.** Sei $p \in \mathbb{N}^*$ eine Primzahl.

(a) Die beiden Symbole $\oplus$ und $\odot$ sind etwas umständlich zu schreiben und nicht besonders ästhetisch. Wir haben sie bisher verwendet, um im Beweis von Theorem 4.5.8 optisch klar zwischen den Operationen auf $\mathbb{Z}_p$ und den Operationen auf $\mathbb{Z}$ zu unterscheiden.

[32] Warum müssen wir nicht auch die Gleichheit $1 \cdot a = a$ überprüfen?

[33] Oder genauer gesagt: Es erfordert mehr theoretische Vorarbeit.

Es ist jedoch üblich – und wir werden es von nun an ebenso handhaben – anstelle von $\oplus$ und $\odot$ ebenfalls einfach $+$ und $\cdot$ zu schreiben. Man muss dann aus dem Kontext erkennen, welche Operation gemeint ist.

(b) Häufig sieht man anstelle der Notation $\mathbb{Z}_p$ auf die Notation $\mathbb{F}_p$. Das $\mathbb{F}$ stammt hierbei aus dem Englischen, denn das englische Wort für die algebraische Struktur **Körper** lautet **field**.

Wir schließen diesen Abschnitt mit der Beobachtung, dass man aus Lemma 4.5.7 das Theorem 3.3.3 über die Eindeutigkeit der Primfaktorzerlegung von natürlichen Zahlen herleiten kann. Den Beweises dieses Theorems hatten wir bis jetzt aufgeschoben.

Beweis von Theorem 3.3.3. Angenommen, eine natürlich Zahl $n \geq 2$ besitzt zwei verschiedene Primfaktorzerlegungen. In dem man alle Primzahlen, die in beiden Primfaktorzerlegungen vorkommen, kürzt, erhält man Primzahlen $q_1, \ldots, q_k$ und $r_1, \ldots, r_\ell$ derart, dass $\{q_1 \ldots, q_k\} \cap \{r_1, \ldots, r_\ell\} = \emptyset$ und

$$q_1 \cdot \cdots \cdot q_k = r_1 \cdot \cdots \cdot r_\ell$$

gilt. Also teilt q_1 das Produkt $r_1 \cdot (r_2 \cdot \cdots \cdot r_\ell)$. Da q_1 prim ist, folgt aus Lemma 4.5.7, dass q_1 mindestens eine der beiden Zahlen r_1 oder $r_2 \cdot \cdots \cdot r_\ell$ teilt. Da r_1 prim und ungleich q_1 ist, teilt q_1 nicht r_1, also teilt q_1 die Zahl $r_2 \cdot \cdots \cdot r_\ell$. Nun Iterieren wir dieses Argument und erhalten somit schlussendlich, dass q_1 die Zahl r_ℓ teilt. Aber r_ℓ ist ebenfalls prim und ungleich q_1, also ist das ein Widerspruch. □

Kapitel 5

Geometrie in der komplexen Ebene

Einstiegsfragen. (a) Welche Lösungen x hat die Gleichung $x^2 = 9$? Und die Gleichung $x^2 = -1$?

(b) Welche Beispiele für Körper fallen Ihnen ein?

(c) Setzen Sie sich an einen Tisch und legen Sie eine Landkarte vor sich. Stellen Sie eine Spielfigur (oder einen anderen Gegenstand) auf eine Stadt Ihrer Wahl und tun Sie dann zwei Dinge: (1) Verschieben Sie die Figur fünf Zentimeter nach rechts (aus der Perspektive von Ihrem Stuhl aus betrachtet) und (2) drehen Sie dann die Karte 90 Grad gegen den Uhrzeigersinn um ihren Mittelpunkt.

Macht es für die Endposition der Figur einen Unterschied, wenn man die Schritte (1) und (2) in umgekehrter Reihenfolge durchführt?

(d) Was sagt nochmal der Satz von Pythagoras? Kennen Sie auch eine Variante des Satzes von Pythagoras für Dreiecke, die nicht rechtwinklig sind?

5.1 Der Körper der komplexen Zahlen

Der ursprüngliche Sinn sogenannter **komplexer Zahlen** bestand darin, für bestimmte Gleichungen, die in $\mathbb{R}$ keine Lösung besitzen,[1] dennoch Lösungen zu definieren, die sich in einem geeigneten Sinne „vernünftig“ verhalten. Aus heutiger Sicht geht der Nutzen komplexer Zahlen jedoch weit hierüber hinaus.

Wir beginnen zunächst damit, die Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ durch geeignet definierte Operationen zu einem Körper zu machen:

[1] Wie zum Beispiel $x^2 = -1$.

Definition 5.1.1 (Der Körper der komplexen Zahlen)**.** Seien $+ : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ und $\cdot : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ definiert durch

$$\alpha + \beta = \begin{pmatrix} \alpha_1 + \beta_1 \\ \alpha_2 + \beta_2 \end{pmatrix}$$

und

$$\alpha \cdot \beta = \begin{pmatrix} \alpha_1\beta_1 - \alpha_2\beta_2 \\ \alpha_1\beta_2 + \alpha_2\beta_1 \end{pmatrix}$$

für alle $\alpha, \beta \in \mathbb{R}^2$.

Das Tupel $(\mathbb{R}^2, +, \cdot)$ nennt man den **Körper der komplexen Zahlen**. Wenn man $\mathbb{R}^2$ mit diesen beiden Verknüpfungen ausstattet, ist es üblicher, anstelle von $\mathbb{R}^2$ die Notation $\mathbb{C}$ zu verwenden. Somit notiert man den Körper der komplexen Zahlen dann mit $(\mathbb{C}, +, \cdot)$.

Man kann zeigen:

Proposition 5.1.2. *Der Körper der komplexen Zahlen ist tatsächlich ein Körper. Die neutralen Elemente der Addition und Multiplikation sind*

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \textit{und} \qquad \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Beweis. Das Überprüfen der meisten Körperaxiome ist Routine. Interessant ist in erster Linie die Existenz von multiplikativ inverse Elementen – dies stellen wir als Übungsaufgabe. □

Der in Definition 4.5.1 eingeführten Notation für neutrale Element in Körpern folgend schreiben wir für das additiv bzw. multiplikativ neutrale Element

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \text{bzw.} \qquad \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

kurz 0 bzw. 1.

Mit komplexen Zahlen in der obigen Darstellung zu rechnen, ist recht ungemütlich. Um zu einer besser handhabbaren Darstellung zu gelangen, ist die folgende Überlegung hilfreich:

Diskussion 5.1.3. (a) Wenn Sie $\mathbb{R}$ als Zahlenstrahl zeichnen, und $\mathbb{R}^2$ als Ebene, dann ist es naheliegend, den Zahlenstrahl als Rechtswertachse des Koordinatensystems von $\mathbb{R}^2$ einzuzeichnen. In diesem Sinne kann man $\mathbb{R}$ geometrisch als eine Teilmenge von $\mathbb{R}^2$ auffassen. Rechnerisch bedeutet dies, dass man jedes $r \in \mathbb{R}$ mit dem Tupel

$$\begin{pmatrix} r \\ 0 \end{pmatrix}$$

identifiziert.[2] Wenn man dies tut, dann stellt man fest, dass die Rechenoperationen auf $\mathbb{R}^2 = \mathbb{C}$, die in Definition 5.1.1 eingeführt wurden, genau der üblichen Addition und Multiplikation reeller Zahlen entsprechen, wenn man Sie auf $\mathbb{R}$ einschränkt: Für alle $r, s \in \mathbb{R}$ gilt nämlich

$$\begin{pmatrix} r \\ 0 \end{pmatrix} + \begin{pmatrix} s \\ 0 \end{pmatrix} = \begin{pmatrix} r+s \\ 0 \end{pmatrix}$$

und

$$\begin{pmatrix} r \\ 0 \end{pmatrix} \begin{pmatrix} s \\ 0 \end{pmatrix} = \begin{pmatrix} rs \\ 0 \end{pmatrix};$$

dies folgt direkt aus der Definition von $+$ und $\cdot$ auf $\mathbb{C} = \mathbb{R}^2$.

Man sagt deshalb auch, dass $\mathbb{R}$ ein **Teilkörper** von $\mathbb{C}$ ist.

(b) Nun führt man noch die folgende Notation und Terminologie ein: Man nennt das Element

$$\mathrm{i} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}$$

die **imaginäre Einheit**. Sie erfüllt die Gleichung $\mathrm{i}^2 = -1$ (das werden wir in den Übungen zeigen).

Mit Hilfe der imaginären Einheit kann man komplexe Zahlen in viel übersichtlicherer Form schreiben. Wenn wir nämlich wie oben erläutert jede reelle Zahl als ein Element von $\mathbb{R}$ auffassen, dann folgt aus der Definition der Multiplikation auf $\mathbb{C}$ für alle $\alpha \in \mathbb{C}$ die Formel

$$\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} \alpha_2 \\ 0 \end{pmatrix} = \alpha_1 + \mathrm{i}\,\alpha_2.$$

Die reelle Zahl α_1 heißt der **Realteil** von α, und die reelle Zahl α_2 heißt der **Imaginärteil** von α; wir kürzen Sie mit der Notation

$$\mathrm{Re}\,\alpha := \alpha_1 \qquad \text{und} \qquad \mathrm{Im}\,\alpha := \alpha_2$$

ab.

[2] Beachten Sie, dass r und das Tupel nicht wirklich gleich sind in dem Sinne, wie wir die Gleichheit zweier Tupel definiert haben. Wenn man das, was hier steht, völlig präzise aufschreiben möchte, muss man eine injektive Abbildung $\mathbb{R} \to \mathbb{R}^2$ betrachten, die jedem $r \in \mathbb{R}$ das entsprechende Tupel in $\mathbb{R}^2$ zuweist, und dann über sogenannte **Einbettungen** und **Isomorphismen** von Körpern sprechen – diesen terminologischen und konzeptuellen Aufwand wollen wir an dieser Stelle aber vermeiden, denn er bringt uns hier nicht wirklich weiter.
Deshalb sind wir lieber ein wenig ungenau und fassen, wann immer wir von den komplexen Zahlen sprechen – aber wirklich nur dann – $\mathbb{R}$ ab sofort als Teilmenge des $\mathbb{R}^2$ auf.

Wir können – und werden – also ab sofort jede komplexe Zahl α in der Form

$$\alpha = \operatorname{Re}\alpha + \mathrm{i}\operatorname{Im}\alpha$$

schreiben. Indem man die üblichen Rechenregeln in Körpern verwendet und zudem von der Rechenregel $\mathrm{i}^2 = -1$ Gebrauch macht, kann man mit dieser Darstellung komplexer Zahlen bereits recht übersichtlich rechnen.

Außerdem ist es somit noch etwas intuitiver, die reellen Zahlen als Teilmenge der komplexen Zahlen aufzufassen, denn die reellen Zahlen sind somit einfach diejenigen komplexen Zahl, deren Imaginärteil gleich 0 ist. Oder anders ausgedrückt: Jede reelle Zahl r lässt sich in der Form

$$r = r + \mathrm{i}\,0$$

als komplexe Zahl auffassen.

5.2 Die komplexe Zahlenebene

Daran, wie wir komplexe Zahlen in Abschnitt 5.1 eingeführt haben, sehen Sie, dass jede komplexe Zahl als ein Punkt der Ebene aufgefasst werden kann. Den Realteil der Zahl trägt man dabei üblicher Weise nach rechts an und den Imaginärteil nach oben. Die Rechtswert-Achse in dieser Ebene ist somit die reelle Achse; sie besteht aus den reellen Zahlen. Man bezeichnet $\mathbb{C}$ deshalb oft auch als **komplexe Zahlenebene**. Manchmal spricht man stattdessen – zu Ehren des Mathematikers Carl Friedrich Gauß – auch von der **Gaußschen Zahlenebene**.

Um mit komplexen Zahlen geometrisch arbeiten zu können, sind einige Konzepte wichtig, die wir in diesem Abschnitt besprechen.

Definition 5.2.1 (Betrag einer komplexen Zahl)**.** Sei $z \in \mathbb{C}$. Die Zahl

$$|z| \coloneqq \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2} \in [0, \infty)$$

heißt der **Betrag** von z.

Mit Hilfe des Satzes von Pythagoras sehen Sie sofort, dass der Betrag $|z|$ einer komplexen Zahl z tatsächlich angibt, wie weit z vom Ursprung entfernt ist.

