Mathematik für das Lehramt an der Grund- und Mittelstufe sowie an Sonderschulen
Teil I: WiSe 06/07
Teil II: SoSe 07

Bodo Werner
mailto:werner@math.uni-hamburg.de

22. Juli 2012

Inhaltsverzeichnis

Teil I

Grundlagen

Kapitel 1

Vorbemerkungen

1.1 Desillusionierung

Es tut mir leid, dass ich mit etwas Negativem beginne. Es ist aber sehr wichtig, hier von Anfang an für Klarheit zu sorgen.

Viele StudentInnen glauben, sie bräuchten im Laufe ihres Studiums nur so viel Mathematik zu lernen, wie sie in der Schule benötigen. Möglichst soll sie sich sogar auf die Grundschulmathematik beschränken. Das ist eine **Illusion**.

Die Prüfungsordnung sieht 40 SWS Fachwissenschaft Mathematik vor - mehr als die IngenieurstudentInnen an der TU Harburg.

Aber keine Angst: Das Staatsexamen und die vorangehende Zwischenprüfung verlangen von Ihnen im Stoffumfang erheblich weniger als von den IngenieurstudentInnen. Dafür wird von Ihnen mathematisches Denkvermögen in den vermittelten mathematischen Strukturen, die durchaus schulbezogen sind, verlangt. Das wird für alle diejenigen von Ihnen, die sich hier einen leichten Gang erhoffen, ein **Schock** sein. Für die anderen wird das Mathematikstudium jedoch nicht nur Anstrengung, sondern auch Befriedigung und Freude bereiten. Lassen Sie sich auf das Abenteuer Mathematik ein!!

1.2 Ziele

In Teil I des Skripts möchte ich die *Grundlagen der Mathematik* vermitteln, mit denen Sie zum Teil schon in der Schule konfrontiert wurden und die die grundlegenden Begriffe und Konzepte der Mathematik darstellen. Hierunter verstehe ich *Zahlen, Mengen, Relationen, Funktionen, vollständige Induktion, Kombinatorik, Gruppen* und *Aussagenlogik*. Auf diesen Grundlagen bauen die nachfolgenden Teile auf.

Mathematische Sprache und ihre Vokabeln

Die mit diesen Grundlagen verbundenen Begriffe (z.B. **irrationale Zahl, modulo, Vereinigung, Mengendifferenz, Verkettung von Abbildungen, Funktionsgraph, leere Menge, kartesisches Produkt,....**) sind für Sie z.T. nicht neu, müssen aber wie Basis-**Vokabeln** der **mathematischen Sprache** gelernt und *verstanden* werden. Mit diesen (und vielen weiteren) Vokabeln wird später immer wieder umgegangen, d.h. sie fließen permanent in die Argumente und in die Erklärungen ein, auch in Ihre schriftlichen Hausarbeiten. Ich schätze, dass in jeder Vorlesung etwa zehn neue mathematische Begriffe geprägt werden.

Sie werden daher schnell frustriert sein, wenn Sie diese „Vokabeln“ nicht beherrschen. Daher müssen Sie diese lernen, stets mit einem nicht unerheblichen Anteil von *Auswendiglernen*, aber auch verbunden mit einem gewissen Verständnis für das Umfeld, in dem dieser Begriff auftaucht.

Ich empfehle daher, ein chronologisches *Vokabelheft* anzulegen, in das Sie den jeweiligen neuen Begriff, seine Bedeutung (Definition) und Beispiele für Aussagen schreiben, in denen dieser Begriff in einem erkennbaren Zusammenhang vorkommt. Diese Empfehlung gilt nicht nur für den Grundlagenteil, sondern für den gesamten Vorlesungszyklus. Wenn Sie später Probleme bekommen und sich bei mir Rat holen, ist die Vorlage Ihres Vokabelhefts die beste Gewähr, dass ich mit für Sie Zeit nehme.

Die mathematische Sprache dient auch der sprachlichen Erläuterung von Schemata, von Algorithmen oder einfach von Sachverhalten (was versteht man unter der Kreiszahl π?). Aber auch bei der Formulierung von *Ideen* bei der kreativen Lösung von Problemen ist die mathematische Sprache unerlässlich.

Die mathematische Fachsprache setzt die deutsche Sprache voraus. Bei jedem Satz muss es Objekt und Prädikat geben, auch Satzzeichen sind notwendig.

Für diejenigen unter Ihnen, für die Deutsch nicht die Muttersprache ist: Als LehrerIn ist es unerlässlich, dass Sie die deutsche Sprache beherrschen. Wir werden von der Behörde angehalten, dies bei den Prüfungen mit zu berücksichtigen.

Anbindung an die Schulmathematik

Ich strebe eine enge Anlehnung an die Schulmathematik an, aus einer etwas anderen Position – in dem Sinne, dass *sprachliche Präzision*, auch, aber nicht ausschließlich, demonstriert an *Beweistechniken*, sowie der *Anwendungsbezug* zu unserer Umwelt und unserem Alltag stärker betont werden als in der Schule. Dabei sollen – wo immer möglich – auch Grundschulbezüge hergestellt werden. Ziel wird es sein, dass Sie am Ende des Vorlesungszyklus das gesamte Spektrum der Schulmathematik sicher beherrschen und darüber hinaus Einblick genommen haben in einige Aspekte der Fachwissenschaft Mathematik. Immer dann, wenn Sie Wissenslücken in Ihrer Schulmathematik entdecken: Füllen Sie sie umgehend!

Anwendungsbezug

Wie schon gesagt, sollen diejenigen Bereiche der Mathematik, die etwas mit der unmittelbaren Bedeutung im Alltag zu tun haben, mit denen wir z.B. über die Medien konfrontiert werden (Exponentielles Wachstum, Hochrechnungen, Risikoüberlegungen, quantitative Angaben jeder Art inkl. ihrer grafischen Veranschaulichung, Stichproben von Statistiken, u.a.) in den jeweiligen Kontext eingeordnet werden.

Brain Gym

Mathematik betreiben ist auch ein Gehirntraining. Sie lernen *logisches Denken*. Hoffentlich. Der in Ihrem Gehirn ablaufende Denkprozess soll von mir angeregt werden, bedarf aber Ihrerseits auch der Bereitschaft zur *Anstrengung*. Wie jede Gymnastik. Wo immer es geht, möchte ich Sie zu eigenständigem mathematischen Denken bewegen. Der Mathematikunterricht heutzutage scheint mir zu sehr auf das Training von Techniken ausgerichtet zu sein als auf ein anspruchsvolles Denktraining.

Gedächtnis

Dabei darf man eines aber nicht verkennen: eine ganz wesentliche Rolle spielt das Gedächtnis, sowohl das kurzfristige als auch das langfristige. Ersteres besonders bei Kopfrechenaufgaben, wenn man Zwischenergebnisse „abspeichern“ und wieder hervorzaubern muss. Auch bei Termumformungen spielt dies eine Rolle. Wer sieht z.B. sofort, dass

$$(a-b)^2+(a+b)^2=2(a^2+b^2)?$$

Bei diesem Beispiel spielt nicht nur das kurzfristige Gedächtnis eine Rolle, sondern auch das langfristige, das in diesem Fall die *binomischen Formeln* (z.B. $(a+b)^2=a^2+2ab+b^2$) bereit halten muss. Um Lernerfolge zu haben, müssen Sie Ihr *Gedächtnis* systematisch trainieren. Wie ich auch in meinem zunehmenden Alter. Scheuen Sie sich nicht, *auswendig zu lernen*. Meine Testklausuren, die ich regelmäßig einstreuen werde, werden in aller erster Linie überprüfen, ob Sie ausreichend (auswendig) gelernt haben.

Allgemeinbildung

Ich lege sehr viel Wert auf mathematische Allgemeinbildung, vor allem solche, die außerhalb mathematischer Expertenkreise mit Mathematik verbunden ist. Z.B.

- Was ist die Quadratur des Kreises?
- Was ist der Goldene Schnitt?
- Was ist exponentielles Wachstum?

- Wie kommt es zur Kalenderrechnung (Schaltjahre)?
- Was ist das Geheimnisvolle an Primzahlen? Wieso spielen sie in der Verschlüsselung von Botschaften eine Rolle?
- Warum kommen so häufig 2er-Potenzen (256, 512, 1024) in der Computertechnik vor?
- Was versteht man unter Zufall und Wahrscheinlichkeit?
- Was sind die wesentlichen Aspekte der beschreibenden Statistik?

Diese Allgemeinbildung werde ich, wo immer sinnvoll, ansprechen und versuchen, sie Ihnen zu vermitteln. Nach Möglichkeit wird auch eine *historische Einbindung* erfolgen.

Was sollten Sie mitbringen?

Natürlich gibt es auch eine gewisse Allgemeinbildung in Mathematik, deren Vorhandensein ich hier voraussetze, etwa die Unterscheidung zwischen Gradmaß und Bogenmaß bei Winkeln, die Definition und grundlegenden Eigenschaften von trigonometrischen Funktionen, Kenntnisse über Koordinatensysteme, Rechentechniken für Dezimalzahlen, Bruchrechnung, quadratische Gleichungen, Schaubilder von Funktionen mit Hoch- und Tiefpunkten, geometrische Konzepte (Dreieck, Kreis, Parallelogramm.....), kurz, alles, was zum „Kerncurriculum“ der Mathematik an den verschiedenen Schulstufen – bishin zur Oberstufe – zählt.
Ein Teil dieser Allgemeinbildung bezieht sich auf *Techniken* wie Umgehen mit mathematischen Termen, z.B. auf binomische Formeln, Rechnen mit Brüchen, Lösen von Gleichungen, Beherrschung von Potenzgesetzen. Wenn Sie hier Defizite haben, sollten Sie *jede* Möglichkeit ergreifen, diese zu beheben.
Vielleicht wichtiger als reine Vorkenntnisse sind „Sekundärfähigkeiten“ wie *Konzentrationsfähigkeit*, die *Fähigkeit zuzuhören* und vor allem *Geduld*. Sie werden selten auf Anhieb alles verstehen. Die Vorlesung und das Skript geben einen Anstoß, mehr nicht. Den Rest müssen Sie durch *Gedankenarbeit* leisten, d.h. es ist eine *Anstrengung* Ihrerseits erforderlich. Hierzu bedarf es auch *geistiger Kondition*, die man durch tägliches Üben verbessern kann – wie auch im Sport z.B. im Langstreckenlauf.

1.3 Inhalte

In dem Vorlesungszyklus Mathe I-IV werden die folgenden Themenblöcke laut dem vereinbarten Kerncurriculum vom März 2003 zur Sprache kommen:

- Grundlagen (Mengen, Abbildungen, Relationen, Zahlen, Kombinatorik, Verknüpfungen, Gruppen, Körper)
- Lineare Algebra (Vektoren und lineare Abbildungen)

- Analysis (Reelle Folgen, Grenzwerte, Reihen, Reelle Funktionen)
- Elementare Zahlentheorie
- Stochastik
- Geometrie
- Mathematische Modelle

Einige Themenblöcke werden in den aufbauenden Vorlesungen und Proseminaren vertieft. Die Geometrie wird bei mir nur rudimentär angesprochen. Die Blöcke werden sich zum Teil durchdringen.

1.4 Didaktik der Mathematik

Ein besonderes Augenmerk werde ich auch auf die Didaktik der Mathematik legen. Obwohl ich hier hierzu unerfahren bin, werde ich hierzu hin und wieder etwas einzubringen versuchen.
Eines habe ich schon gelernt: Bei uns allen, auch Ihren späteren Schülern, gibt es zwei Grundformen logischen Denkens, das *prädidative Denken*, das auf die Analyse von Beziehungen und Strukturen, d.h. auf Gesetzmäßigkeiten ausgerichtet ist, und das *funktionale Denken*, das sich auf die Organisation von Handlungsfolgen (Schemata!) und auf die Analyse von Wirkungsweisen bezieht[1].

1.5 Zwischenprüfung

Die Zwischenprüfung nach Mathe I-II bezieht sich i.W. auf die ersten beiden Themenblöcke – etwas angereichert in dem eben genannten Sinne durch Stochastik und Mathematische Modelle. Sie wird voraussichtlich in der Woche 10.-15.9.07 stattfinden. Wer hier verhindert ist oder nicht besteht, wird von mir eine zweite Chance erhalten - voraussichtlich Mitte Februar 2008.

1.6 Übungen

Neben den beiden wöchentlichen 2-stündigen Vorlesungen am Di und Fr 8.30-10.00 Uhr finden dienstags 5 Übungsgruppen statt (2-stündig), drei von 10.15-11.45 Uhr und zwei von 12.00-13.30 Uhr. Diese Übungsgruppen werden zur Hälfte von Dozenten (Herr Strade – 2 Gruppen und ich – 3 Gruppen) und von studentischen TutorInnen (Lena Sebastian, Marcel Biskup, Nicole Beisiegel, Julia Mohr und Stephanie Eller) durchgeführt. Im Dozententeil wird der Stoff der Vorlesungen in der Woche zuvor wieder aufgegriffen, hier können Verständnisprobleme zur

[1] Hefendehl-Hebeker, 2003, DMV-Jahresbericht

Sprache kommen. Jede Woche werden ca. 4 Übungsaufgaben gestellt, die eine Woche später abgegeben werden sollen. In dem Tutorenteil werden einige dieser Übungsaufgaben besprochen und von StudentInnen vorgetragen.
Die Aufteilung auf die Übungsgruppen wird am ersten Vorlesungstag, dem 24.10.06 vorgenommen.

1.7 Scheine

Zu jeder der vier Vorlesungen Mathe I-IV kann ein Übungsschein erworben werden. Drei von ihnen schreibt die Prüfungsordnung vor. Wöchentlich werden Aufgaben gestellt, die in Gruppen bis zu drei Personen eine Woche später abgegeben und korrigiert werden. Dabei werden Punkte vergeben. Ferner werden in regelmäßigen Abständen innerhalb der Vorlesung 30-minütige individuelle *Testklausuren* geschrieben (etwa 3 pro Semester), die ebenfalls mit Punkten bewertet werden. In der letzten Semesterwoche gibt es eine 90-minütige Klausur, die den Schwierigkeitsgrad von Zwischenprüfungsaufgaben hat.
Ein Übungsschein erhält, wer in *beiden* Bewertungen (Klausuren und Übungsaufgaben) 50% der Punkte erhält. Dabei muss gewährleistet sein, dass bei Übungsgruppen, die zwei oder drei Personen umfassen, jede Person angemessen zu den Lösungen beiträgt. Dies wird in den Übungsgruppen oder bei nicht regelmäßiger Teilnahme an den Übungen durch ein Gespräch mit Herrn Strade oder mir überprüft.
Diese Kriterien sind so bemessen, dass Abwesenheiten wegen Krankheit oder anderer Gründe aufgefangen werden können.

1.8 Anforderungen

Interesse und zeitlicher Aufwand

Von Ihnen erwarte ich zwei Dinge: *Interesse an Mathematik* und *intensives Bemühen*. Letzteres bedeutet für je eine (4V+2Ü)-Lehrveranstaltung einen *zeitlichen Aufwand* von etwa 200 Zeitstunden Vor-, Nachbereitungs- und Durchführungszeit während eines Semesters. Sie werden sich wahrscheinlich ein anderes Fach als Mathematik wählen müssen, wenn Sie diese Zeit nicht aufbringen wollen – etwa dem verführerischen Motto folgend, dass Sie in der Grund- oder Sonderschule doch mit viel weniger Mathematik auskommen. Bei mir werden Sie mit dieser Haltung aber weder Scheine machen noch Prüfungen bestehen. Mein Ziel ist es, Sie zu einer kompetenten MathematikerIn auszubilden, die die Schulmathematik wirklich durchschaut, selbst Mathematik betreiben kann und – das ist das Wesentlichste – SchülerInnen für die Mathematik begeistern kann. Ich weiß, dass es einen scheinbaren Widerspruch gibt zwischen dem Ziel, Sie für Mathematik zu begeistern, und dem gleichzeitig auf Sie ausgeübten Leistungsdruck. Nach vielen Jahren Erfahrung weiß ich, dass in aller Regel (nicht alle Menschen sind gleich) ersteres nicht ohne letzteres geht.

Die Frage Warum?

Interesse an Mathematik bedeutet, dass Sie an einer Antwort auf eine Frage „Warum?“ interessiert sind. Wenn es Ihnen vollständig wurscht ist, warum die von C.F. Gauss (1777-1855) erfundenen komplexen Zahlen, angeführt durch die imaginäre Einheit $i := \sqrt{-1}$, eine fundamentale Rolle in der Mathematik spielen oder warum Tests auf die Wirksamkeit von Medikamenten ohne die Normalverteilung nicht durchgeführt werden können oder was Wachstumsraten mit dem Ableitungsbegriff zu tun haben, werden Sie schwerlich motivierbar sein. Neugierde ist die Voraussetzung alles wissenschaftlichen Tuns - Sie sollen hier einen kleinen Einblick in die Wissenschaft Mathematik bekommen. Aber nicht resignieren: Wenn dieses Interesse nicht von vornherein da ist, kann es noch kommen. Lassen Sie sich auf das „Abenteuer Mathematik“ ein.

Welche Rolle spielt Begabung und Vorwissen?

Natürlich bedarf es bei Ihnen auch einer gewissen Begabung für Mathematik, die durch Interesse alleine noch nicht gewährleistet ist. Es ist z.B. bekannt, dass manche Schüler mit dem Umgehen mit Variablen, Unbekannten oder Platzhaltern in algebraischen Ausdrücken Probleme haben. Wer z.B. bei einem Funktionsausdruck $f(x) = x^2$ sehr wohl $f(2) = 4$ rechnen kann, aber mit $f(a+3)$ $(= (a+3)^2 = a^2 + 6a + 9)$ nichts anfangen kann, oder wer zwar die Gleichung $2x + 3 = 4 - x$, aber nicht die Gleichung $ax + b = c - dx$ nach x auflösen kann, oder wer mit der Aussage, dass $g(x) := \sqrt{x}$ die Umkehrfunktion von $f(x) = x^2$ ist, partout nichts anfangen kann, wird hier Probleme bekommen. Überhaupt wird es schon von Bedeutung sein, was Sie in der Schule an Mathematik gelernt haben. Sie haben jedoch die Chance, bestehende Mängel auszugleichen. Aber, wenn diese Schwächen ganz prinzipieller Art sind, die schon in der Mittelstufe lokalisiert sind, sehe ich schwarz. Dann kann die Konsequenz nur sein, dass Sie dies frühzeitig bemerken und das Fach wechseln.

1.9 Skript und Unterrichtsstil

Es wird ein Skript in Form einer PDF-Datei geben, dessen aktuelle Version man im Internet findet.
Zum Lesen benötigt man den *Acrobat-Reader* – i.a. genügt ein „Doppelklick“, um eine solche PDF-Datei zu öffnen, da der Acrobat-Reader i.a. schon installiert ist. Wenn Sie zu Hause nicht über einen Internetzugang verfügen, können Sie mit Hilfe einer Kennung, die Sie von mir bekommen, unsere PC-Pools benutzen.

