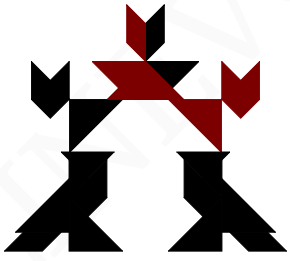
LEHRBUCH

Mathematik für die Informatik I

Lineare Algebra und Diskrete Mathematik

Samuel Hetterich



Analogverlag

Bibliographische Informationen Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detailliertere bibliographische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN 978-3-947940-00-4

1. Auflage

Analogverlag Samuel Hetterich, Idsteiner Straße 149, D-60326 Frankfurt

Umschlaggestaltung: Analogverlag Samuel Hetterich, Idsteiner Straße 149, D-60326 Frankfurt

Druck: buchdruckerei24.de, Morgenbergstraße 41, D-08525 Plauen

Printed in Germany

Vorwort

Das Studium der Grundlagen der Mathematik stellt viele Studierende der Informatik vor große Herausforderungen. Mit diesem Buch möchte ich all jenen ein Hilfsmittel an die Hand geben, diese erste Klippe des Informatikstudiums zu umschiffen. Ich lese im dritten Jahr epochal die Grundlagenvorlesungen „Mathematik für die Informatik I“ und „Mathematik für die Informatik II“ über die Themenfelder der lineare Algebra, Analysis, diskreten Mathematik und Numerik an der Goethe-Universität Frankfurt am Main. Das vorliegende Lehrbuch entstand in der Dynamik eines kritischen Prozesses zwischen der von mir gehaltenen Vorlesung und dem Austausch mit meinen Studierenden der vergangenen Jahre. Viele Beispiele und Abbildungen entwickelte ich, um gezielt meine Vorlesung anschaulicher und lebendiger zu gestalten. In seiner jetzigen Form vermag es sicherlich auch Studierenden anderer Universitäten eine Hilfe in den ersten Semestern ihres Studiums sein. Auch deshalb bin ich dankbar für jede Anmerkung, jeden Verbesserungsvorschlag und ehrliche Kritik der Vergangenheit aber auch der Zukunft. Die Skripte zu der gleichnamigen Vorlesung vorangegangener Semester gehalten von Herrn Dr. Hartwig Bosse und Professor Dr. Amin Coja-Oghlan dienten mir als Quelle der Inspiration, Abschnitte durfte ich übernehmen - dafür danke ich herzlich.

Ein Wort zum Inhalt des Lehrbuchs

Bei der Auswahl der Themen haben mich zwei Grundsätze geleitet.

- **Methodisch** sollen Leser befähigt werden, mathematische Inhalte lesen und formulieren zu können. Dabei sollen Sie ein solides Fundament und ein grundlegendes Verständnis der formalen und abstrakten mathematischen Herangehensweise entwickeln.
- **Inhaltlich** sollen Leser über grundlegende Themen der linearen Algebra und diskreten Mathematik informiert werden. Es ist sicherlich

nicht möglich, alle diejenigen Themenfelder der linearen Algebra und der diskreten Mathematik in vollem Umfang zu behandeln, die Studierende der Informatik im Laufe ihrer weiteren Studien konfrontieren werden. Deshalb muss eine Auswahl geschehen, die ich sorgfältig und im Gespräch mit meinen Kollegen aus der Informatik getätigt habe. Dabei habe ich den Fokus bewusst auf die saubere Vermittlung der Grundlagen gelegt. Anwendungen können dann leicht erschlossen werden. Insbesondere habe ich davon abgesehen, übermäßig viele, aus der Informatik motivierte, zum Teil sehr sperrige Anwendungen zu skizzieren. Andere Bücher tun dies um sich den Anstrich der für Studierende der Informatik leicht zu verdauenden und dadurch auch leichter zu vermittelnden Mathematik zu geben. Ich bin davon überzeugt, dass viele dieser zum Teil sehr komplexen Objekte gerade Studierende zu Beginn ihres Studiums überfordern und dadurch nicht zu einer wachsenden Motivation beitragen. Sie sind meist nicht die optimalen ersten Beispiel für die behandelten Themen, verwischen wesentliche Merkmale und machen die Relevanz der Objekte nur ungenügend deutlich. Hat man das vorliegende Lehrbuch mit viel Einsatz und Ausdauer durchgearbeitet, sollte es einem ohnehin leicht fallen, komplexere mathematische Fragestellungen, wie sie in der Informatik auftauchen, zu studieren.

Schlussendlich mündete dieser Ansatz in ein Lehrbuch mit vier Teilen und insgesamt 13 Kapiteln.

Dabei möchte der erste Teil Grundlagen vermitteln. Grundlegende Begriffe und Objekte, wie Zahlen, Mengen und Abbildungen aber auch einführende Worte zur formalen Sprache und Beweisprinzipien finden hier ihren Platz. Ein Kapitel über Graphen schließt sich an. Graphen spielen in der Informatik als Werkzeug der Modellierung eine wichtige Rolle.

In einem zweiten Teil wird die Theorie des Rechnens entfaltet. Rechnen ist sicherlich eine grundlegende Kompetenz für jeden, der mit „Rechnern“ zu tun hat. In einem ersten Kapitel werden zunächst die Konzepte von Teilbarkeit, Faktorisierung und dem Rechnen mit Resten entfaltet und der euklidische Algorithmus eingeführt. Dieses algorithmische Verfahren ist ein starkes Werkzeug und ein Grundbaustein in vielen praktischen Anwendungen der Informatik. Neben dem chinesischen Restsatz wird außerdem die eulersche φ-Funktion studiert. Das Kapitel hat überdies vorbereitendem Charakter für das zweite Kapitel dieses Teils. Dort wird die mathematische Abstraktion des Rechnens betrachtet. Rechnen wird abstrahiert und algebraische Strukturen mit ihren Verknüpfungen treten

an die Stelle von Zahlen und bekannten Rechenoperationen. Gruppen, Ringe, Körper und Vektorräume sind solche Strukturen, studiert werden sie über strukturerhaltende Abbildungen. Auf Vektorräumen werden diese als lineare Abbildungen bezeichnet. Anwendung finden viele Konzepte dieses Teils vor allem im vierten Teil des Buchs.

Im dritten Teil des Buchs werden Vektorräume studiert. Sie werden beschreiben und klassifiziert, indem ihnen Basis und Dimension zugeordnet werden. Bei diesem Unterfangen helfen lineare Abbildungen, welche sich als Matrizen darstellen lassen. Dabei erschließt sich der Name „lineare Algebra“ - das Rechnen mit linearen Abbildungen. Im Kontext des Studiums von Matrizen und linearen Abbildungen tauchen Konzepte wie Kerne, Orthogonalität, Normen, Metriken, Eigenwerte und Eigenräume, Diagonalisierbarkeit und die Determinante auf. Lineare Gleichungssysteme sind allgegenwärtig in diesem Unterfangen, welche mithilfe des Gaußschen Eliminationsverfahren gelöst werden.

Im vierten Teil werden zwei Aspekte der Kommunikation von Daten studiert. Dabei sind die Kryptographie und die Kodierungstheorie nicht zu verwechseln. In der Kryptographie geht es um die sichere Kommunikation von Geheimnissen. In der Kodierungstheorie geht es um die fehlererkennende und fehlerkorrigierende Kommunikation und Speicherung von Daten. In der Kryptographie beschränken wir uns auf das RSA-Schema und die RSA-Signatur. Das erste realisiert sichere Kommunikation ohne vorherigen Schlüsselaustausch, das zweite eine fälschungssichere digitale Unterschrift zur eindeutigen Authentifizierung. In der Kodierungstheorie werden vor allem lineare Codes im Fokus des Interesses stehen.

Ein Wort zum Studium mit dem Lehrbuch

Dieses Lehrbuch möchte genau das sein: Ein Lehrer für jeden grundlegend am Thema interessierten Leser. Es hat zum Ziel, die abstrakten mathematischen Theorien nicht bloß sauber (und deshalb nur für Experten), sondern vor allem für Jedermann lesbar darzustellen. Es will das Wissen an den Mann bringen, möchte lehren. Damit dies gelingt, sind einige Hinweis notwendig.

„Eine Sprache erlernt man, indem man sie spricht“ und „Wiederholung ist die Mutter allen Lernens“, dies beiden zweifellos wahren Aussagen gelten auch für das Erlernen mathematischer Inhalte. Nur wer sich mit den abstrakten Definitionen und Aussagen auseinandersetzt und sie dadurch „verdaut“, Zeit investiert und übt, wird sie wirklich erfassen. Diesen Aufwand können Ihnen weder noch so gute (und praxisorientierte) Bü-

cher, keine noch so „freshen“ Erklärvideos und online Tutorials aber auch keine Vorlesung abnehmen - diesen Aufwand werden Sie selbst betreiben müssen.

Doch es gibt Bedingungen, die diesen Prozess begünstigen - bei der Konzeption dieses Lehrbuchs habe ich dies berücksichtigt. Wenn Sie sich die folgenden Aspekte durchlesen, sollte Ihnen auch klar werden, warum ich immer noch an das „analoge Lehrbuch“ glaube, dass man anfassen, beschreiben, blättern und zerlesen kann.

- **Schlüssige, klare Darstellung „aus einem Guss“.** Möchte man neue mathematische Inhalte erfassen, dann stellt die Abstraktion vor große Herausforderung. Es gibt nichts dem Lernerfolg gleich hinderliches, wie sekundäre Aspekte, die den klaren Blick auf das Wesentlich verwehren. Solche Aspekte können die ungenau und wechselnde Notation (Benennung) der auftretenden mathematischen Objekte, die unterschiedlichen ersten Sicht- und Herangehensweisen oder ungenügende oder falsche Motivation der Inhalte sowie schlecht gewählte Beispiele sein.
  Das vorliegende Buch ist „aus einem Guss geschrieben“. Die gleiche Symbolik der Mengenlehre beispielsweise, wie sie in dem Grundlagenkapitel eingeführt wird, findet sich auch noch auf der letzten Seite des Buchs. Verwirrung durch variierender Notation sollte so vermieden sein.
  Das Lehrbuch setzt an keiner Stelle etwas voraus, das der Leser sich nicht aus der Darstellung erschließen könnte. Auch deshalb werden in den unterschiedlichen Kapiteln hin und wieder zunächst unwichtig erscheinende Aspekte studiert, die in einem späteren Kapitel dann jedoch nützlich sind. In dem Lehrbuch wird verlässlich alle das erklärt, was zum Verständnis notwendig ist. Damit sollte das Lesen dieses Lehrbuchs eine Wohltat im Vergleich zur Recherche im Internet sein. Viele Online-Inhalte, welche vorgeben, ein mathematisches Thema verständlich zu behandeln, entpuppen sich bei näherem Hinsehen vor allem für Lernende als verwirrend und nur schwer eingängig.
  Einen zweiten interessanten Blickpunkt liefert die Lerntheorie. Lernen heißt Verknüpfen. Dazu muss Wissen aufbereitet, sortiert und an existierendes Wissen angedockt werden. In einer Zeit ständiger Verfügbarkeit allen Wissens (man kann schnell googeln oder auf Wikipedia nachlesen) sind wir es nicht mehr gewohnt (oder vielleicht schon nicht mehr in der Lage), Wissen dauerhaft für uns selbst zu

erschließen. Das ist fatal. Das Lehrbuch möchte Ihnen helfen, die behandelten Inhalte wirklich zu lernen. Dabei fördert es durch seine aufeinander aufbauende Struktur das Verknüpfen von Wissen.
In diesem Lehrbuch wird das mathematische Wissen aus der Schule vorausgesetzt. Sollten Sie dabei eigene Defizite feststellen, empfehle ich einen Online-Mathematik-Brückenkurs, der den Übergang von der Schule an die Universität unterstützten möchte. Abiturrelevantes mathematisches Grundlagenwissen kann dort wiederholt und aufgefrischt werden. Sie finden Ihn unter `www.ombplus.de`.

- **Intuitive Beispiele.** Um abstrakte Definitionen oder Objekte aber auch mathematische Aussagen zu erfassen, helfen intuitive Beispiele. In dem vorliegenden Lehrbuch findet sich eine Vielzahl ausführlich kommentierter Beispiele. Dabei wird besonders auf eine ausführliche Darstellung der Rechenwege Wert gelegt. Das hilft den Durchblick zu erlangen und Abstraktes mit Leben gefüllt besser zu erinnern.
- **Unterstützende Illustrationen.** Was in Worten umständlich beschrieben wird, kann oft leichter in einer Grafik erfasst werden. Deshalb verfügt das Lehrbuch über zahlreiche als Illustration und Beweisskizze unterstützende Abbildungen.
- **Hilfreiche Bemerkungen.** Das Lehrbuch ist durchsetzt mit einer großen Zahl von Bemerkungen. Sie ergänzen den Lesefluss und helfen Neues zu erfassen, es abzugrenzen und einzuordnen. Wieder gilt der Grundsatz: „Lernen heißt Verknüpfen“. In Bemerkungen möchte der Autor mit den Lesenden und dem schon gelernten Wissen in den Dialog treten.
- **Übungsaufgaben.** Wer nicht selbst Hand anlegt, wird schnell wieder vergessen. An jedes Kapitel schließt sich eine Sammlung von Übungsaufgaben an. Dabei finden sich Übungsaufgaben in unterschiedlicher Farbkodierung. Grüne Aufgaben sind sehr einfache Aufgaben, blaue Aufgaben sind generelle Aufgaben von unterschiedlichem (aber nicht sehr leichtem) Schwierigkeitsgrad. Orange Aufgaben sind Programmieraufgaben in Sage - siehe unten. Rote Aufgaben sind Beweisaufgabe, die in der Regel von höherem Schwierigkeitsgrad sind. Dabei stehen Ihnen insgesamt über 400 Übungsaufgaben zur Verfügung.
- **Kontrolle und Rekapitulation.** Um Ihren eigenen Lernfortschritt zu kontrollieren, sind die Übungsaufgaben um eine gelbe Kategorie ergänzt. Dabei handelt es sich um eine Sammlung von „einfachen“ Verständnisfragen, die mit Ja oder Nein zu beantworten sind. Kontrollieren Sie mit diesen Aufgaben Ihr Verständnis und Ihren

Lernfortschritt nach der Lektüre eines jeden Kapitels.

- **Platz für Entfaltung.** Das Lehrbuch bietet einen breiten Schreibrand. Dieser breite Streifen an der Buchaußenseite fasst nicht nur gedruckte Anmerkungen und Abbildungen, sondern bietet Raum für Ihre Notizen. Markieren und kommentieren Sie die Inhalte, notieren Sie Ihre Fragen oder gefundene Antworten, ergänzen Sie Zwischenschritte und halten Sie Eselsbrücken fest. Der Raum gehört Ihnen, nutzen Sie ihn.
- **Ein gutes Gefühl.** Mit Emotionen verknüpftes Wissen bleibt. Der berühmte erste Kuss, der Ort an dem Sie das Fußball-WM-Finale 2014 gesehen haben, aber auch Ihre erste 5 in der Schule. Das Lehrbuch ist bewusst wertig produziert, also in Farbe gedruckt mit einem Hartcover versehen. Sie sollen gerne Zeit mit ihm verbringen. Das Lehrbuch darf Ihnen ein treuer Begleiter sein. Bücher sind Freunde. Sie werden viel zusammen durchmachen, das schweißt zusammen. Mein Lehrbuch der linearen Algebra aus dem ersten Semester findet immer noch seinen Ehrenplatz in meinem Bücherregal. Die von Notizen übersäten Seiten sehe ich immer noch vor mir, wenn ich meine Augen schließe und mich erinnere. Diese Erfahrung wünsche ich mit Ihrem persönlichen Exemplar des Lehrbuchs auch Ihnen .
- **Sage.** Was wäre ein Lehrbuch der Mathematik für Informatiker ohne den Einsatz von hilfreicher Software. Verteilt über das Buch helfen Ihnen kleine „Sage-Boxen„ und „Sage-Aufgaben“ die mathematische Software Sage zu erlernen. Mit ihr können Sie sich den Inhalten programmierend nähern. Das hilft sicherlich beim Verständnis und dem besseren Erinnern dieser.
- **Übersichtlichkeit.** Das Buch ist in Farbe gedruckt. Das soll die Übersichtlichkeit verbessern. Definitionen sind gelb, Beispiel grün, Bemerkungen blau, mathematische Aussagen rot und alles, was mit Sage zu tun hat orange markiert. Die Beispiele und Bemerkungen, die den Lesefluss ergänzen sollen, sind etwas kleiner gedruckt. Beweise, wie zusammenhängende den Lesefluss ergänzende Teil,e werden jeweils durch eine Überschrift und eine kleine Box, einen kleinen Fuchs oder eine feine Linie in entsprechender Farbe eingefasst.

Zwei gut gemeinte Ratschläge sollen diese „Gebrauchsanweisung“ abrunden: Bleiben Sie am Ball und lassen Sie sich nicht frustrieren. Das Studium der Mathematik bedarf Ausdauer und Frustrationstoleranz. Geben Sie sich die Zeit, die Sie brauchen - beißen Sie sich rein. Es ist sicherlich naiv zu glaube, Sie könnten das Buch an einem Wochenende verschlingen.

Das Erlernen der Mathematik braucht „Verdauungszeit“. Vertrauen Sie mir jedoch, dass Sie in drei Jahren, wenn sie die Inhalte verdaut und Komplexeres in Ihrem Studium erlernt haben werden, das Lehrbuch ungläubig aufschlagen. Ungläubig, weil Ihnen die Inhalte lange nicht mehr so schwer und abstrakt erscheinen, wie sie das in den nächsten Wochen und Monaten tun werden.