Bemerkung 5.2.2 (Der Betrag einer reellen Zahl)**.** Da jede reelle Zahl r auch eine komplexe Zahl ist, haben wir in Definition 5.2.1 automatisch auch den Betrag von reellen Zahlen definiert. Es ist wichtig sich klar zu machen, dass diese Definition mit der Definition des reellen Betrags übereinstimmt, die sie für reelle Zahlen wahrscheinlich schon einmal gesehen haben: Für jedes $r \in \mathbb{R}$ gilt wegen $\operatorname{Re} r = r$ und $\operatorname{Im} r = 0$ die Formel

$$|r| = \sqrt{r^2} = \begin{cases} r & \text{falls } r \geq 0, \\ -r & \text{falls } r < 0. \end{cases}$$

Insbesondere gilt $|r| = r$ für jedes $r \in [0, \infty)$.

Bei der Addition zweier komplexer Zahlen addieren sich deren Real- und Imaginärteil. Deshalb kann man die Addition komplexer Zahlen geometrisch als die Verschiebung eines Vektors in der Ebene um einen anderen Vektor interpretieren – so, wie Sie es für Vektoren in $\mathbb{R}^2$ (und allgemeiner für Vektoren aus $\mathbb{R}^n$) aus der Linearen Algebra gewohnt sind. Wenn man diese Beobachtung mit der Definition des Betrags kombiniert, kann man einige interessante geometrische Formen leicht mit Hilfe komplexer Zahlen ausdrücken. Wir illustrieren das an einigen Beispielen:

Beispiele 5.2.3. (a) Die Menge

$$\{z \in \mathbb{C} \mid |z| \leq 1\}$$

ist die Kreisscheibe um den Nullpunkt mit Radius 1; die Randlinie ist in der Menge enthalten. Man bezeichnet

(b) Die Menge

$$\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$$

ist die Kreislinie um den Nullpunkt mit Radius 1. Man nennt $\mathbb{T}$ auch die **Einheitskreislinie**.

(c) Die Menge

$$\{z \in \mathbb{C} \mid |z - (1+\mathrm{i})| \leq 2\}$$

ist die Kreisscheibe mit Mittelpunkt $1+\mathrm{i}$ und Radius 2; die Randlinie ist in der Menge enthalten.

(d) Die Menge

$$\{z \in \mathbb{C} \mid |z - (1+\mathrm{i})| \leq 2\}$$

ist die Kreisscheibe mit Mittelpunkt $1+\mathrm{i}$ und Radius 2, wobei die Randlinie nicht in der Menge enthalten ist.

(e) Die Menge

$$\{z \in \mathbb{C} \mid 0 \leq \operatorname{Re} z \leq 1 \text{ und } 0 \leq \operatorname{Im} z \leq 2\}$$

ist die Rechtecksfläche mit Eckpunkten $0, 1, 2\,\mathrm{i}, 1+2\,\mathrm{i}$. Alle Randlinien sind in der Menge enthalten.

Das Konzept in der folgenden Definition ist – insbesondere auch in Kombination mit dem Betrag komplexer Zahlen – sehr nützlich.

Definition 5.2.4 (Konjugiert komplexe Zahl)**.** Für jedes $z = \operatorname{Re} z + \mathrm{i} \operatorname{Im} z \in \mathbb{C}$ nennt man

$$\overline{z} := \operatorname{Re} z - \mathrm{i} \operatorname{Im} z \in \mathbb{C}$$

die **konjugiert komplexe Zahl** zu z.

Geometrisch ist $\overline{z}$ diejenige Zahl in der komplexen Zahlenebene, die entsteht, wenn man z an der reellen Achse spiegelt. Man beachte, dass für jedes komplexe Zahl z die Gleichheit $\overline{\overline{z}} = z$ gilt.

Um mit komplexen Zahlen effizient rechnen zu können, sind eine Reihe von Rechenregeln sehr nützlich. Wir sammeln sie in der folgendes Proposition.

Proposition 5.2.5 (Rechenregeln für Beträge und konjugiert komplexe Zahlen)**.** *Seien $z, z_1, z_2 \in \mathbb{C}$.*

(a) *Es gilt $z \in \mathbb{R}$ genau dann, wenn $z = \overline{z}$ ist.*

(b) *Es gilt $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.*

(c) *Es gilt $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.*

(d) *Es gilt $z = 0$ genau dann, wenn $\overline{z} = 0$ gilt. Falls $z \neq 0$ ist, gilt $\overline{1/z} = 1/\overline{z}$.*

(e) *Es gilt $|z|^2 = z\overline{z}$ und $|z| = |\overline{z}|$.*

(f) *Es gilt $z = 0$ genau dann, wenn $|z| = 0$ ist. Falls $z \neq 0$ ist, gilt $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.*

(g) *Es gilt $|z_1 z_2| = |z_1|\,|z_2|$.*

(h) *Es gilt die sogenannte **Dreiecksungleichung** $|z_1 + z_2| \leq |z_1| + |z_2|$.*

(i) *Falls $z \neq 0$ ist, gilt $|1/z| = 1/|z|$.*

Beweis. (a) "⇒" Sei $z \in \mathbb{R}$. Dann ist $\operatorname{Im} z = 0$ und somit $\overline{z} = \operatorname{Re} z - \mathrm{i} \operatorname{Im} z = \operatorname{Re} z = \operatorname{Re} z + \mathrm{i} \operatorname{Im} z = z$.

"⇐" Sei $z = \overline{z}$. Dann ist $\operatorname{Re} z + \mathrm{i} \operatorname{Im} z = z = \overline{z} = \operatorname{Re} z - \mathrm{i} \operatorname{Im} z$, somit $2\,\mathrm{i} \operatorname{Im} z = 0$ und folglich $\operatorname{Im} z = 0$.

(b) und (c) Diese Eigenschaften kann man direkt nachrechnen.

(d) Sei $z \neq 0$. Dann ist $\operatorname{Re} z \neq 0$ oder $\operatorname{Im} z \neq 0$ und somit auch $\overline{z} \neq 0$. Aus (c) folgt

$$\overline{z} \cdot \overline{\frac{1}{z}} = \overline{z \cdot \frac{1}{z}} = \overline{1} = 1$$

und somit folgt die Behauptung, in dem wir durch $\overline{z}$ teilen.

(e) Es gilt $z\overline{z} = (\operatorname{Re} z + \mathrm{i} \operatorname{Im} z)(\operatorname{Re} z - \mathrm{i} \operatorname{Im} z) = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = |z|^2$. Die Gleichung $|z| = |\overline{z}|$ kann man direkt nachrechnen.

(f) Jeder der beiden Aussagen $z = 0$ und $\overline{z} = 0$ ist äquivalent zu $\operatorname{Re} z = \operatorname{Im} z = 0$, also sind die beiden Aussagen auch äquivalent zueinander.

Sei nun $z \neq 0$ (und somit, wie soeben bewiesen, $|z| \neq 0$). Dann ist auch $\overline{z} \neq 0$ und somit

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{\overline{z}}{|z|^2},$$

wobei die zweite Gleichheit aus (e) folgt.

(g) Das folgt leicht aus (c) und (e).

(h) Zunächst beachten wir, dass für jedes komplexe Zahl z die Ungleichung $\operatorname{Re} z \leq |rez| = \sqrt{(\operatorname{Re} z)^2} \leq |z|$ gilt. Damit folgt

$$\operatorname{Re}(z_1\overline{z_2}) \leq |\operatorname{Re}(z_1\overline{z_2})| \leq |z_1\overline{z_2}| = |z_1|\,|\overline{z_2}| = |z_1|\,|z_2|\,,$$

wobei die erste Gleichheit aus (g) und die zweite Gleichheit aus (e) folgt.

Nun verwenden wir die Abkürzungen $x_k = \operatorname{Re} z_k$ und $y_k = \operatorname{Im} z_k$ für jedes $k \in \{1, 2\}$. Dann ist $z_1 + z_2 = (x_1 + x_2) + \mathrm{i}(y_1 + y_2)$ und somit

$$\begin{aligned}
|z_1 + z_2|^2 &= (x_1 + x_2)^2 + (y_1 + y_2)^2 \\
&= x_1^2 + x_2^2 + 2x_1x_2 + y_1^2 + y_2^2 + 2y_1y_2 \\
&= |z_1|^2 + |z_2|^2 + 2(\underbrace{x_1x_2 + y_1y_2}_{=\operatorname{Re}(z_1\overline{z_2})}) \\
&\leq |z_1|^2 + |z_2|^2 + 2\,|z_1|\,|z_2| = \big(\,|z_1| + |z_2|\,\big)^2.
\end{aligned}$$

Ziehen der Quadratwurzel zeigt nun die Behauptung.

(i) Sei $z \neq 0$. Wir wissen bereits aus (f), dass dann auch $|z| \neq 0$ gilt. Außerdem folgt aus (g)

$$|z| \left|\frac{1}{z}\right| = \left|z\frac{1}{z}\right| = |1| = 1.$$

Teilen durch $|z|$ liefert die Behauptung. □

Als nächstes wollen wir über Winkel in der komplexen Ebene sprechen. In der Mathematik ist es üblich, Winkel im **Bogenmaß** zu messen. Das bedeutet man schaut sich auf der Einheitkreislinie an, welche Länge des Kreissegment hat, das zu einem Winkel gehört und definiert den Winkel im Bogenmaß dann als die Länge des Kreissegments. Zum Beispiel hat eine volle Umdrehung den Winkel 2π, eine halbe Umdrehung den Winkel π und eine Viertel Umdrehung den Winkel $\pi/2$. Eine Umdrehung, die im Gradmaß 60 Grad entspricht, entspricht im Bogenmaß $\frac{1}{3\pi}$.

Definition 5.2.6 (Winkel einer komplexen Zahl)**.** Sei $z \in \mathbb{C}^* = \mathbb{C}\setminus\{0\}$. Wenn man z mit dem Ursprung verbindet, schließt die Verbindungslinie mit der positiven reellen Achse einen **Winkel** θ ein – wobei der Winkel von der reellen Achse aus gegen den Uhrzeigersinn gemessen wird.[3]

Wir nennen θ den **Winkel von** z oder das **Argument von** z.[4]

[3] Genauer: Wir definieren den Winkel als positive, wenn wir gegen den Uhrzeigersinn messen. Winkeln, die im Uhrzeigersinn gemessen werden, ordnen wir negative Werte zu.

[4] Bitte beachten Sie, dass hier wieder einmal ein Begriff überladen wird. Die Bezeichnung „Argument“ für den Winkel einer komplexen Zahl ist historisch bedingt und darf nicht mit dem Argument einer Funktion verwechselt werden.

Bemerkung 5.2.7 (Nicht-Eindeutigkeit des Winkels)**.** Beachten Sie unbedingt, dass der Winkel einer komplexen Zahl genau genommen gar nicht eindeutig bestimmt ist – denn Sie können zu jedem Winkel ein ganzzahliges Vielfaches einer vollen Umdrehung hinzuzählen oder abziehen ohne die komplexe Zahl zu verändern.

Zum Beispiel lässt sich der Zahl i der Winkel $\pi/2$ oder der Winkel $2\pi + \pi/2$ oder der Winkel $4\pi + \pi/2$ oder der Winkel $-2\pi + \pi/2$ zuordnen.

Um den Winkel eindeutig zu machen, muss man ihn aus einem festen Intervall der Länge 2π wählen.[5] Häufig wählt man den Winkel einer komplexen Zahl aus dem Intervall $[0, 2\pi)$ oder aus dem Intervall $[-\pi, \pi)$.

Ein faszinierender Aspekt an der Multiplikation komplexer Zahlen ist – neben der Tatsache $\mathrm{i}^2 = -1$ – dass sie eine geometrische Bedeutung für die Winkel der involvierten Zahlen besitzt. Es gilt nämlich das folgende Lemma:

Lemma 5.2.8 (Multiplikation von Zahlen auf dem Einheitskreis)**.** *Seien $a, b \in \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$, wobei a den Winkel φ_a und b den Winkel φ_b besitzt.*

Dann gilt auch $ab \in \mathbb{T}$ und ab besitzt den Winkel $\varphi_a + \varphi_b$.