Mein Skript enthält eine Reihe von **Links** auf andere WWW-Seiten, die ich in meine Vorlesungen mit nutze und auf die sich auch Übungsaufgaben beziehen können. Es ist also unbedingt notwendig, dass Sie sich eine gewisse Fähigkeit im Umgang mit Computern und dem Internet aneignen. Diese Fähigkeit ist ja sowieso ein Muss für zukünftige LehrerInnen.

Eines der wichtigsten Links ist der zu Mathe Online Wien. Hier können Sie z.T. spielerisch (Schul-)Mathematik lernen!
Aber auch der historische Hintergrund kann interessant sein. Häufig werden Begriffe und Sätze mit den Namen von Mathematiker/innen verbunden. Wenn Sie mehr über deren Wirken wissen wollen, so benutzen Sie den Link auf Indexes of Biographies (University of St. Andrews - Schottland).

Die **fett** gedruckten Worte in dem Skript kennzeichnen meist *neue Begriffe*, die in dem Umfeld dieses Wortes *definiert* werden. Zuweilen wird die Definition eines besonders wichtigen Begriffs durch einen eigenständigen, mit **Definition** beginnenden Absatz vorgenommen. In jedem Fall handelt es sich um wichtige *Vokabeln*, deren Bedeutung Sie lernen sollten!
Wichtige mathematische Aussagen werden mit **Satz** eingeleitet und nach dem Wörtchen **Beweis:** bewiesen.

1.10 Menschliches

Sie werden nicht immer mit mir und meiner Vorlesung zufrieden sein. Meine Bitte: Geben Sie mir Rückkopplung! Wenn ich zu schnell bin, wenn man mein Tafelbild nicht lesen kann, wenn Übungsaufgaben unverständlich sind, wenn Sie etwas partout nicht verstanden haben. Fragen Sie auch in den Vorlesungen nach!
Ich werde Sie ernst nehmen, auch wenn Sie nicht zu den „Cracks“ gehören. Ich werde versuchen, in meinem Rahmen und in meinen Möglichkeiten auf Ihre Probleme einzugehen. Sie sind mir insbesondere in meinen Sprechzeiten (Mi 10-11, Do 14-15) willkommen, aber auch eine Email wird möglichst beantwortet.

Miteinander Umgehen

So wie Sie von mir Freundlichkeit, Ansprechbarkeit und Toleranz erwarten, so erwarte ich auch von Ihnen ähnliches. Ich bin kein „Dickhäuter“ und werde daher in der Vorlesung und in den Übungsgruppen Ruhe einfordern. Was keineswegs heißt, dass man nicht einer Frage oder einer Bemerkung Luft machen darf. Es heißt nur, dass störende Unterhaltungen mit Nachbarn nicht willkommen sind. Aber gelacht werden darf natürlich – schön, wenn es hierzu Gelegenheiten gibt. Und das Allerwichtigste: **Mathematik kann viel Spaß machen!** Ich hoffe, dass ich Ihnen dies vermitteln kann. Noch mehr hoffe ich, dass Sie **Freude** haben, Mathematik zu betreiben.

Kapitel 2

Zahlen – erster Zugang

2.1 Einführung

Mit Zahlen fängt der Mathematikunterricht in der Grundschule an, sie bilden den Startpunkt jeglicher Mathematik. Hier soll ein erster naiver Zugang vorgestellt werden, der in späteren Abschnitten vertieft wird.
Die Geschichte der Zahlen ist u.a. mit den Kulturen der Babylonier, der Ägypter, der Inder, der Chinesen und der Griechen verknüpft. Zahlen haben in vielen Kulturen und Religionen eine große symbolische Bedeutung. Stellvertretend seien die www-Dokumente Sieben - eine perfekte Zahl zum Auftreten der Zahl SIEBEN in diversen Kulturen und Religionen und Null (Wikipedia) zur Geschichte der Zahl NULL genannt.
Unter Zahlen (Mathematik-Portal) können Sie viele der hier angesprochenen Themen behandelt sehen. Unbedingt lesen!!

2.2 Natürliche, ganze, rationale, reelle, komplexe Zahlen

Siehe auch Hierarchie der Zahlen (Mathematik-Portal).
Die Zahlen 1, 2, 3, ... heißen **natürliche Zahlen**, von diesen gibt es *unendlich viele*. Gäbe es nämlich eine größte und nennen wir diese G, so ist auch deren *Nachfolger* $G+1$ eine natürliche Zahl – ein Widerspruch[1].
Ob die Zahl Null (0) als *natürlich* angesehen werden sollte, darüber wird gestritten. Jedenfalls haben SchülerInnen mit einer Rechenschwäche (Dyskalkulie) große Probleme mit der Null. Wir zählen sie zunächst nicht zu den natürlichen Zahlen.

[1] Dies könnte man als ersten **Beweis** auffassen. Das ist im strengen Sinne aber nicht der Fall. Hierzu müssten wir die natürlichen Zahlen axiomatisch mit Hilfe der Peanoaxiome definieren – was auch später geschieht. Das, was hier wie ein Beweis erscheint, wird dann zu einem Axiom.

Als nächstes kommen die negativen Zahlen -1, -2, -3,.... – eine weitere gedankliche Hürde im Grundschulunterricht[2]. Diese bilden zusammen mit den natürlichen Zahlen und der Null die **ganzen Zahlen**.
Die nächste Stufe bilden die **rationalen Zahlen** – Brüche $\frac{p}{q}$ mit ganzen Zahlen p (**Zähler**) und $q \neq 0$ (**Nenner**). Hierbei kann man annehmen, dass der Bruch *gekürzt* ist, d.h., dass p und q **teilerfremd** sind, bzw. dass ihr größter gemeinsamer Teiler Eins ist: $ggT(p,q) = 1$. Dann sind die Darstellungen von *positiven* rationalen Zahlen mit natürlichen Zahlen als **Zähler** und **Nenner** *eindeutig*[3], die negativen rationalen Zahlen schreibt man als $-\frac{p}{q}$ mit natürlichen Zahlen p, q. Offensichtlich sind ganze Zahlen auch rationale Zahlen – man wähle den Nenner $q = 1$.
Rationale Zahlen geben *Teilungsverhältnisse* wieder, so kann man eine Strecke im Verhältnis $p : q$ teilen. Dies spielt in der *Harmonielehre* eine große Rolle, man denke nur bei der Erzeugung von Tönen an das Abgreifen von Gitarrensaiten. So entspricht das Teilungsverhältnis $2 : 3$ einer *Quinte*.
Schon bei den Griechen war der Begriff **kommensurabel** von Bedeutung: Zwei Strecken heißen kommensurabel, falls es eine Längeneinheit gibt, so dass die eine Strecke p und die andere Strecke q Längeneinheiten misst – mit natürlichen Zahlen p und q. Anders ausgedrückt: Das Längenverhältnis beider Strecken ist rational, ein Bruch $\frac{p}{q}$.
Dass es auch nichtkommensurable Strecken gibt, war in der Antike ein gewisser Schock. So sind Kante und Diagonale eines Quadrats nicht kommensurabel! Denn nach dem Satz von Pythagoras gilt $d^2 = 2a^2$, falls a die Kanten- und d die Diagonallänge ist. Damit ist $d/a = x := \sqrt{2}$, das ist die Zahl x mit $x^2 = 2$. Diese Zahl kann aber nicht rational sein (s. unseren ersten Beweis in Kap. 2.6.1), sie ist **irrational**.

Also gibt es neben den rationalen Zahlen auch noch irrationale Zahlen. Diese bilden zusammen mit den rationalen Zahlen die **reellen Zahlen**. Diese kann man auf einem *Zahlenstrahl* veranschaulichen, der keinerlei „Lücken“ aufweist. Man spricht von einem *Kontinuum*. In einem gewissen Sinne gibt es viel mehr irrationale Zahlen als rationale Zahlen[4]!

Die wichtigste mathematische Konstante ist die **Kreiszahl** π, die man als den Umfang (etwa in Metern) eines Kreises mit Durchmesser 1 (Meter) definieren kann. Diese erweist sich als irrational! Wenn sie rational wäre, würde die *Quadratur des Kreises* gelingen. Hierunter versteht man die Möglichkeit, zu einem Kreis mit Zirkel und Lineal ein flächengleiches Quadrat zu konstruieren. Aus der Irrationalität von π folgt, dass Radius r eines Kreises und Kantenlänge a eines zum Kreis flächengleichen Quadrates, für die also $a^2 = r^2\pi$ gilt, inkommensurabel sind: Denn ein rationales a/r hat zur Folge, dass $\pi = \frac{a^2}{r^2}$ ebenfalls rational ist.
Siehe auch Die Kreiszahl PI (Mathematik-Portal)

Zwei weitere sehr wichtigste Konstanten der Mathematik sind:

[2] Mit ihrer Hilfe kann die Subtraktion auf die Addition zurückgeführt werden: $a - b = a + (-b)$
[3] Es gibt eine und nur eine Darstellung.
[4] Die rationalen Zahlen sind „abzählbar“, nicht aber die irrationalen Zahlen.

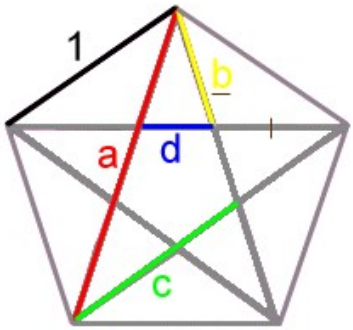


Abbildung 2.1: Goldener Schnitt im Pentagon

- Die (große) **Goldene-Schnitt-Zahl**,

$$\Phi = \frac{1}{2}(\sqrt{5}+1)$$

bzw. ihr Inverses – die kleine Goldene-Schnitt-Zahl $\phi = \frac{1}{2}(\sqrt{5}-1)$, s. Abb. 2.1. Hier sehen Sie ein regelmäßiges Fünfeck (**Pentagon**), der Ausgangspunkt für einen 5-zackigen Stern (**Pentagramm**) ist, das in Goethes Faust Mephisto daran hindert, das Studierzimmer des Faust zu verlassen. Es gilt

$$\Phi = \frac{a}{c} = \frac{c}{b} = \frac{b}{d},$$

d.h., es wimmelt im regelmäßigen Fünfeck nur so von „Goldenen Dreiecken“. Dies sind gleichschenklige Dreiecke, deren Seitenverhältnisse gleich Φ (oder ϕ) sind.

Man sagt, dass eine Strecke *golden geteilt* wird, wenn sich die ganze Seite zur längeren Teilseite, wie die längere zur kürzeren Teilseite verhält. In diesem Sinne sehen Sie in Abb. 2.1 eine Vielzahl von golden geteilten Strecken.

Siehe auch Der goldene Schnitt (Mathematik-Portal).

- Die **Eulersche Zahl**

$$e = \lim_{n\to\infty}(1+\frac{1}{n})^n,$$

wobei wir an dieser Stelle nicht davon ausgehen, dass Sie den Limesbegriff wirklich verstanden haben.

Siehe auch Die Eulersche Zahl e (Mathematik-Portal).

Die Kreiszahl und die Eulersche Zahl sind irrational, ja sogar transzendent[5].

[5]nicht algebraisch. Algebraisch heißt eine Zahl, wenn sie Lösung einer Gleichung n-ten Grades mit rationalen Koeffizienten ist. $\sqrt{2}$ ist algebraisch als Lösung von $x^2 = 2$, ebenso die Goldene Schnittzahl.

Abbildung 2.2: C.F. Gauss

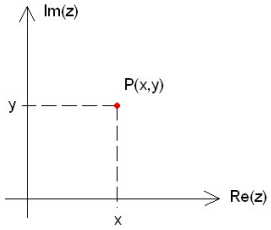


Abbildung 2.3: Punkt in der komplexen Zahlenebene

Die *komplexen Zahlen* sind mit einer gewissen Mystik umgeben, man lese nur nach in „`Der junge Törless`“ von ROBERT MUSIL [6]. Es gibt etwas, was man *imaginäre Einheit* nennt und mit i abkürzt, welche die quadratische Gleichung $x^2 = -1$ löst. Dass es so etwas gibt, erscheint unglaublich – solange man noch im reellen Zahlenbereich verhaftet ist, da für reelle Zahlen x niemals $x^2 < 0$ gilt. Den Weg aus diesem Puzzle hat C.F. Gauss (Abb. 2.2) gewiesen, der mit *Zahlenpaaren* $z = (x, y)$ (meist als $z = x + iy$ notiert) und reellen Zahlen $x = Re(z)$ und $y = Im(z)$ rechnete (s. Fig. 2.3)[7], indem er Multiplikations[8]- und Additionsregeln aufstellte. Dabei ergibt sich

$$(0, 1) \cdot (0, 1) = (-1, 0). \tag{2.1}$$

Die Zahlenpaare $(a, 0)$, die an der zweiten Stelle eine Null haben, verhalten sich dabei wie reelle Zahlen a. Nun bezeichnete Gauss das spezielle Zahlenpaar $(0, 1)$ als *imaginäre Einheit* i – und schon wird aus (2.1) die Aussage $i^2 = i \cdot i = -1$. Mehr hierzu an anderer Stelle.
Es gibt eine Webseite Rechnen mit komplexen Zahlen (Uni Kiel), aus der hervorgeht, dass die

[6] Törless im Gespräch mit Hilde: „Dann kannst Du mir vielleicht weiterhelfen. Mich verwirren nämlich die imaginären Zahlen“. Hilde war verblüfft. Erinnerte aber sogleich: „$i^2 = -1$“. „Das verstehe ich bereits nicht. Die Zahl gibt es doch überhaupt nicht. Jede Zahl, ob positiv oder negativ, gibt zum Quadrat erhoben etwas Positives. Es kann daher gar keine wirkliche Zahl geben, welche die Quadratwurzel von etwas Negativem wäre“.

[7] Re steht für Realteil und Im für Imaginärteil.

[8] $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$ bzw. $(a + ib) \cdot (c + id) = ac - bd + i(ad + bc)$.

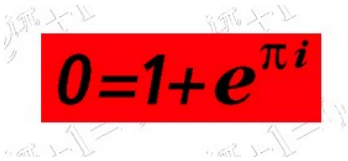


Abbildung 2.4: Schönste Formel der Mathematik

komplexen Zahlen schon von G. Cardono (1501-1576) „entdeckt“ wurden.
Siehe auch Die imaginäre Einheit (Mathematik-Portal)

2.2.1 Schönste Formel der Mathematik

Ich schließe dieses Kapitel mit der schönsten Formel der Mathematik, die die 5 wichtigsten Zahlen $0, 1, \pi, e$ und die imaginäre Einheit i in Beziehung setzt:

$$e^{\pi i} + 1 = 0,$$

siehe Abb. 2.4
Siehe auch Eine bemerkenswerte Formel (Mathematik-Portal)

2.2.2 Mengen und Zahlen

Im nächsten Abschnitt werden *Mengen* eingeführt. In diesem Kapitel habe ich den Mengenbegriff vermieden – zu Lasten längerer Sätze. Hier möchte ich mich damit begnügen zu erwähnen, dass die natürlichen Zahlen eine Menge – genannt $\mathbb{N}$, die ganzen Zahlen eine Menge $\mathbb{Z}$, die rationalen eine Menge $\mathbb{Q}$, die reellen Zahlen eine Menge $\mathbb{R}$ und die komplexen Zahlen eine Menge $\mathbb{C}$ bilden. Statt „n ist eine natürliche Zahl“ schreiben wir später „$n \in \mathbb{N}$“. Siehe auch Kap. 3.3 oder auch die Webseite Mengen und ihre Beschreibung (Mathe Online Wien).

2.3 Arithmetische Operatoren

Mit Zahlen kann man rechnen: Man kann je zwei Zahlen a, b addieren, multiplizieren, subtrahieren und dividieren (sofern der Divisor $\neq 0$). Man schreibt für die **Summe** $a + b$, für das **Produkt** $a \cdot b$, für die **Differenz** $a - b$ und für den **Quotienten** a/b oder auch $\frac{a}{b}$. Man nennt $+, \cdot, -, /$ **arithmetische Operatoren**[9]. Bei der Subtraktion $a - b$ kann man auf die Addition zurückgreifen, wenn man $a + \tilde{b}$ mit $\tilde{b} := -b$ rechnet[10]. Genauso kann man statt a/b auch $a \cdot \tilde{b}$ schreiben, wenn $\tilde{b} := 1/b$ gesetzt wird[11].

[9] In Kap. 5.2.3 werden wir diese als Abbildungen auf einem kartesischen Produkt (binäre Verknüpfungen) erkennen.

[10] $\tilde{b} = -b$ heißt **additives Inverse** von b.

[11] $\tilde{b} = 1/b$ heißt das **multiplikative Inverse** von b.

Diese Operatoren werden noch im Rahmen von *Gruppen* (Kap. 8) behandelt. Sie sind Spezialfälle von *binären Verknüpfungen*.
Hier können wir kurz innehalten und uns überlegen, welche Probleme des „Alltags“ eigentlich Addition, Subtraktion, Multiplikation oder Division erfordern[12].
Arithmetische Operatoren bilden das Herzstück aller Programmiersprachen. Hier kommen noch logische und Vergleichsoperatoren hinzu.
Zwei weitere arithmetische Operatoren, die auf der Menge der ganzen Zahlen wirken, sind von Bedeutung: die *Division ohne Rest* (div) und die Berechnung des Restes bei einer Division (*mod*[13]). So gilt „7 div 3 = 2“ und „7 mod 3 = 1“. Aus der Schule kennen Sie „7 durch 3 = 2 Rest 1“ oder so ähnlich. Das Rechnen mit Resten ist ausgesprochen wichtig und wird später in Kap. 8 behandelt.

2.3.1 Potenzen

In der Grundschule fängt man mit der Addition von natürlichen Zahlen m und n an. Ihre Multiplikation wird auf die Addition zurückgeführt: es ist $m \cdot n = n + n + \cdots + n$ (m-mal)[14]. In diesem Sinne ist $m \cdot n$ eigentlich nur eine Abkürzung für einen länglichen Ausdruck mit sich wiederholenden Teilen. Das ist genauso der Fall bei **Potenzen** a^n für beliebige reelle Zahlen a und natürliche, positive Zahlen n: $a^n = a \cdot a \cdot \cdots \cdot a$ (n-mal).
Die Potenzgesetze

$$a^{n+m} = a^n \cdot a^m, \quad (a^n)^m = a^{nm}$$

sind dann unmittelbar einsichtig[15].