Ein Wort zu Sage

Das Lehrbuch ist gewürzt mit Anmerkungen, die Ihnen die mathematische Software SageMath, oder kurz Sage, näher bringen möchten. Sage ist ein freies Open Source Mathematiksystem. Es ist eine auf Python basierende Oberfläche und stellt Ihnen ein starkes Werkzeug zur computergestützten Analyse von mathematischen Objekten zur Verfügung. Ich gehe davon aus, dass Sie, als Informatik affiner Leser, in der Lage sein sollten, Sage auf Ihrem Rechner verfügbar und sich mit der grundlegend Syntax vertraut zu machen. Sie finden die Software unter `www.sagemath.org/de/`. Erste Schritte in einem online Tutorial können Sie unter `doc.sagemath.org/html/de/tutorial/` gehen.

Grundsätzlich gibt es über die behandelte Materie verteilt computerorientierte Aspekte. Dann sind Sie herzlich eingeladen die Software Sage zu nutzen, um „spielerisch“ programmierend den Stoff zu erfassen. Unter den Übungsaufgaben finden Sie einige Anstöße und Anregungen dazu. Verteilt im Buch sind manche und zum Teil recht ausführliche Programme in Sage eingestreut. Sicherlich könnte dies noch ausführlicher geschehen, denn bei vielen der behandelten Inhalte ist das Rechnen mit der Hand mühsam. Ist beispielsweise in der linearen Algebra der fünfzehnte Kern einer Matrix zu berechnen, greift man sicherlich gerne auf Sage zurück. Tun Sie das bitte, doch gehen Sie dabei sicher, dass Sie verstanden haben, wie jeweils per Hand gerechnet werden müsste, stünde kein Computer zur Verfügung.

Letzte erste Worte

Bei Anregungen, Kritik, Verbesserungsvorschlägen oder falls Sie Fehler finden, melden Sie sich gerne per Mail unter hetterich@math.uni-frankfurt.de. Dann ist nun alles gesagt und es kann losgehen. Ich wünsche Ihnen viel Erfolg bei Ihren Studien.

Frankfurt, im Sommer 2018

Samuel Hetterich

0 Inhaltsverzeichnis

I Grundlagen

1 Grundbegriffe

Das Wort Mathematik stammt aus dem Griechischen *mathēmatikē téchnē*, was sich als „die Kunst des Lernens“ übersetzen lässt. Mittels Beobachtung von Zahlen und geometrischen Mustern werden Regelmäßigkeiten erkannt (erlernt) und in einer formalen und abstrakten Sprache beschrieben. Diese abstrakten Strukturen werden dann durch logische Denkschritte untersucht und weiter entfaltet. Man kann die Mathematik also auch als durch reale Muster inspirierte philosophische (gedankliche) Übung verstehen. Ob diese abstrakten Gebilde noch etwas mit einer realen Anwendung zu tun haben, ist (für einen echten Mathematiker) dann erst mal sekundär. Dennoch lassen sich (für einen Informatiker) glücklicherweise viele reale Fragestellungen in einer mathematisch abstrakten Formulierung fassen. Eine Lösung des formalen Problems in der abstrakten Welt der Mathematik verhilft dann zu einer ganz praktischen Lösung in der realen Welt der ursprünglichen Fragestellung.

Die Mathematik als solch ein starkes Werkzeug begreifen und hoffentlich auch verwenden zu können, setzt eine intensive Auseinandersetzung mit ihr voraus. Insbesondere sind grundlegende Konzepte zu begreifen. In diesem Kapitel möchten wir quasi die DNA der Mathematik untersuchen. Dazu gehören Zahlen, die mathematische Logik, der Mengenbegriff, Abbildungen und Relationen. Bevor wir dies tun, wollen wir noch kurz etwas genauer erörtern, wie das Gebilde der Mathematik entfaltet wird.

Die Mathematik - ein auf Axiomen gegründetes logisches Bauwerk

Möchte man mit dem Bundesminister für Finanzen über den Bundeshaushaltsplan diskutieren, sollte man sich zur Vorbereitung des Gesprächs zumindest mit Budgetprinzipien, Konjunkturparametern und dem Bundesfinanzplan auseinandergesetzt haben. Bevor man über komplexere Fragestellungen nachdenkt und diskutiert, sollte man sich also zunächst mit dem Grundlagenwissen vertraut machen. T tiefer liegende Komplexe bauen auf Grundlagen auf. Diese Binsenweisheit, dass Wissen aufeinander aufbaut und es tiefer liegendes Wissen und Grundlagenwissen gibt, ist ein treffendes Bild für die Mathematik.

Jeder weiß, was eine gerade natürliche Zahl ist. Es ist eine natürliche Zahl, welche durch 2 teilbar ist. Aber was ist überhaupt eine „natürliche Zahl“ und wie ist „Teilbarkeit durch 2“ definiert? Offensichtlich liegen der Definition einer geraden natürlichen Zahl weitere Definitionen zugrunde.

Weiter kann man fragen, ob die 10 eine gerade natürliche Zahl ist? Ja, wenn Teilbarkeit einer Zahl m durch 2 definiert ist, als die Existenz einer Zahl k, so dass $2 \cdot k = m$ ist. In dem Beispiel wäre dann $k = 5$ und es gilt $2 \cdot 5 = 10$. Eine Definition beschreibt oder benennt also ein Objekt, welches bestimmte Eigenschaften besitzt. Diese Eigenschaften wiederum sind Aussagen, welche den Wert „wahr“ oder „falsch“ annehmen können.

Aber wie tief muss man graben? Lässt sich jede Eigenschaft einer Definition auf eine andere Definition zurückführen? Die Antwort lautet Nein! Es gibt Definitionen, welche (manche geforderten) Eigenschaften ganz grundlegend festsetzen. Die Definition der natürlichen Zahlen ist ein Beispiel für eine solche grundlegende Definition. Die Eigenschaften, welche die natürlichen Zahlen beschreiben, werden einfach als wahr angenommen. Eine Menge, welche diese Eigenschaften besitzt, ist per Definition die Menge der natürlichen Zahlen.

Die grundlegenden Aussagen, welche sich nicht mehr auf andere Definitionen beziehen, werden **Axiome** genannt. Axiome sind sozusagen das Fundament der Mathematik. Höher liegende Aussagen sind durch logische Schlüsse aus den Axiomen als „wahr“ abgeleitet worden. Die geschickte und richtige Wahl der Axiome ist also dafür ausschlaggebend, wie sich das Gebäude der Mathematik darstellt, welche Aussagen „wahr“ oder „falsch“ sind. Die Mathematik ist somit ein abstraktes Modell unseres Denkens, welches mit den passenden Axiomen und den Gesetzen der Logik eine Sammlung von Aussagen als wahr benennt. Zum Beispiel, dass in einem rechtwinkligen Dreieck die Quadrate der kurzen Seiten dem Quadrat der langen Seite entsprechen - der Satz des Pythagoras. Hilft diese Einsicht in der abstrakten Welt der Mathematik auch in der Praxis, beim Bau eines Hauses beispielsweise, dann stellt sich die Wahl der Axiome, aus denen sich diese Aussage als wahr ableiten lässt, als durchaus sinnvoll heraus.

In der Praxis begegnen einem Axiome eher selten. Vielmehr kennt man eine Reihe von höher liegenden Definitionen und mathematischen Aussagen. Der Satz des Pythagoras ist eine solche Aussage. Wir möchten nicht viel tiefer in diese philosophische Grundlage der Mathematik eintauchen, uns aber bewusst halten: Jede mathematische Aussage, die wir als „wahr“ benennen, müssen wir logisch auf eine Aussage zurückführen, von der wir wissen, dass sie als „wahr“ aus den Axiomen abgeleitet wurde. Dieser

Vorgang des logischen Ableitens wird als *Beweis* bezeichnet. Eine ganze Reihe von Aussagen, werden wir nennen und darauf vertrauen, dass die Mathematiker ihre Arbeit gut und zuverlässig getan und sie auf die Axiome zurückgeführt haben (das wird vor allem bei der *Schulmathematik* der Fall sein). Wir werden diese Aussagen also nicht beweisen, sondern als Grundlage eigener Beweise nutzen.

Warum macht man sich diese „Beweisarbeit“? Es gibt zwei Gründe: Verlässlichkeit und Verständnis.

- Eine Aussage, die als wahr bewiesen wurde, gilt. Sie kann angewendet werden. Lässt sich ein Problem mathematisch modellieren, dann gelten für das mathematische Modell sofort jegliche als wahr bewiesene Aussagen. Das kann zum Beispiel die Laufzeit eines durch einen Graphen modellierten Suchalgorithmus betreffen. Möglicherweise kann mittels einer Formel, die bewiesenermaßen auf allen Graphen gilt, diese berechnet werden. Dazu muss diese Formel dann nicht für jeden Graphen neu überprüft werden, der Beweis hat ein für alle Mal die Verlässlichkeit der Formel belegt.
- Beweise schärfen aber auch den Blick auf mathematische Zusammenhänge und steigern damit das tatsächliche Verständnis der Aussage. Kennt man zum Beispiel einen geometrischen Beweis des Satzes von Pythagoras, wie in Abbildung 1.1 skizziert, dann erscheint einem die Aussage weniger mystisch oder beliebig zu sein.

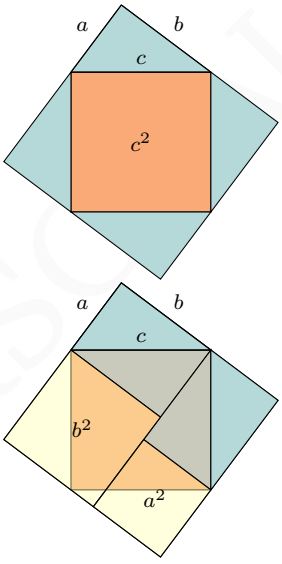


Abb. 1.1.

Geometrischer Beweis des Satzes von Pythagoras.

Die Informatik ist historisch betrachtet aus der Mathematik hervorgegangen. Durch die Entwicklung von Computern wurde es in der Mitte des vergangenen Jahrhunderts möglich, durch automatisierte Rechenverfahren anspruchsvolle Berechnungen durchzuführen. Bis heute müssen Probleme zunächst in eine mathematische, formale Sprache übersetzt und dann für den Computer implementiert werden. Es ist deshalb unabdingbar für einen Informatiker die grundlegende Mathematik, formale Sprachen und logisches Schließen zu studieren.

Wir haben jetzt schon von mathematischen Aussagen und Beweisen aber auch von Zahlen, Mengen, Abbildungen und Relationen gesprochen. Wir werden uns nun diese Begriffe näher anschauen. Dabei werden wir in den einzelnen Abschnitten immer wieder vorgreifen oder besser auf Schulwissen zurückgreifen (werden also zum Beispiel im Abschnitt über mathematische Aussagen von Mengen und den natürlichen Zahlen reden). Das hätten wir durch einen formal sauberen und stringenten Ansatz auch umgehen können. Wir sind allerdings davon überzeugt, dass das vielleicht

noch nicht formale, aber anschauliche Verständnis dieser Objekte ungemein hilft, nach und nach die formal sauberen, sicherlich zum Teil recht abstrakten, Definitionen jeweils mittels Beispielen mit Leben füllen zu können.

1.1 Mathematische Aussagen

Unter einer mathematischen Aussage versteht man eine mathematische Formel oder eine formal-logische Aussage, der ein Wahrheitswert „wahr“ oder „falsch“ zugewiesen werden kann. Dabei gelten zwei Regeln.

- Eine mathematische Aussage ist entweder „wahr“ oder „falsch“ (es gibt keine dritte Möglichkeit).
- Eine mathematische Aussage kann nicht gleichzeitig „wahr“ und „falsch“ sein.

Anmerkung. Diese zwei grundlegenden Regeln werden auch als das Prinzip des ausgeschlossenen Dritten und das Prinzip der Widerspruchsfreiheit genannt.

BEISPIEL 1.1. Wir betrachten für verschiedene Ausdrücke, ob sie unsere Definition einer mathematischen Aussage entsprechen.

- Der Ausdruck „$x^3 - 7x + 1$“ ist *keine* mathematische Aussage, sondern nur ein mathematischer Term.
- Der Ausdruck „$x^2 - 2x + 1 = 0$“ ist eine mathematische Aussage (die je nach Wert von x wahr oder falsch ist).
- Der Ausdruck „$1 = 0$“ ist eine mathematische Aussage, die falsch ist.
- Der Ausdruck „4 ist eine Quadratzahl“ ist eine mathematische Aussage, die richtig ist.
- Die Goldbach-Vermutung „Jede gerade natürliche Zahl größer als 2 kann als Summe zweier Primzahlen geschrieben werden.“ ist eine mathematische Aussage, von der bisher nicht klar ist, ob sie wahr oder falsch ist.

■

1.1.1 Bausteine mathematischer Aussagen

```
# Variablen definieren
sage: n=var('n')
```

Wir möchten nicht zu tief in die Aussagenlogik (welche in der Prädikatenlogik fortgeführt wird) einsteigen und sehen von einer vollständig formalen Einführung der verwendeten Begrifflichkeiten ab. Im Folgenden ein kleiner Überblick der „Bausteine“, welche in mathematischen Aussa-

gen verwendet werden. Im Anschluss werden wir logische Operatoren etwas ausführlicher betrachten.

- Ein **mathematisches Objekt** ist eines der in den unterschiedlichsten Teilgebieten der Mathematik eingeführten und studierten abstrakten Objekte. Das können Zahlen, Mengen, Vektoren oder geometrische Körper, aber auch Abbildungen, Graphen, Terme und vieles mehr sein.
- Eine **Variable** ist ein Platzhalter für mathematische Objekte in einer mathematischen Aussage und wird manchmal auch als *Veränderliche* bezeichnet. Als Variable dienen beliebige Zeichen. An jeder Stelle in einer mathematischen Aussage, an der dieselbe Variable auftaucht, muss bei einer **Belegung** der Variable dasselbe mathematische Objekt auftauchen. Eine Variable kann mit einem **Definitionsbereich** (eine Menge zulässiger Objekte) ausgestattet sein, muss dies jedoch nicht. Ist kein Definitionsbereich angegeben, darf eine Variable in der mathematischen Aussage mit jedem mathematischen Objekt belegt werden. Abhängig von der konkreten Belegung kann die Aussage dann wahr oder falsch sein.
- Ein **Operator** ist eine mathematische Vorschrift, zur Erzeugung von mathematischen Objekten aus mathematischen Objekten (Summenzeichen, Rechenvorschriften, Integral, Elementzeichen, Gleichheitszeichen).
- Ein **logischer Operator** ist eine Vorschrift zur Erzeugung von mathematischen Aussagen aus mathematischen Aussagen oder mathematischen Objekten (vergleichen oder verknüpfen). In der folgenden Tabelle sind die von uns verwendeten logischen Operatoren aufgelistet.

Negation	$\neg$	„ Es gilt nicht . . . “	$(\neg[n \geq 2])$
ODER	$\vee$	„ Es gilt . . . oder . . . “	$([n \geq 2] \vee [n \leq 2])$
Exklusives ODER	$\dot{\vee}$	„ Es gilt entweder . . . oder . . . “	$([n \geq 2] \dot{\vee} [n \leq 2])$
UND	$\wedge$	„ Es gilt . . . und . . . “	$([n \geq 2] \wedge [n \leq 2])$

- Ein **Quantor** spezifiziert, ob eine Aussage für (mindestens) ein, für genau ein, für alle oder für kein mathematisches Objekt gilt.

Allquantor	$\forall$	„ Für alle . . . “	$(\forall n \in \mathbb{N} : n \geq 0)$
Existenzquantor	$\exists$	„ Es existiert (min.) ein . . . “	$(\exists n \in \mathbb{N} : n \geq 5)$
	$\exists!$	„ Es existiert **genau** ein . . . “	$(\exists! n \in \mathbb{N} : n^2 = 9)$
	$\nexists$	„ Es existiert **kein** . . . “	$(\nexists n \in \mathbb{N} : n < 0)$

- Es werden **Klammern** in mathematischen Aussagen gesetzt, um

deutlich zu machen, auf welche Teile der Aussage sich beispielsweise ein logischer Quantor bezieht. Sie tragen so zur besseren Lesbarkeit bei. Wir schreiben mathematische Aussagen nun stets mit eckigen Klammern und nicht wie bislang in Anführungszeichen.

- Ein **technisches Zeichen** ist ein Symbol, welches die Lesbarkeit einer formal notierten mathematischen Aussage verbessern soll. Dabei verwendet man Kommata und häufig einen Doppelpunkt. Das Komma trennt Aussagebausteine, der Doppelpunkt lässt sich als „... mit (der Eigenschaft)...“, „... ist ...“ oder „... so, dass...“ übersetzen.

```
sage: # Negation und ODER
sage: n = var('n')
sage: (n>=2).negation()
n < 2
sage: a,b = 4,5
sage: a==b|b==4
False
```

Wir nennen zunächst einige Beispiele, komplexere Beispiele tauchen später in diesem Abschnitt und verteilt über das ganze Buch auf.

BEISPIEL 1.2. Im Folgenden einige mathematische Aussagen, welche die soeben vorgestellten Bausteine verwenden.

- $n \cdot n = 36$
  $\leftrightarrow$ „n mal n ist gleich 36“
  $\rightsquigarrow$ Die Aussage ist wahr oder falsch je nach Belegung der Variablen n.
- $\exists n \in \mathbb{N} : n \cdot n = 36$
  $\leftrightarrow$ „es existiert eine natürliche Zahl n mit n mal n ist gleich 40“
  $\rightsquigarrow$ Die Aussage ist wahr ($n = 6$).
- $\forall n \in \mathbb{N} : n \cdot n = 36$
  $\leftrightarrow$ „für alle natürlichen Zahlen ist n mal n gleich 36“
  $\rightsquigarrow$ Die Aussage ist falsch.

1.1.2 Ein Wort zu logischen Operatoren

Man kann Aussagen mithilfe von logischen Operatoren verändern oder miteinander verknüpfen. Wir beschreiben die drei wichtigsten logischen Operatoren etwas genauer.