Den Beweis führen wir in der Vorlesung geometrisch.[6] Hier im Manuskript geben wir den Beweis nicht an.[7]

Es ist wichtig sich klar zu machen, dass jede Zahl in $\mathbb{C}^*$ durch Angabe ihres Betrages und ihres Winkel eindeutig beschrieben werden kann.[8] Deshalb erhalten wir, indem wir Proposition 5.2.5(g) und Lemma 5.2.8 kombinieren, eine rein geometrische Beschreibung der Multiplikation komplexer Zahlen:

Theorem 5.2.9 (Geometrische Bedeutung der Multiplikation in $\mathbb{C}$)**.** *Für alle von Null verschiedenen[9] komplexen Zahl $z_1, z_2 \in \mathbb{C}^*$ gilt:*

(a) *Man erhält den Betrag von $z_1 z_2$, indem man die Beträge von z_1 und z_2 multipliziert.*

(b) *Man erhält den Winkel von z_1 und z_2 indem man die Winkel von z_1 und z_2 addiert.*

Beweis. (a) Das haben wir bereits in Proposition 5.2.5(g) bewiesen.

[5] Wobei ein Endpunkt im Intervall enthalten seien muss und der andere nicht.

[6] Wobei wir ihn uns der Einfachkeit halber nur für Winkel $\varphi_a, \varphi_b > 0$ ansehen, welche zusammen nicht mehr als eine Viertel Umdrehung beschreiben. Diese Situation ist recht übersichtlich und man kann an ihr bereits gut den bemerkenswerten Zusammenhang zwischen Multiplikation in $\mathbb{C}$ und Addition von Winkeln erkennen.

[7] Aus dem sehr profanen Grund, dass der Beweis eine recht komplexe Zeichnung beinhaltet und ich in diesem Moment gerade nicht genügend Zeit habe um die Zeichnung ordentlich zu TEXen.

[8] Während umgekehrt aber der Winkel nicht eindeutig durch die komplexe Zahl bestimmt ist, wie wir in Bemerkung 5.2.7 besprochen haben.

[9] Bitte überlegen Sie sich: Weshalb nehmen wir in diesem Theorem an, dass z_1 und z_2 ungleich 0 sind? Was passiert, wenn eine der beiden Zahlen gleich 0 ist?

(b) Sei φ_1 der Winkel von z_1 und φ_2 der Winkel von z_2. Wir definieren $u_1 \coloneqq z_1/|z_1|$ und $u_2 \coloneqq z_2/|z_2|$. Dann haben u_1 und u_2 ebenfalls die Winkel φ_1 beziehungsweise φ_2, weil u_1 und u_2 nur gestauchte oder gestreckte Versionen von z_1 und z_2 sind. Außerdem gilt laut Proposition 5.2.5(g)

$$|u_1| = \left| z_1 \frac{1}{|z_1|} \right| = |z_1| \left| \frac{1}{|z_1|} \right| = |z_1| \left| \frac{1}{|z_1|} \right| = |z_1| \frac{1}{|z_1|} = 1$$

und ebenso $|u_2| = 1$, also sind u_1 und u_2 beide in $\mathbb{T}$. Laut Lemma 5.2.8 ist deshalb $\varphi_1 + \varphi_2$ der Winkel von $u_1 u_2$. Zugleich gilt

$$z_1 z_2 = |z_1|\,|z_2|\,u_1 u_2,$$

das heißt, $z_1 z_2$ ist ein positives Vielfaches von $u_1 u_2$ und hat somit denselben Winkel wie $u_1 u_2$ – also den Winkel $\varphi_1 + \varphi_2$. □

Beispiel 5.2.10 (Multiplikation mit **i** und **− i**)**.** Die Zahl i besitzt den Winkel $\pi/2$ und den Betrag 1. Wenn man eine Zahl z mit i multipliziert, bleibt also der Betrag von z erhalten und der Winkel wird um $\pi/2$ – das heißt, um eine Viertel Drehung gegen den Uhrzeigersinn – erhöht.

Die Zahl $-\mathrm{i}$ wiederum hat den Winkel $-\pi/2$ und ebenfalls den Betrag 1. Wenn man also eine Zahl z mit $-\mathrm{i}$ multipliziert, dann bleibt der Betrag der Zahl gleich, aber die Zahl wird um eine Viertel Drehung im Uhrzeigersinn gedreht.

5.3 Bewegungen in der Ebene

Wenn wir zu einer komplexen Zahl z eine weitere komplexe Zahl b addieren, dann wir z um b verschoben – denn die Addition von komplexen Zahlen ist genau die Vektoraddition im $\mathbb{R}^2$. Außerdem wissen Sie aus Theorem 5.2.9 folgendes: Wenn wir z mit einer Zahl $a \in \mathbb{T}$ multiplizieren, dann wird z um den Winkel von a gedreht (und der Betrag von z ändert sich nicht wegen $|a| = 1$.

Kombinationen von Drehungen und Verschiebungen in der komplexen Ebene nennt man **Bewegungen**. Lassen Sie uns das in der folgenden Definition sauber aufschreiben.

Definition 5.3.1 (Bewegungen in $\mathbb{C}$)**.** Eine Funktion $f\colon \mathbb{C} \to \mathbb{C}$ nennt man eine **Bewegung**, falls es ein $a \in \mathbb{T}$ und ein $b \in \mathbb{C}$ gibt derart, dass

$$f(z) = az + b$$

für alle $z \in \mathbb{C}$ gilt.

Die Menge aller Bewegungen auf $\mathbb{C}$ bezeichnen wir im Folgenden mit $\mathrm{Bew}(\mathbb{C})$.

Um das folgendes Resultat zu verstehen, muss man sich zuerst an Beispiel 4.3.1 erinnern: Für jedes Menge X ist $(\mathcal{S}(X), \circ)$ eine Gruppe; dabei bezeichnet $\mathcal{S}(X)$ die Menge der bijektiven Abbildungen $X \to X$ und $\circ$ die Komposition von Abbildungen.

Proposition 5.3.2 (Die Bewegungen bilden eine Gruppe)**.** *Die Menge* $\mathrm{Bew}(\mathbb{C})$ *der Bewegungen auf* $\mathbb{C}$ *ist eine Untergruppe von* $(\mathcal{S}(\mathbb{C}), \circ)$.

Beweis. Wir zeigen zuerst, dass $\mathrm{Bew}(\mathbb{C}) \subseteq \mathcal{S}(\mathbb{C})$ gilt. Sei dazu $f \in \mathrm{Bew}(\mathbb{C})$. Dann gibt es komplexe Zahlen $a \in \mathbb{T}$ und $b \in \mathbb{C}$ derart, dass $f(z) = az + b$ für alle $z \in \mathbb{C}$ gilt. Wir müssen zeigen, dass f bijektiv ist.

Injektivität: Seien $z_1, z_2 \in \mathbb{C}$ mit $f(z_1) = f(z_2)$. Dann gilt $az_1 + b = az_2 + b$. Weil $a \neq 0$ ist, folgt daraus $z_1 = z_2$.

Surjektivität: Sei $y \in \mathbb{C}$. Wir müssen zeigen, dass es ein $z \in \mathbb{C}$ mit der Eigenschaft $f(z) = y$ gibt. Wähle dazu $z := \frac{1}{a}(y - b) \in \mathbb{C}$. Dann rechnet man leicht nach, dass tatsächlich $f(z) = y$ ist.

Wir prüfen nun die Untergruppenaxiome nach:

(UG1) Das neutrale Elemente der Gruppe $(\mathcal{S}(\mathbb{C}), \circ)$ ist die identische Abbildung $\mathrm{id}_{\mathbb{C}}$. Sie ist in $\mathrm{Bew}(\mathbb{C})$ enthalten, denn für alle $z \in \mathbb{C}$ gilt

$$\mathrm{id}_{\mathbb{C}}(z) = z = 1 \cdot z + 0.$$

(UG2) Seien $f_1, f_2 \in \mathrm{Bew}(\mathbb{C})$. Dann gibt es komplexe Zahlen $a_1, a_2 \in \mathbb{T}$ und $b_1, b_2 \in \mathbb{C}$ mit der Eigenschaft

$$f_1(z) = a_1 z + b_1 \qquad \text{und} \qquad f_2(z) = a_2 z + b_2$$

für alle $z \in \mathbb{C}$. Somit folgt für alle $z \in \mathbb{C}$

$$(f_2 \circ f_1)(z) = a_2 f_1(z) + b_2 = a_2\big(a_1 z + b_1\big) + b_2 = a_2 a_1 z + a_2 b_1 + b_2.$$

Wegen $a_2 a_1 \in \mathbb{T}$ und $a_2 b_1 + b_2 \in \mathbb{C}$ ist also auch $f_2 \circ f_1 \in \mathrm{Bew}(\mathbb{C})$.

(UG3) Sei $f \in \mathrm{Bew}(\mathbb{C})$. Dann gibt es komplexe Zahlen $a \in \mathbb{T}$ und $b \in \mathbb{C}$ derart, dass $f(z) = az + b$ für alle $z \in \mathbb{C}$ gilt. Man kann leicht überprüfen, dass die Umkehrfunktion f^{-1} von f durch die Formel

$$f^{-1}(z) = \frac{1}{a}(z - b) = \frac{1}{a}z + (-\frac{b}{a})$$

für alle $z \in \mathbb{C}$ gegeben ist; man beachte hierbei, dass $a \neq 0$ gilt, da $a \in \mathbb{T}$ ist. Wegen $1/a \in \mathbb{T}$ ist also auch $f^{-1} \in \mathrm{Bew}(\mathbb{C})$. □

Beispiel 5.3.3 (Hintereinanderausführung von zwei Bewegungen)**.** Betrachten Sie die beiden Bewegungen $f_1, f_2 \colon \mathbb{C} \to \mathbb{C}$, die durch

$$f_1(z) = \mathrm{i}\, z + 1 - \mathrm{i} \qquad \text{und} \qquad f_2(z) = -z + 1$$

gegeben sind. Geometrische tun die beiden Funktionen f_1 und f_2 das folgende:

- Die Bewegung f_1 dreht alle Punkte in der komplexen Ebene zunächst um eine Viertel Drehung gegen den Uhrzeigersinn und verschiebt die gedrehten Punkte anschließend um 1 nach rechts und 1 nach unten.

- Die Bewegung f_2 dreht alle Punkte in der komplexen Ebene zunächst um eine halbe Drehung[10] und verschiebt die gedrehten Punkte anschließend um 1 nach rechts.

Nun berechnen wir, was die Hintereinanderausführungen $f_2 \circ f_1$ und $f_1 \circ f_2$ tun: Für alle $z \in \mathbb{C}$ gilt

$$(f_2 \circ f_1)(z) = f_2(f_1(z)) = -f_1(z) + 1 = -(\mathrm{i}\, z + 1 - \mathrm{i}) + 1 = -\mathrm{i}\, z + \mathrm{i}\,.$$

und

$$(f_1 \circ f_2)(z) = f_1(f_2(z)) = \mathrm{i}\, f_2(z) + 1 - \mathrm{i} = \mathrm{i}(-z + 1) + 1 - \mathrm{i} = -\mathrm{i}\, z + 1.$$

Das bedeutet:

- Die Funktion $f_2 \circ f_1$ dreht alle Punkte in der komplexen Ebene zunächst um eine Dreiviertel Drehung gegen den Uhrzeigersinn[11] und verschiebt die gedrehten Punkte anschließend um 1 nach oben.
- Die Funktion $f_1 \circ f_2$ dreht ebenfalls alle Punkte in der komplexen Ebene zunächst um eine Dreiviertel Drehung gegen den Uhrzeigersinn, verschiebt die gedrehten Punkte dann allerdings um 1 nach rechts.

Insbesondere ist also $f_1 \circ f_2 \neq f_2 \circ f_1$. Somit ist die Gruppe $(\mathrm{Bew}(\mathbb{C}), \circ)$ nicht kommutativ.

5.4 Trigonometrische Funktionen und Polarkoordinaten komplexer Zahlen

Im vorangehenden Abschnitt haben wir bereits diskutiert, dass jede komplexe Zahl z eindeutig durch ihren Betrag $|z|$ und Ihren Winkel bestimmt ist. Den Zusammenhang zwischen diesen beiden Größen und dem Real- und Imaginärteil von z möchten wir nun noch etwas systematischer untersuchen. Dafür sind die folgenden Funktionen hilfreich:

Definition 5.4.1 (Cosinus und Sinus)**.** Sei $\varphi \in \mathbb{R}$ und sei $z \in \mathbb{T}$ diejenige Zahl auf der komplexen Einheitskreislinie mit Winkel φ.[12] Man nennt die Zahlen

$$\cos(\varphi) \coloneqq \mathrm{Re}\, z \qquad \text{und} \qquad \sin(\varphi) \coloneqq \mathrm{Im}\, z$$

den **Cosinus** und den **Sinus** von φ.