Mit ein wenig Aufwand kann man a^b für irgendeine reelle Zahl b und eine positive Zahl a definieren, so dass die Potenzgesetze gelten. Bei dieser **Potenz** heißt a die **Basis** und b der **Exponent**. In diesem Sinne ist auch die Potenzierung eine arithmetische Operation. Näheres erfahren Sie später.
Siehe auch Potenzrechnung (Mathematik-Portal)

2.4 Teilbarkeit und Primzahlen

Eine natürliche Zahl p **teilt** eine andere Zahl q, falls es eine dritte natürliche Zahl r mit $q = r \cdot p$ gibt[16]. Man sagt auch, dass p ein **Teiler** von q ist.
Eine Primzahl ist eine natürliche Zahl ≥ 2, die nur durch 1 und sich selbst teilbar ist. Jede natürliche Zahl $m \geq 2$ besitzt eine **eindeutige Primfaktorzerlegung**, die angibt, welche

[12] Wann haben Sie zuletzt dividiert?
[13] sprich: modulo.
[14] „Verblüffender Weise“ (?) ist auch $m \cdot n = n \cdot m = m + m + \cdots + m$ (n-mal)
[15] Richtig beweisen können wir dies mit dem *Prinzip der vollständigen Induktion*
[16] Natürlich wissen Sie, was es heißt, dass eine Zahl eine andere teilt. Mit dieser Definition kann man aber Aussagen *beweisen*.. Z.B. die Aussage, dass wenn a teilt b und b teilt c, dann teilt a auch c

Primzahl wie oft als Teiler von m auftritt. So haben wir die Primzahlfaktorisierungen

$$54 = 2 \cdot 3 \cdot 3 \cdot 3, \quad 125 = 3 \cdot 5 \cdot 5.$$

Es ist gar nicht so einfach, präzise zu notieren, was eine Primfaktorzerlegung ist. Ich versuche es: Zu jeder Zahl m gibt es paarweise verschiedene Primzahlen $p_1 < p_2 < \cdots < p_s$ und natürliche Zahlen $n_j \geq 1, j = 1, 2, ..., s$, mit

$$m = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_s^{n_s}.$$

Zur mathematischen Allgemeinbildung gehört die Aussage und deren Beweis, dass es unendlich viele Primzahlen gibt. Wir formulieren dieses als unseren ersten von EUKLID (325-265 v.Chr) stammenden

Satz 2.1. *Es gibt unendlich viele Primzahlen.*

Beweis: Wir führen einen *Widerspruchsbeweis*[17]. Angenommen, die Behauptung (Aussage) des Satzes ist falsch[18]. Dann gibt es nur endlich viele Primzahlen. Dann können wir diese zu $p_1 < p_2 < .... < p_n$ *durchnummerieren*[19]. Nun betrachten wir den Nachfolger p des Produktes aller dieser Primzahlen:

$$p := p_1 \cdot p_2 \cdots p_n + 1.$$

Offensichtlich ist p größer als alle Primzahlen $p_j, j = 1, 2, ..., n$. Damit kann p selbst aber keine Primzahl sein. Sie muss also durch eine der Primzahlen p_j teilbar sein – aber das kann wegen der speziellen Konstruktion nicht der Fall sein, da sich bei der Division von p durch ein p_j stets der Rest 1 ergibt. ∎

Dieser Beweis gehört zur Allgemeinbildung. Die indirekte Beweisführung wird Ihnen noch häufiger begegnen. Dass man so argumentieren kann, beruht auf einem *Axiom der Aussagenlogik*, nämlich dem Axiom *tertium non datur*, *es gibt nichts drittes neben „wahr“ und „falsch“*. Danach kann eine Aussage nur wahr oder falsch sein - etwas drittes gibt es nicht.

Auf Primzahlen und andere „Zahlenspielereien“ werden Sie sicher im Verlaufe Ihres Studiums im Umfeld von *Elementarer Zahlentheorie* stoßen.
Hier möchte ich nur schon auf die Webseite Primzahlgeheimnisse (Uni Wuppertal) hinweisen.
Interessant ist auch die Webseite Die Geschichte der Primzahlen (D.Bonhoeffer-Gymnasium in Wiehl).
Einen guten Überblick bietet Primzahlen (Webportal der DMV).
Es gibt eine Reihe noch ungelöster Probleme im Bereich von Primzahlen. Z.B. die Frage, ob es unendlich viele *Primzahlzwillinge* (wie 11,13 oder 17,19 oder 29,31) gibt.

[17] Manchmal auch indirekter Beweis genannt.

[18] Diese Annahme werden wir zu einem Widerspruch führen. Das bedeutet, dass die Annahme („Es gibt nur endlich viele Primzahlen“) falsch und damit die Behauptung des Satzes doch richtig ist. Siehe auch hierzu das Kap. 10.4.

[19] Die **Indizierung** von Variablen ist ein großartiges Hilfsmittel!

2.4.1 Mersenne'sche und Fermat'sche Primzahlen

Dieses Kapitel soll einen kleinen Einblick in *Primzahlen* geben.
Schon die alten Griechen wussten, dass Zahlen der Form $2^n - 1$ Kandidaten für Primzahlen sind – wenn n selbst eine Primzahl ist[20]. MERSENNE (1588-1648) hat solche Zahlen genauer untersucht und gezeigt, dass man für $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ wirklich Primzahlen erhält, aber nicht für die ausgelassenen Primzahlen $11, 23, 29$. Daher nennt man Primzahlen der Form $2^p - 1$ mit einer Primzahl p **Mersenne'sche Primzahlen**.
FERMAT (1601-1665) hat Primzahlen der Form 2^n+1 untersucht. Dabei handelt es sich nur dann um Primzahlen, wenn $n = 2^k$ eine 2er-Potenz ist (wird als Übungsaufgabe egstellt werden). Aber nicht alle solche Zahlen sind Primzahlen, beispielsweise ist $2^{32} + 1$ keine Primzahl, wie EULER (1707-1783) entdeckte. Primzahlen der Form $2^{2^k} + 1$ nennt man **Fermat'sche Primzahlen**.
Die Griechen haben sich auch für **perfekte Zahlen** interessiert. Das sind solche, die sich als Summe aller ihrer „echten" Teiler darstellen lassen. Beispielsweise sind 6, 28 und 496 perfekt. Interessanterweise sind alle diese drei perfekten Zahlen von der Form $(2^n - 1) \cdot 2^{n-1}$ mit einer Primzahl n[21]. Das wussten die Griechen schon.

2.5 Darstellung von Zahlen

Unser wohl aus Indien (5. Jhd) stammendes Dezimalsystem ist eine großartige Leistung. Mit nur 10 **Ziffern** 0, 1, 2, ..., 9 werden Zahlen dargestellt. Um diesen „Code" zu verstehen, muss man auf 10er-Potenzen zurückgreifen. So ist z.B. die Zahl 123,45 (kaufmännische Notation; die wissenschaftliche Notation lautet 123.45) zu interpretieren als[22]

$$123,45 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 + 4 \cdot 10^{-1} + 5 \cdot 10^{-2}.$$

Jede rationale Zahl lässt sich als ein endlicher oder ein periodischer Dezimalbruch darstellen[23]. Letzterer ist der Spezialfall eines **unendlichen Dezimalbruchs**. Um zu verstehen, was das ist, betrachten wir die allgemeine Form eines solchen: Seien $a_0, ..., a_m$ die Ziffern vor dem Punkt und $b_1, b_2, ...$ die nach dem Komma, also

$$x = a_m a_{m-1} \cdots a_0, b_1 b_2 b_3 \cdots b_n \cdots ,$$

in 10er-Potenzen

$$x = a_m \cdot 10^m + a_{m-1} 10^{m-1} \cdots a_0 \cdot 10^0 + b_1 \cdot 10^{-1} + \cdots + b_n \cdot 10^{-n} + \cdots .$$

[20] Wenn n keine Primzahl ist, ist auch $2^n - 1$ keine. Der Beweis ist einfach. Ist $n = j \cdot k$, so wird $2^n - 1$ von $2^j - 1$ (und von $2^k - 1$) geteilt. Siehe Satz 2.4

[21] Für $n = 2$ erhält man 6, für $n = 3$ die Zahl 28 und für $n = 4$ die Zahl 496.

[22] Erinnern Sie sich: $10^{-2} = \frac{1}{10^2}$.

[23] Bei der Division treten laufend Reste auf, die niemals größer als der Nenner sein können. Daher ist entweder der Rest Null – endlicher Dezimalbruch – oder die Folge der Reste wiederholt sich ab einem Rest, der zum zweiten Mal vorkommt.

Dies ist eine *unendliche Reihe*.

Siehe auch Umwandlung von Dezmalbrüche in gewöhnliche Brüche (Mathematik-Portal)

2.6 Anhang

Hier wollen wir kleinere Beweise führen, an denen Sie Beweistechniken einüben können.
Siehe auch Beweistechnik (Wikipedia)

2.6.1 Die Irrationalität von Wurzel aus 2

Satz 2.2. *$\sqrt{2}$ ist irrational.*

Beweis: Wir haben zu zeigen: Es gibt keine natürlichen Zahlen p, q mit der Eigenschaft $\sqrt{2} = \frac{p}{q}$.
Wie schon in unserem ersten Satz 2.1 führen wir wieder einen *Widerspruchsbeweis*.
Angenommen, $\sqrt{2}$ ist doch eine rationale Zahl, d.h., es gibt natürliche Zahlen p, q mit $\sqrt{2} = \frac{p}{q}$.
Wir können annehmen, dass p und q nicht beide Vielfache von 2 sind (sonst: kürzen!).
Aus $\sqrt{2} = \frac{p}{q}$ folgt $\sqrt{2} \cdot \sqrt{2} = \frac{p}{q} \cdot \frac{p}{q}$, dies ist gleichbedeutend mit $2 = \frac{p^2}{q^2}$ bzw. mit $2q^2 = p^2$. Also ist p^2 und damit auch p eine gerade Zahl[24]. Hieraus folgt, dass auch q selbst gerade sein muss: Da p gerade ist, gibt es eine natürliche Zahl k mit $p = 2k$. Dann ist $p^2 = 4k^2$, also – oben eingesetzt – $2q^2 = 4k^2$ und $q^2 = 2k^2$.
Dieses Ergebnis steht aber im Widerspruch zur Annahme, dass es sich bei p und q *nicht* um zwei gerade Zahlen handeln soll. Unsere Annahme ($\sqrt{2}$ rational) war also falsch. Damit ist die Behauptung bewiesen. ∎

2.6.2 Charakterisierung von geraden und ungeraden Zahlen

Was eine (un)gerade Zahl ist, weiß jeder: Eine gerade Zahl ist eine Zahl, die durch 2 teilbar ist, eine ungerade Zahl ist eine Zahl, die *nicht* gerade ist. Benutzen wir die Definition von „*2 ist Teiler von n*“, so ergibt sich: *Jede gerade Zahl n lässt sich in der Form $n = 2m$ mit einer natürlichen Zahl m darstellen.* Ist nun die folgende Aussage trivial? „Jede ungerade Zahl n lässt sich in der Form $n = 2m - 1$ mit einer natürlichen Zahl m darstellen“. Ein Beweis könnte so gehen: Jede zweite Zahl ist gerade. Wenn n ungerade ist, so ist $n + 1$ gerade, d.h. es gibt ein m mit $n + 1 = 2m$, woraus das Gewünschte folgt.
Jetzt können wir auch zeigen (eigentlich ein Sätzchen):

Satz 2.3. *Das Produkt zweier ungerader Zahlen p und q ist ungerade.*

Beweis: Da p und q ungerade sind, gibt es natürliche Zahlen m und n, so dass $p = 2m - 1, q = 2n - 1$. Jetzt folgt $pq = 4mn - 2(m + n) + 1 = 2(2mn - m - n) + 1$, also $pq = 2r' + 1$ mit der Zahl $r' := 2mn - m - n$. Setze $r := r' + 1$. Dann ist $pq = 2r - 1$ und r ist eine natürlich Zahl. Dies bedeutet aber, dass pq ungerade ist. Dies ist ein Beispiel für einen direkten Beweis! ∎

[24] Das Quadrat einer ungeraden Zahl ist stets ungerade.

2.6.3 Mersennsche Primzahlen

In Kap. 2.4.1 wurde behauptet:

Satz 2.4. *Ist n keine Primzahl, so ist auch $2^n - 1$ keine Primzahl.*

Aus diesem Satz folgt die in Kap. 2.4.1 erwähnte Tatsache, dass Mersennsche Primzahlen der Form $2^n - 1$ nur für Primzahlen n auftreten. Denn das logische Gesetz der Kontraposition[25] besagt, dass die beiden Aussagen „*Wenn n keine Primzahl ist, dann ist $2^n - 1$ keine Primzahl*“ und „*Wenn $2^n - 1$ eine Primzahl ist, dann ist n eine Primzahl*“ logisch äquivalent sind.
Beweis von Satz 2.4:
Wenn n keine Primzahl ist, gibt es natürliche Zahlen j und k, beide weder 1 noch n, mit $n = j \cdot k$. Dann ist $\ell := 2^j - 1$ weder 1 noch $2^n - 1$, so dass wir mit dem Beweis fertig sind, wenn wir zeigen, dass ℓ die Zahl $2^n - 1$ teilt[26]
Der Grund für unsere Behauptung liegt in der *geometrischen Summenformel*

$$1 + x + x^2 + \cdots + x^m = \frac{x^{m+1} - 1}{x - 1},$$

die uns noch öfters begegnen wird und die mit vollständiger Induktion bewiesen werden kann. Diese gilt für beliebige reelle Zahlen x. Für natürliche Zahlen x folgt, dass $x - 1$ stets den Vorgänger $x^k - 1$ einer x-Potenz x^k teilt.
Hier haben wir es mit $2^n - 1 = 2^{jk} - 1 = (2^j)^k - 1$, also $x = 2^j$ zu tun, so dass wir die gewünschte Behauptung erhalten. ∎

[25] „Aus A folgt B“ ist äquivalent zu „Aus Nicht B folgt Nicht A“.

[26] Hier kann man schon mit Beispielen die Aussage glaubhaft machen, sie aber nicht beweisen. Z.B. teilt $j = 3$ die Zahl $n = 6$ und $\ell = 2^j - 1 = 7$ teilt $2^n - 1 = 63$.

Kapitel 3

Mengen

3.1 Einführung

Die mathematische Sprache basiert ganz wesentlich auf dem Mengenbegriff und den mit diesem verbundenen weiteren Begriffen wie *Teilmenge, Durchschnitt, Vereinigung, ...* Die Mengenlehre geht auf *Georg Cantor (1845 – 1918)* zurück, der mit Hilfe seiner Mengenlehre die Analysis, insbesondere den Begriff der Unendlichkeit von *Zahlenmengen* präzisieren wollte. Von ihm stammt die folgende Definition (1895): *Unter einer „Menge“ verstehen wir jede Zusammenfassung M von bestimmten wohlunterscheidbaren Objekten M unserer Anschauung oder unseres Denkens (welche die „Elemente“ von M genannt werden) zu einem Ganzen.*

In den 70er Jahren wurde die Mengenlehre unter den Namen „Neue Mathematik“ im Unterricht der Grundschulen eingeführt. Ziel war es, neben der Vermittlung von Rechenfertigkeiten auch Denkfähigkeit und Abstraktionsvermögen der Kinder zu fördern. Die wissenschaftlich formalisierte Mengenlehre entsprach jedoch nicht dem pädagogischen Anspruch, kindgerecht zu sein. So beschränkte sich die Mengenlehre an den Schulen damit, Mengendiagramme zu zeichnen bzw. bunte Plastikplättchen zu legen. Die neue Mathematik scheiterte letztendlich daran, dass sie keine Verbindung zur traditionellen Mathematik herstellen konnte. Zudem waren sowohl Lehrer als auch Eltern damit vollkommen überfordert.

Die Mengenlehre wird häufig mit der (wesentlich älteren) Logik (Kap. 10) in Verbindung gebracht. Dies liegt daran, dass eine *Menge A* mit der *Aussage* „$x \in A$“ verknüpft wird. Dann entsprechen die Mengenoperatoren „Vereinigung“ bzw. „Durchschnitt“ genau den logischen Operatoren „oder“ bzw. „und“.

Eine Einführung in Mengen liefert `Mathe online` (Wien).

Einen Überblick zur Mengenlehre gibt die Enzyklopädie *Wikipedia*, von der auch der obige Absatz stammt.

3.2 Logische Symbole

Dieser Abschnitt hat nicht direkt mit Mengen zu tun. Es ist nur eine passende Gelegenheit, in der Mathematik übliche, abkürzende Schreibweisen einzuführen.

1. $\forall$: für alle, für jedes
2. $\exists$: es gibt (wenigstens) ein, es existiert
3. A und B sind im Folgenden *Aussagen*
   - $A \Longrightarrow B$: Aus A folgt B (oder: wenn A, dann B) (oder A impliziert B)
   - $A \Longleftrightarrow B$: A ist genau dann wahr, wenn B wahr ist[1] (oder A und B sind gleichwertig)
   - $A :\Longleftrightarrow B$: A wird durch B definiert (festgelegt).
4. $A := B$: A wird durch B definiert (festgelegt). Hier sind A und B irgendwelche Ausdrücke.
5. $\vee$: Das logische „oder“
6. $\wedge$: Das logische „und“

Einige dieser Abkürzungen sind gewöhnungsbedürftig, insbesondere dürfte die Bedeutung der „Variablen“ A, B erst im Laufe der Zeit klar werden. Erst der häufige Umgang mit ihnen wird sie vertraut machen. $\Longrightarrow$, $\Longleftrightarrow$, $\wedge$ und $\vee$ sind *logische Operatoren*: Mit ihnen werden *Aussagen verknüpft*. Mehr hierzu später unter „Aussagenlogik“ in Kap. 10. Auch die sogenannten *Quantoren* $\forall, \exists$ haben ihren Ursprung in der Aussagenlogik.

Erste Beispiele von Aussagen, die solche Abkürzungen verwenden:

- $$x^2 + 1 > 0 \quad \forall x$$

  oder auch

  $$\forall x : \; x^2 + 1 > 0$$

  Diese Aussage ist wahr.

- (Definition von *ungerade*)

  $$n \in \mathbb{N} \text{ ist } \textbf{ungerade} \; :\Longleftrightarrow \quad \exists m \in \mathbb{N} : \; n = 2m - 1.$$

[1] „genau dann“ heißt hier folgendes: Aus A folgt B und aus B folgt A.

- (Falls *ungerade* z.B. schon durch *nicht durch 2 teilbar* definiert worden wäre)

$$n \in \mathbb{N} \text{ ist ungerade } \iff \quad \exists m \in \mathbb{N} : \; n = 2m - 1.$$

- $$x < 0 \Longrightarrow x^2 > 0$$

- $$x + 1 > 2 \iff x > 1$$

- Es ist $(2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1 = 2m' + 1$ mit $m' := 2m^2 + 2m$.

- $$x > 2 \wedge x < 3$$

  (lies: „$x > 2$ “*und* „$x < 3$“) heißt, dass x zwischen 2 und 3 liegt.