- **Negation.** Die Negation oder auch Verneinung einer Aussage $\mathcal{A}$ ist die Aussage $\neg\mathcal{A}$, welche genau dann wahr ist, wenn $\mathcal{A}$ falsch ist und genau dann falsch ist, wenn $\mathcal{A}$ wahr ist. Wendet man diese Definition auf $\neg\mathcal{A}$ an, stellt man fest, dass $\mathcal{A}$ die Negation der Aussage $\neg\mathcal{A}$ ist.
- **Konjunktion.** Die Konjunktion oder UND-Verknüpfung zweier Aussagen $\mathcal{A}$ und $\mathcal{B}$ ist eine Aussage $\mathcal{A} \wedge \mathcal{B}$ welche wahr ist, wenn $\mathcal{A}$ und $\mathcal{B}$ wahr sind und falsch ist, wenn mindestens eine der Aussagen $\mathcal{A}$ oder $\mathcal{B}$ falsch ist.

- Die Negation der Disjunktion $\mathcal{A} \vee \mathcal{B} = [n \in \mathbb{N} : n \leq 5] \vee [n \in \mathbb{N} : n \geq 3]$ ist

$$\begin{aligned} \neg[\mathcal{A} \vee \mathcal{B}] &= \neg[\quad [n \in \mathbb{N} : n \leq 5] \vee \quad [n \in \mathbb{N} : n \geq 3]] \\ &= \quad \neg[n \in \mathbb{N} : n \leq 5] \wedge \neg\, [n \in \mathbb{N} : n \geq 3] \\ &= \quad\ [n \in \mathbb{N} : n > 5] \wedge \quad [n \in \mathbb{N} : n < 3]. \end{aligned}$$

  Die Aussage $[n \in \mathbb{N} : n > 5] \wedge [n \in \mathbb{N} : n < 3]$ ist für keine natürlichen Zahlen wahr.

■

1.1.3 Implikation und Äquivalenz

Es gelten in gewissem Sinne „Rechenregeln“ für mathematische Aussagen. Dabei spielen die Begriffe der ***Äquivalenz*** und der ***Implikation*** eine entscheidende Rolle, welche mathematische Aussagen in Relation setzen. Diese beiden Begriffe sind wahrlich Schlüsselkonzepte der Mathematik. Sie sind die Formalisierung logischer Schlüsse.

DEFINITION 1.7. Es seinen $\mathcal{A}$ und $\mathcal{B}$ mathematische Aussagen.

Es ***impliziert*** $\mathcal{A}$ die Aussage $\mathcal{B}$ wenn gilt: $\mathcal{B}$ ist immer wahr, wenn $\mathcal{A}$ wahr ist. In diesem Fall schreibt man

$$\mathcal{A} \Longrightarrow \mathcal{B}.$$

Es sind $\mathcal{A}$ und $\mathcal{B}$ ***äquivalent***, wenn $\mathcal{A}$ die Aussage $\mathcal{B}$ impliziert und umgekehrt auch $\mathcal{B}$ die Aussage $\mathcal{A}$ impliziert. In diesem Fall schreibt man

$$\mathcal{A} \Longleftrightarrow \mathcal{B}.$$

BEMERKUNG 1.8. Es seinen $\mathcal{A}$ und $\mathcal{B}$ mathematische Aussagen.

- Es impliziere die Aussage $\mathcal{A}$ die Aussage $\mathcal{B}$. Man sagt dann auch, dass $\mathcal{B}$ aus $\mathcal{A}$ folgt oder dass $\mathcal{A}$ **hinreichend** für $\mathcal{B}$ ist und umgekehrt, dass $\mathcal{B}$ **notwendig** für $\mathcal{A}$ ist. In mathematisch-sprachlichen Formulierungen findet man die Formel „wenn $\mathcal{A}$, dann $\mathcal{B}$“.
- Es seien die Aussagen $\mathcal{A}$ und $\mathcal{B}$ äquivalent. Man sagt dann auch, dass $\mathcal{A}$ **notwendig und hinreichend** für $\mathcal{B}$ ist. In mathematisch-sprachlichen Formulierungen findet man die Formel „$\mathcal{A}$ genau dann, wenn $\mathcal{B}$“.

Die Begriffe „notwendig“ und „hinreichend“ kann man sich gut merken.

Ist $\mathcal{A}$ hinreichend für $\mathcal{B}$ (also $\mathcal{A}$ impliziert $\mathcal{B}$), dann ist $\mathcal{B}$ sicher wahr, wenn $\mathcal{A}$ wahr ist. Es ist also $\mathcal{B}$ unter Garantie wahr, wenn $\mathcal{A}$ wahr ist. Das $\mathcal{A}$ wahr ist, reicht aus (ist hinreichend), um zu wissen, dass auch $\mathcal{B}$ wahr ist. Im Umkehrschluss kann man allerdings nichts über $\mathcal{B}$ sagen, wenn $\mathcal{A}$ nicht wahr ist. Denn dann kann $\mathcal{B}$ wahr oder falsch sein.

Ist $\mathcal{B}$ notwendig für $\mathcal{A}$ (also $\mathcal{A}$ impliziert $\mathcal{B}$), dann ist $\mathcal{A}$ bestimmt nicht wahr, wenn $\mathcal{B}$ nicht wahr ist. Denn wäre $\mathcal{A}$ wahr, wäre sicher auch $\mathcal{B}$ wahr. ■

Betrachten wir je ein Beispiel für eine Implikation, die keine Äquivalenz ist und eine Äquivalenz, die per Definition eine zweifache Implikation ist.

BEISPIEL 1.9. Es ist

$$[n \geq 5] \Longrightarrow [n \geq 3]$$

Die Aussage $\mathcal{A} = [n \geq 5]$ impliziert die Aussage $\mathcal{B} = [n \geq 3]$ (wenn $n \geq 5$ ist, dann gilt sicherlich auch $n \geq 3$).

Umgekehrt ist dies jedoch nicht der Fall, $\mathcal{B}$ impliziert $\mathcal{A}$ nicht. Wähle dazu $n = 3$. Dann ist Aussage $\mathcal{B}$ wahr, Aussage $\mathcal{A}$ jedoch nicht.

Also sind die Aussagen $\mathcal{A}$ und $\mathcal{B}$ nicht äquivalent, es impliziert $\mathcal{A}$ zwar $\mathcal{B}$ aber $\mathcal{B}$ impliziert $\mathcal{A}$ nicht. ■

BEISPIEL 1.10. Es gilt sicherlich, dass ein Dreieck genau dann gleichseitig ist, wenn alle Seiten die gleiche Länge haben.

Formal betrachtet, liegen zwei Aussagen vor

$$\mathcal{A} = [\text{„Ein Dreieck ist gleichseitig.“}]$$
$$\mathcal{B} = [\text{„Die Seiten eines Dreiecks sind gleich lang.“}].$$

Die Aussage $\mathcal{A}$ impliziert die Aussage $\mathcal{B}$. Ist ein Dreieck gleichseitig, dann sind die Seiten gleich lang. Die Umkehrung ist in diesem Fall ebenfalls richtig. Die Aussage $\mathcal{B}$ impliziert auch die Aussage $\mathcal{A}$, denn ein Dreieck, dessen Seiten gleich lang sind, ist ein gleichseitiges Dreieck. Es gilt also

$$[\text{„Ein Dreieck ist gleichseitig.“}] \Leftrightarrow [\text{„Die Seiten eines Dreiecks sind gleich lang.“}]$$

■

Wir sammeln nun noch einige recht nützliche und erhellende Hinweise bezüglich Implikation und Äquivalenz.

BEMERKUNG 1.11. Im Fall der Äquivalenz sind die Aussagen entweder beide wahr oder beide falsch - sie sind gleichwertig. Daher erschließt sich der Name aus dem Lateinischen: *aequus* „gleich“ und *valere* „wert sein“. ■

BEMERKUNG 1.12. Eine schöne Veranschaulichung für den Unterschied zwischen Äquivalenz und Implikation ist diese Eselsbrücke, welche den Sachverhalt der Implikation veranschaulicht.

Implikation. Wenn es geregnet hat, ist die Straße nass.

Keine Implikation. Wenn die Straße nass ist, heißt das nicht zwangsläufig, dass es geregnet hat.

$$\text{„Es hat geregnet.“} \Longrightarrow \text{„Die Straße ist nass.“}$$

$$\text{„Die Straße ist nass.“} \not\Longrightarrow \text{„Es hat geregnet.“}$$

- Die Assoziativgesetze

$$[\mathcal{A} \wedge \mathcal{B}] \wedge \mathcal{C} \Leftrightarrow \mathcal{A} \wedge [\mathcal{B} \wedge \mathcal{C}] \text{ und } \mathcal{A} \vee \mathcal{B} \Leftrightarrow \mathcal{B} \vee \mathcal{A}$$

- Die Distributivgesetze

$$[\mathcal{A} \wedge \mathcal{B}] \vee \mathcal{C} \Leftrightarrow [\mathcal{A} \vee \mathcal{C}] \wedge [\mathcal{B} \vee \mathcal{C}] \text{ und } [\mathcal{A} \vee \mathcal{B}] \wedge \mathcal{C} \Leftrightarrow [\mathcal{A} \wedge \mathcal{C}] \vee [\mathcal{B} \wedge \mathcal{C}]$$

Tatsächlich müsste man dieses Lemma nun als wahr beweisen. Das ist nicht weiter schwer und wer möchte, darf dies gerne tun (die Definitionen der logischen Operatoren noch einmal näher betrachten). Bevor wir uns näher mit Beweisen beschäftigen, führen wir Mengen und Abbildungen ein, um Sätze formulieren zu können, anhand derer wir grundlegende Beweisprinzipien erlernen können.

1.2 Mengen

Um Mathematik betreiben zu können, ist der Begriff der Menge unumgänglich. Aufgrund einiger Komplikationen in den Details können wir Mengen leider nicht im strengen mathematischen Sinne sauber definieren. Für unsere Zwecke bedienen wir uns der (naiven) Mengendefinition von Georg Cantor (1845-1918), dem Begründer der Mengentheorie.

DEFINITION 1.23. Eine **Menge** ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen. Diese Objekte werden als **Elemente** bezeichnet.

Diese sehr einleuchtende und der alltäglichen Verwendung des Begriffs der Menge sehr nahe Umschreibung führt allerdings bei näherer Untersuchung zu Problemen.

BEMERKUNG 1.24. Definiert man Mengen als „Zusammenfassung unterscheidbarer Objekte“, wie wir es getan haben, so ergibt sich das folgende als das „Russelsche Antinomie“ bezeichnete Paradoxon. Sei A die Menge der Mengen, welche sich nicht selbst enthalten. Wir werden nun zeigen, dass es diese Menge nicht geben kann. Dazu betrachten wir die einfache Aussage [die Menge A enthält sich selbst].

Es gibt nun zwei Möglichkeiten für den Wahrheitsgehalt dieser Aussage.

wahr $\rightarrow$ Die Menge A enthält sich selbst.

Dann ist A keine Menge, die sich selbst nicht enthält. Dann ist A aber per Definition der Menge A nicht in A enthalten. ↯ Ein Widerspruch.

falsch $\rightarrow$ Die Menge A enthält sich nicht selbst.

Dann ist A eine Menge, die sich selbst nicht enthält. Dann ist A aber per Definition der Menge A in A enthalten. $\lightning$ Ein Widerspruch.

■

Wir werden uns dennoch an die naive Definition der Menge halten. In der grundlegenden Mathematik spielen die angedeuteten Komplikationen keine Rolle. Wir wollen uns direkt einige Konventionen und Definitionen bezüglich der Notation grundlegender Begriffe im Kontext von Mengen anschauen.

DEFINITION 1.25. Es sei A eine Menge.

- Die Schreibweise $x \in A$ bedeutet, dass x ein **Element** der Menge A ist.
- Mengen werden mit „{“ und „}“ den *Mengenklammern* geschrieben.
- Eine Menge ist definiert, wenn angegeben ist, welche Elemente in ihr enthalten sind. Dies kann *deskriptiv* - durch Angabe einer definierenden Eigenschaft ($A = \{n \in \mathbb{N} : n \text{ ist gerade}\}$) - und *konstruktiv* - durch Aufzählung aller in ihr enthaltenen Elemente ($A = \{2, 4, 6, 8, 10\}$) - geschehen. Wenn bei Mengen mit unendlich vielen Elementen das Bildungsgesetz klar ist, können auch unendliche Aufzählungen verwendet werden ($A = \{2, 4, 6, 8, \ldots\}$).
- Eine Menge A heißt **endlich**, wenn A nur endlich viele Elemente besitzt.
- Die Anzahl der Elemente einer endlichen Menge A wird als die **Kardinalität** von A bezeichnet und mit $|A|$ notiert (auch **Mächtigkeit** genannt). Ist A nicht endlich, so schreibt man $|A| = \infty$.
- Die **leere Menge** notiert mit $\emptyset$ ist diejenige Menge, die keine Elemente enthält. Sie hat Kardinalität 0.

BEMERKUNG 1.26. Elemente in Mengen tauchen nur einmal auf. So ist die Menge $M_1 = \{1, 2, 2\}$ gleich der Menge $M_2 = \{1, 2\}$. Manchmal unterscheidet man diese Mengen und bezeichnet erstere dann als **Multimengen**. In einer Multimenge darf ein und dasselbe Element mehr als einmal aufgezählt werden. ■

BEISPIEL 1.27. Die Menge $A = \{1, 4, 8\}$ ist eine endliche Menge mit der Kardinalität $|A| = 3$. Die Menge $B = \{1, 3, 5, 7, \ldots\}$ der ungeraden natürlichen Zahlen ist keine endliche Menge und es ist $|B| = \infty$. ■

Man kann Mengen auf Gleichheit hin untersuchen und aus ihnen weitere Mengen gewinnen.

```
# Menge
sage: M=Set([1,2])
sage: 6 in M
False
sage: 2 in M
True
# Kardinalität einer Menge
sage: M.cardinality()
2
# die leere Menge
sage: Set([]).is_empty()
True
sage: M.random_element()
1
```

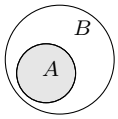


Abb. 1.2.

Die Teilmenge $A \subset B$.

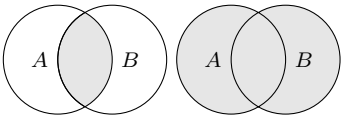


Abb. 1.3.

Der Schnitt $A \cap B$ und die Vereinigung $A \cup B$.

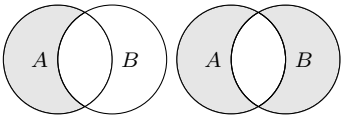


Abb. 1.4.

Die Differenz $A - B$ und die symmetrische Differenz $A \triangle B$.

```
# Identische Mengen
sage: M1,M2=Set([1,2]),Set([1,2,2])
sage: M1==M2
True
sage: M3=Set([2,3])
# Teilmengen
sage: list(M1.subsets())
[{}, {1}, {2}, {1, 2}]
sage: Set([1]) in M1.subsets()
True
# Vereinigung
sage: M1.union(M3)
{1,2,3}
# Durchschnitt
sage: M1.intersection(M3)
{2}
# Differenz
sage: M1.difference(M3)
{2}
sage: M1-M3==M1.difference(M3)
True
# Symmetrische Differenz
sage: M1.symmetric_difference(M3)
{1, 3}
# Kartesisches Produkt
sage: cartesian_product([M1, M3])
The Cartesian product of (1,2,
1,3)
# Potenzmenge
sage: Set(M1.subsets())
[{}, {1}, {2}, {1, 2}]
```

DEFINITION 1.28. Es seien A und B zwei Mengen.

- Wir nennen die Mengen A und B **gleich**, wenn sie die gleichen Elemente enthalten.
- Es bedeutet $A \subset B$ (bzw. $B \supset A$), dass A eine **Teilmenge** von B ist, das heißt jedes Element von A ist auch ein Element von B.
- Eine Teilmenge A von B heißt **echt**, wenn A nicht gleich B oder der leeren Menge ist.
- Mit $A \cup B$ bezeichnen wir die **Vereinigung** von A und B; die Menge aller Elemente, die in A oder in B enthalten sind.
- Außerdem ist $A \cap B$ der **Durchschnitt** von A und B; die Menge aller Elemente, die in A und B enthalten sind.
- Mit $A \setminus B$, gesprochen „A **ohne** B“, bezeichnen wir die Menge aller Elemente von A, die nicht Element von B sind (auch **Differenz** genannt).
- Mit $A \triangle B$ bezeichnen wir die **symmetrische Differenz** von A und B; die Menge aller Elemente, die entweder in A oder in B aber nicht in beiden Mengen enthalten sind.
- Es bezeichnet $A \times B$ die **Produktmenge** von A und B, die Menge aller geordneten Paare (x, y) mit $x \in A$ und $y \in B$ (auch **kartesisches Produkt** genannt).
- Mit A^n bezeichnen wir das n-fache kartesische Produkt von A mit sich selbst. Die Elemente von A^n sind die geordneten n-Tupel $(x_1, \ldots, x_n)$ mit $x_1, \ldots, x_n \in A$.
- Für eine Menge A is die **Potenzmenge** $\mathcal{P}(A)$ die Menge aller Teilmengen von A inklusive der leeren Menge $\emptyset$.

BEMERKUNG 1.29. In den Abbildungen 1.2 bis 1.4 sind **Venn**-Diagramme gezeigt, welche grundlegende Konzepte von Mengen veranschaulichen. Es sei darauf hingewiesen, dass das Malen eines Venn-Diagramms keine mathematisch formale Argumentation ist. Dennoch können solche Diagramme helfen, nötige Argumentationsschritte zu identifizieren. ■

BEISPIEL 1.30. Es seien die drei Mengen $A = \{1, 4, 6, 8, 9\}$, $B = \{1, 2, 3, 6, 7\}$ und $C = \{3, 6\}$ gegeben.

- Es ist weder A gleich B noch A gleich C noch B gleich C. Denn die 9 ist nur in A enthalten, die 2 nur in B.
- Es ist $C \subset B$, denn jedes Element aus C ist ebenfalls ein Element aus B.
- Es ist $A \cup B = \{1, 2, 3, 4, 6, 7, 8, 9\}$ die Vereinigung der Mengen A und B.
- Es ist $A \cap B = \{1, 6\}$ der Schnitt der Mengen A und B.
- Es ist $A \setminus B = \{4, 8, 9\}$ die Menge A ohne B.