[10] Hier spielt es keine Rolle ob entgegen oder im Uhrzeigersinn. Weshalb spielt das keine Rolle?

[11] Genauso gut können wir auch sagen: Um eine Viertel Drehung im Umzeigersinn.

[12] Wobei wir, wie schon zuvor, den Winkel im Bogenmaß messen – das heißt, der Winkel 2π entspricht einer vollen Umdrehung.

Damit haben wir also zwei Funktionen $\cos\colon \mathbb{R} \to \mathbb{R}$ und $\sin\colon \mathbb{R} \to \mathbb{R}$ definiert. Die folgenden Eigenschaften dieser Funktionen folgen geometrisch sofort aus ihrer Definition.

Proposition 5.4.2 (Einige Eigenschaften von Cosinus und Sinus)**.** *Die Funktionen* $\cos, \sin\colon \mathbb{R} \to \mathbb{R}$ *besitzen die folgenden Eigenschaften:*

(a) *Für alle* $\varphi \in \mathbb{R}$ *gilt* $\cos(\varphi) \in [-1, 1]$ *und* $\sin(\varphi) \in [-1, 1]$.

(b) *Die beiden Funktionen* cos *und* sin *sind* 2π*-periodisch, das heißt, für alle* $\varphi \in \mathbb{R}$ *und alle* $n \in \mathbb{Z}$ *gilt*

$$\cos(\varphi) = \cos(\varphi + n2\pi) \quad \textit{und} \quad \sin(\varphi) = \sin(\varphi + n2\pi).$$

(c) *Die Nullstellen der Funktion* cos *sind genau die Zahlen* $(n + \frac{1}{2})\pi$ *mit* $n \in \mathbb{Z}$.
Die Nullstellen der Funktion sin *sind genau die Zahlen* $n\pi$ *mit* $n \in \mathbb{Z}$.

(d) *Die Funktion* cos *nimmt genau an den Stellen* $2\pi n$ *mit* $n \in \mathbb{Z}$ *den Wert* 1 *an und sie nimmt genau an den Stellen* $2\pi n + \pi$ *mit* $n \in \mathbb{Z}$ *den Wert* -1 *an.*
Die Funktion sin *nimmt genau an den Stellen* $2\pi n + \frac{\pi}{2}$ *mit* $n \in \mathbb{Z}$ *den Wert* 1 *an und nimmt genau an den Stellen* $2\pi n - \frac{\pi}{2}$ *mit* $n \in \mathbb{Z}$ *den Wert* -1 *an.*

(e) *Für alle* $\varphi \in \mathbb{R}$ *gilt*

$$\cos(-\varphi) = \cos(\varphi) \qquad \textit{und} \qquad \sin(-\varphi) = -\sin(\varphi).$$

Wir können die Tatsache, dass sich bei der Multiplikation zweier komplexer Zahlen ihre Winkel addieren, verwenden um das folgende Resultat zu beweisen.

Theorem 5.4.3 (Additionstheorem)**.** *Seien* $\varphi_1, \varphi_2 \in \mathbb{R}$. *Dann gilt*

$$\cos(\varphi_1 + \varphi_2) = \cos(\varphi_1)\cos(\varphi_2) - \sin(\varphi_1)\sin(\varphi_2)$$

und

$$\sin(\varphi_1 + \varphi_2) = \cos(\varphi_1)\sin(\varphi_2) + \sin(\varphi_1)\cos(\varphi_2).$$

Beweis. Seien $z_1, z_2 \in \mathbb{T}$ die beiden Zahlen auf der komplexen Einheitskreislinie mit Winkel φ_1 und φ_2. Dann hat die Zahl $z_1 z_2$ laut Theorem 5.2.9(b) den Winkel $\varphi_1 + \varphi_2$. Also gilt laut Definition 5.4.1

$$\begin{aligned} \cos(\varphi_1) &= \operatorname{Re} z_1, \quad \cos(\varphi_2) = \operatorname{Re} z_2, \quad \cos(\varphi_1 + \varphi_2) = \operatorname{Re}(z_1 z_2), \\ \sin(\varphi_1) &= \operatorname{Im} z_1, \quad \sin(\varphi_2) = \operatorname{Im} z_2, \quad \sin(\varphi_1 + \varphi_2) = \operatorname{Im}(z_1 z_2). \end{aligned}$$

Somit ist

$$\cos(\varphi_1 + \varphi_2) + \mathrm{i}\sin(\varphi_1 + \varphi_2) = z_1 z_2$$

$$= \big(\cos(\varphi_1) + \mathrm{i}\sin(\varphi_1)\big)\big(\cos(\varphi_2) + \mathrm{i}\sin(\varphi_2)\big)$$
$$= \big(\cos(\varphi_1)\cos(\varphi_2) - \sin(\varphi_1)\sin(\varphi_2)\big) + \mathrm{i}\,\big(\cos(\varphi_1)\sin(\varphi_2) + \sin(\varphi_1)\cos(\varphi_2)\big).$$

Indem wir Real- und Imaginärteil dieser Gleichung nehmen, erhalten wir die beiden behaupteten Gleichheiten. □

Als Konsequenz erhalten wir insbesondere den folgenden Zusammenhang zwischen der Cosinus- und der Sinus-Funktion:

Korollar 5.4.4 (Der Cosinus ist ein verschobener Sinus)**.** *Für jedes $\varphi \in \mathbb{R}$ gilt*

$$\sin(\varphi + \frac{\pi}{2}) = \cos(\varphi).$$

Beweis. Lassen Sie uns die zweite Formel in Theorem 5.4.3 auf die beiden Winkel $\varphi_1 := \varphi$ und $\varphi_2 := \frac{\pi}{2}$ anwenden. Dann erhalten wir

$$\sin(\varphi + \frac{\pi}{2}) = \cos(\varphi)\sin(\frac{\pi}{2}) + \sin(\varphi)\cos(\frac{\pi}{2}) = \cos(\varphi),$$

wobei wir für die letzte Gleichheit verwendet haben, dass $\sin(\frac{\pi}{2}) = 1$ und $\cos(\frac{\pi}{2}) = 0$ gilt. □

Das folgende Resultat ist eine einfache Konsequenz aus der Definition von Cosinus und Sinus. Aber wegen seiner Wichtigkeit bezeichnen wir es als „Theorem“ statt nur als „Proposition“.

Theorem 5.4.5 (Polarkoordinatendarstellung komplexer Zahlen)**.** *Sei $z \in \mathbb{C}^*$ mit Winkel $\varphi \in \mathbb{R}$. Dann gilt*

$$z = |z|\,\big(\cos(\varphi) + \mathrm{i}\sin(\varphi)\big).$$

Beweis. Setze $u := \frac{z}{|z|}$. Dann besitzt u ebenfalls den Winkel φ und außerdem gilt $|u| = 1$ und somit $u \in \mathbb{T}$. Laut Definition 5.4.1 ist somit

$$\frac{z}{|z|} = u = \operatorname{Re} u + \mathrm{i}\operatorname{Im} u = \cos(\varphi) + \mathrm{i}\sin(\varphi).$$

Multiplizieren dieser Gleichheit mit $|z|$ liefert die behauptete Formel. □

Proposition 5.4.6 (Einige wichtige Werte von Cosinus und Sinus)**.** *Die Cosinus und die Sinusfunktion nehmen an den Stellen in der folgenden Tabelle die angegebenen Werte an:*

φ im Bogenmaß	0	$\frac{2\pi}{12}$	$\frac{2\pi}{8}$	$\frac{2\pi}{6}$	$\frac{2\pi}{4}$
φ im Gradmaß	$0°$	$30°$	$45°$	$60°$	$90°$
$\cos(\varphi)$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0
$\cos(\varphi)$ *(Merkhilfe)*	$\frac{\sqrt{4}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{1}}{2}$	$\frac{\sqrt{0}}{2}$
$\sin(\varphi)$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1
$\sin(\varphi)$ *(Merkhilfe)*	$\frac{\sqrt{0}}{2}$	$\frac{\sqrt{1}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{4}}{2}$.

Beweis. Es genügt die behaupteten Werte für den Cosinus zu beweisen; die Werte für den Sinus folgen dann aus Symmetrieüberlegungen.

Für die einzelnen Werte das Cosinus geben wir in der Vorlesungen geometrische Beweise an.[13] □

Bemerkung 5.4.7 (Tangens)**.** Aus Cosinus und Sinus kann man noch weitere trigonometrische Funktionen bauen. Zum Beispiel ist der **Tangens** die Funktion

$$\tan : \mathbb{R} \setminus \{(n + \frac{1}{2})\pi \mid \ n \in \mathbb{Z}\} \to \mathbb{R},$$
$$\varphi \mapsto \frac{\sin(\varphi)}{\cos(\varphi)}.$$

Wir besprechen den Tangens an dieser Stelle nicht weiter. Er wird später in Analysis I wieder auftauchen.

In der Vorlesung Analysis I werden Sie noch eine ganze andere Perspektive auf den Cosinus und den Sinus kennen lernen, in der es nicht nur im geometrische, sondern auch um analytische Eigenschaften geht.

5.5 Polynomfunktionen und rationale Funktionen

Zum Abschluss von Kapitel 5 sprechen wir noch über zwei wichtige Klasse von Funktionen: Polynomfunktionen und rationale Funktionen. Vermutlich kennen Sie solche Funktionen auf den reellen Zahlen schon aus der Schule. Nun wollen wir auch komplexe Zahlen einsetzen.

Definition 5.5.1 (Polynomfunktion)**.** Eine Funktion $f\colon \mathbb{C} \to \mathbb{C}$ bezeichnet man als **Polynomfunktion**, falls es ein $n \in \mathbb{N}$ und komplexe Zahlen $a_0, \ldots, a_n \in \mathbb{C}$ gibt derart, dass

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = \sum_{k=0}^{n} a_k z^k$$

gilt. In diesem Fall heißen die Zahlen $a_0, \ldots, a_n$ **Koeffizienten** der Polynomfunktion f. Falls $a_n \neq 0$ ist, dann sagen wir, dass f den **Grad** n besitzt. Falls $f = 0$ ist (und es somit keinen Koeffizenten gibt, der $\neq 0$ ist), sagen wir, dass f den Grad $-\infty$ besitzt.

Mit Methoden der Analysis (genauer: mit Hilfe der Ableitung von Funktionen) kann man zeigen, dass Koeffizienten einer Polynomfunktion – und somit auch ihr Grad – eindeutig bestimmt sind. Man schreibt häufig $\deg(f)$ für den Grad einer Polynomfunktion f.[14]

[13] Sollte ich Zeit dafür finden, trage ich hier im Manuskript die für den Beweis notwendigen Skizzen nach. Das kann ich im Moment aber nicht versprechen.

[14] Von Englisch „degree“.

Beispiele 5.5.2 (Der Grad einiger Polynomfunktionen)**.** (a) Die Polynomfunktion $f_1\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto z^3 + z - \mathrm{i}$ besitzt den Grad 3.

(b) Die Polynomfunktion $f_2\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto 0 \cdot z^5 + z^2 + 1$ besitzt ebenfalls den Grad 3.

(c) Die Polynomfunktion $f_3\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto z - 2\,\mathrm{i}$ besitzt den Grad 1.

(d) Die Polynomfunktion $f_4\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto -20$ besitzt den Grad 0.

(e) Die Polynomfunktion $f_5\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto 0$ besitzt den Grad $-\infty$.

Auch für Polynomfunktionen gibt es eine Variante des Teilen mit Rests: Die folgenden Proposition kann man mit Hilfe von Polynomdivision beweisen, die Sie vermutlich aus der Schule kennen.

Proposition 5.5.3 (Teilen mit Rest für Polynomfunktionen)**.** *Seien $f, q\colon \mathbb{C} \to \mathbb{C}$ Polynomfunktionen mit $q \neq 0$. Dann gibt es eine Polynomfunktion $c, r\colon \mathbb{C} \to \mathbb{C}$ mit* $\deg(r) < \deg(q)$ *derart, dass*

$$f(z) = c(z)q(z) + r(z)$$

für alle $z \in \mathbb{C}$ gilt.

Eine Phänomen, das Sie vermutlich ebenfalls schon einmal in der Schule gesehen haben, ist, dass es Polynomfunktionen gibt, die keine reelle Nullstelle besitzen.