- $$x > 0 \vee x < 3$$

  (lies: „$x > 0$ “*oder* „$x < 3$ “) Dies bedeutet keinerlei Einschränkung für die Zahl x.

- (Definition von *Teiler*) $p \in \mathbb{N}$ ist ein **Teiler** von $q \in \mathbb{N} : \iff \exists r \in \mathbb{N} : \; q = r \cdot p$

Das Zeichen „$A := B$“ wurde in der Vorlesung schon mehrfach benutzt, z.B. wurde die Multiplikation von Punkten (a, b) und (c, d) durch

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc)$$

„definiert“.

Hinweis: Links und rechts von den logischen Symbolen $\Longrightarrow$ und $\iff$ oder auch von $: \iff$ stehen stets **Aussagen**, während links und rechts des Gleichheitszeichen $=$ oder auch von $:=$ stets irgendwelche **Ausdrücke (Terme)** stehen, z.B. Zahlen, Mengen,....

3.3 Grundbegriffe der naiven Mengenlehre

Definition 3.1. *Eine* **Menge** *ist eine Zusammenfassung von wohlbestimmten und wohlunterschiedenen Objekten unseres Denkens oder unserer Anschauung, welche die* **Elemente der Menge** *genannt werden, zu einem Ganzen. Die Objekte heißen* **Elemente** *der Menge.*

Bemerkungen:
1) Diese Definition geht auf *Georg Cantor (1845 – 1918)* zurück. Sie ist keine „richtige“, sondern nur eine „naive“ Definition, da der neue Begriff „Menge“ nicht auf schon bekannte Begriffe zurückgeführt wird.
2) „wohlbestimmt“: Es ist eindeutig feststellbar, ob ein Objekt x zu einer Menge M gehört oder nicht, in Zeichen $x \in M$ (sprich: x *in* M oder x ist Element von M) oder $x \notin M$ (sprich x *nicht in* M oder x ist nicht Element von M).
3) „wohlunterschieden“: Kein Objekt gehört mehrfach zu einer Menge.
4) Mengen können angegeben werden durch eine (unvollständige) Auflistung aller Elemente oder durch Angabe von Eigenschaften, die ihren Elementen zukommen. Dabei werden **Mengenklammern** (geschweifte Klammern) verwendet. Die *Reihenfolge* der Elemente innerhalb der Mengenklammern ist dabei unerheblich. Als Trennzeichen der Elemente einer Menge wird i.A. ein Komma benutzt, bei Dezimalzahlen auch ein Semikolon[2].

Beispiele:
1) Die Menge $\{Nina, Sandra, Torsten\}$ von Studierenden, die eine Übungsgruppe bilden (Aufzählung). Es kommt nicht auf die Reihenfolge an, d.h. bei $\{Sandra, Torsten, Nina\}$ handelt es sich um dieselbe Menge.
2) Die Menge $M = \{1, 2, 3, 4\}$ der natürlichen Zahlen 1 bis 4. Da es nicht auf die Reihenfolge der Elemente ankommt – es handelt sich um eine reine Auflistung –, gilt auch $M = \{4, 2, 3, 1\}$.
3) Die Menge M aller Primzahlen zwischen 10 und 20. Es geht auch so:

$$M = \{x | x \text{ ist Primzahl, und es gilt } 10 \leq x \leq 20\}.$$

Dies ist die Bescheibung einer Menge durch eine Eigenschaft.
4) Jetzt folgt das wichtigste Beispiel: Die **natürlichen, ganzen, rationalen, reellen und komplexen Zahlen** bilden **Mengen**, für deren Namen wir eine einheitliche Bezeichnung einführen: $\mathbb{N}$ für die Menge der natürlichen, $\mathbb{N}_\mathbf{0}$ für die natürlichen Zahlen plus der Null, $\mathbb{Z}$ für die Menge der ganzen, $\mathbb{Q}$ für die Menge der rationalen, $\mathbb{R}$ für die Menge der reellen und $\mathbb{C}$ für die Menge der komplexen Zahlen. Die Schreibweise $\mathbb{N} = \{1, 2, 3, \ldots\}$ ist auch möglich – eine unvollständige Auflistung.
Bisher hatten wir immer gesagt: „n ist eine natürliche Zahl“. Jetzt können wir hierfür kurz schreiben: $n \in \mathbb{N}$.
5) Die Menge der ungeraden natürlichen Zahlen lässt sich jetzt so fassen:

$$M = \{n \in \mathbb{N} : \exists m \in \mathbb{N} : n = 2 \cdot m - 1\}$$

Beachten Sie, dass hier die Menge durch eine *Eigenschaft* bestimmt wird, die nach dem Doppelpunkt beschrieben wird. Üblich ist auch die gleichwertige Schreibweise mit einem senkrechten Strich:

$$M = \{n \in \mathbb{N} | \exists m \in \mathbb{N} : n = 2 \cdot m - 1\}$$

[2]Vor drei Jahren hatte ich Dezimalbrüche in der wissenschaftlichen Gleitpunktdarstellung geschrieben, so dass es hier keiner Besonderheit bedurfte. Da in den Schulen aber die kaufmännische Darstellung der Dezimalbrüche üblich ist, habe ich mich zu einer Umstellung entschlossen.

6) Die Menge der Buchstaben, aus denen das Wort SEMESTER gebildet wird: $M = \{S, M, E, T, R\}$ – achten Sie darauf, dass es bei der Auflistung nicht auf die Reihenfolge ankommt.
7) $\{z \in \mathbb{Z} \mid z^2 - z = 6\} = \{-2, 3\}, \qquad \{z \in \mathbb{N} \mid z^2 - z = 6\} = \{3\}.$
8) $\{n \in \mathbb{N} : n < 2 \vee n = 4\} = \{1, 4\}$
9) $M = \{1,234; 2,45; 5\}$ enthält drei Zahlen. Wegen ihrer Dezimalbruchdarstellung wird ein Semikolon als Trennzeichen verwendet.

Eine Menge heißt **endlich**, falls sie eine endliche Anzahl von Elementen besitzt. Diese lassen sich im Prinzip vollständig auflisten – wenn der Raum hierfür reicht. Mengen, die nicht endlich sind, heißen **unendlich**. Die Zahlenmengen $\mathbb{N}, \mathbb{Z}, ...$ sind offensichtlich alle unendliche Mengen. Die *Mächtigkeit* einer Menge hängt mit ihrer Größe zusammen. Je mehr Elemente eine Menge enthält, desto „mächtiger“ sollte sie sein. Bei endlichen Mengen kann man ihre Mächtigkeit durch die **Anzahl** ihrer Elemente messen. Bei unendlichen Mengen geht das nicht. Wenn wir *Abbildungen* behandeln, werden wir den Begriff *gleichmächtig* kennenlernen (Def. 5.12). Dabei wird eine verblüffende Konsequenz sein, dass die Menge $\mathbb{N}$ und die Menge aller geraden natürlichen Zahlen gleichmächtig sein werden.
Bem.: Die Elemente einer Menge können durchaus selbst Mengen sein. Insofern gibt $M = \{1, \{1, 2\}\}$ einen (allerdings nicht recht einsehbaren) Sinn.

Definition 3.2. *Für eine endliche Menge A bezeichnet $|\mathbf{A}|$ die Anzahl der Elemente von A.*

Beispiel: $|\{2, 7, \{1, 4\}\}| = 3$.

3.3.1 Teilmenge

Definition 3.3. *Seien A, B beliebige Mengen.*
a) A heißt **Teilmenge** *von B, geschrieben $A \subset B \iff$ Jedes Element von A ist auch Element von B.*
b) $A = B \iff$ $A \subset B$ und $B \subset A$. In Worten: $A = B$ genau dann, wenn jedes Element von A auch Element von B ist und jedes Element von B auch Element von A ist.

Bemerkungen:
Statt des Teilmengen-Symbols $\subset$ findet man in anderen Skripten und in Lehrbüchern auch das Symbol $\subseteq$, mit dem deutlicher assoziiert wird, dass eine Teilmenge A von B nicht zwingend eine **echte Teilmenge** in dem Sinne ist, dass zwar $A \subset B$, aber $A \neq B$ gilt. In solchen Texten bedeutet $A \subset B$, dass A eine echte Teilmenge von B ist. Bei mir nicht!
Jede Menge ist Teilmenge von sich selbst, es gilt also $A \subset A$. Aber natürlich ist A keine echte Teilmenge von A.

Beispiel: $\{1\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

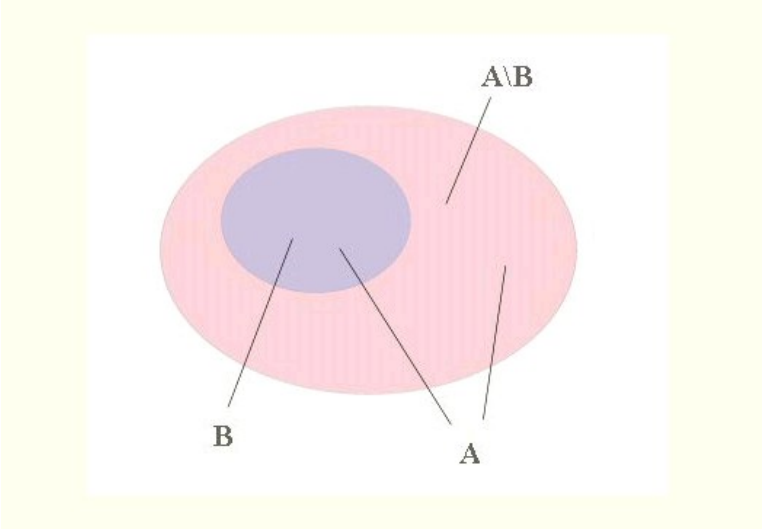


Abbildung 3.1: Differenzmenge von A und B

3.3.2 Vereinigung, Durchschnitt, Komplement

Definition 3.4. *Seien $A, B \subset M$ und M irgendeine „Grundmenge“.*
a) $A \cup B := \{x \in M \mid x \in A$ oder $x \in B\}$ heißt die **Vereinigung** *von A und B.*
b) $A \cap B := \{x \in M \mid x \in A$ und $x \in B\}$ heißt der **Durchschnitt** *von A und B.*
c) $A \setminus B := \{x \in M \mid x \in A$ und $x \notin B\}$ heißt die **Differenzmenge** *von A und B (Reihenfolge ist wichtig!).*
d) $\overline{A} := \{x \in M \mid x \notin A\}$ heißt das **Komplement** *von A (in M). Zuweilen schreiben wir auch A^c statt $\overline{A}$.*

Die Differenzmenge von A und B ist offensichtlich das Komplement von B in A, wenn $B \subset A$, s. Abb. 3.1. Allgemein gilt

$$A \setminus B = A \cap \overline{B},$$

wie man sich leicht überzeugt (Zeichnung!).
Sie spüren wahrscheinlich schon: $\cup$ und $\cap$ haben eine gewisse Ähnlichkeit mit den arithmetischen Operatoren „Addition“ und „Multiplikation“. Nur, dass die „Summanden“, bzw. „Faktoren“ nicht Zahlen, sondern Mengen sind! Wir nennen $\cup$ und $\cap$ **Mengenoperatoren**. Sie können im *Venndiagramm* veranschaulicht werden, s.Abb. 3.1 und 3.2.

3.3.3 Leere Menge

Enthält eine Menge kein einziges Element, so heißt sie **leere Menge**, geschrieben $\emptyset$. In der Schule, sonst nirgends, wird auch die Bezeichnung $\{\}$ verwendet.

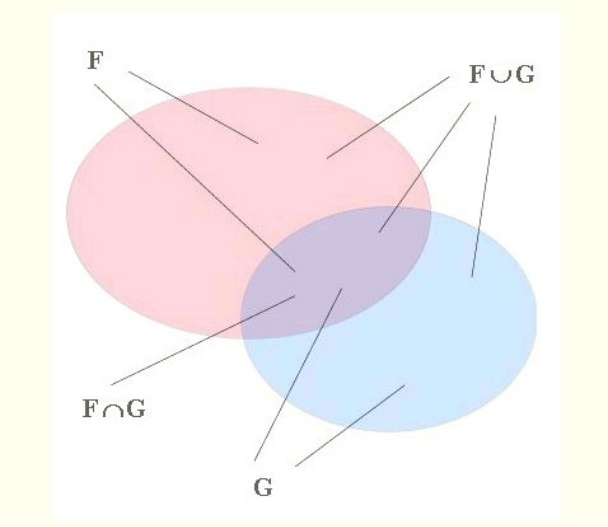


Abbildung 3.2: Vereinigung und Durchschnitt von F und G

Es gibt nur *eine* leere Menge. So ist die Menge aller Primzahlen zwischen 24 und 28 gleich der Menge aller fliegenden Elefanten im Geomatikum. Es gilt – auch dies ist gewöhnungsbedürftig – $\emptyset \subset A$ für jede Menge A! Dass dies formal richtig ist, liegt an Axiomen der Aussagenlogik, nach denen die Aussage „*Für alle* $x \in \emptyset$ *gilt* $x \in A$“ wahr ist, da der Bedingungsteil $x \in \emptyset$ niemals wahr ist. Sie können es aber auch einfach als eine zweckmäßige Vereinbarung (ähnlich wie die Potenzregel $a^0 := 1$) auffassen.
Aber lassen Sie sich hierdurch nicht verwirren. Wichtig ist hier erst einmal nur der Begriff *disjunkt* im Zusammenhang mit der leeren Menge: Zwei Mengen A und B heißen **disjunkt** $:\Longleftrightarrow\ A \cap B = \emptyset$, wenn also A und B keine gemeinsamen Elemente besitzen. Letzteres kann man verstehen. Um dann dennoch $A \cap B$ als Menge erkennen zu können, muss man die leere Menge einführen. Diese Konstruktion ist noch viel abstrakter als die der Zahl Null, die Sie auf keinen Fall mit der leeren Menge verwechseln dürfen.

Hinweis:

$$0 \neq \emptyset, \quad |\emptyset| = 0.$$

3.3.4 Rechenregeln und etwas Logik

Satz 3.5. *Es seien $A, B, C \subset M$ beliebige Mengen. Dann gelten*
a) $A \cap (B \cap C) = (A \cap B) \cap C, \qquad A \cup (B \cup C) = (A \cup B) \cup C$ *(Assoziativgesetze)*
b) $A \cap B = B \cap A, \qquad A \cup B = B \cup A$ *(Kommutativgesetze)*
c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(Distributivgesetze)*

d) $A \cap M = A, \quad A \cup M = M, \quad A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A$
e) $A \cap \overline{A} = \emptyset, \quad A \cup \overline{A} = M$
f) $\overline{\overline{A}} = A$
g) $\overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$ *(Regeln von de Morgan)*

Zum **Beweis**:
Mir kommt es an dieser Stelle nicht darauf an, dass Sie hier eine formal korrekte Form eines Beweises lernen, sondern dass die jeweiligen Aussagen verstanden werden und wenigstens „begründet“ werden können. Hierzu sollten zu Beginn Zeichnungen angefertigt werden (analog zu den Abb. 3.1 und 3.2), die die Aussagen untermauern.
Formal korrekte Beweise erfordern ein sicheres Umgehen mit einigen Regeln der (axiomatischen) Aussagenlogik. Hier ergibt sich eine gute Gelegenheit, hierzu einen ersten Kontakt herzustellen. Betrachten wir z.B. wie in g) die Aussage „$x \in \overline{A \cap B}$“. Diese ist offensichtlich – nach Definition des Komplements – gleichwertig mit der Aussage „$x \notin (A \cap B)$“, ausgesprochen nach Definition des Durchnitts „*x ist nicht sowohl in A als auch in B enthalten*“. Unser logischer Sachverstand (welchen Regeln folgt dieser?) sagt uns, dass diese Aussage gleichwertig ist mit „$x \notin A$ **oder** $x \notin B$“. Nach Definition des Komplements bedeutet diese Aussage „$x \in \overline{A}$ **oder** $x \in \overline{B}$“ bzw. nach Definition der Vereinigung „$x \in \overline{A} \cup \overline{B}$“. Damit ist die erste Regel in g) bewiesen.

Können Sie folgen? Versuchen wir es mit logischen Regeln: Bezeichne mit a die Aussage „$x \in A$“ und mit b die Aussage „$x \in B$“. Unsere Aussage „*x ist nicht sowohl in A als auch in B enthalten*“ lautet: „*Es gilt nicht* $a \wedge b$“. Aussagen kann man verneinen und man erhält so neue Aussagen. Die Verneinung von a nenne ich $\overline{a}$ („$x \notin A$“ bzw. „$x \in \overline{A}$“). Entsprechend $\overline{b}$. Ein logisches Gesetz lautet „*Nicht* $(a \wedge b) = \overline{a} \vee \overline{b}$“.

Vielleicht verstehen Sie aber auch den folgenden Beweis besser: Wir zeigen denselben Sachverhalt $\overline{A \cap B} = \overline{A} \cup \overline{B}$, indem wir alle vier möglichen Fälle

1. $x \in A$ und $x \in B$,
2. $x \in A$ und $x \notin B$,
3. $x \notin A$ und $x \in B$,
4. $x \notin A$ und $x \notin B$

in einer Tabelle untersuchen. In der Tabelle 3.1 bedeutet eine 1 „*x ist Element von*“ und eine 0 „*x ist nicht Element von*“.
Da die Einträge in den fett gekennzeichneten Spalten übereinstimmen, ist die Behauptung bewiesen. ∎

Mit diesem Beweis wollen wir uns hier begnügen. Die anderen Aussagen werden z.T. in den Übungen behandelt. Sie können sich auch selbst daran versuchen.

Tabelle 3.1: Beweis von Satz 3.5 g

A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cup \overline{B}$
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

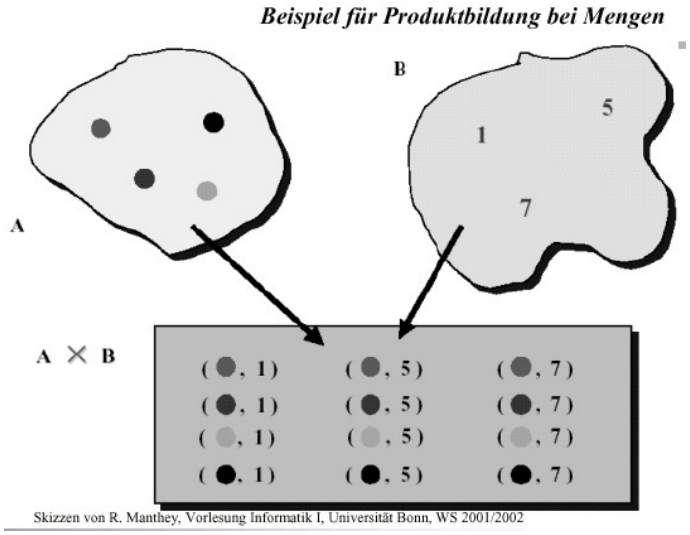


Abbildung 3.3: Kartesisches Produkt

3.3.5 Kartesisches Produkt

Definition 3.6. *Seien A, B beliebige Mengen. Dann heißt*

$$A \times B := \{(a, b) \mid a \in A, b \in B\} \quad \textbf{kartesisches Produkt} \textit{ der Mengen } A \textit{ und } B,$$

siehe Abb. 3.3. Ein Element (a, b) von $A \times B$ heißt **geordnetes Paar**.