- Es ist $A \triangle B = \{2, 4, 7, 8, 9\}$ die symmetrische Differenz von A und B.

Es seien die Mengen $A' = \{1, 2, 3\}$ und $B' = \{3, 4\}$ gegeben. Dann ist

$$A' \times B' = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

das kartesische Produkt von A' und B'. Außerdem ist

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

die Potenzmenge von A'. ■

Ein weiteres sehr nützliches Konzept ist die Partition einer Menge. Dabei wird eine Menge A in disjunkte Teilmengen aufgeteilt, so dass jedes Element von A in genau einer dieser Teilmengen liegt.

DEFINITION 1.31. Es sei A eine Menge. Dann nennt man die Mengen $B_1, \ldots, B_n$ eine **Partition** der Menge A, wenn

- $\emptyset \neq B_i \subset A$ für alle $i = 1, \ldots n$
- $B_1 \cup \ldots \cup B_n = A$
- $B_i \cap B_j = \emptyset$ für alle $i, j \in \mathbb{N}$ mit $1 \leq i < j \leq n$.

BEISPIEL 1.32. Es sei die Menge $A = \{1, 4, 6, 8, 9\}$ gegeben. Dann bilden die Mengen $B_1 = \{1, 4\}, B_2 = \{6, 8\}$ und $B_3 = \{9\}$ eine Partition der Menge A. Denn es gilt $B_1 \cap B_2 = \emptyset$, $B_1 \cap B_3 = \emptyset$ und $B_2 \cap B_3 = \emptyset$, aber $B_1 \cup B_2 \cup B_3 = A$. Die Mengen $B_1' = \{1, 9, \}$ und $B_2' = \{4, 6, 8\}$ bilden genauso eine Partition von A, wie die Menge $B_1'' = A$. ■

In einem gewissen Sinne lässt sich mit Mengen und den **Operatoren** Durchschnitt und Vereinigung (Differenz und dem kartesischen Produkt) rechnen. Es gelten die folgenden „Rechenregeln“.

LEMMA 1.33. Für beliebige Mengen A, B und C gelten die folgenden Gesetze bezüglich der Vereinigung und des Durchschnitts.

- Die Kommutativgesetze

$$A \cap B = B \cap A \text{ und } A \cup B = B \cup A.$$

- Die Assoziativgesetze

$$(A \cap B) \cap C = A \cap (B \cap C) \text{ und } (A \cup B) \cup C = A \cup (B \cup C).$$

- Die Distributivgesetze

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \text{ und}$$
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Wir möchten später einen Teil dieses Lemmas beweisen. Es dient uns als Beispiel für Beweise von Aussagen über Mengen. Bevor wir das tun, werden wir noch Zahlen und Abbildungen einführen. An dieser Stelle

möchten wir jedoch noch an den Binomialkoeffizienten erinnern. Der Binomialkoeffizient ist mithilfe der **Fakultät** einer natürlichen Zahl definiert.

DEFINITION 1.34. Die **Fakultät einer natürlichen Zahl** ist eine Abbildung, welche eine natürliche Zahl $n \in \mathbb{N}^*$ auf das Produkt $1 \cdot 2 \cdots (n-1) \cdot n$ und die 0 auf 1 abbildet. Man schreibt dann $n! = 1 \cdot 2 \cdots (n-1) \cdot n$ bzw. $0! = 1$.

BEISPIEL 1.35. Es ist zum Beispiel $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$ oder $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 720 \cdot 7 = 1540$.

Der Binomialkoeffizient ist eine natürliche Zahl, die von zwei Parametern, jeweils natürliche Zahlen, abhängt.

DEFINITION 1.36. Für zwei natürliche Zahlen $n, k \in \mathbb{N}$ mit $n \geq k$ ist der **Binomialkoeffizient**

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

BEMERKUNG 1.37. Der Name erschließt sich aus der Tatsache, dass der Binomialkoeffizient als Koeffizient des k-ten Summanden der n-fachen Potenz eines Binoms der Form $(a+b)$ auftaucht. Nach dem binomischen Lehrsatz ist nämlich

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

Warum haben wir den Binomialkoeffizienten im Kontext von Mengen erinnert? Tatsächlich zählt der Binomialkoeffizient kombinatorisch betrachtet die Anzahl der k-elementigen Teilmengen einer Menge mit n Elementen.

LEMMA 1.38. Sei M eine Menge der Kardinalität $|M| = n$. Dann hat M genau $\binom{n}{k}$ verschiedene Teilmengen der Kardinalität k.

BEISPIEL 1.39. Die Menge $M = \{1,2,3,4,5\}$ mit Kardinalität 5 hat also $\binom{5}{3} = \frac{5!}{(5-3)! \cdot 3!} = 10$ Teilmengen der Kardinalität 3. Es sind

$$\begin{array}{llll} M_1 = \{1,2,3\}, & M_2 = \{1,2,4\}, & M_3 = \{1,2,5\}, & M_4 = \{1,3,4\}, \\ M_5 = \{1,3,5\}, & M_6 = \{1,4,5\}, & M_7 = \{2,3,4\}, & M_8 = \{2,3,5\}, \\ M_9 = \{2,4,5\}, & M_{10} = \{3,4,5\}. & & \end{array}$$

1.3 Zahlen

Zahlen sind ein alltägliches Konzept. Man trifft Zahlen der Form

$$23,\ 7,\ 1991,\ 0,\ -10,\ \frac{17}{89},\ 0,\overline{34},\ 8{,}99,\ \pi.$$

Diese Zahlen sind alles reelle, manche natürliche, ganze, rationale oder irrationale Zahlen. Wie sich diese Zahlenbereiche voneinander abgrenzen, möchten wir nun kurz beleuchten. Dabei definieren wir zunächst die natürlichen Zahlen und erwähnen dann, dass die ganzen Zahlen eine Zahlenbereichserweiterung der natürlichen und die rationalen Zahlen wiederum eine Erweiterung der ganzen Zahlen darstellen. Die reellen Zahlen sind etwas komplizierter aber ebenfalls als eine Zahlenbereichserweiterung aus den rationalen Zahlen zu gewinnen.

Aus diesem Abschnitt sollten Sie im Wesentlichen die Notation für die natürlichen, ganzen, rationalen und reellen Zahlen mitnehmen. Diese Zahlenbereiche kennen Sie sicherlich schon aus der Schule. Bitte frischen Sie Ihr Wissen dazu auf. Der Abschnitt ist für den interessierten Leser gedacht, welcher ein leichtes Beispiel sehen möchte, wie Axiome zu „bekannten“ Objekten wie den natürlichen Zahlen aussehen. Das mutet kompliziert an, angesichts der Tatsache, dass selbst Vorschulkinder sie aufzählen und Grundschüler sicher mit ihnen rechnen können.

1.3.1 Die natürlichen Zahlen

Wir möchten der in der Einleitung geschilderten Übersetzung von Beobachtung in eine formale abstrakte Sprache anhand der natürlichen Zahlen nachspüren. Die natürlichen Zahlen $0, 1, 2, 3, \ldots$ sind sicherlich aus der Schule bekannt. Doch was sind die grundlegenden definierenden Eigenschaften der natürlichen Zahlen? Der italienische Mathematiker Guiseppe Peano formulierte 1889 fünf Axiome, welche die natürlichen Zahlen bis heute definieren. Sie werden im zur Ehre als die Peano-Axiome bezeichnet.

Die Peano-Axiome

Wir beginnen mit der formalen Definition.

DEFINITION 1.40. Wir nennen eine Menge $\mathbb{N}$ **die Menge der natürlichen Zahlen**, wenn sie die folgenden Eigenschaften besitzt.

P1. $0 \in \mathbb{N}$
[Es gibt eine natürliche Zahl, welche mit 0 bezeichnet wird.]

P2. $\forall n(n \in \mathbb{N} \Rightarrow n' \in \mathbb{N})$
[Für jede natürliche Zahl n gibt es eine natürliche Zahl n', welche als Nachfolger bezeichnet wird.]

P3. $\forall n(n \in \mathbb{N} \Rightarrow n' \neq 0)$
[Die 0 ist kein Nachfolger einer natürlichen Zahl.]

P4. $\forall n, m(m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n))$
[Natürliche Zahlen mit gleichem Nachfolger sind gleich.]

P5. $\forall N(0 \in N \wedge \forall n(n \in \mathbb{N} \Rightarrow (n \in X \Rightarrow n' \in N)) \Rightarrow \mathbb{N} \subseteq N)$
[Enthält eine Menge N die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger n', sind die natürlichen Zahlen eine Teilmenge von N.]

BEMERKUNG 1.41. Dass jede natürliche Zahl einen Nachfolger besitzt, sorgt dafür, dass die natürlichen Zahlen „der Größe nach“ sortiert werden können. Beginnend mit der 0 folgt der Nachfolger der 0 welchen wir mit 1 bezeichnen, folgt der Nachfolger der 1, welchen wir mit 2 bezeichnen, folgt der Nachfolger der 2, welchen wir mit 2 bezeichnen, ... ■

Das Axiom **P5** wird auch als **Induktionsaxiom** bezeichnet und ist Grundlage des Beweisprinzips der vollständigen Induktion, welches wir in Abschnitt 1.5 kennen lernen werden.

Ob die natürlichen Zahlen bei 0 oder erst bei 1 anfangen ist letztlich Frage der Vereinbarung. In der Zahlentheorie, einem Teilgebiet der Mathematik, ist es üblich die 0 nicht zu den natürlichen Zahlen zu zählen, in der Informatik zählt die 0 üblicherweise zu den natürlichen Zahlen. Daran halten wir uns in diesem Buch.

Rechnen mit natürlichen Zahlen

Die Addition zweier natürlicher Zahlen ist folgendermaßen definiert.

- Für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt $n + 0 = n$.
- Für alle natürlichen Zahlen $n, m \in \mathbb{N}$ gilt $n + m' = (n + m)'$.

Die erste Eigenschaft klingt gewohnt. Die zweite Eigenschaft in Worten lautet: Die Summe einer natürlichen Zahl n und dem Nachfolger m' einer natürlichen Zahl m entspricht dem Nachfolger der Summe der natürlichen Zahl n und der natürlichen Zahl m. Hilft das in der Praxis weiter? Wieder ist eine Summe zweier natürlicher Zahlen zu „berechnen“. Allerdings

von π bricht nicht ab und wird nicht periodisch. Es ist

$$\pi = 3.14159265358979323846264338327950288419716939937510 58\ldots.$$

DEFINITION 1.42. Wir bezeichnen mit

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

die Menge der ***ganzen Zahlen***, mit

$$\mathbb{Q} = \left\{ \frac{n}{m} : n, m \in \mathbb{Z} \text{ mit } m \neq 0 \right\}$$

die Menge der ***rationalen Zahlen*** und mit $\mathbb{R}$ die Menge der ***reellen Zahlen***.

Häufig wird der Zahlenbereich weiter eingeschränkt, wir nutzen dazu die folgende Notation.

DEFINITION 1.43. Bezeichnet Z einen Zahlenbereich, so ist für eine Zahl $x \in Z$

$$Z_{\leq x} = \{z \in Z : x \leq z\} \qquad Z_{<x} = \{z \in Z : x < z\}$$
$$Z_{\geq x} = \{z \in Z : x \geq z\} \qquad Z_{>x} = \{z \in Z : x > z\}.$$

Weiter bezeichnet Z^+ die echt positiven Zahlen des Zahlenbereichs Z.

BEISPIEL 1.44. Es bezeichnen $\mathbb{Z}_{\geq 0}, \mathbb{Q}_{\geq 0}, R_{\geq 0}$ bzw. $\mathbb{Z}_{\leq 0}, \mathbb{Q}_{\leq 0}, R_{\leq 0}$ die nicht negativen bzw. nicht positiven ganzen, rationalen und reellen Zahlen. Es ist also beispielsweise

$$\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} : x \geq 0\}.$$

Im Kontrast dazu ist $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\}$. ■

1.4 Abbildungen

Genauso wie Mengen sind Abbildungen zwischen diesen ein grundlegendes Werkzeug der Mathematik in all ihren Teilgebieten. Sie sind das Mittel der Wahl, wenn man eine Beziehung zwischen zwei Mengen herstellen möchte. Man kann zum Beispiel die Menge „alle Studenten, die eine Klausur mitgeschrieben haben“ mit der Menge „Klausurnoten“ in Verbindung bringen, indem man jedem Studenten eine Note zuordnet. Diese

Zuordnung entspricht einer Abbildung. Ein Student wird dabei auf seine Klausurnote „abgebildet“. Wir starten mit grundlegenden Definitionen von Abbildungen.

DEFINITION 1.45 (Abbildungen). Eine **Abbildung** (oder auch **Funktion**) $f : D \to B, x \mapsto f(x)$ bildet Werte aus dem **Definitionsbereich** D, eine beliebige Menge, in den **Bildbereich** B, eine beliebige Menge, ab. Jedem Element $x \in D$ wird durch f genau ein **Bild** $f(x) \in B$ zugeordnet. Gilt $f(x) = y$ für ein $y \in B$, so nennt man x das **Urbild** von y.

BEMERKUNG 1.46. Die Schlüsselerkenntnis bei der Definition von Abbildungen besteht darin, dass wirklich jedem(!) Element des Definitionsbereichs genau ein(!) Element (sein Bild) aus dem Bildbereich zugeordnet wird. Andersherum gilt das nicht, nicht jedes Element des Bildbereichs muss auch tatsächlich das Bild eines Elements (ein Urbild) aus dem Definitionsbereich sein und ein und dasselbe Element aus dem Bildbereich kann das Bild mehrerer Elemente aus dem Definitionsbereich sein. Also, für eine Abbildung $f : D \to B, x \mapsto f(x)$ hat jedes $x \in D$ genau ein Bild $f(x)$, aber nicht jedes Element $y \in B$ muss ein Urbild besitzen.

Das kann man sich anhand des eingangs erwähnten Beispiels klar machen. Jeder Student, der die Klausur mitgeschrieben hat, bekommt eine Klausurnote zugeordnet. Aber es könnten alle Studenten (die Urbilder) die gleiche Note, zum Beispiel die Bestnote, (ihr Bild) erhalten. Alle anderen Noten sind in diesem Fall keinem Studenten zugeordnet worden, sie besitzen keine Urbilder. Die Bestnote, vorausgesetzt, es haben mindestens zwei Studenten die Klausur mitgeschrieben, wurde in dem geschilderten Fall mehreren Studenten zugeordnet, besitzt also mehr als ein Urbild. ■

BEISPIEL 1.47. Betrachtet man die Mengen $D = \{0, \frac{1}{2}, 1\}$ und $B = \{3, 7, 9, 10\}$, dann gibt es eine Abbildung $f : D \to B$ mit

$$0 \mapsto f(0) = 9, \quad \frac{1}{2} \mapsto f(\frac{1}{2}) = 8, \quad 1 \mapsto f(1) = 3,$$

welche die Elemente aus D auf Elemente aus B abbildet. Siehe dazu die Skizze in Abbildung 1.5. ■

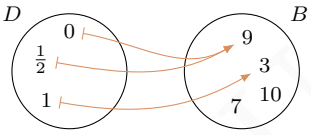


Abb. 1.5.

Illustration der Abbildung aus Beispiel 1.47.

BEISPIEL 1.48. Betrachte die Menge $N = \{2, 3, 4, 5, 6, 7\}$. Dann ordnet die Abbildung $f : N \to Z$ mit

$$2 \mapsto f(2) = 2, \quad 3 \mapsto f(3) = 3, \quad 4 \mapsto f(4) = 2,$$
$$5 \mapsto f(5) = 5, \quad 6 \mapsto f(6) = 3, \quad 7 \mapsto f(7) = 7$$

den natürlichen Zahlen $2, \ldots, 7$ die größte Primzahl zu, die sie teilt. Siehe dazu die Skizze in Abbildung 1.6. ■

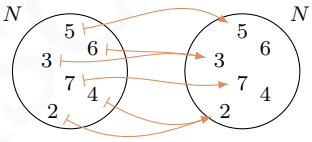


Abb. 1.6.

Illustration der Abbildung aus Beispiel 1.48.

BEISPIEL 1.49. Die Abbildung $g : \mathbb{R} \to \mathbb{R}_{\geq 0}$ mit $y \mapsto f(y) = y^2$ bildet jede reelle Zahl auf ihr Quadrat ab. Siehe dazu den skizzierten Funktionsgraphen in Abbildung 1.7. ■

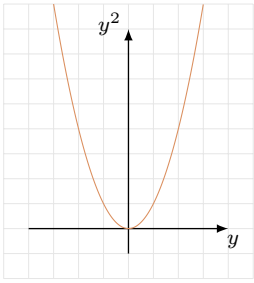


Abb. 1.7.

Illustration der Abbildung aus Beispiel 1.49.

Noch eine kleine Bemerkung bezüglich der Notation.

BEMERKUNG 1.50. In Beispiel 1.49 wird deutlich, dass die Mengen, die den

Definitionsbereich und den Bildbereich bilden, nicht zwangsläufig mit D und B bezeichnet werden müssen. Auch kann die Abbildung einen anderen Namen als f tragen und die Abbildungsvariable muss nicht zwangsläufig x heißen.

In der Literatur wird der Bildbereich manchmal auch als Wertebereich bezeichnet. ■

Da Abbildungen in der Mathematik eine weitreichende Bedeutung haben, gibt es eine Vielzahl weiterer Definitionen. Zunächst verallgemeinern wir die Begriffe des Bildes und Urbildes auf Teilmengen des Bild- bzw. Definitionsbereichs.

DEFINITION 1.51. Sei $f : D \to B, x \mapsto f(x)$ eine Abbildung. Für eine Teilmenge $Z \subset D$ ist

$$f(Z) = \{f(z) : z \in Z\}$$

die **Bildmenge** (manchmal auch einfach das Bild) von Z unter f. Wir nennen $f(D)$ auch das **Bild** von f und schreiben $\mathsf{Bild}(f) = f(D)$. Umgekehrt bezeichnen wir für $C \subset B$ mit

$$f^{-1}(C) = \{x \in D : f(x) \in C\}$$

die **Urbildmenge** (manchmal auch einfach das Urbild) von C unter f.