Beispiel 5.5.4 (Nullstellen in $\mathbb{R}$ vs. $\mathbb{C}$)**.** Betrachten Sie die Funktion $f : \mathbb{C} \to \mathbb{C}$, $z \mapsto z^2 + 1$. Für jede reelle Zahl z gilt $f(z) \in \mathbb{R}$ und $f(z) \geq 1$. Somit gibt es keine reelle Zahl z mit der Eigenschaft $f(z) = 0$.

Es gibt allerdings eine komplexe Zahl z mit der Eigenschaft $f(z) = 0$ – beispielsweise die Zahl $z = \mathrm{i}$.

Wir können sogar noch mehr sagen: Wir alle komplexen Zahlen z gilt nämlich

$$f(z) = z^2 + 1 = (z - \mathrm{i})(z + \mathrm{i}).$$

Weil ein Produkt in einem Körper genau dann 0 ist, wenn mindestens einer der Faktoren 0 ist, sehen wir also, dass $f(z) = 0$ genau dann gilt, wenn $z = \mathrm{i}$ oder $z = -\mathrm{i}$ gilt.

Die Beobachtung aus dem vorangehenden Beispiel lässt sich auf jede andere Polynomfunktionen verallgemeinern. Das ist der Inhalt des folgenden Satzes.

Theorem 5.5.5 (Fundamentalsatz der Algebra)**.** *Sei $f\colon \mathbb{C} \to \mathbb{C}$ eine Polynomfunktion vom Grad $n \geq 1$.*

(a) *Die Funktion f hat mindestens eine Nullstelle in $\mathbb{C}$, das heißt es gibt ein $z_1 \in \mathbb{C}$ mit der Eigenschaft $f(z_1) = 0$.*

(b) *Genauer gilt: Es gibt Zahlen* $a \in \mathbb{C}$ *und* $z_1, \ldots, z_n \in \mathbb{C}$ *derart, dass*

$$f(z) = a(z - z_1)(z - z_2) \cdot \cdots \cdot (z - z_n) \qquad \text{für alle } z \in \mathbb{C}$$

gilt.[15] *Insbesondere gilt* $f(z) = 0$ *genau dann, wenn* z *eine der Zahlen* $z_1, \ldots, z_n$ *ist.*

Beweis. (a) Diese Aussage ist, trotz des Namens des Satzes, eher ein analytisches Resultat. Einen Beweis können Sie zum Beispiel in einer Analysis- oder einer Funktionentheorie-Vorlesung sehen.

(b) Wir beweisen die Behauptung per Induktion über n. Für jedes $n \in \mathbb{N}^*$ sei $A(n)$ die Aussage „Für jedes Polynomfunktion $f\colon \mathbb{C} \to \mathbb{C}$ vom Grad n gibt Zahlen $z_1, \ldots, z_n$ derart, dass $f(z) = (z - z_1) \cdot \cdots \cdot (z - z_n)$ für alle $z \in \mathbb{C}$ gilt."

Wir zeigen zunächst, dass $A(1)$ wahr ist. Sei dazu $f\colon \mathbb{C} \to \mathbb{C}$ eine Polynomfunktion vom Grad 1. Dann gibt es $a_0, a_1 \in \mathbb{C}$ mit $a_1 \neq 0$ und derart, dass $f(z) = a_1 z + a_0$ für alle $z \in \mathbb{C}$ gilt. Setze nun $z_1 \coloneqq -a_0/a_1$. Dann gilt für alle $z \in \mathbb{C}$

$$f(z) = a_1(z - z_1)$$

und somit ist $A(1)$ gezeigt.

Nun zeigen wir für jedes $n \in \mathbb{N}^*$ die Implikation $A(n) \Rightarrow A(n+1)$. Sei dazu $n \in \mathbb{N}^*$ beliebig und sei $A(n)$ wahr. Sei $f\colon \mathbb{C} \to \mathbb{C}$ eine Polynomfunktion vom Grad $n+1$. Laut Aussage (a) gibt es eine komplexe Zahl – nennen wir sie z_{n+1} – mit der Eigenschaft $f(z_{n+1}) = 0$.

Betrachten Sie nun die Polynomfunktion $q\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto z - z_{n+1}$; sie hat Grad 1. Laut Proposition 5.5.3 gibt es Polynomfunktionen $c, r\colon \mathbb{C} \to \mathbb{C}$ mit $\deg(r) < \deg(q) = 1$ derart, dass

$$f(z) = c(z)q(z) + r(z)$$

für alle $z \in \mathbb{C}$ gilt. Insbesondere gilt

$$0 = f(z_{n+1}) = c(z_{n+1})q(z_{n+1}) + r(z_{n+1}) = r(z_{n+1}),$$

wobei wir im letzten Schritt verwendet haben, dass $q(z_{n+1}) = z_{n+1} - z_{n+1} = 0$ gilt. Da r höchstens Grad 1 besitzt, ist r eine konstante Funktion und somit folgt $r = 0$. Es ist also

$$f(z) = c(z)q(z)$$

für alle $z \in \mathbb{C}$. Da f den Grad $n+1$ und q den Grad 1 besitzt, besitzt c den Grad n. Deshalb folgt aus $A(n)$, dass es Zahlen $a \in \mathbb{C}$ und $z_1, \ldots, z_n \in \mathbb{C}$ gibt derart, dass

$$c(z) = (z - z_1) \cdot \cdots \cdot (z - z_n)$$

[15] Man kann sich übrigens leicht überlegen, dass die Zahl a der Koeffizient der Polynomfunktion f vor dem Term z^n ist.

für alle $z \in \mathbb{C}$ gilt. Also folgt

$$f(z) = c(z)q(z) = (z - z_1) \cdot \dots \cdot (z - z_n)(z - z_{n+1})$$

für alle $z \in \mathbb{C}$. Also ist $A(n+1)$ wahr.

Aufgrund der Prinzips der vollständigen Induktion folgt dass $A(n)$ für alle $n \in \mathbb{N}^*$ wahr ist. Damit ist die Behauptung bewiesen. □

Bemerkung 5.5.6 (Rationale Funktionen)**.** Unter einer **rationalen Funktion** versteht man eine Funktion, die ein Quotient zweier Polynomfunktionen ist. Wenn man das Polynom im Nenner in Linearfaktoren zerlegt – was laut Theorem 5.5.5(b) immer möglich ist – kann man die größtmögliche Teilmenge von $\mathbb{C}$ finden, auf der sich solch eine rationale Funktion definieren lässt. Wir demonstrieren das kurz an einem einfachen Beispiel:

Betrachten Sie die Polynomfunktion $q\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto z^3 - 3z + 2$. Wir können diese Funktion schreiben als $q(z) = (z-1)(z-2)$ für alle $z \in \mathbb{C}$. Somit können wir die rationale Funktion $\mathbb{C} \setminus \{1, 2\} \to \mathbb{C}$, $z \mapsto \frac{1}{q(z)}$ definieren.

Mehr zu rationalen Funktionen werden Sie in verschiedenen Analysis-Vorlesungen lernen.

Kapitel 6

Relationen und Quotientenstrukturen

Einstiegsfragen. (a) Was ist eigentlich eine negative Zahl?

(b) Versuchen Sie die folgende Tabelle zu vervollständigen:

Tierart	Farbmusterung des Fells
Zebra	schwarz-weiß gestreift
Eisbär	einfarbig weiß
Löwin	
Tiger	
Pferd	
Gepard	
Hund	

Was denken Sie dazu?

6.1 Was ist eine Relation?

Definition 6.1.1 (Relation)**.** Sei X eine Menge. Eine **Relation auf X** ist eine Teilmenge R von $X \times X$. Um für zwei Elemente $x, y \in X$ auszudrücken, dass $(x, y) \in R$ gilt, schreibt man häufig auch $x\,R\,y$.

Die auf den ersten Blick etwas merkwürdige Infix-Notation „$x\,R\,y$“ in der vorangehenden Definition wird klarer, wenn man sich zwei typische Beispiele für Relationen auf den reellen Zahlen ansieht:

Beispiele 6.1.2 (Ordnungsrelationen auf $\mathbb{R}$)**.** (a) Betrachten Sie auf $\mathbb{R}$ die Relation

$$\leq \coloneqq \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \ x \text{ ist kleiner oder gleich } y\}.$$

Für $x, y \in \mathbb{R}$ hat dann $x \leq y$ die übliche Bedeutung, die Sie bereits aus der Schule kennen.

(b) Betrachten Sie auf $\mathbb{R}$ die Relation

$$< \coloneqq \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \ x \text{ ist strikt kleiner als } y\}.$$

Dann hat für $x, y \in \mathbb{R}$ die Notation $x < y$ ebenfalls die Bedeutung, die Sie für diese Notation bereits aus der Schule kennen.

Die übliche Ordnung der reellen Zahlen lässt sich axiomatisieren, in dem man die folgende Klasse von Relationen definiert:

Definition 6.1.3 (Partielle und totale Ordnungen)**.** Sei X eine Menge. Eine Relation $\leq \subseteq X \times X$ nennt man eine **partielle Ordnung auf X**, falls sie die folgenden Axiome erfüllt:

(PO1) **Reflexivität:** Für alle $x \in X$ gilt $x \leq x$.

(PO2) **Anti-Symmetrie:** Für alle $x, y \in X$ gilt folgende Implikation:
$(x \leq y \text{ und } y \leq x) \Rightarrow x = y$

(PO3) **Transitivität:** Für alle $x, y, z \in X$ gilt folgende Implikation: $(x \leq y$ und $y \leq z) \Rightarrow x \leq z$

Wenn zusätzliche das folgende Axiom erfüllt ist, dann nennt man die partielle Ordnung $\leq$ eine **totale Ordnung** oder eine **lineare Ordnung** auf X:

(TO) **Totalität:** Für alle $x, y \in X$ gilt $x \leq y$ oder $y \leq x$.

Beispiel 6.1.4 (Die Ordnung auf $\mathbb{R}$)**.** Die Relation $\leq$ auf $\mathbb{R}$ist eine totale Ordnung.

Beispiel 6.1.5 (Eine partielle Ordnung, die nicht total ist)**.** Lassen Sie uns auf $\mathbb{N}^*$ die Relation

$$\mid \coloneqq \{(m, n) \in \mathbb{N}^* \times \mathbb{N}^* \mid \ m \text{ teilt } n\}$$

definieren. Dann ist $\mid$ eine partielle Ordnung, die nicht total ist.

Beweis. Wir überprüfen zuerst, dass $\mid$ die Axiome einer partiellen Ordnung erfüllt:

(PO1) Für jedes $n \in \mathbb{N}^*$ gilt, dass n sich selbst teilt, also ist $n \mid n$.

(PO2) Seien $m, n \in \mathbb{N}^*$ mit $m \mid n$ und $n \mid m$. Dann gibt es Zahlen $a, b \in \mathbb{N}^*$ mit $n = am$ und $m = bn$. Also folgt $n = abn$, somit $ab = 1$ und wegen $a, b \in \mathbb{N}^*$ folglich $a = b = 1$. Somit ist $m = n$.

(PO3) Seien $\ell, m, n \in \mathbb{N}^*$ mit $\ell \mid m$ und $m \mid n$. Dann gibt es Zahlen $a, b \in \mathbb{N}^*$ mit $m = a\ell$ und $n = bm$. Somit ist $n = ba\ell$, also gilt auch $\ell \mid n$.

Nun zeigen wir noch, dass die partielle Ordnung $\mid$ nicht total ist: Betrachten Sie dazu zum Beispiel die Zahlen $2, 3 \in \mathbb{N}^*$. Dann gilt weder $2 \mid 3$ noch $3 \mid 2$. Also ist (TO) nicht erfüllt. □

6.2 Äquivalenzrelationen und die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$

Definition 6.2.1 (Äquivalenzrelation)**.** Sei X eine Menge. Eine Relation $\sim$ auf X nennt man eine **Äquivalenzrelation**, falls sie die folgenden Axiome erfüllt:

(ÄR1) **Reflexivität:** Für alle $x \in X$ gilt $x \sim x$.