Neu ist hier die Notation (a, b) für ein *geordnetes Paar*. $A \times B$ besteht aus allen geordneten Paaren (a, b) mit $a \in A$ und $b \in B$.
Vertraut müsste Ihnen diese Begriffsbildung aus der Schule sein, wenn $A = B = \mathbb{R}$. Dann kann man ein geordnetes Paar (x, y) als einen *Punkt* mit den *kartesischen Koordinaten* x und y deuten (s. Abb. 3.4).
Wenn x und y Dezimalzahlen sind, z.B. $x = 1,256$ und $y = 3,23$, so wird auch ein Semikolon (aber nur dann!!!) an Stelle des Kommas verwendet: $(1,256; 3,23)$ ist ein geordnetes Paar von Zahlen.
Analog definiert man $A \times B \times C := \{(a, b, c) \mid a \in A, b \in B, c \in C\}$, usw.

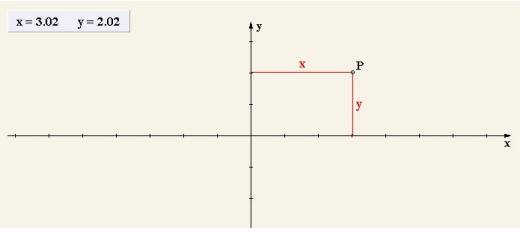


Abbildung 3.4: Kartesische Koordinaten

Für $A \times A \times \cdots \times A$ (n-mal) schreibt man auch auch kurz A^n.

Beispiele:
1) $\{1,2\} \times \{x,y\} = \{(1,x),(1,y),(2,x),(2,y)\}$.
2) $\{1,2\}^3 = \{1,2\} \times \{1,2\} \times \{1,2\} = \{(1,1,1),(1,1,2),\ldots,(2,2,2)\}$ (insgesamt acht Elemente).
3) A sei die Menge aller Nachnamen, B die Menge aller Geburtsdaten und C die Menge aller (Augen-) Farben. Dann kann man jeden Menschen durch ein **geordnetes Tripel** $(a,b,c) \in A \times B \times C$ darstellen.
4) Als immatrikulierte StudentIn sind Sie als Datensatz einer Datenbank im Computer des Studierendenzentrums als „n-Tupel“ $(a_1, a_2, ..., a_n)$ eines kartesischen Produkts $A_1 \times A_2 \times \cdots \times A_n$ gespeichert. Was werden die Mengen $A_1, ..., A_n$ sein? Gefällt es Ihnen, zu einem *n-Tupel* reduziert zu werden?

Bemerkung: Für endliche Mengen M ist ja $|M|$ die Anzahl ihrer Elemente. Dann gilt $|A \times B| = |A| \cdot |B|$. Diese Regel ist die einfachste Regel der Kombinatorik, sie heißt **Produktregel**[3]. Schon in der Grundschule wird sie angewendet, wenn man z.B. die Kästchen eines vertikal und horizontal unterteilten Rechtecks zählt. Man kann jede der $|A|$ Möglichkeiten für die erste *Komponente* a des geordneten Paares (a,b) mit jeder der $|B|$ Möglichkeiten für die zweite Komponente b kombinieren.

Warnung: Man unterscheide die Menge A von ihrer Anzahl $|A|$.

Aus der Produktregel folgt auch $|A^n| = |A|^n$ für alle endlichen Mengen A. Können Sie das verstehen? Für $n = 2$ ist dies ein Spezialfall obiger Produktregel, für $n = 3$ kann man diese ebenfalls anwenden, wenn man $A^3 = (A \times A) \times A$ schreibt, $B := A \times A$ setzt und $|(A \times A) \times A| = |A \times A| \cdot |A|$ beachtet. So wird der Fall $n = 3$ auf den Fall $n = 2$ zurückgeführt. Dies ist ein sogenannter „Induktionsschritt“, ein Teilschritt der „vollständigen Induktion“, siehe Kap. 6.

Warnung: Man beachte den Unterschied zwischen dem geordneten Paar (a,b) und der Menge $\{a,b\}$.

[3]Noch einfacher ist die **Summenregel** $|A \cup B| = |A| + |B|$ für disjunkte Mengen A und B.

3.3.6 Potenzmenge

Definition 3.7. *Sei M eine beliebige Menge. Die* **Potenzmenge** *von M, geschrieben Pot M, ist die Menge aller Teilmengen von M.*

Hier sind die Elemente von Pot M alle selbst wieder Mengen! Da $\emptyset \subset M$ für jede Menge M, enthält Pot M stets mindestens ein Element, so dass Pot $\emptyset = \{\emptyset\} \neq \emptyset$ gilt! Ist $M \neq \emptyset$, so enthält Pot M mindestens zwei Elemente: neben $\emptyset$ mindestens noch M selbst.

Beispiele:
1) $M = \{1, 2\} \Longrightarrow \text{Pot}M = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
2) $\text{Pot}(\text{Pot } M) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\{2\}\}, \{M\}, \{\emptyset, \{1\}\}, \{\emptyset, \{2\}\}, \{\emptyset, M\}, \{\{1\}, \{2\}\},$
$\{\{1\}, M\}, \{\{2\}, M\}, \{\emptyset, \{1\}, \{2\}\}, \{\emptyset, \{1\}, M\}, \{\emptyset, \{2\}, M\}, \{\{1\}, \{2\}, M\}, \text{Pot}M\}$.
3) Sei $A = \{x\}, B = \{a, b\}$. Dann ist $\text{Pot}(A \times B) = \{\emptyset, \{(x, a)\}, \{(x, b)\}, \{(x, a), (x, b)\}\}$.
4) Pot $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$.

Später werden wir beweisen, dass im Falle $|M| = n$ für die Mächtigkeit der Potenzmenge $|\text{Pot } M| = 2^n = 2^{|M|}$ gilt.

Warnung:

$$Pot\,\emptyset \neq \emptyset$$

Wo kommen solche Potenzmengen vor? Sei M die Menge aller HörerInnen dieser Vorlesung. Jetzt interessieren wir uns für die Teilmenge von M, deren „Elemente“ in dieser Woche sämtliche Testaufgaben eines Tests richtig lösen. Dann liefert der Test genau ein Element der Potenzmenge Pot M. Ist dieses Element $\emptyset$, so hat keiner alle Aufgaben gelöst, ist dieses Element ganz M, so waren alle erfolgreich. Insgesamt gibt es $2^{|M|}$ mögliche Resultate.

In der Kombinatorik werden wir nach allen Teilmengen von M mit gleicher Anzahl $k \leq |M|$ fragen. Wenn $|M| = n$, so führt diese Frage auf den *Binomialkoeffizienten* $\binom{n}{k}$.

In der Stochastik betrachtet man Zufallsexperimente, z.B. den Wurf eines Würfels. Alle möglichen Ergebnisse bilden den *Merkmalraum* Ω, z.B. $\Omega = \{1, 2, 3, 4, 5, 6\}$. Jeder Teilmenge $A \subset \Omega$ ordnet man sodann eine Wahrscheinlichkeit $P(A)$ zu, das ist die Wahrscheinlichkeit, dass das Ergebnis des Zufallsexperimentes in A liegt. Pot Ω nennt man dann die Menge aller *Ereignisse*.

3.3.7 Paradoxa

Unerwartete Komplikationen (Mathe Online)
Die naive Mengenlehre führt zu Widersprüchen, wenn die Objekte, die einer Menge angehören, „wild“ ausgewählt werden. Das bekannteste Beispiel stammt von B. Russel (1872 - 1970): Man betrachtet alle Mengen, die sich nicht selbst als Elemente enthalten und versucht aus diesen eine „Menge“ zu bilden :

$$M := \{A \text{ ist eine Menge} : A \notin A\}$$

Wenn M wirklich eine Menge ist, gibt es genau eine von zwei Möglichkeiten: $M \in M$ oder $M \notin M$. Nach Defintion von M führt jede dieser Annahmen zu einem Widerspruch.
Die logische Grundstruktur dieses Widerspruchs wird oft in folgendes Gewand gekleidet: Ein Dorfbarbier rasiert alle Männer im Dorf, die sich nicht selbst rasieren. Frage: Rasiert er sich selbst?
Angenommen, er rasiert sich selbst, dann rasiert er sich nicht (denn er rasiert ja nur all jene, die sich nicht selbst rasieren) - ein klarer Widerspruch. Die Annahme muss falsch sein.
Angenommen, er rasiert sich nicht selbst, dann rasiert er sich sehr wohl (denn er rasiert ja alle, die sich nicht selbst rasieren) - wieder ein klarer Widerspruch. Auch diese Annahme ist falsch!
Das „Grundübel“ dieser Beispiele sind *selbstbezogene* Aussagen wie $M \in M$.
Auch die Konstruktion der „Menge aller Mengen“ ist an sich widersprüchlich – solch eine Menge kann es nicht geben. Denn die („größere“) Potenzmenge dieser Menge wäre ja wieder eine Menge ..... Dieses Paradoxon geht schon auf Cantor zurück.
Einen guten Überblick gibt die Webseite Selbstbezüge(Prof. Urban, Internatschule Wien)
Siehe auch Bertrand-Russell: Sein Paradoxon wird 100 Jahre alt (Süddeutsche Zeitung vom 1.6.2001; Pressetimmen des Mathematik-Portals).
Um diese Paradoxa zu vermeiden, muss man auf die *axiomatische Mengenlehre* statt auf die *naive* Mengenlehre zurückgreifen. Zum Glück werden uns nur „harmlose“ Mengen begegnen.

Kapitel 4

Relationen

4.1 Einführung

Relationen bedeuten umgangssprachlich *Beziehungen*, in denen zwei Dinge zueinander stehen können. Wir kennen *Verwandtschaftsbeziehungen* zwischen Personen, *Partnerschaftsbeziehungen* zwischen Städten, usw. In der Mathematik interessieren wir uns vor allem für Relationen zwischen Zahlen, aber auch Mengen. Eine der wichtigsten ist die *Ordnungsrelation* „$x \leq y$“ auf der Menge $\mathbb{R}$ und die Teilbarkeitsrelation „n teilt m“ auf der Menge $\mathbb{N}$. Man führt gewisse abstrakte Eigenschaften von Relationen (*Reflexivität, (Anti-) Symmetrie, Transitivität*) ein und kommt dadurch auf die wichtigsten Typen von Relationen, die *Ordnungsrelationen* und die *Äquivalenzrelationen*. Letztere erlauben es, gewisse Dinge in einem bestimmten Sinne als *gleich* (eben *äquivalent*) anzusehen. In diesem Sinne kann man z.B. zwei Geburtsdaten als gleich ansehen, wenn man das Geburtsjahr außer Acht lässt und nur auf den Monat und den Tag achtet[1].
Ein anderes Beispiel aus der Geometrie: Es macht Sinn, zwei Dreiecke als äquivalent oder auch „gleich“ anzusehen, wenn sie deckungsgleich sind. Genauso gut könnte man sie als äquivalent ansehen, wenn sie ähnlich sind.
Dieses Kapitel ist relativ abstrakt. Ich werde wahrscheinlich die beiden Beweise dieses Kapitels in der Vorlesung nur skizzieren. Wichtig ist mir, dass Sie die Begriffe *Ordnungs-* und *Äquivalenzrelation* an Hand der $\leq$-Relation von reellen Zahlen und an Hand der Kongruenzrelation R_s („gleicher Rest bei Division durch s“, s. 4.2) von ganzen Zahlen verstehen und insbesondere bei letzterer wissen, was die Äquivalenzklassen sind. Die neuen Begriffe sind allerdings gut geeignet, formales logisches Denken zu schulen. Die Vorgehensweise ist typisch für viele Bereiche der Mathematik, aber auch der Informatik – im Internet findet man unter dem Stichwort *Relationen* einige Skripte aus der Informatik.

Einer der wichtigsten Begriffe der Mathematik ist der der *Funktion* (auch *Abbildung* genannt),

[1] Dies ist mathematisch eine *Kongruenzrelation* von Zahlen modulo einer vorgegebenen Zahl (hier 365), s. Def.4.2.

s. Kap. 5. Dieser Begriff hängt eng mit dem der Relationen zusammen.

Siehe auch Gleichheit und Ordnung (Mathematik-Portal)

4.2 Definition und Beispiele

Wir interessieren uns für gewisse Teilmengen eines *kartesischen Produktes* $A \times B$ von zwei Mengen A und B, siehe Kap. 3.3.5.

Definition 4.1. *Seien A, B beliebige Mengen. Jede Teilmenge $R \subset A \times B$ heißt* **Relation von A nach B.** *Ist $A = B$, (also $R \subset A \times A$), so heißt R auch* **(zweistellige, binäre) Relation auf A.**

Beispiele:
1) Sei A die Menge aller europäischen Hauptstädte und B die Menge aller Länder. Dann ist $R := \{(a, b) \in A \times B \mid a \text{ ist Hauptstadt von } b\}$ eine Relation. Es gilt (Rom, Italien) $\in R$, (Wien, Belgien) $\notin R$. Man könnte dieser Relation den Namen „Hauptstadtrelation“ geben.

2) Sei A die Menge aller Personen in diesem Hörsaal, R sei die Menge aller Personen-Paare, die direkt nebeneinander sitzen („Nachbarschaftsrelation“). Eine Person steht höchstens mit zwei anderen in dieser Nachbarschaftsrelation, die am Rande einer Reihe sitzenden Personen stehen höchstens mit einer Person in Relation, manche vielleicht auch mit keiner.

3) $A := \mathbb{N}$, $(a, b) \in R \subset \mathbb{N} \times \mathbb{N} :\Longleftrightarrow\ a \leq b$. Hier gilt $(1, 4) \in R, (3, 2) \notin R$. R ist die bekannte $\leq$ – Relation. Statt $(m, n) \in R$ schreibt man natürlich auch $m \leq n$.

4) Sei $T := \{(a, b) \in \mathbb{N}^2 \mid a \text{ und } b \text{ haben beim Teilen durch 3 den gleichen Rest}\}$. Statt $(2, 5) \in T$ schreibt man auch $2 \equiv 5 \bmod 3$ und nennt 2 und 5 *kongruent modulo 3*. Diese Relation spielt in der Zahlentheorie eine große Rolle. Daher bringen wir hier die allgemeine Definition:

Definition 4.2. *Zwei ganze Zahlen m, n heißen* **kongruent modulo** *einer natürlichen Zahl s genau dann, wenn s teilt $(m - n)$ bzw. (hiermit äquivalent) wenn m und n bei Division durch s denselben* **Rest** *haben. Diese Relation nennen wir* **Kongruenzrelation** *bezüglich s. Genauer: Die Kongruenzrelation modulo s, genannt R_s, ist durch*

$$(m, n) \in R_s :\Longleftrightarrow\ \ s \text{ teilt } (m - n) \tag{4.1}$$

definiert.
Satt $(m, n) \in R_s$ schreibt man i.A.

$$m \equiv n \bmod s.$$

Beispiele: $(19, 25) \in R_6, (22, 28) \notin R_4$.

Die oben behauptete Äquivalenz

$$m \equiv n \bmod s \Longleftrightarrow m \bmod s = n \bmod s$$

ist deshalb nicht sofort offensichtlich, da die Modulo-Operation $m \bmod s$ insbesondere für negative Zahlen m noch nicht präzise definiert wurde. Bevor das nachgeholt wird, muss darauf hingewiesen werden, dass $\equiv$ nicht durch ein Gleichheitszeichen ersetzt werden darf. Keineswegs gilt stets

$$m \equiv n \bmod s \Longleftrightarrow m = n \bmod s,$$

da $n \bmod s$ als Rest aus $\{0, 1, ..., s-1\}$ ist.

Definition modulo:
Es gilt für $s \in \mathbb{N}$ und $m \in \mathbb{Z}$:

$$r = m \bmod s : \Longleftrightarrow \exists k \in \mathbb{Z} : m = k \cdot s + r \ \wedge \ r \in \mathbb{N}_0 \text{ mit } 0 \leq r < s.$$

Bemerkung: Weil $r := m \bmod s$ ein Rest bei der Division durch s ist, wird $0 \leq r < s$ verlangt.

Bei der Division mit Rest hatten wir bisher nur Zahlen aus $\mathbb{N}_0$ betrachtet. Jetzt kommen auch *negative Zahlen* aus $\mathbb{Z}$ ins Spiel. Z.B. ist $(-17, 25) \in R_6$ oder anders ausgedrückt:

$$-17 \equiv 25 \bmod 6,$$

weil 6 ein Teiler von -42 ist. Oben wird behauptet, dass

$$-17 \bmod 6 = 25 \bmod 6 (= 1)$$

ist. Wieso? Warum hat -17 geteilt durch 6 den Rest 1? Eine Erklärung geht so: -18 geteilt durch 6 ist -3 – ohne Rest! -17 ist um Eins größer als -18, diese Eins bleibt als Rest! Anders ausgedrückt: Es gilt $-17 = (-3) \cdot 6 + 1$, d.h. in obiger modulo-Definition ist $k = -3$ (für $s := 6$ und $m := -17$).
Wer genau hinschaut, merkt, dass die Definition von „Teiler“ in Kap. 2.4 sich nur auf natürliche, nicht auf ganze Zahlen bezog. Aber ich denke, Sie verstehen dies auch so. Wer eine präzise Definition braucht, sei versorgt:

Definition 4.3. *$n \in \mathbb{Z}$ ist* **Teiler** *von $m \in \mathbb{Z}$ genau dann, wenn es ein $r \in \mathbb{Z}$ gibt mit $m = r \cdot n$. Etwas formaler:*

$$n \in \mathbb{Z} \text{ ist } \textbf{Teiler} \text{ von } m \in \mathbb{Z} : \Longleftrightarrow \exists r \in \mathbb{Z} : m = r \cdot n.$$

Das bedeutet, dass jede ganze Zahl ein Teiler der Null ist!

Schreibweisen: Jetzt sei R wieder irgend eine Relation von A nach B. Statt $(a, b) \in R$ schreibt man auch aRb oder $a \sim_R b$ oder auch einfach $a \sim b$, letzteres besonders bei Äquivalenzrelationen, s. Kap. 4.4.