BEISPIEL 1.52. Wir betrachten die Abbildung $f : N \to N$ aus Beispiel 1.52. Dann ist $Z = \{3, 5, 6\}$ eine Teilmenge von N, dem Definitionsbereich. Es gilt $f(Z) = \{f(3), f(5), f(6)\} = \{3, 5\}$ ist die Bildmenge von Z unter f.

Für die Menge $C = \{2, 7\}$, eine Teilmenge des Bildbereichs N, ist $f^{-1}(C) = \{2, 4, 7\}$ die Urbildmenge von C unter f, die Menge aller Urbilder von 2 und 7, den Elementen aus C. ■

Man kann eine Funktion durch eine Restriktion in ihrem Definitionsbereich einschränken.

DEFINITION 1.53. Sei $f : D \to B, x \mapsto f(x)$ eine Abbildung und $D' \subset D$ eine Teilmenge des Definitionsbereichs von f. Dann nennen wir die Abbildung $f|_{D'} : D' \to, x \mapsto f(x)$ die **Restriktion** von f auf D'.

BEMERKUNG 1.54. Die Restriktion einer Abbildung „vergisst die Elemente aus dem Definitionsbereich, die nicht in der Teilmenge D' von D liegen und bildet nur noch Elemente aus D' ab. Auf dieser Teilmenge D' entsprechen die Bilder jedoch ihren Bildern unter f. Die Restriktion wird manchmal auch als Einschränkung, die deutsche Übersetzung von Restriktion, bezeichnet, denn man schränkt den Definitionsbereich auf eine Teilmenge ein. ■

BEISPIEL 1.55. Wir betrachten erneut die Abbildung $f : N \to N$ aus Beispiel 1.52 und die Teilmenge $Z = \{3, 5, 6\}$ von N, dem Definitionsbereich. Dann ist

$f|_Z : Z \to N$ die Restriktion von f auf Z mit

$$3 \mapsto f(3) = 3, \quad 5 \mapsto f(5) = 5, \quad 6 \mapsto f(6) = 3.$$

■

1.4.1 Injektivität, Surjektivität und Bijektivität

Abbildungen können, egal welche Mengen beteiligt sind, ob Zahlen oder sonstige mathematische Objekte, drei ganz grundlegende Eigenschaften besitzen. Dabei kommt es alleine auf die Zuordnung der Elemente und nicht deren mathematische Eigenschaften an. Grob gesprochen wird geklärt, ob Elemente aus dem Definitionsbereich alle Elemente des Bildbereichs „treffen“und ob es manche Elemente gibt, die mehrfach „getroffen“ werden.

DEFINITION 1.56. Eine Abbildung $f : D \to B$ heißt

- **injektiv**, wenn je zwei verschiedene $x, x' \in D$ auch verschiedene Bilder besitzen, wenn also gilt
$$x \neq x' \implies f(x) \neq f(x').$$
- **surjektiv**, wenn jeder Bildpunkt $y \in B$ tatsächlich auch ein Urbild $x \in D$ besitzt mit $y = f(x)$,wenn also gilt
$$\forall\, y \in B\ \exists\, x \in D : f(x) = y.$$
- **bijektiv**, wenn f injektiv und surjektiv ist.

Es helfen die Skizzen in den Abbildungen 1.8 bis 1.11 und die folgenden erklärenden Worte, sich diese drei grundlegenden Begriffe für Abbildungen vorzustellen. Es sei vorweg noch einmal betont, dass jede Abbildung *jedem* Element des Definitionsbereichs auch ein Element aus dem Bildbereich zuordnet.

- **Injektivität.** Die Definition der Injektivität kann man sich anschaulich vorstellen als dass die Definitionsmenge D in den Bildbereich „injiziert wird. Jeder Punkt im Definitionsbereich besitzt einen *eigenen* Punkt im Bildbereich.
- **Surjektivität.** Eine surjektive Abbildung dagegen „deckt den ganzen Bildbereich ab“, jeder Bildpunkt im Bildbereich wird bei einer surjektiven Abbildung auch tatsächlich getroffen. Bei einer surjektiven Abbildung stimmen also Bildbereich und Bildmenge überein.

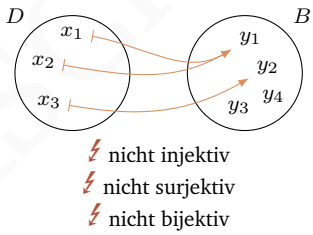


Abb. 1.8.
Illustration einer nicht injektiven und nicht surjektiven Abbildung.

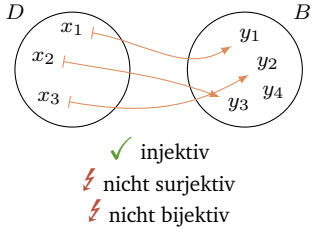


Abb. 1.9.
Illustration einer injektiven aber nicht surjektiven Abbildung.

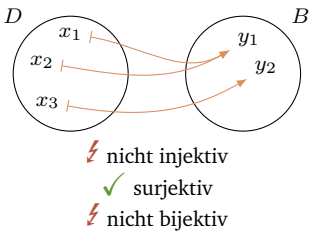


Abb. 1.10.

Illustration einer nicht injektiven aber surjektiven Abbildung.

Die Bildmenge ist nämlich die Menge der Punkte im Bildbereich, die tatsächlich getroffen werden.

- **Bijektivität.** Eine bijektive Abbildung stellt eine eins-zu-eins-Relation zwischen Definitionsmenge D und Bildbereich B her. Jedes $x \in D$ hat zum einen „sein eigenes“ Bild $f(x) \in B$ (injektiv) und zum anderen hat jeder Punkt $y \in B$ auch ein Urbild $x' \in D$ mit $f(x') = y$ (surjektiv). Bei endlichem Definitions- und/oder Bildbereich folgt daraus direkt, dass diese gleich viele Elemente besitzen.

Es helfen nun sicherlich einige Beispiele.

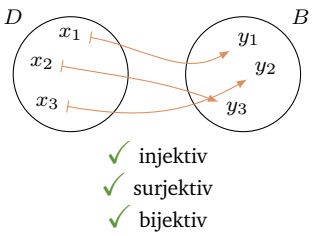


Abb. 1.11.

Illustration einer injektiven und surjektiven also bijektiven Abbildung.

BEISPIEL 1.57. Wir betrachten die Mengen $D' = \{1,2,3,4\}, D = \{1,2,3\}, B = \{5,6,7,8\}$ und $B' = \{5,6,7\}$.

- Die Abbildung $f : D \to B$ mit
$$1 \mapsto f(1) = 5, \quad 2 \mapsto f(2) = 5, \quad 3 \mapsto f(3) = 7.$$
ist nicht injektiv und nicht surjektiv. Es gibt mit $x = 1$ und $x' = 2$ zwei verschiedene Elemente in D mit $5 = f(1) = f(x) = f(x') = f(2) = 5$ (nicht injektiv) und es gibt mit $y = 8$ ein Element in B, für welches kein Urbild in D existiert (nicht surjektiv).
- Die Abbildung $f : D \to B$ mit
$$1 \mapsto f(1) = 5, \quad 2 \mapsto f(2) = 6, \quad 3 \mapsto f(3) = 7.$$
ist injektiv aber nicht surjektiv. Es gibt nicht zwei verschiedene Elemente x, x' in D mit $f(x) = f(x')$ (injektiv) aber es gibt mit $y = 8$ jedoch ein Element in B, für welches kein Urbild in D existiert (nicht surjektiv).
- Die Abbildung $f : D' \to B'$ mit
$$1 \mapsto f(1) = 5, \quad 2 \mapsto f(2) = 5, \quad 3 \mapsto f(3) = 6, \quad 3 \mapsto f(4) = 7.$$
ist nicht injektiv aber surjektiv. Es gibt mit $x = 1$ und $x' = 2$ zwei verschiedene Elemente in D mit $5 = f(1) = f(x) = f(x') = f(2) = 5$ (nicht injektiv) und es gibt kein Element in B', für welches kein Urbild in D existiert (surjektiv).
- Die Abbildung $f : D \to B'$ mit
$$1 \mapsto f(1) = 5, \quad 2 \mapsto f(2) = 6, \quad 3 \mapsto f(3) = 7.$$
ist injektiv und surjektiv. Es gibt nicht zwei verschiedene Elemente x, x' in D mit $f(x) = f(x')$ (injektiv) und es gibt kein Element in B', für welches kein Urbild in D existiert (surjektiv).

■

BEISPIEL 1.58. Wir betrachten nun noch Abbildungen über unendlichen Mengen. Da bieten sich die reellen Zahlen an. Am besten macht man sich zu den einzelnen Abbildungen jeweils eine kleine Skizze, um sich die Aussagen klar zu machen.

- Die Abbildung $f : \mathbb{R} \to \mathbb{R}\ x \mapsto x^3 + x$ ist nicht injektiv aber surjektiv.
- Die Abbildung $f : \mathbb{R} \to \mathbb{R}\ x \mapsto 2^x$ ist injektiv aber nicht surjektiv.

BEISPIEL 1.67. Die Abbildung $f : D \to B'$ aus Beispiel 1.57 ist bijektiv. Wir erhalten die Umkehrabbildung von f in $f^{-1} : B' \to D$ mit

$$5 \mapsto f^{-1}(5) = 1, \quad 6 \mapsto f^{-1}(6) = 2, \quad 7 \mapsto f^{-1}(7) = 3.$$

Die Abbildung $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq} \; x \mapsto x^2$ aus Beispiel 1.58 ist ebenfalls bijektiv. Wir erhalten die Umkehrabbildung von f in $f^{-1} : B' \to D$ mit $x \mapsto f^{-1}(x) = \sqrt{x}$. ■

Hat eine Abbildung eine Umkehrabbildung, dann gibt es einen Zusammenhang zur Identitätsabbildung.

LEMMA 1.68. Sei $f : D \to B$ eine bijektive Abbildung. Dann ist

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_D.$$

Beweis. Der Beweis ist eine Übungsaufgabe. ■

Die Summe und das Produkt

In der Mathematik treten häufig Verknüpfungen von Elementen auf. Das können zum Beispiel die Vereinigung oder der Schnitt von Mengen oder die Summe oder das Produkt von reellen Zahlen sein. Möchte man mehr als je zwei Elemente miteinander verknüpfen, gibt es dafür eine abkürzende Schreibweise, die wir nun kennenlernen. Um das zu tun, definieren wir den Index einer Menge B. Dazu nutzen wir allgemein Abbildungen einer Indexmenge I in die mit einem Index zu versehende Menge B. Man gibt Elementen aus der Menge B quasi einen Namen aus I.

Das formale Konzept kann sehr verwirrend aussehen, in der Praxis sind die Symbole doch meist harmlos. Wen die Definitionen und Bemerkungen in diesem Abschnitt verwirren, sollte sich einfach mit den Beispielen begnügen.

DEFINITION 1.69. Es seien D und B eine Menge. Es sei weiterhin eine injektive Abbildung $f : D \to B, x \mapsto f(x)$ gegeben. Wir nennen f dann einen **Index** von B über der **Indexmenge** D und nennen für ein $b \in f(D)$ mit $f(d) = b$ das Element d den **Index** von b. Wir schreiben dann mitunter etwas lax für die Abbildung f auch einfach $(f(x))_{x \in D}$ und für ein Element $d \in D$ auch $f(d) = f_d$.

BEMERKUNG 1.70. Ist $D = \{1, 2, \ldots, k\} \subset \mathbb{N}$, dann entsprechen die Bilder unter dem Index f einer Menge B über der Indexmenge D einem Tupel $(f(1), \ldots, f(k))$ welches in dem kartesischen Produkt B^k enthalten ist. Ein solcher Index wählt sich also k Elemente aus B aus und schreibt sie „sortiert“ und „nummeriert“ in ein Tupel.

Ist B eine endliche Menge der Kardinalität k und f eine bijektive Abbildung, wird jedem Element aus der Menge B ein Index aus der Menge der natürlichen Zahlen von 1 bis k zugeordnet. Dieser Fall ist sicherlich der am häufigsten auftretende.

Manchmal bezeichnet man die Indexmenge D auch den Index, dann sollte aber klar sein, welches Element aus D, welchem Element aus B zugeordnet ist. ■

BEISPIEL 1.71. Sei $D = \{\alpha, \beta, \gamma\}$ eine Menge griechischer und $B = \{a, b, c, d, e\}$ eine Menge lateinischer Buchstaben. Wir erhalten durch die Abbildung $f : D \to B$ mit

$$f_\alpha = f(\alpha) = b, \qquad f_\beta = f(\beta) = d, \qquad f_\gamma = f(\gamma) = b$$

einen Index von B über D.

Sei $D' = \{1, 2, 3, 4, 5\}$. Dann erhalten wir durch die Abbildung $f : D' \to B$ mit

$$f_1 = f(1) = a,\ f_2 = f(2) = d,\ f_3 = f(3) = b,\ f_4 = f(4) = c,\ f_5 = f(5) = d$$

einen Index von B über D'. ■

Wir wenden das Konzept von Indexmengen direkt an, um die Vereinigung und den Schnitt von beliebig vielen Mengen verkürzt aufschreiben zu können.

DEFINITION 1.72. Seien A und D beliebige Mengen und $B : D \to \mathcal{P}(A)$ ein Index auf der Potenzmenge, also der Menge aller Teilmengen von A. Dann bezeichnet

$$\bigcup_{i \in D} B_i = \{x \in A : \text{ es gibt ein } i \in I \text{ mit } x \in B_i\}$$

die Vereinigung aller Mengen in $(B_i)_{i \in I}$. Analog ist

$$\bigcap_{i \in D} B_i = \{x \in A : \text{ für alle } i \in I \text{ gilt } x \in B_i\}$$

der Durchschnitt aller Mengen in $(B_i)_{i \in I}$.

BEISPIEL 1.73. Betrachte die Menge $A = \{a, b, c, d, e, f, g, h\}$ und die Menge $I = \{1, 2, 3, 4\}$ mit dem Index $B : I \to A$ mit

$$B_1 = B(1) = \{a, b, c\}, \quad B_2 = B(2) = \{a, h\},$$
$$B_3 = B(3) = \{a, c, h\}, \quad B_4 = B(4) = \{c, h\}$$

Dann ist

$$\begin{aligned}\bigcup_{i \in I} B_i &= B_1 \cup B_2 \cup B_3 \cup B_4 \\ &= \{a, b, c\} \cup \{a, b, h\} \cup \{a, c, h\} \cup \{a, h\} = \{a, b, c, h\}\end{aligned}$$

$$\begin{aligned}\bigcap_{i \in I} B_i &= B_1 \cap B_2 \cap B_3 \cap B_4 \\ &= \{a, b, c\} \cap \{a, b, h\} \cap \{a, c, h\} \cap \{a, h\} = \{a\}.\end{aligned}$$

1.5 Beweise

Was versteht man unter dem Beweis einer mathematischen Aussage $\mathcal{A}$? Ein Beweis ist eine logisch nachvollziehbare Kette von Implikationen an deren Anfang Axiome - also Grundannahmen - und schon als wahr gezeigte Aussagen stehen und an deren Ende die Aussage $\mathcal{A}$ steht. Seien die Axiome und schon gezeigten Aussagen in der mathematischen Aussage $\mathcal{B}$ zusammengefasst sein. Ein Beweis zeigt also die Implikation $\mathcal{B} \implies \mathcal{A}$.

Wenn Axiome das Fundament und mathematische Aussagen die Bausteine des großen Bauwerks der Mathematik sind, so sind Beweise der Mörtel zwischen den Steinen. Axiome sind per Definition oder besser Konvention, wahr. Jede weitere Aussage muss als eine logische Schlussfolgerung, als eine Folge von Implikationen als wahr bewiesen werden. Das bedarf Kreativität, die Fähigkeit abstrakte Objekte zu sehen, zu durchdenken und tiefer zu begreifen, Zusammenhänge aufzudecken.

Beweisen zu lernen stellt viele Studenten zu Beginn ihrer Studien vor eine große Herausforderung. Es gibt zwei grundlegende Herausforderungen, das Nachvollziehen von Beweisen und das Führen von Beweisen. Zunächst erscheint jeder Beweis eine großes Kunstwerk zu sein, schleierhaft, wie ein Mensch solche verworrenen Gedankenstränge erdenken kann. Jede Aussage, ein völlig anderer Beweis. Und das macht ja durchaus Sinn, zwei unterschiedliche Aussagen erfordern unterschiedliche Beweisführungen. Doch bald entdeckt man, dass gewisse Muster, Tricks, Abkürzungen oder besser Methoden immer wieder auftauchen. Je schneller solche Kniffe erkannt werden, umso leichter fällt das Nachvollziehen von Beweisen. Man stellt fest, das logisches Denken eine Sprache ist, die man leichter spricht, je mehr man geübt hat.

Das Nachvollziehen von Beweisen ist ein erster Schritt, Beweise zu führen ein notwendiger zweiter. Nur so wird man sich darüber klar, ob man die Richtigkeit einer mathematischen Aussage auch wirklich verstanden hat. Die Herausforderung besteht darin, sich zunächst selbst mit Bleistift und Notizzettel bewaffnet einen Weg logischer Implikationen von den Voraussetzungen zur zu beweisenden Aussage zu bahnen. Wie oft gerät man dabei auf Holzwege, bleibt stecken und sieht keinen Ausweg, bestreitet unnötige Umwege, weil eine Abkürzung nicht entdeckt wird. Nachdem man einen Weg, eine Folge von Implikationen gebahnt hat, steht eine weitere Herausforderung ins Haus. Der Beweis muss zu Papier gebracht

werden. Das hat zwei gute Gründe und ist keine Schikane.