(ÄR2) **Symmetrie:** Für alle $x, y \in X$ gilt:[1]
$(x \sim y \Rightarrow y \sim x)$

(ÄR3) **Transitivität:** Für alle $x, y, z \in X$ gilt folgende Implikation: ($x \sim y$ und $y \sim z$) $\Rightarrow x \sim z$

Beachten Sie, dass sich Äquivalenzrelationen nur in einem Punkt von partiellen Ordnungen unterscheiden: Im zweiten Axiom verlangt man Symmetrie anstelle von Anti-Symmetrie. Diese – auf den ersten Blick vielleicht klein erscheinende – Änderung sorgt aber dafür, dass Äquivalenzrelationen sich völlig anders verhalten als partielle Ordnungen.

Wir diskutieren zunächst ein paar Beispiele.

Beispiele 6.2.2 (Einige Beispiele für Äquivalenzrelationen)**.** (a) Sei M die Menge aller Menschen. Für alle $x, y \in M$ definieren wir $x \sim y$ genau dann, wenn x gleich groß ist wie y (gemessen in der Körperhöhe). Dann ist $\sim$ eine Äquivalenzrelation auf M.

Beweis. (ÄR1) Sei $x \in M$. Dann ist x gleich groß wie x, also gilt $x \sim x$.

(ÄR2) Seien $x, y \in M$ mit $x \sim y$. Dann ist x gleich groß wie y und somit ist y auch gleich groß wie x. Also gilt $y \sim x$.

(ÄR3) Seien $x, y, z \in M$ und sei $x \sim y$ und $y \sim z$. Dann ist x gleich groß wie y und y gleich groß wie z. Also ist x gleich große wie z und somit gilt $x \sim z$. □

(b) Sie $n \in \mathbb{Z} \setminus \{0\}$. Für alle $k, \ell \in \mathbb{Z}$ definieren wir $k \equiv_n \ell$ genau dann, wenn $k - \ell$ durch n teilbar ist. Dann ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. (ÄR1) Sei $k \in \mathbb{Z}$. Dann ist $k - k = 0$ durch n teilbar, also gilt $k \equiv_n k$.

(ÄR2) Seien $k, \ell \in \mathbb{Z}$ mit $k \equiv_n \ell$. Dann ist $k - \ell$ durch n teilbar. Somit ist $\ell - k = -(k - \ell)$ ebenfalls durch n teilbar. Also gilt auch $\ell \equiv_n k$.

(ÄR3) Seien $j, k, \ell \in \mathbb{Z}$ mit $j \equiv_n k$ und $k \equiv_n \ell$. Dann sind $j - k$ und $k - \ell$ beide durch n teilbar. Somit ist

$$j - \ell = (j - k) + (k - \ell)$$

ebenfalls durch n teilbar, also gilt auch $j \equiv_n \ell$. □

[1] Beachten Sie, dass man genau so gut auch fordern kann, dass für alle $x, y \in X$ die Bedingung „$x \sim y \Leftrightarrow y \sim x$“ gilt. Weshalb macht das keinen Unterschied?

(c) Die übliche Relation $\leq$ auf $\mathbb{R}$ ist keine Äquivalenzrelation.

Es gilt nämlich zum Beispiel $1 \leq 2$, aber nicht $2 \leq 1$, also ist das Axiom (ÄR2) nicht erfüllt.

Bemerkungen 6.2.3 (Äquivalenz modulo n)**.** Sei $n \in \mathbb{Z} \setminus \{0\}$.

(a) Für zwei Zahlen $k, \ell \in \mathbb{Z}$ schreibt man für die Aussage $k \equiv_n \ell$ auch häufig

$$k \equiv \ell \pmod{n}$$

und spricht dies aus als „k ist kongruent zu ℓ modulo n“.

(b) Sei nun zusätzliche $n > 0$, das heißt $n \in \mathbb{N}^*$. Dann können wir die Notation für das Teilen mit Rest verwenden, die wir in Definition 4.4.1 eingeführt haben.

Für $k, \ell \in \mathbb{Z}$ ist die Bedingung $k \equiv_n \ell$ – oder anders geschrieben: $k \equiv \ell \pmod{n}$ – gleichbedeutend mit $\mathrm{Rest}(k - \ell, n) = 0$.

Für jedes $k \in \mathbb{Z}$ gilt außerdem: Es ist $\mathrm{Rest}(k, n)$ diejenige Zahl $r \in \{0, \ldots, n-1\}$, für die $k \equiv_n r$ gilt.

Definition 6.2.4 (Äquivalenzklasse)**.** Sei X eine Menge und $\sim$ eine Äquivalenzrelation auf X.

(a) Für jedes $x_0 \in X$ nennt man die Menge

$$[x_0] \coloneqq \{x \in X \mid x \sim x_0\}$$

die **Äquivalenzklasse von x_0** bezüglich der Äquivalenzrelation $\sim$.

(b) Eine Teilmenge $M \subseteq X$ nennt man eine **Äquivalenzklasse von $\sim$**, falls es ein $x_0 \in X$ mit der Eigenschaft $M = [x_0]$ gibt.

(c) Die Menge aller Äquivalenzklassen von $\sim$ bezeichnet man mit $X/\sim$.[2]

Es folgt sofort aus der vorangehenden Definition, dass eine Äquivalenzklasse immer nichtleer ist. Außerdem hat man die folgende sehr nützliche Eigenschaft von Äquivalenzklassen:

Proposition 6.2.5 (Eigenschaften von Äquivalenzklassen)**.** *Sei X eine Menge und $\sim$ eine Äquivalenzrelation auf X. Dann ist X die disjunkte Vereinigung aller Äquivalenzklassen von $\sim$, das heißt, es gilt:*

(a) *Für zwei Äquivalenzklassen $M, N \subseteq X$ von $\sim$ gilt entweder $M = N$ oder $M \cap N = \emptyset$.*

(b) *Für jedes Äquivalenzklasse $M \subseteq X$ von $\sim$ und jedes Element $x \in M$ gilt $M = [x]$.*

[2] Beachten Sie, dass also $X/\sim \subseteq \mathcal{P}(X)$ ist.

(c) *Für zwei Elemente $x, y \in X$ gilt $[x] = [y]$ genau dann, wenn $x \sim y$ ist.*

(d) *Die Menge X ist die Vereinigung aller Äquivalenzklassen von $\sim$, das heißt, es gilt $X = \bigcup_{M \in X/\sim} M = \bigcup_{x \in X} [x]$.*

Beweis. (a) Seien $M, N \subseteq X$ zwei Äquivalenzklassen von X. Dann gibt es Elemente $x_0, x_1 \in X$ derart, dass

$$M = [x_0] \quad \text{und} \quad N = [x_1]$$

gilt. Wegen $(R1)$ ist insbesondere somit $x_0 \in M$ und $x_1 \in N$, also sind M und N nichtleer. Deshalb kann nicht zugleich $M = N$ und $M \cap N = \emptyset$ gelten. Wir zeigen nun, dass aber eine dieser beiden Aussagen gilt. Sei dazu $M \cap N \neq \emptyset$; dann gibt es ein $y \in M \cap N$. Wir müssen $M = N$ zeigen.

"$\subseteq$" Sei $x \in M$. Dann ist $x \sim x_0$. Wegen $y \in M$ gilt zugleich $y \sim x_0$ und wegen (ÄR2) somit $x_0 \sim y$. Also folgt aus (ÄR3), dass $x \sim y$ gilt. Wegen $y \in N$ gilt außerdem $y \sim x_1$ und nochmalige Anwendung von (ÄR3) liefert somit $x \sim x_1$. Somit ist $x \in N$.

"$\supseteq$" Diese Inklusion beweist man genauso wie die vorangehende, nur mit umgekehrten Bezeichnungen.

(b) Sei M eine Äquivalenzklasse von $\sim$ und $x \in M$. Wegen $x \in M$ und $x \in [x]$ sind die beiden Äquivalenzklassen M und $[x]$ nicht disjunkt, also stimmen sie laut (a) überein.

(c) Seien $x, y \in X$.

"$\Rightarrow$" Sei $[x] = [y]$. Dann gilt gilt $x \in [x] = [y]$ und somit $x \sim y$.

"$\Leftarrow$" Sei $x \sim y$. Dann gilt $x \in [x]$ and $x \in [y]$. Also haben die beiden Äquivalenzklassen $[x]$ und $[y]$ nichtleeren Durchschnitt, also folgt aus (a), dass $[x] = [y]$ gilt.

(d) Die zweite Gleichheit folgt direkt aus (a). Wir müssen also nur $X = \bigcup_{M \in X/\sim} M$ zeigen.

"$\supseteq$" Sei $x \in \bigcup_{M \in X/\sim} M$. Dann gibt es eine Äquivalenzklasse $M \in X/\sim$ derart, dass $x \in M$ ist. Wegen $M \subseteq X$ folgt $x \in X$.

"$\subseteq$" Sei $x \in X$. Dann ist $M \coloneqq \{y \in X \mid y \sim x\}$ eine Äquivalenzklasse von $\sim$ – das heißt, $M \in X/\sim$ – und es gilt $x \in M$. Also ist $x \in \bigcup_{M \in X/\sim} M$. □

Beispiel 6.2.6 (Zerlegung von $\mathbb{Z}$ in Äquivalenzklassen modulo $\boldsymbol{n}\mathbb{Z}$)**.** Sei $n \in \mathbb{N}^*$. Dann besitzt $\equiv_n$ genau n Äquivalenzklassen, nämlich die Mengen

$$\begin{aligned}
[0] &= \{k \in \mathbb{Z} \mid n \mid k - 0\} = \{0 + nj \mid j \in \mathbb{Z}\} =: 0 + n\mathbb{Z}, \\
[1] &= \{k \in \mathbb{Z} \mid n \mid k - 1\} = \{1 + nj \mid j \in \mathbb{Z}\} =: 1 + n\mathbb{Z}, \\
&\vdots \\
[n-1] &= \{k \in \mathbb{Z} \mid n \mid k - (n-1)\} = \{(n-1) + nj \mid j \in \mathbb{Z}\} =: (n-1) + n\mathbb{Z}.
\end{aligned}$$

Beweis. Die behaupteten Mengengleichheiten folgen direkt aus der Definition von $\equiv_n$.

Als nächstes zeigen wir, dass alle aufgelisteten Äquivalenzklassen verschieden sind. Seien dazu $j, k \in \{0, 1, \ldots, n-1\}$ mit $j \neq k$. Dann ist $j - k$ nicht durch n teilbar, also gilt nicht $j \equiv_n k$. Somit ist laut Proposition 6.2.5(c) $[j] \neq [k]$.

Nun zeigen wir noch, dass jede Äquivalenzklasse von $\equiv_n$ tatsächlich in der obigen Liste auftaucht. Sei dazu M eine beliebige Äquivalenzklasse von $\equiv_n$. Dann gibt es ein $k \in \mathbb{Z}$ mit $M = [k]$. Wenn wir $r \coloneqq \mathrm{Rest}(k, n)$ setzen, ist $r \in \{0, 1, \ldots, n-1\}$ und $k - r$ ist durch n teilbar, das heißt es gilt $k \equiv_n r$. Somit ist $M = [k] = [r]$. □

Definition 6.2.7 (Addition auf $\mathbb{Z}/n\mathbb{Z}$)**.** Sei $n \in \mathbb{N}^*$. Wir verwenden die Notation $\mathbb{Z}/\equiv_n = : \mathbb{Z}/n\mathbb{Z}$ und wir definieren eine binäre Operation

$$+ \colon (\mathbb{Z}/n\mathbb{Z})^2 \to \mathbb{Z}/n\mathbb{Z}$$

folgendermaßen: Für alle Äquivalenzklassen $M, N \in \mathbb{Z}/n\mathbb{Z}$ wählen wir beliebige Elemente $j \in M$ und $k \in N$ aus und definieren

$$M + N \coloneqq [j + k].$$

Kurz gesagt definieren wir also $[j] + [k] \coloneqq [j + k]$ für alle $[j], [k] \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 6.2.8 (Wohldefiniertheit der Addition auf $\mathbb{Z}/n\mathbb{Z}$)**.** *Die Abbildung $+$ aus Definition 6.2.7 ist wohldefiniert – das heißt, $[j+k]$ hängt nicht davon ab, welches Element $j \in M$ und welches Element $k \in N$ wir verwenden.*

Beweis. Seien $M, N \in \mathbb{Z}/n\mathbb{Z}$ und seien $j, \tilde{j} \in M$ und $k, \tilde{k} \in N$. Dann sind $j - \tilde{j}$ und $k - \tilde{k}$ durch n teilbar. Daraus folgt, dass

$$(j + k) - (\tilde{j} + \tilde{k}) = (j - \tilde{j}) + (k - \tilde{k})$$

auch durch n teilbar ist, also ist $[j + k] = [\tilde{j} + \tilde{k}]$. □

Proposition 6.2.9 ($\mathbb{Z}/n\mathbb{Z}$ ist eine Gruppe)**.** *Sei $n \in \mathbb{N}^*$ und sei $+ \colon (\mathbb{Z}/n\mathbb{Z})^2 \to \mathbb{Z}/n\mathbb{Z}$ die Abbildung aus Definition 6.2.7. Dann ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine kommutative Gruppe.*

Beweis. (G0) Seien $M, N \in \mathbb{Z}/n\mathbb{Z}$. Wegen Definition 6.2.7 ist $M + N$ ebenfalls eine Äquivalenzklasse der Äquivalenzrelation $\equiv_n$ ist, das heißt, es gilt auch $M + N \in \mathbb{Z}/n\mathbb{Z}$.