4.3 Reflexivität, (Anti-)Symmetrie und Transitivität

Definition 4.4. *Sei R eine Relation auf A. Man nennt die Relation R*
(r) **reflexiv**, *falls für alle $a \in A$ stets $(a, a) \in R$ folgt.*
(s) **symmetrisch**, *falls für alle $a \in A$ und alle $b \in A$ aus $(a, b) \in R$ stets $(b, a) \in R$ folgt.*
(t) **transitiv**, *falls für alle $a, b, c \in A$ aus $(a, b) \in R$ und $(b, c) \in R$ stets $(a, c) \in R$ folgt.*
(as) **antisymmetrisch**, *falls für alle $a, b \in A$ aus $(a, b) \in R$ mit $a \neq b$ stets $(b, a) \notin R$ folgt.*

Bemerkung: Alle diese Eigenschaften sind von dem Typ „Für alle ....$\in A$ folgt aus ....A1..... stets ....A2....“. Dabei sind A1 und A2 gewisse Aussagen. Dabei brauchen nur die Fälle betrachtet zu werden, bei denen die *Voraussetzungen* A1 wahr sind. Wenn z.B. $A := \{1, 2\}$ und $R := \{(1, 1), (2, 2)\}$, so ist (r) erfüllt, aber auch alle anderen Eigenschaften (es handelt sich um die Gleichheits-Relation), z.B. auch (as), „obwohl“ es gar keinen Fall gibt mit $(a, b) \in R, a \neq b$. Man soll sich davor hüten, aus der „Nicht-Symmetrie“ auf die Antisymmetrie zu schließen. Z.B. ist mit $A := \{1, 2, 3\}$ die Relation $R : \{(1, 2), (2, 1), (2, 3)\}$ weder symmetrisch (hier fehlt $(3, 2)$) noch antisymmetrisch (hier müsste $(1, 2)$ oder $(2, 1)$ gestrichen werden).

Für die Beispiele 2), 3), 4) des vorangehenden Kap. 4.2 gilt:

	(r)	(s)	(t)	(as)
Nachbar	$-$	$+$	$-$	$-$
$\leq$	$+$	$-$	$+$	$+$
modulo 3	$+$	$+$	$+$	$-$

Uns interessieren folgende Fragen:
1) Gibt es Relationen, die alle vier Eigenschaften gleichzeitig erfüllen?
2) Welche Kombinationen der Eigenschaften sind nicht möglich?

Die Antwort auf die erste Frage lautet: Es gibt nur eine solche Relation, nämlich die Gleichheitsrelation.
Beschränkt man sich auf die Eigenschaften $(r), (s)$ und (t), so ist jede Kombination hieraus möglich.

Beispiel: Sei $A := \{a, b, c\}$ eine Menge. Die Relation $R_1 := \{(a, a), (b, c), (c, b)\}$ ist symmetrisch, aber nicht reflexiv und nicht transitiv, $R_2 := \{(a, a), (b, b)\}$ ist nicht reflexiv (es fehlt (c, c)), erfüllt aber (s) und (t). Mancher LeserIn mag dieses Beispiel Kopfzerbrechen machen, da die Namen für die Elemente von A identisch sind mit denen, die in den Bedingungen (r), (s), (as) und (t) vorkommen. Daher mag es einfacher sein, im ersten Beispiel die Elemente von A in $A := \{x, y, z\}$ „umzutaufen“. Dann gilt $R_1 = \{(x, x), (y, z), (z, y)\}$. Nun ist R_1 nicht reflexiv, weil die Paare (y, y) und (z, z) fehlen. Zur Symmetrie sind nur die Paare (a, b) mit $a \neq b$ zu betrachten. Da hier sowohl (y, z) als auch (z, y) in R_1 liegen, ist (s) erfüllt, während (as) nicht gilt – eben wegen dieses „Doppelpacks“. Nun zur Transitivität: Hier sind nur solche Fälle zu

betrachten, in denen ein „Doppelpack“ (a, b) und (b, c) zur Relation gehören. Und zwar nur die Fälle, in denen $a \neq b$ und $b \neq c$ – denn sonst ist die Folgerung $(a, c) \in R$ „trivial“. In unserer Relation R_1 muss man nur das Paar $(y, x), (x, y)$ betrachten und erhält einen Widerspruch zu (t), da aus (t) $(y, y) \in R_1$ folgen müsste.

4.4 Äquivalenzrelationen und Ordnungsrelationen

Definition 4.5. *Sei R eine Relation auf A. Man nennt die Relation R*

(1) **Äquivalenzrelation**, *falls sie reflexiv, symmetrisch und transitiv ist.*

(2) **Ordnungsrelation**, *falls sie reflexiv, antisymmetrisch und transitiv ist.*

Die Gleichheitsrelation ist die einzige Relation, die gleichzeitig Äquivalenz– und Ordnungsrelation ist. Ein weiteres und sehr wichtiges Beispiel für eine Äquivalenzrelation ist die Kongruenz–Relation R_s in Def. 4.2. Für Zahlen sind $\leq$ bzw. $\geq$ Ordnungsrelationen. Die Kleiner–Relation $<$ ist keine Ordnungsrelation, da sie nicht reflexiv ist!

Die „Teilungs-Relation“ R auf $\mathbb{N}$, definiert durch „$(m, n) \in R :\iff m$ teilt n“ ist eine Ordnungsrelation! Siehe Übungen.

Frage: Ist $R = \{(a, b), (a, c), (b, d), (c, d), (a, d), (a, a), (b, b), (c, c), (d, d)\}$ eine Ordnungs– oder eine Äquivalenzrelation auf $A := \{a, b, c, d\}$?
Antwort: (r) ist erfüllt, weil die ganze „Diagonale“ $\{(a, a), (b, b), (c, c), (d, d)\}$ von A Teilmenge von R ist. (s) ist nicht erfüllt, da zwar $(b, d) \in R$, aber $(d, b) \notin R$. Dagegen ist R antisymmetrisch, da zwar $(a, b) \in R$, aber $(b, a) \notin R$, desgleichen $(a, c) \in R$, aber $(c, a) \notin R$, desgleichen $(a, d) \in R$, aber $(d, a) \notin R$, desgleichen $(b, d) \in R$, aber $(d, b) \notin R$, desgleichen $(c, d) \in R$, aber $(d, c) \notin R$. Die Transitivität (t) ist ebenfalls erfüllt. Die einzigen nichttrivialen Fälle, in denen die Voraussetzung in (t) zutrifft, sind $(a, c) \in R, (c, d) \in R$ (hier folgt in der Tat $(a, d) \in R$) sowie $(a, b) \in R, (b, d) \in R$ (auch hier folgt $(a, d) \in R$). Es handelt sich also um eine Ordnungsrelation.

4.4.1 Äquivalenzklassen

Ich begnüge mich mit Beispielen und verzichte auf eine strenge Definition von Äquivalenzklassen.
Schauen wir uns die Kongruenzrelation R_s in Def. 4.2 an, für die zwei Zahlen m und n kongruent modulo s heißen, wenn sie bei Teilung durch s denselben Rest haben (kurz: $m \equiv n \bmod s$). Diese Relation ist eine Äquivalenzrelation. Hier gibt es s verschiedene Reste, beginnend bei 0, endend bei $s-1$. Betrachten wir alle (ganzen) Zahlen, die denselben Rest $r \in \{0, 1, ..., s-1\}$ haben, so bilden diese eine „(Äquivalenz-) Klasse“. Ist z.B. $s = 3$, so bilden $\{\ldots, -9, -6, -3, 0, 3, 6, 9, ...\}$ die eine mit Rest $r := 0$. Dagegen ist $\{\ldots, -8, -5, -2, 1, 4, 7, 10, ...\}$ die zweite zum Rest $r := 1$ und $\{\ldots, -7, -4, -1, 2, 5, 8, 11, ...\}$ die letzte Klasse mit Rest $r := 2$. Falls Sie mit den negativen Zahlen in diesen Klassen Schwierigkeiten haben: Schauen Sie sich noch einmal Def. 4.3 an.

Ein zweites Beispiel soll diesen Abschnitt beenden:
Sei M die Menge aller Dreiecke in der Anschauungsebene. Dann bildet die Kongruenzrelation (oder auch die Ähnlichkeitsrelation) eine Äquivalenzrelation. Eine Äquivalenzklasse besteht aus deckungsgleichen (oder ähnlichen) Dreiecken. Es gibt unendlich viele solche Klassen. Bei ähnlichen Dreiecken ist jede Klasse durch drei Winkel, die sich zu 180 Grad aufaddieren, gegeben.

4.5 Datenbanken

Ein *Datensatz* ist mathematisch nichts anderes als ein n-Tupel aus einem kartesischen Produkt $A := A_1 \times A_2 \times \cdots \times A_n$. Viele (hundert) Datensätze bilden dann eine endliche Teilmenge des kartesischen Produkts A, sind also mathematisch eine *n-stellige Relation*. Bei *relationalen Datenbanken* hat man es mit verschiedenen Relationen zu verschiedenen kartesischen Produkten zu tun, die z.T. in einer Komponente (einem *Datenfeld*) übereinstimmen.
Beispiel: Die eine Relation R_1 beziehe sich auf die *Stammdaten* von Studierenden (Name, Adresse, Geburtsdatum, Matrikelnummer, etc)[2], die andere Relation R_2 sei eine *Prüfungstabelle* (Matrikelnummer, Prüfungsfach, Note, Datum der Prüfung, PrüferIn, etc). Diese beiden Relationen haben mindestens ein gemeinsames Datenfeld (die Matrikelnummer). Daher kann man eine neue Relation R von R_1 nach R_2 dadurch definieren, dass wir aRb schreiben, wenn die Matrikelnummerkomponenten von a und b übereinstimmen, wenn also die betroffenen Personen identisch sind. R ist eine Relation von Relationen! Verstanden?

[2] A_1 ist dann eine Menge von Namen, A_2 eine Menge von Adressen, A_3 eine Menge von „Daten“ (hier als Plural von Datum), A_4 die Menge aller 8-stelligen positiven Zahlen, etc.

Kapitel 5

Funktionen (Abbildungen)

5.1 Einführung

Der nach dem der *Menge* wichtigste mathematische Sprachbegriff ist der einer *Funktion*, auch *Abbildung* genannt. Wenn man von *funktionalem Zusammenhang* spricht, ist eine Funktion im Spiel. Eine Funktion f ordnet einer *unabhängigen Variablen* x einer Menge A eine von x *abhängige Variable* $y = f(x)$ einer anderen Menge B zu: Es besteht ein funktionaler Zusammenhang zwischen $x \in A$ und $y = f(x) \in B$, z.B. zwischen dem Einkommen x und der hiermit verbundenen (Einkommen-) Steuer y. Man kann eine Funktion auch als „Input-Output-Maschine“ ansehen: x geht hinein, $y = f(x)$ kommt heraus. Wir werden $f : A \to B$ schreiben.
Es gibt eine Beziehung zwischen Funktionen und Relationen, wobei man x und $y = f(x)$ zu einem geordneten Paar (x, y) zusammenfasst. In diesem Sinne kann man Funktionen auch als spezielle Relationen auffassen. Dieser Zusammenhang ist aber nicht essentiell, allenfalls ist er von Bedeutung, wenn man den *Graph einer Funktion* (bei reellen Funktionen spricht man auch von *Funktionsbild*) betrachtet.
Eine sehr liebevolle und ausführliche Einführung: Funktionen 1 (Mathe Online).
Siehe auch Applet zur funktionalen Abhängigkeit (Mathe Online).

Die vielleicht wichtigste Klasse – insbesondere aus Sicht der Anwendungen und der Schulmathematik – von Funktionen sind die *reellen Funktionen*, für die die Variablen x und y reelle Zahlen sind. Die *Differential- und Integralrechnung* arbeitet mit diesen Funktionen. Diese kann man mittels ihrer *Graphen* zeichnerisch veranschaulichen und viele Eigenschaften grafisch beschreiben. *Kurvendiskussionen* in der Schule mögen Sie daran erinnern. Wir werden uns in späteren Kapiteln, insbesondere im Rahmen der Analysis, ausführlich mit den wichtigsten reellen Funktionen beschäftigen (Potenz-, Exponential-, trigonometrische Funktionen,...), auf diese allerdings auch jetzt schon am Rande eingehen.
Diese reellen Funktionen sind Ihnen von der Schule her sehr vertraut. Wahrscheinlich haben Sie von *Funktionsgleichungen* $y = f(x)$ gesprochen — eine Sprechweise, die ich für nicht sehr glücklich halte.

Für dieses Kapitel ist es ganz wesentlich, dass Sie den *abstrakten* Funktionsbegriff $f : A \to B$ verstehen, wobei A und B beliebige Mengen sein können. Dazu muss man sich vorrübergehend von dem aus der Schule her bekannten Funktionsbegriff lösen.

5.2 Abbildungen / Funktionen

Definition 5.1. *Seien A und B beliebige nichtleere Mengen. Eine* **Abbildung** *(oder auch* **Funktion***) f von A nach B ist eine Zuordnung, die jedem $a \in A$ genau ein $b \in B$ zuordnet. Man schreibt $f : A \to B$ und nennt A den* **Definitionsbereich** *und B den* **Bildbereich** *von f. Das $b \in B$, welches dem* **Argument** *$a \in A$ zugeordnet wird, wird als* **Funktionswert** *$b = f(a)$ notiert. Die Zuordnung wird mit $a \mapsto b = f(a)$ beschrieben. Zusammengefasst:*

$$f : \left\{ \begin{array}{ccc} A & \to & B \\ a & \mapsto & f(a) = b \end{array} \right.$$

„*Es gibt genau ein*“ ist eine typisch mathematische Sprechweise. Sie bedeutet, dass es erstens eins gibt und zweitens, dass es nicht mehr als eins gibt. Z.B. hat jeder Mensch genau eine Mutter, aber nicht jede Mutter hat genau ein Kind. Wenn A die Menge aller jemals lebender Menschen und B die Menge aller jemals lebender Mütter ist, so ist die Zuordnung, die jedem $a \in A$ dessen Mutter b zuordnet, eine Abbildung. Nicht aber die Zuordnung, die jeder Mutter $b \in B$ ihr Kind zuordnet, da eine Frau ja mehr als ein Kind haben kann.

Diese Definition hat die Schwäche, dass der Begriff *Zuordnung* mathematisch nicht rigoros definiert ist. Deswegen ist die folgende Definition mathematisch befriedigender, aber etwas schwieriger zu verstehen:

Definition 5.2. *Seien A und B beliebige nichtleere Mengen. Eine Relation f von A nach B heißt* **Abbildung** *(oder auch* **Funktion***)* $:\iff$

$$\forall a \in A : \qquad \textit{es gibt genau ein } b \in B \ : \ (a, b) \in f$$

Um die Brücke zur ersten Definition 5.1 zu schlagen, greift man auf den Begriff *Zuordnung* zurück: Jedem $a \in A$ wird das *eindeutig bestimmte* $b \in B$ mit $(a, b) \in f$ *zugeordnet.*

Zur Veranschaulichung einer Abbildung ist zuweilen ein „Pfeildiagramm“ (s. Abb. 5.1) nützlich. Manchmal schreibt man auch kurz $f(x)$ an Stelle von f. Oder gar $y(x)$. Das ist aber mathematisch ungenau und soll hier vermieden werden, auch wenn es seinen „Reiz“ wegen der Kürze ($f(x) = x^2, f(x) = \sqrt{x}, ...$) hat. Das x hat hier eher die Bedeutung eines *Platzhalters.*

Warnung: Man unterscheide zwischen **Funktion** f und **Funktionswert** $f(x)$.

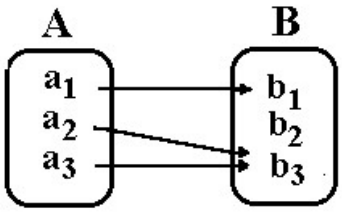


Abbildung 5.1: Funktion als Zuordnung

Die Schreibweise $f = x^2$ an Stelle von $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist falsch. Die Schreibweise $f(x) = x^2$ ist unschön, aber nicht falsch.

Andere Sprechweisen: Die Funktion *wirkt auf die Elemente von A*, sie wird auf diese *angewandt (angewendet)*. Elemente von A werden in die Funktion *eingesetzt*. Jedes Element von A wird auf ein Element von B *abgebildet*.

5.2.1 Reelle Funktionen und ihre graphische Darstellung

In der Schule (und auch hier) spielen **reelle Funktionen** $f : \mathbb{R} \to \mathbb{R}$ eine ganz wesentliche Rolle, z.B.

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x) = x^2 \end{array} \right. ,$$

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x) = \sin(x) \end{array} \right. ,$$

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x) = \frac{1}{1+x^2} \end{array} \right. .$$

Andere wichtige Funktionsklassen sollen schon erwähnt werden: **Potenzfunktionen** $x \mapsto x^n$ mit $n \in \mathbb{N}$ oder allgemeiner (mit einem Exponenten $b \in \mathbb{R}_+$) $x \mapsto x^b$, **Exponentialfunktionen** $x \mapsto a^x$ mit einer Basis $a > 0$, **trigonometrische Funktionen**[1] $x \mapsto \sin(ax + b)$ mit $a, b \in \mathbb{R}$ und der **Logarithmus zur Basis** a (die Umkehrfunktion von $x \mapsto a^x$), die nur für positive Zahlen x definiert ist: $x \mapsto^a \log(x)$.
Wenn wir bei diesen reellen Funktionen auf die ursprüngliche Definition als Relation zurückgreifen, haben wir es mit

$$G(f) := \{(x, f(x)) : x \in \mathbb{R}\},$$

der Menge aller Zahlenpaare zu tun, die als Punkte in einem Koordinatensystem das **Funktionsbild** von f liefern[2], das auch **(Funktions-)Graph** von f genannt wird (auch für allgemeine

[1] Es gilt $\cos(x) = \sin(x + \pi/2)$.
[2] Hierbei beschränkt man sich i.A. auf ein Intervall $[a, b]$ für das Argument x.