- Beim Aufschreiben eines Beweises fällt auf, ob man vielleicht eine Implikation zu leichtfertig gezogen, einen Spezialfall vergessen, etwas schlicht übersehen hat und so eine Lücke im Beweis noch zu schließen ist.
- Außerdem sollte der Beweis für eine unbeteiligte Person nachvollziehbar sein. Wir sollten uns ganz grundsätzlich im Leben häufiger der Kritik anderer aussetzen. Das hilft uns selbst zu allererst. Es ist kaum müßig zu erwähnen, dass dieser zweite Grund voraussetzt, dass ein Beweis leserlich notiert wird. Alle Gedanken, die für die Implikation wichtig sind sollen erwähnt, alle Variablen definiert, jede leicht zu übersehende Schlussfolgerung schriftlich gezogen werden. Dabei helfen Regeln eines guten Stils. Diesen zu erwerben bedarf Übung.

Dieses Buch führt viele Beweise auf, überspringen Sie diese nicht leichtfertig. Nur wer eine Sprache im Alltag spricht, beherrscht sie wirklich.

Zusammenfassend setzt die Fähigkeit zu beweisen Kreativität und Fingerfertigkeit voraus. Letztere holen sie sich, indem Sie üben, üben und üben. Wir werden nun einige Kniffe kennenlernen, die in Beweisen häufig auftreten. Im Laufe der Lektüre dieses Buches können Sie gerne in diesen Abschnitt zurückblättern und sich diese Methoden erneut in Erinnerung rufen.

Zum Schluss dieser einführenden Worte noch ein Hinweis an Informatiker, die sich vor Beweisen scheuen. Ein Informatiker ist häufig mit der Notwendigkeit von Beweisen konfrontiert. Selbst dann, wenn er nicht in der theoretischen Informatik tätig ist. In der Praxis stellt sich oft die Frage, ob ein Protokoll funktioniert, ein Algorithmus in erlebbarer Zeit selbst für leicht zu übersehende Spezialfälle die gewünschte Ausgabe liefert. Zudem werden praktische Probleme häufig in mathematische Modelle übersetzt. Dann profitieren Sie, als Informatiker, von der reichhaltigen mathematischen Theorie, die sich entfaltet und werden in den Genuss kommen, sichere Schlussfolgerungen für Ihre Implementierung zu ziehen, die sie ohne die Fähigkeit zu beweisen, mit großer Unsicherheit vage vermutet hätten.

1.5.1 Direkter und indirekter Beweis

Wir nehmen an, eine mathematische Aussage $\mathcal{A}$ sei zu zeigen. Der direkte Beweis nimmt die in $\mathcal{B}$ zusammengefassten Axiome und schon als wahr bewiesenen Aussagen und stellt eine Kette von Implikationen auf, die $\mathcal{A}$ implizieren.

Direkter Beweis.

$$\mathcal{B} \implies \mathcal{C}_1 \implies \mathcal{C}_2 \implies \ldots \implies \mathcal{C}_n \implies \mathcal{A}$$

BEISPIEL 1.77. Sei die mathematische Aussage

$$\mathcal{A} = [\text{Das Quadrat einer ungeraden natürlichen Zahl ist gerade.}]$$

zu beweisen.

Es gilt für eine ungerade Zahl $n \in \mathbb{N}$, dass man sie schreiben kann $n = 2 \cdot k + 1$ für eine natürliche Zahl $k \in \mathbb{N}$. Dann ist nach der 1. Binomischen Formel

$$n^2 = (2 \cdot k + 1)^2 = (2 \cdot k)^2 + 2 \cdot 2 \cdot k + 1^2 = 2 \cdot (2 \cdot k^2 + 2 \cdot k) + 1.$$

Da $k' = (2 \cdot k^2 + 2 \cdot k)$ wieder eine natürliche Zahl $k' \in \mathbb{N}$ ist, gilt $n^2 = 2 \cdot k' + 1$, also ist n^2 eine ungerade Zahl.

Formal notiert lautet dieser Beweis

$$\begin{aligned}
\mathcal{B} &\implies [\,[n \in \mathbb{N} \text{ ist ungerade }] \implies [\exists k \in \mathbb{N} : n = 2 \cdot k + 1] &&] = \mathcal{C}_1 \\
&\implies [\,[n \in \mathbb{N} \text{ ist ungerade }] \implies [\exists k \in \mathbb{N} : n^2 = (2 \cdot k)^2 + 4 \cdot k + 1^2]\,] = \mathcal{C}_2 \\
&\implies [\,[n \in \mathbb{N} \text{ ist ungerade }] \implies [\exists k' \in \mathbb{N} : n^2 = 2 \cdot k' + 1] &&] = \mathcal{C}_3 \\
&\implies [\,[n \in \mathbb{N} \text{ ist ungerade }] \implies [n^2 \text{ ist ungerade }] &&] = \mathcal{A}.
\end{aligned}$$

■

Das logische Prinzip hinter dem Beweisprinzip des indirekten Beweises haben wir schon in Bemerkung 1.14 beobachtet. Um zu zeigen, dass $\mathcal{B} \Rightarrow \mathcal{A}$ kann man auch zeigen, dass $\neg\mathcal{A} \Rightarrow \neg\mathcal{B}$.

Indirekter Beweis.

$$[\neg\mathcal{A} \implies \mathcal{C}_1 \implies \mathcal{C}_2 \implies \ldots \implies \mathcal{C}_n \implies \neg\mathcal{B}] \implies [\mathcal{B} \implies \mathcal{A}]$$

BEMERKUNG 1.78. In anderen Worten wird beim indirekten Beweis vorausgesetzt, dass $\mathcal{B}$ wahr ist. Dann negiert man die Aussage $\mathcal{A}$ zu $\neg\mathcal{A}$, setzt diese Aussage als wahr und schlussfolgert, dass die zu $\mathcal{B}$ negierte Aussage $\neg\mathcal{B}$ wahr ist - im Widerspruch zur Voraussetzung, dass $\mathcal{B}$ wahr ist. Also kann $\neg\mathcal{A}$ nicht wahr sein - also ist $\mathcal{A}$ wahr. Aus diesem Grund wird ein indirekter Beweis auch als *Widerspruchsbeweis* bezeichnet. ■

BEISPIEL 1.79. Sei die mathematische Aussage

$$\mathcal{A} = [\text{Es gibt keine bijektive Abbildung von } D = \{2, 3\} \text{ in die Menge } B = \{0\}]$$

BEISPIEL 1.82. Betrachte die Abbildung $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x - 2$. Wir möchten die Aussage beweisen, dass die Abbildung f eine Nullstelle hat.

Konstruktiver Beweis. Wir geben eine Nullstelle an mit $x_0 = 2$, denn man rechnet leicht nach, dass $f(x_0) = f(2) = x - 2 = 0$ ist.

Nicht-konstruktiver Beweis. Wir wissen, dass f eine stetige Funktion auf den reellen Zahlen ist. Stetig bedeutet anschaulich gesprochen, dass man den Funktionsgraphen zeichnen kann, ohne den Stift abzusetzen oder genauer, dass für zwei Werte y_1 und y_2 aus dem Bild von f auch das ganze Intervall $[y_1, y_2]$ im Bild von f liegt. Da die Funktion f an der Stelle $x_1 = 0$ negativ mit $y_1 = f(x_1) = 0 - 2 = -2$ und an der Stelle $x_2 = 10$ positiv mit $y_2 = f(x_2) = 10 - 2 = 8$ ist, liegt auch das ganze Intervall $[-2, 8]$ im Bild von f. Also gibt es ein x_0 mit $f(x_0) = 0 \in [-2, 8]$.

■

Fallunterscheidung

Manche Aussagen lassen sich in Fälle unterscheiden. Die zu beweisende Aussage muss dann für jeden Fall einzeln bewiesen werden. Was wie ein Nachteil klingt, ist ein Vorteil, denn für jeden dieser Fälle darf man eine weitere, den Fall charakterisierende Voraussetzung annehmen, die Beweise können dadurch leichter oder übersichtlicher werden. Wichtig ist dabei, dass jeder Fall der ursprünglichen Aussage abgedeckt wird, man die Aussage also nicht bloß für leichte Spezialfälle beweist. Man spricht dann auch von einer vollständigen Fallunterscheidung. Eine zu beweisende Aussage $\mathcal{A}$ wird dabei zu

$$\mathcal{A} \iff [\mathcal{A} \wedge \mathcal{F}_1] \vee \cdots \vee [\mathcal{A} \wedge \mathcal{F}_n]$$

für die n Fälle $\mathcal{F}_1, \ldots, \mathcal{F}_n$. Die einzelnen Fälle sind durch ein ODER miteinander verknüpft. Das führt auch dazu, dass die Fälle nicht zwangsläufig verschieden sein müssen, wichtig ist alleine, dass jeder Fall abgedeckt ist.

Vollständige Fallunterscheidung

$$[\mathcal{A} \wedge \mathcal{F}_1] \vee \cdots \vee [\mathcal{A} \wedge \mathcal{F}_n] \iff \mathcal{A}$$

BEMERKUNG 1.83. Mit der Formulierung **ohne Beschränkung der Allgemeinheit (o.B.d.A.)** wird zum Ausdruck gebracht, dass eine Einschränkung (zum Beispiel des Wertebereichs einer Variablen) nur zur Vereinfachung der Beweisführung vorausgesetzt wird (insbesondere zur Verringerung der Schreibarbeit), ohne dass die Gültigkeit der im Anschluss getroffenen Aussagen in Bezug auf die Allgemeinheit darunter leidet. Der Beweis wird nur für einen von mehreren möglichen Fällen geführt. Dies geschieht unter der Bedingung, dass die anderen Fälle in analoger

Weise bewiesen werden können (z.B. bei Symmetrie). Durch o.B.d.A. können auch triviale Sonderfälle ausgeschlossen werden. ■

Allbeweise

Mathematische Aussagen, die mit dem All-Quantor formuliert sind, lassen sich leicht widerlegen. Sei dazu die Aussage der Form $\mathcal{A} = [\forall x \in M : \mathcal{A}(x)]$ gegeben. Für jedes Element x der Menge M gelte also eine von x abhängige Aussage $\mathcal{A}(x)$. Um diese umfassende Aussage zu widerlegen, muss man nur ein einziges Objekt finden, welches die gewünschte Aussage $\mathcal{A}(x)$ nicht erfüllt.

Allbeweis durch ein Gegenbeispiel widerlegen

$$[\exists x \in M : \neg\mathcal{A}(x)] \implies \neg\mathcal{A}$$

BEISPIEL 1.84. Es sei folgende Aussage zu widerlegen. Alle Primzahlen (eine Zahl mit genau zwei Teilern in $\mathbb{N}$) sind ungerade. Es wäre sehr mühsam, alle Primzahlen zu überprüfen. Dies ist auch nicht nötig. Die Aussage lässt sich nämlich mit dem Gegenbeispiel 2 widerlegen. Die 2 hat zwei natürliche Teiler mit 1 und 2 und ist deshalb eine gerade Primzahl. ■

Mengenbeweise

Mathematische Aussagen über Mengen lassen sich häufig mit folgendem Ansatz beweisen. Es ist zu zeigen, dass eine Aussage für eine ganze Menge M gilt. Dann belegt man eine Variable x mit einem beliebigen Element aus der Menge M und zeigt für diese Variable die zu beweisende Aussage. Dabei hat x genau die Eigenschaften, welche die Elemente der Menge M eint. Die Aussage sollte dann also für jede Belegung der Variablen x mit einem Element aus der Menge M richtig sein.

Mengenbeweise

Wähle $x \in M$ beliebig und zeige die Aussage für x. Da x beliebig aus M gewählt war, gilt die Aussage für ganz M.

BEISPIEL 1.85. Es seien A und B zwei Mengen. Es ist die folgende Aussage zu zeigen. Es gilt $A \cap B \subset B \setminus (B \setminus A)$.

Sei dazu $x \in A \cap B$ beliebig gewählt. Dann ist $x \in A$ und $x \in B$. Also ist $x \notin B \setminus A$ und $x \in B$. Also ist $x \in B \setminus (B \setminus A)$. Da x beliebig gewählt war, gilt $A \cap B \subset B \setminus (B \setminus A)$. ■

Um Aussagen über Mengen zu beweisen, muss häufig die Gleichheit von zwei Mengen nachgewiesen werden. Die Mengen A und B sind gleich,

also $A = B$, wenn sie die gleichen Elemente enthalten. Wie zeigt man das? Ein üblicher Weg ist es, einfach die zwei Aussagen $A \subset B$ und $B \subset A$ zu zeigen, welche zusammengenommen äquivalent zur ursprünglichen Aussage sind. Wenn jedes Element aus A in B und umgekehrt jedes Element von B in A ist, dann sind die Mengen gleich, aber die „enthalten in"-Aussagen sind handlicher zu beweisen.

Mengengleichheit.

$$[A \subset B] \wedge [B \subset A] \implies [A = B]$$

Wenn man so vorgeht, dann schreibt man für die beiden *Richtungen* die Symbole „$\subset$" und „$\supset$". Man könnte diese Symbole lesen als ...

- ... „$\subset$" $\leftrightarrow$ „Wir Zeigen: $[A \subset B]$".
- ... „$\supset$" $\leftrightarrow$ „Wir Zeigen: $[B \subset A]$".

Diese Symbole sind also Abkürzungen und nicht als mathematische Symbole zu deuten.

BEISPIEL 1.86. Wir beweisen exemplarisch die erste der beiden als Distributivgesetze bezeichneten Gleichungen in Lemma 1.1. Zu zeigen ist

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Wir zeigen, dass die rechte Menge in der linken und die linke in der rechten Menge enthalten ist.

„$\subset$": Es sei $x \in (A \cap B) \cup C$ beliebig gewählt. Für x gilt dann:

$$\begin{aligned} & x \in (A \cap B) \cup C \\ \iff\ & [x \in (A \cap B) \vee x \in C] \\ \iff\ & [(x \in A \wedge x \in B) \vee x \in C] \end{aligned} \tag{1.1}$$

Es gibt nun zwei Fälle.

Fall 1 - $x \in C$. Es gilt demnach $x \in A \cup C$ und $x \in B \cup C$.

Fall 2 - $x \notin C$. Es folgen aus (1.1) demnach sofort $x \in A$ und $x \in B$. Damit gilt auch $x \in A \cup C$ und $x \in B \cup C$.

In beiden Fällen gilt also $x \in A \cup C$ und $x \in B \cup C$ und damit

$$x \in (A \cup C) \cap (B \cup C).$$

Da x beliebig gewählt war, gilt also allgemein für alle $x \in (A \cap B) \cup C$, dass

$$x \in (A \cap B) \cup C \qquad \implies \qquad x \in (A \cup C) \cap (B \cup C).$$

Damit gilt nach der Definition von „$\subset$" also $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$.

„⊃“: Es sei $x \in (A \cup C) \cap (B \cup C)$ beliebig gewählt. Für x gilt dann:

$$\begin{aligned} & x \in (A \cup C) && \cap && (B \cup C) \\ \iff & [x \in (A \cup C) && \wedge && x \in (B \cup C)] \\ \iff & [(x \in A \vee x \in C) && \wedge && (x \in B \vee x \in C)] \end{aligned} \tag{1.2}$$

Es gibt nun zwei Fälle.

Fall 1 - $x \in C$**.** Es folgt demnach $x \in (A \cap B) \cup C$. ✓

Fall 2 - $x \notin C$**.** Es folgen aus (1.2) demnach sofort $x \in A$ und $x \in B$ und damit $x \in (A \cup C) \cap (B \cup C)$. ✓

In beiden Fällen gilt also $x \in (A \cap B) \cup C$

Da x beliebig gewählt war, gilt also allgemein für alle $x \in (A \cup C) \cap (B \cup C)$, dass

$$x \in (A \cap B) \cup C \qquad \Leftarrow \qquad x \in (A \cup C) \cap (B \cup C).$$

Damit gilt nach der Definition von Teilmengen also

$$(A \cap B) \cup C \supset (A \cup C) \cap (B \cup C).$$

■

1.5.4 Vollständige Induktion

Die Beweismethode der **vollständigen Induktion** beruht auf dem Induktionsprinzip der natürlichen Zahlen, welches sich zur folgenden Aussage zusammenfassen lässt. Jede nicht-leere Menge natürlicher Zahlen enthält eine kleinste Zahl. Aus dieser Tatsache folgt das folgende Lemma.

LEMMA 1.87 (Induktionsprinzip). Angenommen, eine Menge $A \subset \mathbb{N}$ hat die beiden folgenden Eigenschaften.

i. $0 \in A$
ii. Wenn $0, \dots, n \in A$, dann gilt auch $n + 1 \in A$.

Dann gilt $A = \mathbb{N}$.

Beweis. Angenommen, es ist $A \neq \mathbb{N}$. Dann ist die Menge $B = \mathbb{N} \setminus A$ nicht leer. Folglich gibt es eine kleinste Zahl $x \in B$. Aufgrund von i. ist $x \neq 0$. Ferner gilt $0, \dots, x - 1 \in A$, weil x ja die kleinste Zahl in B ist. Nach ii. gilt also $x \in A$, im Widerspruch zu unserer Annahme, dass $x \in B$. ■

Das Induktionsprinzip ermöglicht es uns, Aussagen der Form $[\forall n \in \mathbb{N} : \mathcal{A}(n)]$ zu beweisen. Dabei geht man nach dem folgendem Schema vor.

i. Zeige, dass die Behauptung für $n = 0$ stimmt.

Summe der ersten $n+1$ vielen natürlichen Zahlen

$$\begin{aligned}\sum_{i=1}^{n+1} i &= (n+1) + \sum_{i=1}^{n} i \\ &= (n+1) + \frac{n(n+1)}{2} \qquad \text{[nach Induktionsannahme (1.3)]} \\ &= \frac{2n+2+n^2+n}{2} = \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$

wie behauptet. ■

1.5.5 Beweise - mehr als ein Weg führt nach Rom

In der Mathematik lassen sich Aussagen häufig auf unterschiedliche Weisen zeigen. Für den Satz des Pythagoras sind beispielsweise mehrere hundert verschiedene Beweise bekannt. Der Satz des Pythagoras ist damit übrigens der meist bewiesene mathematische Satz. Für das folgende Lemma ist ebenfalls mehr als ein Beweis bekannt.