(G1) Seien $L, M, N \in \mathbb{Z}/n\mathbb{Z}$. Wähle Elemente $\ell \in L$, $j \in M$ und $k \in N$; dann gilt $L = [\ell]$, $M = [j]$ und $N = [k]$. Somit ist

$$\begin{aligned} L + (M + N) &= [\ell] + ([j] + [k]) = [\ell] + [j + k] = [\ell + (j + k)] \\ &= [(\ell + j) + k] = [\ell + j] + [k] = ([\ell] + [j]) + [k] = (L + M) + N, \end{aligned}$$

wobei wir für die Gleichheit zwischen der ersten und der zweiten Zeile die Assoziativität der Addition auf $\mathbb{Z}$ benutzt haben.

(G2) Sei $M \in \mathbb{Z}/n\mathbb{Z}$. Wir wählen ein $j \in M$; dann gilt $M = [j]$. Somit ist

$$[0] + M = [0] + [j] = [0 + j] = [j] = M$$

and

$$M + [0] = [j] + [0] = [j + 0] = [j] = M.$$

Also ist $[0] = n\mathbb{Z}$ neutrales Elemente von $\mathbb{Z}/n\mathbb{Z}$.

(G3) Sei $M \in \mathbb{Z}/n\mathbb{Z}$. Wähle ein $j \in M$; dann gilt $M = [j]$. Wir setzen nun $N \coloneqq [-j]$. Dann gilt

$$M + N = [j] + [-j] = [j + (-j)] = [0],$$

also ist N rechtsinverse zu M.

Kommutativität: Seien $M, N \in \mathbb{Z}/n\mathbb{Z}$. Wähle $j \in M$ und $k \in N$; dann gilt $[j] = M$ und $[k] = N$. Somit ist

$$M + N = [j] + [k] = [j + k] = [k + j] = [k] + [j] = N + M,$$

womit auch die Kommutativität bewiesen ist. □

Man nennt die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ eine **Faktorgruppe** oder eine **Quotientengruppe** von $\mathbb{Z}$.

Teil (a) der folgenden Definition kennen Sie bereits auf Aufgabe 2 auf Hausaufgabenblatt 10.

Definition 6.2.10 (Gruppenhomomorphismen- und Isomorphismen)**.** Seien $(G_1, \circ_1)$ und $(G_2, \circ_2)$ Gruppen.

(a) Eine Abbildung $\varphi\colon G_1 \to G_2$ heißt **Gruppenhomomorphismus**, falls $\varphi(a \circ_1 b) = \varphi(a) \circ_2 \varphi(b)$ für alle $a, b \in G_1$ gilt.

(b) Eine Abbildung $\varphi\colon G_1 \to G_2$ heißt **Gruppenisomorphismus**, wenn φ bijektiv und ein Gruppenhomomorphismus ist.

Aus Aufgabe 2(d) auf Hausaufgabenblatt wissen Sie, dass die Umkehrabbildung eines Gruppenisomorphismus ebenfalls ein Gruppenhomomorphismus – und somit wegen ihrer Bijektivität auch ein Gruppenisomorphismus – ist. Anschaulich ist ein Gruppenisomorphismus deshalb eine Abbildung, die in beide Richtungen die Gruppenstruktur erhält. Wenn es zwischen zwei Gruppen $(G_1, \circ_1)$ und $(G_2, \circ_2)$ einen Gruppenisomorphismus gibt – man nennt sie dann **isomorph** –, heißt das also intuitiv, dass sie sich in ihren algebraischen Eigenschaften nicht unterscheiden.

Wir zeigen nun, dass soeben eingeführte Gruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph zu einer Gruppe ist, die sie bereits kennen:

Proposition 6.2.11 (Isomorphie der Gruppen $\mathbb{Z}_{\boldsymbol{n}}$ und $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$)**.** *Sei $n \in \mathbb{N}^*$ und sei $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ gegeben durch $\varphi(k) = [k] = k + n\mathbb{Z}$ für alle $k \in \mathbb{Z}_n = \{0, \ldots, n-1\}$. Dann ist φ ein Gruppenisomorphismus von $(\mathbb{Z}_n, \oplus)$ nach $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Beweis. Wir zeigen zuerst, dass φ ein Gruppenhomomorphismus ist. Seien dazu $j, k \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Dann ist $j \oplus k = \text{Rest}(j+k, n)$ und somit ist $j+k-(j \oplus k)$ durch n teilbar. Also gilt $j + k \equiv_n j \oplus k$, das heißt, die beiden ganzen Zahlen $j + k$ und $j \oplus k$ besitzen bezüglich der Äquivalenzrelation $\equiv_n$ dieselbe Äquivalenzklasse. Somit gilt

$$\varphi(j \oplus k) = [j \oplus k] = [j + k] = [j] + [k] = \varphi(j) + \varphi(k).$$

Als nächstes zeigen wir, dass φ injektiv ist: Seien $j, k \in \mathbb{Z}_n$ und $\varphi(j) = \varphi(k)$. Dann gilt $[j] = [k]$, also $j \equiv_n k$, das heißt, die Differenz $j - k$ ist durch n teilbar. Weil $j - k$ in der Menge $\{-(n-1), \ldots, -1, 0, 1, \ldots, n-1\}$ liegt, folgt daraus, dass $j - k = 0$ ist, das heißt, es gilt $j = k$.

Nun zeigen wir noch die Surjektivität von φ: Die Menge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ besitzt genau n Elemente. Laut Beispiel 6.2.6 besitzt $\mathbb{Z}/n\mathbb{Z}$ ebenfalls genau n Elemente. Deshalb impliziert die bereits bewiesene Injektivität der Funktion $\varphi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{T}$, dass die Funktion auch surjektiv ist. □

Zum Abschluss dieses Abschnitts wollen wir noch besprechen, was Äquivalenzrelationen mit Quotientenvektorräumen aus der Linearen Algebra zu tun haben.

Definition 6.2.12 (Gleichheit modulo eines Untervektorraums)**.** Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und sei $U \subseteq V$ eine Untervektorraum von V. Wir definieren eine Relation $\equiv_U$ auf V folgendermaßen: Für alle $v_1, v_2 \in V$ sei $v_1 \equiv_U v_2$ genau dann, wenn $v_1 - v_2 \in U$ gilt.

Proposition 6.2.13 (Die Äquivalenzklassen der Gleichheit modulo eines Untervektorraums)**.** *Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und sei $U \subseteq V$ eine Untervektorraum von V. Die Relation $\equiv_U$ aus Definition 6.2.12 ist eine Äquivalenzrelation auf V und für jedes $v \in V$ ist die Äquivalenzklasse von v gegeben durch*

$$[v] = \{v + u \mid \ u \in U\} =: v + U.$$

Beweis. Wir zeigen zuerst, dass $\equiv_U$ die Axiome einer Äquivalenzrelation erfüllt.

(ÄR1) Sei $v \in V$. Dann gilt $v - v = 0 \in U$, da U ein Untervektorraum von V ist. Somit ist $v \equiv_U v$.

(ÄR2) Seien $v_1, v_2 \in V$ mit $v_1 \equiv_U v_2$. Dann gilt $v_1 - v_2 \in U$. Somit ist $v_2 - v_1 = -(v_1 - v_2) = (-1) \cdot (v_1 - v_2) \in U$, da U ein Untervektorraum und $-1 \in \mathbb{K}$ ist. Also gilt auch $v_2 \equiv_U v_1$.

(ÄR3) Seien $v_1, v_2, v_3 \in V$ mit $v_1 \equiv_U v_2$ und $v_2 \equiv_U v_3$. Dann gilt $v_1 - v_2 \in U$ und $v_2 - v_3 \in U$ und somit folgt

$$v_1 - v_3 = (v_1 - v_2) + (v_2 - v_3) \in U,$$

also ist auch $v_1 \equiv_U v_3$.

Nun berechnen wir noch die Äquivalenzklassen von $\equiv_U$. Sei $v \in V$. Wir wollen $[v] = \{v + u \mid \ u \in U\}$ zeigen.

"$\subseteq$" Sei $w \in [v]$. Dann gilt $w \equiv_U v$. Deshalb ist $w - v \in U$. $u \coloneqq w - v$ definieren, ist also $u \in U$ und $v = v + u$.

"$\supseteq$" Betrachten wir nun ein Element w der rechtsstehenden Menge; es ist von der Form $w = v + u$ für ein $u \in U$. Somit ist $w - v = u \in U$, also gilt $w \equiv_V v$ und deshalb $w \in [v]$. □

Definition 6.2.14 (Quotientenvektorraum)**.** Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und sei $U \subseteq V$ eine Untervektorraum von V. Dann setzt man $V/U \coloneqq V/\equiv_U$. Man definiert Abbildungen $+\colon (V/U)^2 \to V/U$ und $\cdot : \mathbb{K} \times (V/U) \to V/U$ durch

$$[v_1] + [v_2] \coloneqq [v_1 + v_2],$$
$$\lambda[v] \coloneqq [\lambda v]$$

für alle $v_1, v_2, v \in V$ und alle $\lambda \in \mathbb{K}$.

Das Tupel $(V/U, +, \cdot)$ nennt man den **Quotientenvektorraum von V modulo U**.

Proposition 6.2.15 (Wohldefiniertheit der Verknüpfungen auf Quotientenvektorräumen)**.** *Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und sei $U \subseteq V$ eine Untervektorraum von V. Die Abbildungen $+$ und $\cdot$ aus Definition 6.2.14 sind wohldefiniert.*

Beweis. Seien $v_1, v_2, \tilde{v}_1, \tilde{v}_2 \in V$ mit $[v_1] = [\tilde{v}_1]$ und $[v_2] = [\tilde{v}_2]$. Dann gilt $v_1 - \tilde{v}_1 \in U$ und $v_2 - \tilde{v}_2 \in U$ und somit

$$(v_1 + v_2) - (\tilde{v}_1 + \tilde{v}_2) = (v_1 - \tilde{v}_1) + (v_2 - \tilde{v}_2) \in U,$$

das U ein Untervektorraum von V ist. Also ist $[v_1 + v_2] = [\tilde{v}_1 + \tilde{v}_2]$. n

Seien nun $v, \tilde{v} \in V$ und $\lambda \in \mathbb{K}$ mit $[v] = [\tilde{v}]$. Dann ist $v - \tilde{v} \in U$ und somit folgt

$$\lambda v - \lambda \tilde{v} = \lambda(v - \tilde{v}) \in U,$$

da U ein Untervektorraum von V ist. Also folgt $[\lambda v] = [\lambda \tilde{v}]$. □

Proposition 6.2.16 (Quotientvektorräume sind tatsächlich Vektorräume)**.** *Sei V ein Vektorraum über einem Körper $\mathbb{K}$ und sei $U \subseteq V$ eine Untervektorraum von V. Dann ist der Quotientenvektorraum $(V/U, +, \cdot)$ aus Definition 6.2.14 tatsächlich ein Vektorraum.*

Beweis. Man kann direkt nachrechnen, dass alle Vektorraumaxiome erfüllt sind. Wir verzichten an dieser Stelle auf die Details. □

6.3 Konstruktion der ganzen Zahlen

In diesem Abschnitt wollen wir diskutieren, wie man die ganzen Zahlen konstruieren und ihre Rechenregeln beweisen kann, wenn man schon die natürlichen Zahlen $\mathbb{N}$ mit den dazugehörigen Rechenregeln zur Verfügung hat. Im Prinzip könnte man zu jeder

Zahl $n \in \mathbb{N}^*$ einfach eine weitere Zahl $-n$ definieren, wobei man das Minus an dieser Stelle zunächst nur als ein Symbol auffasst. Dann kann man

$$\mathbb{Z} \coloneqq \mathbb{N} \cup \{-n \mid \ n \in \mathbb{N}^*\}$$

definieren und auf dieser Menge eine Addition und eine Multiplikation einführen. Das ist allerdings sehr mühsam und unübersichtlich: Allein zur Definition der Summe $j+k$ zweier ganzer Zahlen $j, k \in \mathbb{Z}$ muss man sechs Fälle unterscheiden:

- *Fall 1:* Es gilt $j, k \in \mathbb{N}$.