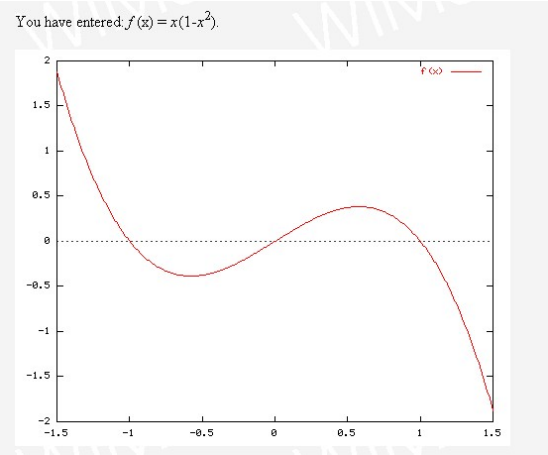


Abbildung 5.2: Graph von $x \mapsto x(1-x^2)$

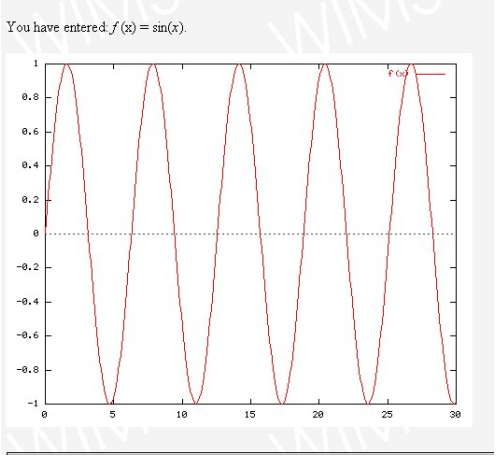


Abbildung 5.3: Graph von $x \mapsto \sin x$

$f : A \to B$), s.Abb. 5.2[3] und 5.3[4]. Häufig liegt ihm eine *Wertetabelle* zu Grunde, siehe Abb. 5.5 und Abb. 5.4.
Die beiden Abbildungen 5.2 und 5.3 wurden mit Hilfe eines Online Calculator (Universität Nizza (F)) im Internet erhalten[5].

Warnung: Man unterscheide zwischen **Funktion** f und **Funktionsbild** $G(f)$.

Es gibt auch eine Reihe von Abbildungen, die in diesem (engen) Sinne keine *reellen* Funktionen

[3] f ist hier auf $[-1.5, 1.5]$ definiert.
[4] f ist hier auf $[0, 30]$ definiert.
[5] Wählen Sie den „Function calculator“.

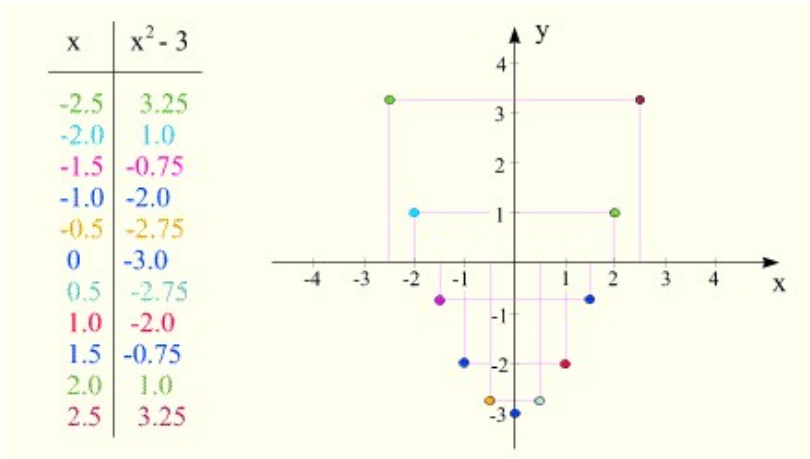


Abbildung 5.4: Wertetabelle und Graph von $x \mapsto x^2 - 3$

sind. Ist z.B. A die Menge aller Studierenden an der Uni HH und B die Menge $B := B_1 \times B_2 \times B_3$ mit $B_1 :=$ Menge aller Namen, $B_2 :=$ Menge aller Adressen und $B_3 :=$ Menge aller Schulen, an denen man die Hochschulreife erwerben kann, so kann man ein $f : A \to B$ definieren, indem man jedem Studierenden $a \in A$ ein Tripel aus Name, Adresse und Schule zuordnet[6].

Nicht jede Relation R von A nach B ist eine Funktion $f : A \to B$ – wenn es z.B. nicht zu jedem $a \in A$ ein $b \in B$ gibt mit $(a, b) \in R$ oder weil es zu einem $a \in A$ mehrere $b \in B$ gibt mit $(a, b) \in R$. Die (binäre) *Eltern-Kind*-Relation auf der Menge aller Menschen A ist z.B. keine Funktion von A nach A, da zum einen nicht jeder Mensch Kinder hat oder auch mehr als ein Kind hat.

5.2.2 Definitionsbereich, Bildbereich, Bildmenge, Urbildmenge

Zunächst sei noch einmal betont, dass „Funktion“ und „Abbildung“ ein und dasselbe sind.
In der Regel werden wir für Abbildungen die Buchstaben $f, g, h, \alpha, \beta, \ldots$ verwenden. Im Falle $f : A \to B$ heißt A **Definitionsbereich** oder **Urbildmenge**, B wird auch **Bildbereich** genannt. $f(x)$ ist der **Wert** von f an der Stelle x und wird auch als **Bildelement** von $x \in A$ in B bezeichnet.

Definition 5.3. *Für $S \subset A$ ist die* **Bildmenge** *von S unter f durch $f(S) := \{f(x) \mid x \in S\}$, die* **Urbildmenge** *von $T \subset B$ durch $f^{-1}(T) := \{a \in A \mid f(a) \in T\}$ definiert.*

Warnung: Ist nach einer **Bildmenge** $f(S)$ oder einer **Urbildmenge** $f^{-1}(T)$ einer Abbildung $f : A \to B$ gefragt, so achte man

[6] Allgemeiner kann man ihm einen ganzen Datensatz zuordnen, der einem kartesischen Produkt $B_1 \times B_2 \times \cdots \times B_n$ angehört, s. Kap. 4.5.

darauf, dass $f(S) \subset B$ und $f^{-1}(T) \subset A$ sein muss. Wenn man in Abb. 5.1 nach $f^{-1}(T)$ mit $T := \{b_2, b_3\}$ fragt, so lautet das Ergebnis $f^{-1}(T) = \{a_2, a_3\}$, nicht etwa $f^{-1}(T) = \{\emptyset, \{a_2, a_3\}\}$, wie etwa 80% einer Übungsgruppe 2003 vermuteten.

Beispiel:

$$f : \left\{ \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (n, m) & \mapsto & n + m \end{array} \right.$$

Es ist $f^{-1}(\{2, 4\}) = \{(1, 1), (1, 3), (2, 2), (3, 1)\}$. Was ändert sich an der Antwort, wenn $\mathbb{N}$ durch $\mathbb{N}_0$ ersetzt wird, wenn also auch Null als Argument zugelassen wird?

Frage: Wenn M_1 die Menge der Hörer im Hörsaal und M_2 die Menge der Tage eines Jahres sind, die wir mit $M_2 = \{1, 2, \ldots, 366\}$ in naheliegender Deutung schreiben, was ist dann bei der Abbildung $f : M_1 \to M_2$, bei der jeder Person der zugehörige Geburtstag zugeordnet wird, mit $f^{-1}(\{1, 2, \ldots, 31\})$ gemeint?

Der Begriff *Urbildmenge* $f^{-1}(T)$ macht erfahrungsgemäß Probleme. Vielleicht hilft die sprachliche Fassung: Es handelt sich hierbei um diejenige Teilmenge S von A, die sich dadurch auszeichnet, dass alle ihre Elemente $s \in S$ nach T abgebildet wird. Lassen Sie sich nicht vom Index -1 verwirren. Dieser Index taucht wieder bei Umkehrfunktionen auf, siehe Kap. 5.2.7.
Beispiel: $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. Sei $T := \{x \in \mathbb{R} : x \leq 0\}$. Dann gilt $f^{-1}(T) = \{0\}$, da $x = 0$ die einzige Zahl ist, die auf etwas nichtpositives abgebildet wird.

5.2.3 Binäre Verknüpfungen

Die *Verknüpfung* ist ein abstraktes, aber ausgesprochen nützliches Struktur-Konzept in der Mathematik.

Definition 5.4. *Eine Abbildung f mit Definitionsbereich $X \times X$ und Bildbereich X wird auch* **binäre (zweistellige) Verknüpfung** *auf X genannt.*

Eine binäre Verknüpfung f ordnet jedem geordneten Paar $x := (a, b) \in X \times X$ ein Bild $y = f(x) = f((a, b)) \in X$ zu[7]. In Kurzform: Verknüpft man zwei Elemente a und b aus X, so erhält man ein drittes Element $c \in X$.
Die wichtigsten Beispiele hierfür sind die **arithmetischen Operatoren** $+, -, \cdot$ und $/$ [8] mit $X = \mathbb{R}$. So wird z.B. zwei Zahlen a und b (genauer dem geordneten Paar (a, b)) ihre Summe $a + b$ zugeordnet.
Aber auch $\cup, \cap, \setminus$ sind binäre Verknüpfungen mit X als einer Menge, die ihrerseits Mengen enthält, z.B. $X = PotM$. Je zwei Mengen A und B (genauer: einem geordneten Paar (A, B) von Mengen) wird z.B. $A \cup B$ zugeordnet.

[7] Statt $f(x) = f((a, b))$ schreiben wir meist $f(a, b)$.
[8] Bei der Division muss der Nenner $\neq 0$ sein.

Ist X eine Menge von *logischen Aussagen*, so stellen die *und-Verknüpfung* $\wedge$ und die *oder-Verknüpfung* $\vee$ **logische Operatoren** (s. Kap. 10) als binäre Verknüpfungen dar. Je zwei Aussagen A und B (genauer: einem geordneten Paar (A, B) von Aussagen) wird z.B. die Aussage $A \wedge B$ (lies: A und B) zugeordnet.
In all diesen Beispielen ist die Verknüpfung *kommutativ*, d.h., es kommt nicht auf die Reihenfolge an, mit der a und b verknüpft werden. Das muss aber nicht sein (s.u.).
Die Algebra basiert auf dem Begriff einer *Gruppe* G, die i.W. durch eine binäre Verknüpfung auf G mit gewissen Eigenschaften definiert ist.
Weiter unten werden wir erklären, wie man Abbildungen *hintereinander ausführt (verkettet)*. Dies wird als eine binäre Verknüpfung auf einer Menge X von Abbildungen gedeutet werden können, die i.A. nicht kommutativ ist! Siehe Kap. 5.2.6.

5.2.4 Rechenregeln

Satz 5.5. *Sei $f : A \to B$ eine beliebige Funktion und seien $A_1, A_2 \subset A$, $B_1, B_2 \subset B$. Dann gelten:*
a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
b) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$
c) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
d) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

Man mache sich die Aussagen an einem Beispiel klar: Sei A die Menge aller HörerInnen und B die Menge der 6 (Übungs-)Gruppen zu dieser Vorlesung. $f : A \to B$ ordne jeder HörerIn ihre Übungsgruppe zu. Nun sei $A_1 \subset A$ die Menge aller in Süddeutschland geborenen und $A_2 \subset A$ die Menge aller „Youngster“($\leq$ 19 Jahre alt). Seien $B_1 \subset B$ meine Gruppen und $B_2 \subset B$ die Vormittagsgruppen.
Dann ist $f(A_1)$ die Menge aller Gruppen mit mindestens einer Süddeutschen – diese Gruppen nenne ich „S-Gruppen“–, $f(A_2)$ die Menge der Gruppen mit mindestens einem Youngster – die Gruppen nenne ich Y-Gruppen. $f(A_1) \cup f(A_2)$ ist dann die Menge der Gruppen, die S- oder Y-Gruppen sind, während $f(A_1 \cup A_2)$ die Menge der Gruppen ist, in denen mindestens eine Süddeutsche oder ein Youngster sitzt. Aussage a) ist offensichtlich, da beide Mengen übereinstimmen.
$f(A_1) \cap f(A_2)$ ist dann die Menge der Gruppen, die S- und Y-Gruppen sind, während $f(A_1 \cap A_2)$ die Menge der Gruppen ist, in denen mindestens ein süddeutsche Youngster sitzt. Aussage b) ist wieder offensichtlich, auch dürfte klar sein, dass Gleichheit i.A. nicht bestehen wird, z.B. wenn es gar keinen „süddeutschen Youngster“ gibt.
Nun ist $f^{-1}(B_1)$ die Menge aller HörerInnen in meinen Gruppen („Werner-Studies“) und $f^{-1}(B_2)$ die Menge aller HörerInnen in den Vormittagsgruppen („Morgen-Studies“).
Dann ist $f^{-1}(B_1) \cup f^{-1}(B_2)$ die Menge der StudentInnen, die Werner- oder Morgen-Studies sind, während $f^{-1}(B_1 \cup B_2)$ die Menge der Studies ist, die Vormittags- oder Werner-Gruppen besuchen. Offensichtlich gilt c). Analog sieht man d) ein.

Beweis von Satz 5.5: zu a) Wieder zeigen wir die Gleichheit der beiden Mengen, indem wir zeigen, dass die eine Teilmenge der anderen ist.
„$\subset$“: Sei $y \in f(A_1 \cup A_2) \Longrightarrow \exists x \in A_1 \cup A_2 : f(x) = y$. Da hieraus $x \in A_1$ oder $x \in A_2$ folgt, ist auch $f(x) \in f(A_1)$ oder $f(x) \in f(A_2)$, also $f(x) = y \in f(A_1) \cup f(A_2)$.
„$\supset$ “: Sei $y \in f(A_1) \cup f(A_2)$, also $y \in f(A_1)$ oder $y \in f(A_2)$. In beiden Fällen folgt $y \in f(A_1 \cup A_2)$, was zu zeigen war.

zu b): Übung! (Warum gilt hier nicht die Gleichheit? Nehmen Sie z.B. die Abbildung, die jedem Mann die Zahl 0 und jeder Frau die Zahl 1 zuordnet (eine männerfeindliche Abbildung). Nun sei A_1 die Menge aller verheirateten und A_2 die Menge aller 1980 geborenen HörerInnen dieser Vorlesung. In beiden Mengen wird es männliche und weibliche Wesen geben, so dass $f(A_1) = \{0, 1\}$ und $f(A_2) = \{0, 1\}$. Wenn aber $A_1 \cap A_2$ nur aus Männern oder nur aus Frauen besteht oder gar die leere Menge ist, so ist $f(A_1 \cap A_2)$ echte Teilmenge von $f(A_1) \cap f(A_2) = \{0, 1\}$.)

zu c): Es gilt $x \in f^{-1}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \vee f(x) \in B_2 \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2)$.
zu d): Ersetze in c) $\cup$ durch $\cap$ und $\vee$ durch $\wedge$. ∎

5.2.5 Injektive, surjektive, bijektive Abbildungen

Definition 5.6. *Eine Abbildung $f : A \to B$ heißt*

(1)	**injektiv**	$:\iff$	$x \neq y \Longrightarrow f(x) \neq f(y)$ *für alle* $x, y \in A$
(2)	**surjektiv**	$:\iff$	*zu jedem* $b \in B$ *existiert ein* $a \in A$ *mit* $f(a) = b$
(3)	**bijektiv**	$:\iff$	f *ist injektiv und surjektiv.*

Bemerkung: Man mache sich diese drei Begriffe für endliche Mengen A und B klar, indem man die Pfeilsichtweise (jedes Element von A wird ein Element von B per Pfeil zugeordnet, s. Abb. 5.1) verwendet. Injektiv heißt dann, dass ein $b \in B$ nicht zweimal von einem Pfeil getroffen wird, surjektiv bedeutet, dass jedes $b \in B$ mindestens einmal getroffen wird, Bijektivität kann nur dann bestehen, wenn $|A| = |B|$.
Injektivität kann auch so ausgedrückt werden: Zwei verscheidene Argumente haben stets verschiedene Bilder.

Wir untersuchen die folgenden Beispiele auf Injektivität/Surjektivität/Bijektivität:
1) Sei $A = \{0, 1, 2\}, B = \{x, y\}$ und $f : A \to B$ durch $f(0) = x, f(1) = y, f(2) = x$ definiert. f ist nicht injektiv ($f(0) = f(2)$), aber surjektiv.
2) $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 1$ ist injektiv, aber nicht surjektiv (1 hat kein Urbild[9]).
3) Auf $\mathbb{N}$ ist die binäre Verknüpfung „+“ wegen $1 + 2 = 2 + 1$ nicht injektiv. Da es zu 1 kein Urbild gibt, ist sie auch nicht surjektiv. Wenn wir „+ “ auf $\mathbb{N}_0$ betrachten, folgt wegen $n = n+0$ die Surjektivität.

[9] 0 ist bei uns keine natürliche Zahl!

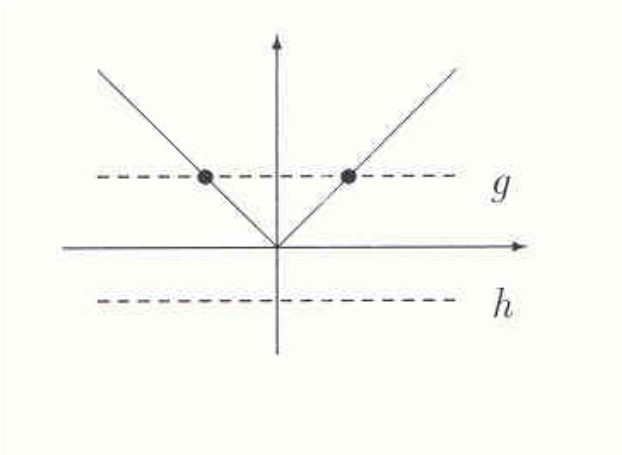


Abbildung 5.5: Graph der Betragsfunktion

4) Die Hörer–Geburtstags–Funktion ist mit hoher Wahrscheinlichkeit nicht surjektiv und auch nicht injektiv[10].

Der folgende Satz ist nicht schwer einzusehen:

Satz 5.7. *Wenn A und B endliche Mengen mit m bzw. n Elementen sind, kann es für $m > n$ keine injektive und für $m < n$ keine surjektiven Abbildungen von A nach B geben.*

Wir werden später beweisen, dass es für $m = n$ genau $m!$ (sprich „m-Fakultät“), $m! := 1 \cdot 2 \cdot \ldots \cdot m$ verschiedene bijektive Abbildungen von A nach B gibt, die auch *Permutationen* von A heißen, wenn $B = A$.
Bei manchen Funktionen kann man aus einer Zeichnung des Funktionsgraphen auf Injektivität usw. schließen.

Wenn bei einer Funktion $f : \mathbb{R} \to \mathbb{R}$ *jede* Parallele zur x–Achse den Graphen von f höchstens/mindestens/genau einmal schneidet, dann ist die Funktion injektiv/surjektiv/bijektiv. Machen Sie sich dies an Hand einer Zeichnung klar!

Beispiele:
1) Die Betragsfunktion f, definiert durch $f(x) := |x|$, ist nicht injektiv (die Gerade g schneidet den Graphen der Funktion *mehr als einmal*) und auch nicht surjektiv (die Gerade h schneidet den Graphen *keinmal*), s.Abb. 5.5.

2) Die Potenzfunktion $f_n : \mathbb{R} \to \mathbb{R}$ mit $f_n(x) := x^n$ mit $n \in \mathbb{N}$ ist für ungerades n bijektiv. Für gerades n ist f_n wegen $f_n(x) = f_n(-x)$ nicht injektiv, und da $f_n(\mathbb{R})$ keine negativen Zahlen enthält, auch nicht surjektiv.