LEMMA 1.90. Sei A eine endliche Menge mit Kardinalität n. Die Potenzmenge $\mathcal{P}(A)$ von A hat Kardinalität 2^n.

Man kann die Menge aller Teilmengen, also die Potenzmenge, mit einer zweiten Menge in Eins-zu-eins-Relation bringt. Der Trick besteht darin, dass dabei jedem Element aus der Potenzmenge genau ein Element aus der zweiten Menge und tatsächlich jedem Element aus der zweiten Menge auch ein Element der Potenzmenge zugeordnet wird. Folglich enthalten beide Mengen genau gleich viele Elemente. Die zweite Menge stellt sich dann schlussendlich als leicht zu zählen heraus.

Eine zweite Möglichkeit die Aussage zu zeigen, besteht in der Anwendung der vollständigen Induktion. Wir betrachten aus Übungszwecken beide Beweise.

Beweis. [von Lemma 1.90 - Variante 1] Sei A eine Menge mit n Elementen. Sei $\mathcal{W}_n$ die Menge aller „Wörter“ bestehend aus den Buchstaben i und d mit genau n Buchstaben.

Es sei f eine bijektive Abbildung der Elemente in A in die Menge der natürlichen Zahlen 1 bis n. Diese Abbildung ordnet die Elemente in A. Für jedes $a \in A$ existiert also eine eindeutiges $1 \leq j \leq n$, so dass $f(a) = j$.

Sei g eine Abbildung die jedem $B \in \mathcal{P}(A)$ das Wort $w \in \mathcal{W}_n$ zuordnet, so

dass für alle $a \in A$ gilt

- der $f(a)$-te Buchstabe von w ist i, wenn $a \in B$ und
- der $f(a)$-te Buchstabe von w ist d, wenn $a \notin B$.

Diese Abbildung ist bijektiv.

Surjektivität. Es ist zu zeigen, dass für jedes Wort $w \in \mathcal{W}_n$ sich eine Menge $B \in \mathcal{P}(A)$ finden lässt, so dass $g(B) = w$.
Formal schreibt sich das als $[\forall\, w \in \mathcal{W}_n\ \exists\, B \in \mathcal{P}(A) : g(B) = w]$.

Sei Q die Menge der Positionen von w, an welchen ein i steht. Sei $B = f^{-1}(Q)$. Es ist nun der $f(a)$-te Buchstabe von w ein i, wenn $a \in B$ und ein d, wenn $a \notin B$. Demnach wird B von g auf w abgebildet. ✔

Injektivität. Es ist zu zeigen, dass es keine zwei verschiedenen Mengen $B, B' \in \mathcal{P}(A)$ mit $g(B) = g(B')$ gibt. Formal schreibt sich das als $[\nexists B, B' \in \mathcal{P}(A) : [B \neq B' \wedge g(B) = g(B')]]$.

Angenommen, es gibt zwei verschiedene Mengen $B, B' \in \mathcal{P}(A)$, so dass $g(B) = g(B')$. Dann gibt es **ohne Beschränkung der Allgemeinheit** ein Element $a \in B$, dass nicht in B' enthalten ist (sonst wäre B eine Teilmenge von B' - aber beide Mengen sind verschieden und somit gäbe es dann ein Element $a \in B'$, dass nicht in B enthalten ist - Umbenennung der Mengen liefert die Behauptung). Dann ist aber der $f(a)$-te Buchstabe von $g(B)$ ein i und der $f(a)$-te Buchstabe von $g(B')$ ein d und somit ist $g(B) \neq g(B')$ - ein Widerspruch zu unserer Annahme. ✔

Wie wir schon bemerkten, haben zwei endliche Mengen genau dann die gleiche Kardinalität, wenn es eine bijektive Abbildung zwischen ihnen gibt.

Wir müssen also nur noch zählen, wie viele Wörter es mit den zwei Buchstaben d und i der Länge n gibt. Für jede der n Positionen gibt es zwei Möglichkeiten. Entweder steht dort ein i oder ein d. Insgesamt gibt es also 2^n unterschiedliche Wörter und somit hat die Potenzmenge einer endlichen Menge mit Kardinalität n selbst Kardinalität 2^n. ■

Beweis. [von Lemma 1.90 - Variante 2] Wir führen die Induktion über n.

Induktionsverankerung: Im Fall $n = 1$ ist die Aussage einfach zu prüfen. Die Potenzmenge besteht in diesem Fall aus den beiden Mengen $\emptyset$ und A selbst.

Induktionsannahme: Wir nehmen als Induktionsvoraussetzung an, dass

die Potenzmenge einer Menge mit n Elementen Kardinalität 2^n habe.

Induktionsschluss: Für den Induktionsschluss nehmen wir an A habe $n+1$ Elemente. Nun zeichnen wir ein Element $a \in A$ aus und betrachten die Menge $A' = A \setminus \{a\}$. Es gilt $|A'| = n$. Nach Induktionsvoraussetzung ist $|\mathcal{P}(A')| = 2^n$.

Wir beobachten, dass jede Teilmenge B von A entweder eine Teilmenge von A' ist oder das Element a enthält (in diesem Fall ist aber $B \setminus \{a\}$ eine Teilmenge von A'). Also können wir jeder Teilmenge $B \subset A$ genau eine Teilmenge von A' zuordnen, nämlich $B \setminus \{a\}$. Dabei wird jede Teilmenge von A' genau zwei Teilmengen von A zugeordnet. Es gibt also zweimal so viele Mengen in $\mathcal{P}(A)$ als in $\mathcal{P}(A')$. Demnach ist

$$|\mathcal{P}(A)| = |\mathcal{P}(A')| \cdot 2 = 2^n \cdot 2 = 2^{n+1},$$

was zu zeigen war. ■

1.6 Relationen

Ähnlich wie Abbildungen, sind Relationen ein universell einsetzbares Werkzeug. Dabei werden Objekte, die zwar nicht identisch sind, aber dennoch in Bezug zueinander stehen, einander zugeordnet. Der mathematische Begriff der Relation greift dieses „in (einem bestimmten) Bezug zueinander stehen“ auf. Er gibt für zwei Objekte entweder die Antwort „Ja, die beiden Objekte stehen in (diesem bestimmten) Bezug zueinander“ oder „Nein, die Objekte stehen nicht in (diesem bestimmten) Bezug zueinander“.

Man könnte zum Beispiel bei einer Menge von Gegenständen den Bezug „hat die gleiche Farbe“ herstellen. Dann stehen alle Gegenstände in diesem Bezug zueinander oder man sagt auch in Relation zueinander, wenn sie die gleiche Farbe haben. Mathematisch formal sauber ist eine Relation eine Sammlung von Paaren, die in Bezug zueinander stehen.

Definition 1.91. Eine **(binäre) Relation** zwischen zwei Mengen A und B ist eine Teilmenge $R \subset A \times B$. Im Falle $A = B$ spricht man von **einer Relation auf** A.

Eine Relation zwischen A und B ist also eine Teilmenge aller Tupel der

Form (a, b) mit $a \in A$ und $b \in B$. Ist ein Tupel (a, b) in einer Relation R enthalten, dann steht das Element a aus der Menge A und das Element b aus der Menge B in der Relation R zueinander.

Wir veranschaulichen den Begriff der Relation an den folgenden sehr unterschiedlichen Beispielen.

BEISPIEL 1.92. Der Operator $>$, in Worten „größer als“, erzeugt eine Relation auf der Menge der natürlichen Zahlen $\mathbb{N}$. Es ist

$$\begin{aligned} R &= \{(a, b) \in \mathbb{N} \times \mathbb{N} : a > b\} \\ &= \{(1, 0),\ \ (2, 0), (2, 1),\ \ (3, 0), (3, 1), (3, 2),\ \ (4, 0), \ldots\} \end{aligned}$$

■

BEISPIEL 1.93. Die Relation $=$, in Worten „ist gleich“, erzeugt ebenfalls eine Relation auf der Menge der natürlichen Zahlen $\mathbb{N}$. Es ist

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a = b\} = \{(0, 0), (1, 1), (2, 2), \ldots\}$$

■

BEISPIEL 1.94. Jede Abbildung ist eine Relation. Sie bringt Urbilder und Bilder in Relation zueinander. Die Tupel, bestehend je aus einem Element aus dem Definitionsbereich $x \in D$ und seinem Bild $f(x)$ einer Abbildung $f : D \to B$, bilden eine Relation zwischen den Mengen D und B. Es ist dann

$$R = \{(x, y) \in D \times B : y = f(x)\}.$$

Betrachten wir dazu die Abbildung $f : D \to B$ aus Beispiel 1.52 zwischen den Mengen $D = \{0, \frac{1}{2}, 1\}$ und $B = \{3, 7, 9, 10\}$ mit

$$0 \mapsto f(0) = 9, \quad \frac{1}{2} \mapsto f\left(\frac{1}{2}\right) = 8, \quad 1 \mapsto f(1) = 3$$

Dann ist die zugehörige Relation schlicht

$$R = \{(x, y) \in D \times B : y = f(x)\} = \left\{(0, 9), \left(\frac{1}{2}, 8\right), (1, 3)\right\}.$$

■

BEISPIEL 1.95. Ein auf den ersten Blick ungewöhnliches aber dennoch sehr einleuchtendes Beispiel bildet der Begriff „verwandt sein mit“, im Englischen *related to*. Er beschreibt eine Relation auf der Menge aller Menschen. ■

Ähnlich wie Abbildungen die grundlegenden Eigenschaften Injektivität, Surjektivität und Bijektivität haben, können Relationen reflexiv, symmetrisch und transitiv sein. Was wir darunter verstehen erklärt die folgende Definition.

Definition 1.96. Eine Relation auf einer Menge A heißt ...

- ... **reflexiv**, wenn für alle $a \in A$ gilt

$$(a, a) \in R.$$

- ... **symmetrisch**, wenn für alle $a, b \in A$ gilt

$$(a, b) \in R \Longrightarrow (b, a) \in R.$$

- ... **transitiv**, wenn für alle $a, b, c \in A$ gilt

$$(a, b) \in R \text{ und } (b, c) \in R \Longrightarrow (a, c) \in R.$$

Wir betrachten direkt einige Beispiel, die wir auf Reflexivität, Symmetrie und Transitivität hin untersuchen.

Beispiel 1.97. Die durch den Operator $>$ induzierte Relation auf den natürlichen Zahlen aus Beispiel 1.92 ist transitiv, aber nicht reflexiv oder symmetrisch.

Reflexivität. Es gilt sicherlich für keine natürliche Zahl $n \in \mathbb{N}$, dass $n > n$ ist. Es reicht allerdings dies nur für ein Element, beispielsweise die $7 \in \mathbb{N}$, zu zeigen. Es gilt nicht $7 > 7$.

Symmetrie. Gilt für zwei natürliche Zahlen $n_1, n_2 \in \mathbb{N}$, dass $n_1 > n_2$ ist, dann sicherlich nicht $n_2 > n_1$. Auch hier reicht es schon für zwei Elemente, zum Beispiel 7 und $9 \in \mathbb{N}$ zu zeigen, dass aus $9 > 7$ nicht $7 > 9$ folgt.

Transitivität. Gilt für drei natürliche Zahlen $n_1, n_2, n_3 \in \mathbb{N}$, dass $n_1 > n_2$ und $n_2 > n_3$ ist, dann auch $n_1 > n_3$. Zum Beispiel ist $9 > 7$ und $7 > 5$, also auch $9 > 5$. Hier ist es dann wichtig, dies für jede mögliche Auswahl von drei natürlichen Zahlen zu zeigen.

Beispiel 1.98. Die durch den Operator $=$ induzierte Relation auf den natürlichen Zahlen aus Beispiel 1.93 ist reflexiv, symmetrisch und transitiv.

Reflexivität. Es gilt sicherlich für jede natürliche Zahl $n \in \mathbb{N}$, dass $n = n$ ist.

Symmetrie. Gilt für zwei natürliche Zahlen $n_1, n_2 \in \mathbb{N}$, dass wenn $n_1 = n_2$ ist, dann sicherlich auch $n_2 = n_1$.

Transitivität. Gilt für drei natürliche Zahlen $n_1, n_2, n_3 \in \mathbb{N}$, dass $n_1 = n_2$ und $n_2 = n_3$ ist, dann auch $n_1 = n_3$.

Beispiel 1.99. Die Teilbarkeitsrelation $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \text{ teilt } b\}$ auf der Menge der natürlichen Zahlen ist reflexiv und transitiv, aber nicht symmetrisch.

Reflexivität. Jede natürliche Zahl teilt sich selbst.

Symmetrie. Gilt für zwei natürliche Zahlen $n_1, n_2 \in \mathbb{N}$, dass wenn n_1 die Zahl

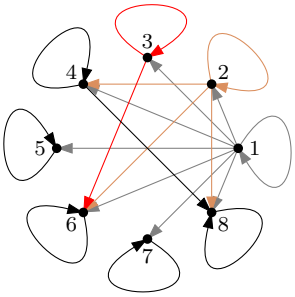


Abb. 1.12.
Die Relation aus Bemerkung 1.100 als gerichteter Graph.

n_2 teilt, dann muss n_2 nicht zwangsläufig n_1 teilen. Zum Beispiel teilt die 3 die 9, aber 9 ist kein Teiler von 3.

Transitivität. Gilt für drei natürliche Zahlen $n_1, n_2, n_3 \in \mathbb{N}$, dass n_1 die Zahl n_2 teilt und n_2 die Zahl n_3 teilt, dann teilt n_1 auch n_3.

BEMERKUNG 1.100. Für eine endliche Menge A kann man Relationen auf A durch einen gerichteten Graphen illustrieren.

Von einem Element $a \in A$ führt genau dann eine gerichtete Kante zu einem Element $b \in A$, wenn $(a, b) \in R$ ist. Der gerichtete Graph in Abbildung 1.12 zeigt den Graphen zur Teilbarkeitsrelation auf $\{1, \dots 8\}$. Konkret ist

$$R = \{(a, b) \in \{1, \dots, 8\} \times \{1, \dots, 8\} : \ a \text{ teilt } b\}$$

die dargestellte Relation.

1.6.1 Äquivalenzrelationen

Das Ziel bei der Verwendung von Äquivalenzrelationen ist, den Begriff „gleich“ (im Sinne von identisch) zu verallgemeinern auf „ähnlich“ bzw. „gleich bezüglich einer Eigenschaft“. Wir haben eingangs schon erwähnt, dass man unterschiedliche Gegenstände in Bezug auf ihre Farbe vergleichen kann.

Bei diesem Unterfangen helfen uns die drei schon kennengelernten Eigenschaften von Relationen. Um den Begriff „gleich“ auf „ähnlich“ zu verallgemeinern, müssen wir nämlich sicherstellen, dass für die Verallgemeinerung weiter gilt, dass ...

- ... ein Gegenstand stets zu sich selbst ähnlich ist. (Reflexivität)
- ... wenn a zu b ähnlich ist, dann auch b zu a. (Symmetrie)
- ... wenn a ähnlich ist zu b und dies wiederum ähnlich ist zu c, so ist auch a ähnlich zu c. (Transitivität)

DEFINITION 1.101. Eine Relation heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

Anmerkung. Die folgenden Argumente klingen sehr einfach, sind sie auch. Aber ohne sie geht's leider nicht. Sie sind ein sanfter Einstieg, für andere Relationen sind die Argumente anspruchsvoller. Da hilft der Rückblick auf diese leichten Argumente, um das Wesentliche der Beweise nicht aus den Augen zu verlieren.

Wir schauen uns einige Beispiele von Relationen an.

BEISPIEL 1.102. Es sei A die Menge aller Schüler einer Schule. Wir definieren die Relation

$$R = \{(a, b) \in A \times A : a \text{ ist in derselben Schulklasse wie } b\}.$$

Die Relation R ist eine Äquivalenzrelation. **Reflexivität.** Natürlich ist jeder Schüler $a \in A$ ein Schüler seiner (eigenen) Schulklasse, es gilt also $(a, a) \in R$.

Gegenstand c, der nicht die gleiche Farbe wie Gegenstand a hat, wird die Suche nach allen Gegenständen, welche die gleiche Farbe wie Gegenstand c haben, nicht einen einzigen Gegenstand finden, der die gleiche Farbe wie Gegenstand a hat.

In der formalen Sprache der Realtion übersetzt sich diese Einsicht zu der Aussage, dass zwei Elemente aus A bezüglich einer Äquivalenzrelation R auf A genau dann dieselbe Äquivalenzklasse haben, wenn sie bezüglich R äquivalent sind. Sind sie nicht äquivalent, dann sind ihre Äquivalenzklassen disjunkt.

LEMMA 1.113. Es sei R eine Äquivalenzrelation über einer Menge A. Für zwei Elemente $a, b \in A$ ist genau dann $[a]_R = [b]_R$, wenn $a \sim_R b$. Ist $a \not\sim_R b$, so gilt $[a]_R \cap [b]_R = \emptyset$.

Beweis. Es ist zunächst zu zeigen, dass für je zwei Elemente $a, b \in A$ genau dann $[a]_R = [b]_R$ ist, wenn $a \sim_R b$. Wir zeigen die beiden Richtungen dieser Äquivalenz.

"$\Longrightarrow$": Sei $[a]_R = [b]_R$ für zwei Elemente $a, b \in A$. Aufgrund der Reflexivität von R ist $(b, b) \in R$ und somit $b \in [b]_R$. Da $[a]_R = [b]_R$ ist, gilt auch $b \in [a]_R$. Also ist $(a, b) \in R$ und somit $a \sim_R b$.

"$\Longleftarrow$": Es gelte $a \sim_R b$ für zwei Elemente $a, b \in A$. Um die Mengengleichheit $[a]_R = [b]_R$ zu zeigen, zeigen wir die beiden Inklusionen $[a]_R \subset [b]_R$ und $[a]_R \supset [b]_R$.