  In diesem Fall ist $j + k$ als die Summe zweier Zahlen aus $\mathbb{N}$ bereits definiert.

- *Fall 2:* Es gilt $j = -m$ und $k = -n$ für zwei Zahlen $m, n \in \mathbb{N}^*$.

  In diesem Fall setzt man $j + k \coloneqq -(m + n)$.

- *Fall 3a:* Es gilt $j \in \mathbb{N}$ und $k = -n$ für ein $n \in \mathbb{N}^*$ und es gilt $n \leq j$.

  In diesem Fall setzt man $j + k \coloneqq j - n$.

- *Fall 3b:* Es gilt $j \in \mathbb{N}$ und $k = -n$ für ein $n \in \mathbb{N}^*$ und es gilt $n > j$.

  In diesem Fall setzt man $j + k \coloneqq -(n - j)$.

- *Fall 4a:* Es gilt $k \in \mathbb{N}$ und $j = -m$ für ein $m \in \mathbb{N}^*$ und es gilt $m \leq k$.

  In diesem Fall setzt man $j + k \coloneqq k - m$.

- *Fall 4b:* Es gilt $k \in \mathbb{N}$ und $j = -m$ für ein $m \in \mathbb{N}^*$ und es gilt $m > k$.

  In diesem Fall setzt man $j + k \coloneqq -(m - k)$.

Sie können sich leicht vorstellen, das es eine furchtbare Aufgabe ist, mit dieser Definition beispielsweise das Assoziativgesetz der Addition nachzuprüfen.

Erfreulicherweise gibt es eine andere Möglichkeit, die ganzen Zahlen zu konstruieren, die etwas abstrakter aber dafür viel effizienter ist – man verwendet Äquivalenzrelationen! Die Grundidee ist folgendermaßen: Man will jede ganzen Zahl schreiben als die Differenz $a-b$ von zwei Zahlen $a, b \in \mathbb{N}$. Die beiden Daten a, b legen die ganze Zahl $a - b$ eindeutig fest. Also *definiert* man einfach die ganze Zahl, die man sich als $a - b$ vorstellt als das Tupel (a, b).

Problematisch ist dabei nur, dass man es verschiedene Tupel gibt, die dieselbe ganze Zahl repräsentieren – denn es gilt ja zum Beispiel $3 - 6 = 4 - 7$. Also muss man die beiden Tupel $(3, 6)$ und $(4, 7)$ als dieselbe ganze Zahl behandeln. Ebenso gilt zum Beispiel $9 - 2 = 13 - 11$, also muss man die beiden Tupel $(9, 2)$ und $(13, 11)$ als dieselbe ganze Zahl behandeln. Zwei Tupel (a, b) und $(\tilde{a}, \tilde{b})$ in $\mathbb{N}^2$ fasst man also dann also dieselbe ganze Zahl auf, wenn $a + \tilde{b} = b + \tilde{a}$ gilt. Das definieren wir jetzt formal:

Proposition und Definition 6.3.1 (Ganze Zahlen als Äquivalenzklassen in $\mathbb{N}^2$)**.** *Wir definieren auf $\mathbb{N}^2$ die Relation $\sim$ folgendermaßen: Für $a_1, a_2, b_1, b_2 \in \mathbb{N}$ setzen wir $(a_1, a_2) \sim (b_1, b_2)$ genau dann, wenn $a_1 + b_2 = b_1 + a_2$ gilt.*

Dann ist $\sim$ eine Äquivalenzrelation auf $\mathbb{N}^2$. Man setzt $\mathbb{Z} \coloneqq \mathbb{N}^2/\sim$ und nennt $\mathbb{Z}$ die ***Menge der ganzen Zahlen****.*

Beweis. (ÄR1) Sei $(a_1, a_2) \in \mathbb{N}^2$. Wegen $a_1 + a_2 = a_1 + a_2$ gilt $(a_1, a_2) \sim (a_1, a_2)$.

(ÄR2) Seien (a_1, a_2) und (b_1, b_2) in $\mathbb{N}^2$ mit $(a_1, a_2) \sim (b_1, b_2)$. Dann gilt $a_1 + b_2 = b_1 + a_2$. Somit ist auch $b_1 + a_2 = a_1 + b_2$, also $(b_1, b_2) \sim (a_1, a_2)$.

(ÄR3) Seien (a_1, a_2), (b_1, b_2) und (c_1, c_2) Elemente von $\mathbb{N}^2$ und gelte $(a_1, a_2) \sim (b_1, b_2)$ und $(b_1, b_2) \sim (c_1, c_2)$. Dann ist $a_1 + b_2 = b_1 + a_2$ und $b_1 + c_2 = c_1 + b_2$. Durch Addition dieser beiden Gleichungen erhält man

$$a_1 + b_2 + b_1 + c_2 = b_1 + a_2 + c_1 + b_2$$

und somit $a_1 + c_2 = c_1 + a_2$. Also ist $(a_1, a_2) \sim (c_1, b_2)$. □

Proposition und Definition 6.3.2 (Addition der ganzen Zahlen)**.** *Sei $\sim$ die Äquivalenzrelation auf $\mathbb{N}^2$ aus Proposition und Definition 6.3.1. Auf $\mathbb{Z} = \mathbb{N}^2/\sim$ definieren wir eine binäre Verknüpfung $+\colon \mathbb{Z} \to \mathbb{Z}$ durch*

$$[(a_1, a_2)] + [(b_1, b_2)] \coloneqq [(a_1 + b_1, a_2 + b_2)]$$

für alle (a_1, a_2) und (b_1, b_2) in $\mathbb{N}^2$. Dann ist $+$ wohldefiniert.

Beweis. Seien $(a_1, a_2), (\tilde{a}_1, \tilde{a}_2), (b_1, b_2), (\tilde{b}_1, \tilde{b}_2) \in \mathbb{N}^2$ mit $[(a_1, a_2)] = [(\tilde{a}_1, \tilde{a}_2)]$ und $[(b_1, b_2)] = [(\tilde{b}_1, \tilde{b}_2)]$. Dann gilt $a_1 + \tilde{a}_2 = \tilde{a}_1 + a_2$ und $b_1 + \tilde{b}_2 = \tilde{b}_1 + b_2$. Durch Addition dieser beiden Gleichungen folgt

$$(a_1 + b_1) + (\tilde{a}_2 + \tilde{b}_2) = (\tilde{a}_1 + \tilde{b}_1) + (a_2 + b_2).$$

Somit ist $[(a_1 + b_1, a_2 + b_2)] = [(\tilde{a}_1, \tilde{b}_1, \tilde{a}_2 + \tilde{b}_2)]$. □

Proposition 6.3.3 (Die additive Gruppe der ganzen Zahlen)**.** *Es ist $(\mathbb{Z}, +)$ eine kommutative Gruppe.*

Beweis. (G0) Für Äquivalenzklassen $[(a_1, a_2)]$ und $[(b_1, b_2)]$ aus $\mathbb{Z} = \mathbb{N}^2/\sim$ ist auch $[(a_1, a_2)] + [(b_1, b_2)] = [(a_1 + b_1, a_2 + b_2)] \in \mathbb{N}^2/\sim = \mathbb{Z}$.

(G1) Seien $[(a_1, a_2)], [(b_1, b_2)], [(c_1, c_2)] \in \mathbb{N}^2/\sim = \mathbb{Z}$. Dann gilt

$$\begin{aligned}
\Big([(a_1, a_2)] + [(b_1, b_2)]\Big) + [(c_1, c_2)] &= [(a_1 + b_1, a_2 + b_2)] + [(c_1, c_2)] \\
&= [((a_1 + b_1) + c_1, (a_2 + b_2) + c_2)] \\
&= [(a_1 + (b_1 + c_1), a_2 + (b_2 + c_2))] \\
&= [(a_1, a_2)] + [(b_1 + c_1, b_2 + c_2)] \\
&= [(a_1, a_2)] + \Big([(b_1, b_2)] + [(c_1, c_2)]\Big),
\end{aligned}$$

wobei die dritte Gleichheit aus der Assoziativität der Addition auf $\mathbb{N}$ folgt.

(G0) Für alle $[(a_1, a_2)] \in \mathbb{Z} = \mathbb{N}^2/\sim$ gilt

$$[(a_1, a_2)] + [(0, 0)] = [(a_1 + 0, a_2 + 0)] = [(a_1, a_2)]$$

und

$$[(0, 0)] + [(a_1, a_2)] = [(0 + a_1, 0 + a_2)] = [(a_1, a_2)],$$

wobei wir verwendet haben, dass 0 neutrales Elemente der Addition auf $\mathbb{N}$ ist. Somit ist $[(0, 0)]$ neutrales Elemente der Verknüpfung $+$ auf $\mathbb{Z}$.

(G3) Seien $[(a_1, a_2)] \in \mathbb{Z} = \mathbb{N}^2/\sim$. Dann gilt

$$[(a_1, a_2)] + [(a_2, a_1)] = [(a_1 + a_2, a_2 + a_1)] = [(a_1 + a_2, a_1 + a_2)] = [(0, 0)]$$

wobei die letzte Gleichheit daraus folgt, dass für jedes $a \in \mathbb{N}$ wegen $a + 0 = 0 + a$ die Tupel (a, a) und $(0, 0)$ äquivalent sind. Also ist $[(a_2, a_1)] \in \mathbb{Z}$ rechtsinvers zu $[(a_1, a_2)]$.

Kommutativität: Seien $[(a_1, a_2), [(b_1, b_2)]] \in \mathbb{Z} = \mathbb{N}^2/\sim$. Dann gilt

$$[(a_1, a_2)] + [(b_1, b_2)] = [(a_1 + b_1, a_2 + b_2)] = [(b_1 + a_2, b_2 + a_2)] = [(b_1, b_2)] + [(a_1, a_2)],$$

wobei die mittlere Gleichheit aus der Kommutativität der Addition auf $\mathbb{N}$ folgt. □

Die vorangehenden Konstruktionen zeigen, wie man die ganzen Zahlen und die Addition auf ihnen konstruieren und die zugehörigen Rechenregeln zeigen kann, wenn man die natürlichen Zahlen und ihre Addition sowie die zugehörigen Rechenregeln bereits zur Verfügung hat. Ebenso kann man auch mit der Multiplikation vorgehen, worauf wir aber an dieser Stelle verzichten.

Zuletzt merken wir noch an, dass man, sobald man $\mathbb{Z}$ mit der zugehörigen Addition und Multiplikation definiert hat, auch den Körper der rationalen Zahlen konstruieren kann, indem man eine ähnliche Vorgehensweise mit einer geeigneten Äquivalenzrelation verwendet.

Appendices

Anhang A

Griechisches Alphabet

In der Mathemathik benutzt man häufig griechische Buchstaben als Variablennamen. Falls Sie einmal einen griechischen Buchstaben lesen oder hören, den Sie nicht kennen, können Sie ihn zum Beispiel in folgender Tabelle nachlesen.

Kleinbuchstabe	Großbuchstabe	Name
α	A	Alpha
β	B	Beta
γ	Γ	Gamma
δ	Δ	Delta
ε	E	Epsilon
ζ	Z	Zeta
η	H	Eta
θ / ϑ	Θ	Theta
ι	I	Iota
κ	K	Kappa
λ	Λ	Lambda
μ	M	My
ν	N	Ny
ξ	Ξ	Xi
o	O	Omikron
Π	π	Pi
ρ / ϱ	P	Rho
σ	Σ	Sigma
τ	T	Tau
υ	Υ	Ypsilon
φ / ϕ	Φ	Phi
χ	X	Chi
ψ	Ψ	Psi
ω	Ω	Omega

Literaturverzeichnis

[For15] Otto Forster. *Algorithmische Zahlentheorie*. Heidelberg: Springer Spektrum, 2nd revised and extended ed. edition, 2015.