„$\subset$" Sei $x \in [a]_R$ beliebig gewählt. Dann ist $(a, x) \in R$. Da $a \sim_R b$ ist auch $(a, b) \in R$: Da R eine Äquivalenzrelation ist, gilt $(a, b), (a, x) \in R \implies (b, a), (a, x) \in R \implies (b, x) \in R$, also ist $x \in [b]_R$. Da x beliebig aus $[a]_R$ gewählt war, gilt $[a]_R \subset [b]_R$.

„$\supset$" Diese Richtung zeigt man analog zu „$\subset$".

Es ist demnach $[a]_R = [b]_R$. Bleibt zu zeigen, dass für zwei Elemente $a, b \in A$ mit $a \not\sim_R b$ stets $[a]_R \cap [b]_R = \emptyset$ gilt.

Angenommen es gibt zwei Elemente $a, b \in A$ mit $a \not\sim_R b$, so dass $[a]_R \cap [b]_R \neq \emptyset$. Dann gibt es ein Element $x \in A$ mit $(a, x) \in R$ und $(b, x) \in R$. Dann ist aber aufgrund der Symmetrie von R auch $(x, b) \in R$ und aufgrund der Transitivität von R gilt dann auch $(a, b) \in R$. Also gilt dann $a \sim_R b$ - ein Widerspruch. Daher gilt $[a]_R \cap [b]_R = \emptyset$. ■

Aus Lemma 1.113 schließen wir, dass es genügt, ein *einziges* Element einer

Äquivalenzklasse zu kennen, um die Äquivalenzklasse zu rekonstruieren.

Definition 1.114. Es sei $M \subset A$ eine Äquivalenzklasse einer Äquivalenzrelation R auf einer Menge A. Ein Element $x \in M$ heißt **Vertreter** der Äquivalenzklasse M, denn es gilt $[x]_R = M$.

Bemerkung 1.115. Es ist wichtig darauf hinzuweisen, dass jedes Element einer Äquivalenklasse Vertreter dieser ist. Es gibt kein Element in einer Äquivalenklasse, dass „gleicher“ als die übrigen Elemente ist oder die Äquivalenzklasse besser oder eindeutiger vertritt. ■

Beispiel 1.116. Wir betrachten erneut die Äquivalenzrelation aus Beispiel 1.102. Es ist also A die Menge aller Schüler einer Schule und

$$R = \{(a,b) \in A \times A : a \text{ ist in derselben Schulklasse wie } b\}.$$

Es sei nun Josua ein Schüler der Schulklasse 5G. Alle Mitschüler aus der Schulklasse von Josua bilden die Äquivalenzklasse von Josua

$$\begin{aligned}[\text{Josua}]_R &= \{b \in A : (\text{Josua}, b) \in R\} \\ &= \{b \in A : b \text{ ist in derselben Schulklasse wie Josua}\} \\ &= \{\text{alle Schüler der 5G}\}.\end{aligned}$$

Jeder Schüler und jede Schülerin aus der 5G ist ein Vertreter seiner (Schul-)Klasse, denn anhand des einzelnen Schülers kann man natürlich die ganze Klasse ermitteln.

Ist Gideon auch in der 5G, also sind Josua und Gideon in derselben (Schul-)Klasse 5G, so gilt $[\text{Josua}]_R = [\text{Gideon}]_R$, denn

$$\begin{aligned}[\text{Gideon}]_R &= \{\text{alle Schüler in der Schulklasse von Gideon}\} \\ &= \{\text{alle Schüler der 5G}\} \\ &= [\text{Josua}]_R\end{aligned}$$

■

Beispiel 1.117. Wir betrachten ebenfalls erneut die Äquivalenzrelationen auf den natürlichen Zahlen aus Beispiel 1.103

$$R = \{(n,m) \in \mathbb{N} \times \mathbb{N} : m \text{ hat denselben Rest beim Teilen durch 2 wie } n\}$$

Die beiden Äquivalenzklassen von R sind

$$\begin{aligned}M_g &= \{2n \quad : n \in \mathbb{N}\} \quad \text{(alle geraden Zahlen)} \quad \text{und} \\ M_u &= \{2n+1 \quad : n \in \mathbb{N}\} \quad \text{(alle ungeraden Zahlen)}.\end{aligned}$$

Ein Vertreter von M_g ist $x = 6 \in M_g$ und es gilt tatsächlich $[6]_R = M_g$. ■

1.7 Aufgaben

MATHEMATISCHE AUSSAGENLOGIK.

1.1 Welche der folgenden Aussagen ist korrekt?

i. Es gibt mathematische Aussagen, die gleichzeitig wahr und falsch sind.
ii. Negiert man eine Aussage mit dem Allquantor $\forall$ tritt der Existenzquantor $\exists$ an seine Stelle.
iii. Impliziert eine Aussage $\mathcal{A}$ eine Aussage $\mathcal{B}$, so impliziert die Aussage $\mathcal{B}$ auch die Aussage $\mathcal{A}$.
iv. Sind zwei Aussagen $\mathcal{A}$ und $\mathcal{B}$ äquivalent, dann sind auch die jeweils negierten Aussagen $\neg\mathcal{A}$ und $\neg\mathcal{B}$ äquivalent.

1.2 Welche der Aussagen "$a^2 + b^2$", "$a^2 + b^2 = (a + b)^2$" und "18 ist durch 4 teilbar" ist eine mathematische Aussage.

1.3 Nennen Sie die Bausteine mathematischer Aussagen, die wir kennen gelernt haben.

1.4 Negieren Sie die Aussage $[\mathcal{A} \iff \mathcal{B}]$.

1.5 Gegeben sei die Aussage

$$\mathcal{A} = [n, m \in \mathbb{N} : n + m = 7].$$

Negieren Sie dies Aussage, also bilden sie $\neg\mathcal{A}$. Finden Sie dann alle Belegungen von n und m, so dass ...

i. ... $\mathcal{A}$ wahr ist.
ii. ... $\neg\mathcal{A}$ wahr ist.

1.6 Negieren Sie die Konjunktion und Disjunktion der beiden Aussagen $[n, m \in \mathbb{N} : n + m \geq 7]$ und $[n, m \in \mathbb{N} : n + m \leq 13]$.

Beachten Sie bei den folgenden Aufgaben, dass nicht danach gefragt wird, ob die genannten Aussagen wahr oder falsch sind.

1.7 Gegeben seien die Aussagen "Jede natürliche Zahl ist von der Form $n = k - 2$ mit einer natürlichen Zahl k" und "Es gibt eine natürliche Zahl n, so dass für jede natürliche Zahl k das Ergebnis von $n + k$ die Zahl 5 ist.".

i. Formulieren Sie diese sprachlichen Aussagen in symbolischer Notation.
ii. Negieren Sie die erhaltenen Aussagen in symbolischer Notation und vereinfachen Sie diese soweit Ihnen ersichtlich.

1.8 Gegeben seien die Aussagen $\mathcal{A} = [\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : n^2 = m + 3^2]$. Negieren Sie diese Aussage und vereinfachen Sie diese soweit Ihnen ersichtlich.

1.9 Ist die folgende Aussage wahr?

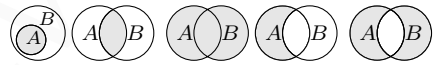
$$[x \in \mathbb{R} : x^2 = -2x - 1] \Leftrightarrow [x \in \mathbb{R} : (x + 1)^2 = 0]$$

MENGEN.

1.10 Welche der folgenden Aussagen ist korrekt?

i. Die Vereinigung zweier Mengen A und B hat stets eine größere Kardinalität als jeweils die Mengen A und B.
ii. Jede nicht-leere Menge hat mindestens zwei Teilmengen.
iii. Jede nicht-leere Menge A hat mindestens zwei Teilmengen, deren Vereinigung eine größerer Kardinalität hat als A.
iv. Jede nicht-leer Menge A hat mindestens zwei Teilmengen, deren Summe ihrer Kardinalitäten größer als die Kardinalität von A ist.

1.11 Es seinen A und B zwei Mengen. Zu welcher aus A und B gewonnenen Menge korrespondiert das jeweilige Venn-Diagramm?



1.12 Es seien die drei Mengen

$$A = \{3, 5, 7, 8, 10\}$$
$$B = \{1, 2, 3, 6, 7\}$$
$$C = \{3, 8\}$$

gegeben.

a) Gilt $A = B$, $A = C$ oder $B = C$?
b) Ist C eine Teilmenge von A oder B? Ist B eine Teilmenge von A?

c) Geben Sie die Vereinigung der Mengen A und C an.
d) Geben Sie den Schnitt der Mengen A und B an.
e) Geben Sie die Differenz $A \setminus B$ an.
f) Geben Sie die symmetrische Differenz von A und B.
g) Geben Sie drei unterschiedliche Partitionen von A an.

1.13 Erörtern Sie den Unterschied zwischen einer Menge, einer Multimenge und einem Tupel.

1.14 Es seien die Mengen $A = \{a, b\}$ und $B = \{x, y, z\}$ gegeben. Geben Sie das kartesische Produkt von A und B und die Potenzmenge von B an.

1.15 Es seinen A und B zwei endliche Mengen. Welche der beiden folgenden Mengen hat die größte Kardinalität? (Das kann auch in einer Fallunterscheidung von der Beschaffenheit von A und B abhängen.)

a) $A \cap B$ oder $B \cup A$?
b) $A \setminus B$ oder $B \setminus A$?
c) $A \setminus B$ oder $B \setminus A$?
d) $\mathcal{P}(A)$ oder $A \times B$?

1.16 Lassen Sie sich die aus den Mengen A, B und C gewonnenen Mengen aus Beispiel 1.30 mit den entsprechenden Sage-Befehlen ausgeben.

1.17 Zeigen Sie, dass für zwei Mengen A und B genau dann $A \cap B \neq \emptyset$ ist, wenn es eine Menge C gibt, die Teilmenge sowohl von A als auch von B ist.

1.18 Zeigen Sie, dass für Mengen A und B stets gilt, dass $A \cap B = B \Leftrightarrow B \subset A$.

1.19 Zeigen Sie, dass für Mengen A, B und C stets gilt, dass $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

1.20 Zeigen Sie, dass für Mengen A und B stets gilt, dass $A \setminus B = A \setminus (B \cap A)$.

1.21 Zeigen Sie, dass für Mengen A und B stets gilt, dass $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

ZAHLEN.

1.22 Welche der folgenden Aussagen ist korrekt?

i. Die Zahl $\frac{19}{34}$ ist eine reelle Zahl.
ii. Die Zahl $\frac{\pi}{34}$ ist eine rationale Zahl.

1.23 Können Sie eine Zahl finden, die zwar eine...

a) ...rationale aber keine ganze Zahl ist?
b) ...reelle aber keine rationale Zahl ist?
c) ...ganze aber keine reelle Zahl ist?

1.24 Zeigen Sie, dass $\sqrt{2}$ keine rationale Zahl ist.

ABBILDUNGEN.

1.25 Welche der folgenden Aussagen ist korrekt? Seien dazu die Mengen D, B und die Abbildung $f : D \to B$ gegeben.

i. Für jedes Element des Definitionsbereichs $x \in D$ gibt es eine Element des Bildbereichs $y \in B$, so dass $f(x) = y$ ist.
ii. Für jedes Element des Definitionsbereichs $x \in D$ gibt es eine Element des Bildbereichs $y \in B$, so dass $f(x) = y$ ist.
iii. Sei D' eine Teilmenge von D. Es gibt eine Restriktion von f auf D'.
iv. Die Abbildung f ist injektiv, wenn jedes Element $y \in B$ ein Urbild besitzt.
v. Die Abbildung f ist surjektiv, wenn je zwei verschiedenen Elemente des Definitionsbereichs unterschiedliche Bilder haben.
vi. Es gibt Abbildungen, die surjektiv aber nicht injektiv sind.
vii. Es gibt Abbildungen, die injektiv aber nicht surjektiv sind.
viii. Es gibt Abbildungen, die weder surjektiv noch injektiv sind.
ix. Es gibt Abbildungen, die bijektiv aber nicht surjektiv sind.
x. Es gibt Abbildungen, die bijektiv aber nicht injektiv sind.
xi. Jede Abbildung besitzt eine Umkehrabbildung.

1.26 Es seien die Mengen $D = \{1, 4, 6, 8, 10, 12\}$ und $B = \{3, 4, 5\}$ gegeben. Dann gibt es eine Abbildung $f : D \to B$ mit

$$1 \mapsto f(1) = 3, \quad 4 \mapsto f(4) = 4, \quad 6 \mapsto f(6) = 4,$$
$$8 \mapsto f(8) = 5, \quad 10 \mapsto f(10) = 4, \quad 12 \mapsto f(12) = 5.$$

a) Wie sieht die Menge $f^{-1}(4)$ aus.
b) Wie sieht die Menge $f^{-1}(\{4, 5\})$ aus.
c) Sei $D' = \{1, 6, 10\} \subset D$. Geben Sie die Restriktion $f|_{D'}$ von f auf die Menge D' an.

1.27 Es sei $f : \mathbb{R} \to \mathbb{R}$ eine Abbildung mit $x \mapsto x^2 + 3x$. Ist die Abbildung f injektiv, surjektiv

und/oder bijektiv?

1.28 Es sei $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ mit $x \mapsto x^2$ eine Abbildung. Ist die Abbildung f surjektiv, injektiv und/oder bijektiv?

1.29 Es sei $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit $x \mapsto \frac{1}{x}$ eine Abbildung. Ist die Abbildung f surjektiv, injektiv und/oder bijektiv?

1.30 Es seien A und B endliche Mengen. Zeigen Sie, dass genau dann eine bijektive Abbildung $f : A \to B$ existiert, wenn $|A| = |B|$ ist.

1.31 Seien mit X und Y zwei nicht-leere Mengen und zwei Abbildungen $f : X \to Y$ und $g : Y \to X$ gegeben mit $g \circ f = \mathrm{id}_X$. Zeigen Sie, dass f injektiv und g surjektiv ist.

1.32 Es seien A und B endliche Mengen. Zeigen Sie, dass eine injektive Abbildung $f : A \to B$ genau dann surjektiv ist, wenn $|A| = |B|$ ist.

1.33 Beweisen Sie Lemma 1.68, also dass für eine bijektive Abbildung $f : D \to B$ gilt

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_D.$$

BEWEISE.

1.34 Welche der folgenden Aussagen ist korrekt?

i. Man kann eine mathematische Aussage $\mathcal{A}$ über direkte oder indirekte Beweise beweisen, wobei der indirekte Beweis, der direkte Beweis von $\neg\mathcal{A}$ ist.
ii. Bei einem Äquivalenzbeweis sind zwei Implikationen zu zeigen.
iii. Man kann jede mathematische Aussage auch mittels vollständiger Induktion beweisen.
iv. Für jede wahre mathematische Aussage gibt es einen eindeutigen korrekten Beweis.

1.35 Nennen Sie die vier „Bestandteile“ der vollständigen Induktion.

1.36 Beweisen Sie die folgende Aussage per vollständiger Induktion.

$$\sum_{k=1}^{n} (2k-1) = n^2 \qquad \text{für alle } n \in \mathbb{N}.$$

1.37 Zeigen Sie die folgende Aussage per vollständiger Induktion

$$\sum_{k=1}^{n} \binom{n}{k}^2 = \binom{2n}{k} \qquad \text{für alle } n \in \mathbb{N}.$$

1.38 Beweisen Sie die folgende Aussage per vollständiger Induktion.

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{für alle } n \in \mathbb{N}.$$

1.39 Zeigen Sie, dass eine endliche nicht-leere Menge genauso viele Teilmengen mit einer geraden Kardinalität wie Teilmengen mit einer ungeraden Kardinalität hat.

RELATIONEN.

1.40 Welche der folgenden Aussagen ist korrekt?

i. Eine Relation auf einer Menge M ist eine Teilmenge des kartesischen Produkts $M \times M$.
ii. Eine Reflexive Relation auf einer Menge M besitzt eine Umkehrabbildung.
iii. Die durch den Operator $<$ - in Worten „kleiner als“ - auf den ganzen Zahlen ist eine Relation.
iv. Die $<$-Relation ist reflexiv, aber nicht bijektiv.
v. Jede Äquivalenzrelation ist symmetrisch.
vi. Die Menge der Äquivalenzklassen einer Äquivalenzrelation auf einer Menge M ist eine Partition der Menge M.
vii. Jedes Element einer Menge M ist Vertreter einer Äquivalenzklasse einer Äquivalenzrelation auf M.

1.41 Es sei durch $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a|b\}$ eine Relation auf $\mathbb{Z}$ definiert. Ist R symmetrisch, reflexiv oder transitiv?

1.42 Sei $\mathcal{K}$ die Mengen aller Kreise in der Ebene $\mathbb{R}^2$. Es sei durch $R_C = \{(a, b) \in \mathcal{K} \times \mathcal{K} : a \text{ schneidet } b\}$ eine Relation auf $\mathcal{K}$ definiert. Ist $\mathbb{R}_C$ reflexiv, symmetrisch und/oder transitiv?

1.43 Es sei durch $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 6|a - b\}$ eine Relation auf $\mathbb{Z}$ definiert.

i. Zeigen Sie, dass R eine Äquivalenzrelation ist.
ii. Wie sehen die Äquivalenzklassen von R aus?
iii. Nenne Sie für jede Äquivalenzklasse zwei unterschiedliche Vertreter.

1.44 Sei die Menge $A = \{1, 2, 3\}$ gegeben.

i. Finden Sie eine Äquivalenzrelation auf A und geben Sie deren Äquivalenzklassen an.
ii. Wie viele Äquivalenzrelationen gibt es auf A insgesamt?

1.45 Sei A eine endliche Menge und $f : A \times A \to \{0, 1\}$ eine beliebige Abbildung. Es definiert $f^{-1}(1) \subset A \times A$ eine Relation R auf A. Schreiben Sie ein Sage-Programm, welches mithilfe einer gegebenen Implementierung von f in Sage als Funktion `f(a,b)` für zwei Elemente a, b A prüft, ob R eine Äquivalenzrelation ist.