[10] Das bekannte *Geburtstagsproblem* der Wahrscheinlichkeit-Rechnung hat als Ergebnis, dass die Wahrscheinlichkeit bei n Hörern dafür, dass zwei Personen am gleichen Tag Geburtstag haben, für $n \geq 30$ größer als 70% ist, s. Mathematik-Seite der Schweiz.

3) Betrachte die beiden reellen Funktionen $f(x) := (x-1)\,x\,(x+1)$ und

$$g(x) := \begin{cases} x+1 & \text{für} \quad x < 0 \\ x-1 & \text{für} \quad x \geq 0 \end{cases}$$

Können Sie ermitteln, ob Injektivität oder Surjektivität vorliegt? (Skizzieren Sie die Funktionsbilder!)

5.2.6 Verkettung von Funktionen

Bei der Hörer-Geburtstags-Funktion $f : M_1 \to M_2$ ist M_1 die Menge der Hörer im Hörsaal und $M_2 = \{1, 2, ..., 366\}$ die Menge, die die Tage eines Jahres beschreibt, wobei z.B. $60 \in M_2$ dem 29.2. und $61 \in M_2$ dem 1.3. entspricht.
Wir fügen diesem Beispiel eine weitere Menge $M_3 = \{Mo, Di, \ldots, Sa, So\}$ hinzu und definieren $g : M_2 \to M_3$ durch die Zuordnung „Jahrestag“ $\mapsto$ entsprechender Wochentag in 2006, beispielsweise $g(12) = Do$[11]. Jetzt kann jedem Hörer der Wochentag seines Geburtstages in 2006 zugeordnet werden, indem die Funktionen f und g miteinander *verkettet* bzw. *hintereinander ausgeführt* werden:

$$g \circ f : \begin{cases} M_1 & \to & M_2 & \to & M_3 \\ p & \mapsto & f(p) & \mapsto & g(f(p)) \end{cases}$$

Es ist also

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

Sprich g Kringel f für $g \circ f$.
Beachte: Die Auswertung von $(g \circ f)(x)$ erfolgt „von rechts nach links“, d.h. zuerst wird die am weitesten rechts stehende Funktion f an der Stelle x ausgewertet, erst danach wird g an dem Bild $f(x)$ ausgewertet!!! Das ist gewöhnungsbedürftig!
In der Deutung von Funktionen als „Input-Output-Maschinen“ kann man die Verkettung von zwei Funktionen als zwei solcher hintereinandergeschalteter Maschinen begreifen, bei denen der Output der ersten der Input der zweiten Maschine ist.
Wir geben eine allgemeine

Definition 5.8. *Seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen, für die der Wertebereich von f der Definitionsbereich von g sein muss. Dann ist die* **Verkettung** *$h := g \circ f : A \to C$ durch*

$$(g \circ f)(x) := g(f(x)),\ x \in A$$

bzw. durch $x \mapsto g(f(x))$ definiert.

[11] Der 12.1.2006 ist ein Donnerstag. Da 2006 kein Schaltjahr ist, setzen wir für den 29.02 $g(60) := g(61) = Mi$, in der Annahme, dass die am 29.02. geborenen ihren Geburtstag am Mi, d. 1.3.06 gefeiert haben.

Beispiel: Seien $g, h : \mathbb{R} \to \mathbb{R}$ definiert durch $g(x) := x - 2$, $h(x) := 2x^3$. Dann gilt für deren Verkettungen $(g \circ h)(x) = 2x^3 - 2$, $(h \circ g)(x) = 2(x-2)^3$.
Im Allgemeinen gilt $g \circ h \neq h \circ g$, d.h. die durch Verkettung definierte *binäre Verknüpfung* von Funktionen ist nicht *kommutativ* (s. Kap. 8.5), d.h. man kann die Reihenfolge der verketteten Funktionen nicht vertauschen. Später werden wir noch weitere Beispiele von nichtkommutativen Verknüpfungen kennenlernen, die häufig mit der Verkettung von Abbildungen zusammenhängen (Matrizenmultiplikationen, Permutationen, Spiegelungen).

Eine weitere Eigenschaft von Verknüpfungen ist die *Assoziativität* (s. Kap. 8.5), wenn drei (oder mehr) Elemente miteinander verknüpft werden. Bei der Addition und Multiplikation von Zahlen gilt natürlich $(a+b)+c = a+(b+c)$ und $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, weshalb man die Klammern auch weglässt. Entsprechendes kennen wir bei Mengen, wenn man die Mengenoperatoren $\cap$ und $\cup$ betrachtet. Genauso gilt

Satz 5.9. *Es gilt*

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

wenn die Verkettungen definiert sind, d.h. wenn $f : A \to B$, $g : B \to C$ und $h : C \to D$ für gewisse Mengen A, B, C und D.

Beweis: Sei $a \in A$ beliebig. Dann gilt $(h \circ (g \circ f))(a) = h(\,(g \circ f)(a)\,) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a)$. ∎

5.2.7 Inverse Abbildung (Umkehrabbildung)

Der restliche Abschnitt handelt von bijektiven Funktionen $f : A \to B$. Da f injektiv (surjektiv) ist, gibt es zu jedem $b \in B$ höchstens (mindestens) ein a mit $f(a) = b$. Daher folgt aus der Bijektivität von f, dass es zu jedem $b \in B$ **genau ein** a mit $f(a) = b$ gibt. Die Umkehrabbildung $g : B \to A$ von f ist die Abbildung, die einem $b \in B$ gerade das zugehörige $a \in A$ zuordnet. Daher ist die folgende Definition sinnvoll:

Definition 5.10. *Sei $f : A \to B$ eine bijektive Abbildung. Dann heißt die Abbildung $g : B \to A$ mit $\{g(b)\} := f^{-1}(\{b\})$ die zu f gehörende* **inverse Abbildung** *oder* **Umkehrabbildung**, *geschrieben $g = f^{-1}$.*

Mit anderen Worten: $g(b)$ ist dasjenige $a \in A$, für das $f(a) = b$ gilt.
Wenn man sich Abbildungen mit Pfeilen vorstellt, bedeutet Bijektivität, dass jedes Element b des Bildbereichs genau einmal durch einen Pfeil getroffen wird. Die inverse Abbildung kehrt die Pfeile einfach um. Daher ist mit f auch f^{-1} ebenfalls bijektiv. Eine nochmalige Umkehrung der Pfeile ergibt wieder f, also

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

Merke: Will man $x := f^{-1}(y)$ bestimmen, muss man $f(x) = y$ nach x „auflösen“. Wenn f eine Bijektion ist, muss dies für jedes $y \in B$ möglich sein und auf genau eine Lösung führen.

Diese Definition wird zunächst verwirren, weil Ihnen der Ausdruck f^{-1} schon im Zusammenhang mit *Urbildmengen* begegnet ist. Das ist didaktisch eine Hürde, die aber nicht vermeidbar ist, weil diese Schreibweise in allen Büchern zu finden ist. Da müssen Sie durch.

Der Begriff *Umkehrabbildung* ist wichtiger als der der Urbildmenge. Konzentrieren Sie sich daher zunächst hierauf. Dass ein Logarithmus Umkehrabbildung einer Exponentialfunktion ist, ist dabei ein ganz zentrales Faktum. Wie auch die, dass die Quadratwurzel Umkehrfunktion vom Quadrieren ist. Genauer: Die Abbildung $f : \mathbb{R}_+ \to \mathbb{R}_+, x \mapsto x^2$ (beachten Sie den eingeschränkten Definitions- und Bildbereich) ist eine Bijektion, weil es zu jedem $y \geq 0$ genau ein $x \geq 0$ mit $x^2 = y$ gibt!! Nämlich $x = \sqrt{y}$ - die positive Quadratwurzel. Daher ist $g : \mathbb{R}_+ \to \mathbb{R}_+, y \mapsto \sqrt{y}$ die Umkehrfunktion $g = f^{-1}$.
Wenn keine Umkehrabbildung von einer Abbildung $f : A \to B$ existiert, ist dennoch f^{-1} im Zusammenhang mit Urbildmengen $f^{-1}(T)$ unter f für $T \subset B$ definiert. Wenn f aber keine Bijektion ist, kann für ein $b \in B$ die spezielle Urbildmenge $f^{-1}(\{b\})$ leer sein oder mehrere Elemente haben kann. Bei bijektivem f ist $f^{-1}(\{b\})$ stets einpunktig.
Wir fassen zusammen: Urbildmengen $f^{-1}(T)$ unter f sind für alle Funktionen f definiert - auch für solche f, die keine Bijektionen sind. Wenn f jedoch bijektiv ist, so ist $f^{-1} : B \to A$ eine Funktion und $f^{-1}(T)$ ist auch die Bildmenge von T unter der inversen Abbildung f^{-1}. Verstanden?

Man kann die inverser Abbildung $g := f^{-1}$ von f auch implizit durch

$$g(f(a)) = a \quad \forall\ a \in A$$

oder durch

$$f(g(b)) = b \quad \forall\, b \in B$$

definieren. Anders ausgedrückt: $g \circ f$ ist die **Identität**[12] i_A auf A, definiert durch $i_A(a) = a \forall\ a \in A$ und $f \circ g = i_B$, die Identität auf B.

Beispiele:
1) Die identische Abbildung $f : \mathbb{R} \to \mathbb{R}, x \mapsto x$, ist zu sich selbst invers.
2) Zu $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := 2x$ ist g mit $g(x) = f^{-1}(x) = \frac{1}{2}x$ invers.
3) Die inverse Abbildung von $x \mapsto x^3$ ist $y \mapsto y^{1/3}$.
4) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ besitzt keine inverse Abbildung, da f nicht surjektiv und nicht injektiv ist. Wohl aber, wenn man den Definitions- und Bildbereich auf $\mathbb{R}_+$ einschränkt. Dann ist $g : \mathbb{R}_+ \to \mathbb{R}_+, y \mapsto \sqrt{y}$ die Umkehrabbildung von f.
5) Sei $a > 0$ und $f : \mathbb{R} \to \mathbb{R}, x \mapsto a^x$ eine Exponentialfunktion, so ist f eine Bijektion zwischen $\mathbb{R}$ und $\mathbb{R}_+$ mit Umkehrabbildung $y \mapsto^a \log(y)$ – der Logarithmus zur Basis a.

Achtung! In den obigen Beispielen wurde mal x, mal y als Argument der Umkehrabbildung verwendet. Beides ist zulässig. Wenn man die Umkehrabbildung

[12] i_A ist sozusagen die „faulste Abbildung“ von A nach A, die es gibt. Sie bildet jedes Element $a \in A$ auf sich selbst ab, lässt also alles, wie es ist.

von f berechnet, wird man i.A. $f(x) = y$ nach $x = f^{-1}(y)$ auflösen. So kann man z.B. die Umkehrabbildung zu $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := 2x$ auch durch $2x = y$, also $x = f^{-1}(y) = \frac{y}{2}$ berechnen, aber hernach $g := f^{-1}$ als $g(x) = \frac{1}{2}x$ notieren.

Bei reellen Funktionen erhält man den Graphen (das Funktionsbild) von f^{-1} durch Spiegelung an der Diagonalen aus dem von f.

Eine wichtige Regel für Umkehrabbildungen von Bijektionen lautet

Satz 5.11. *Sind f und g zwei Bijektionen einer Menge A, so gilt*

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

Dieser Satz wird später im Kapitel 8 über Gruppen in einem etwas allgemeineren Zusammenhang bewiesen und erläutert. Achten Sie darauf, dass bei der Invertierung *die Reihenfolge* umgekehrt wird.

Im Folgenden geht es um die Eigenschaft „Zwei Mengen A und B sind gleichmächtig“. Endliche Mengen werden sich dabei genau dann als „gleichmächtig“ erweisen, wenn $|A| = |B|$, wenn also die Anzahl ihrer Elemente gleich ist. Weil es nämlich in diesem (und nur in diesem) Fall eine Bijektion von A nach B gibt!
Wir verallgemeinern:

Definition 5.12. *Zwei Mengen A, B heißen* **gleichmächtig**, *geschrieben $|A| = |B|$, $:\Longleftrightarrow$*

$$\exists\, f : A \to B \qquad \textit{bijektiv}$$

Beachten Sie, dass für unendliche Mengen A das Symbol $|A|$ alleine keinen Sinn gibt. „$|A| = |B|$“ steht nur stellvertretend für die Aussage „A und B sind gleichmächtig“. Dies in Übereinstimmung mit der Situation endlicher Mengen! Denn „Gleichmächtige *endliche* Mengen haben die gleiche Anzahl von Elementen“.

Beispiel: Es gilt $|\mathbb{Z}| = |\mathbb{N}|$
Um dies zu zeigen, geben wir eine Bijektion $f : \mathbb{N} \to \mathbb{Z}$ an:

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

Frage: Gilt auch $|\mathbb{Z}| = |\mathbb{N}_0|$?

Gleichmächtig definiert eine Äquivalenzrelation! Der Nachweis hiervon wird evtl. in den Übungen geführt.

5.2.8 Folgen

Folgen werden uns im Zusammenhang mit dem *Grenzwertbegriff* in der Analysis begegnen. Hier soll der Begriff *Folge* definiert werden, weil er eng mit dem Abbildungsbegriff zusammenhängt:

Definition 5.13. *Eine* **Folge** *in einer Menge M ist eine Abbildung $a : \mathbb{N} \to M$ oder auch eine Abbildung $a : \mathbb{N}_0 \to M$. Statt $a(n)$ schreibt man meist a_n und nennt a_n das* **n-te Folgenglied** *der Folge.*
Zuweilen schreibt man auch $(a_n)_{n\in\mathbb{N}}$ für eine Folge.

Bestimmte Folgen werden auf unterschiedliche Weisen eingeführt: Meist gibt man das allgemeine Folgenglied a_n an, man kann sie aber auch durch

$$a_1, a_2, a_3, a_4, ...$$

aufzählen, wenn hierdurch das *Bildungsgesetz* der Folge deutlich wird.
Beispiel: $a_n := n^2$ definiert die Folge aller *Quadratzahlen*. Dieses Bildungsgesetz hätten Sie wahrscheinlich auch erkannt, wenn die Folge kurz durch eine Aufzählung

$$1, 4, 9, 16, ...$$

angegeben worden wäre.
Bei Intelligenzaufgaben geht es sehr häufig um die Erkennung von Bildungsgesetzen von Folgen. Durch Fortsetzung der Folgen soll man zeigen, ob man das Bildungsgesetz verstanden hat. Hier eine kleine Auswahl:

- $$1, 3, 5, 7, ...$$
- $$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...$$
- $$-3, 0, 5, 12, 21, ...$$
- $$1, 5, 5, 9, 9, ...$$
- $$1, 1, 2, 3, 5, 8, 13, ...$$

Im vorletzten Fall werden Sie wohl richtig mit 13,13,17,17,... fortgesetzt haben. Dabei haben Sie wahrscheinlich keine „Formel“ für a_n aufgestellt. Diese lautet hier

$$a_n := \begin{cases} 2n+1 & \text{falls } n \text{ gerade} \\ 2n-1 & \text{falls } n \text{ ungerade.} \end{cases}$$

Auch im letzten Fall sind Sie wahrscheinlich auf die nächsten Folgenglieder 21, 34,... gekommen - es handelt sich um die **Fibonaccifolge**. Dabei haben Sie erkannt, dass sich das jeweilige Folgenglied durch die Summe der beiden Vorgänger ergibt. Aber hätten Sie das Bildungsgesetz in der *rekursiven Form*

$$f_{n+1} := f_n + f_{n-1}, f_0 := 0, f_1 := 0$$

hinschreiben können? Zu *Rekursionen* mehr in Kap. 6.5.

5.2.9 Funktionen im Alltag

Wenn man vom „funktionalen Zusammenhang “ (eine PISA-Kompetenz) zwischen zwei Größen x und y spricht, so meint man, dass es Mengen A und B mit $x \in A$ und $y \in B$ und eine Funktion $f : A \to B$ gibt mit $f(x) = y$.
So sollte es z.B. einen funktionalen Zusammenhang zwischen dem Einkommen x einer Person und der zu zahlenden Einkommensteuer y geben. Hier handelt es sich um eine reelle Funktion, die hoffentlich *streng monoton wachsend* ist, für die also aus $x_1 > x_2$ folgt, dass $f(x_1) > f(x_2)$. Eine solche Funktion ist stets injektiv!
Wenn von *zeitlichen Verläufen* einer beobachteten Größe y (Temperatur, Preis, Aktienindex, HörerInnen dieser Vorlesung, mit dem Auto zurückgelegte Kilometer,....) die Rede ist, haben wir es ebenfalls mit reellen Funktionen f zu tun, bei denen die unabhängige Variable die Zeit ist (die meist mit t an Stelle von x bezeichnet wird). Ein Zeitintervall ist ein reelles Intervall[13] $J := [t_1, t_2]$ und es werden Funktionen $f : J \to \mathbb{R}$ betrachtet. Wenn f streng monoton wächst oder fällt, ist f injektiv: Es existiert eine Umkehrfunktion $g := f^{-1} : f(J) \to J$, man kann aus der beobachteten Größe y auf die Zeit t schließen. Das ist natürlich keineswegs immer der Fall: So könnte man nicht sagen, an welchem Tag der Aktienindex DAX bei 2.805 Punkten gelegen hat, jedenfalls nicht, wenn man die letzten 10 Jahre betrachtet.

Die Liste möglicher funktionaler Abhängigkeiten ist beliebig lang: So hängt die Durchschnittstemperatur von der Position auf der Erdkugel ab, die Menge der benötigten Farbe beim Streichen von der Fläche der Wände, etc. Man muss sich aber hüten, in diesen Abhängigkeiten eine Monokausalität zu sehen. In der Regel hängt eine Größe von mehreren Variablen ab: So hängt die Arbeitslosenquote von so vielen Variablen ab, dass Maßnahmen zur Senkung nicht so einfach als richtig oder falsch erkannt werden können. Überhaupt können keinesfalls alle funktionalen Abhängigkeiten präzise erfasst oder quantifiziert werden: So hängt die Zensur ei-

[13] Ein abgeschlossenes Intervall ist durch $[a, b] := \{x \in \mathbb{R} | a \leq x \leq b\}$ definiert.

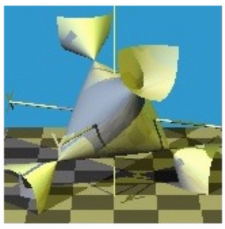


Abbildung 5.6: $x^2 + y^2 + z^2 + 2xyz - 1 = 0$

ner Klassenarbeit ganz sicher von der investierten Vorbereitungszeit[14] ab, ohne dass man diese wirklich zahlenmäßig angeben kann.

5.3 Gleichungen

Was haben Funktionen mit *Gleichungen* zu tun? Wenn wir eine quadratische Gleichung $x^2 + 3x - 2 = 0$ anschauen, wollen wir die Menge $A := \{x : f(x) = 0\}$ der Nullstellen von f mit $f : x \mapsto x^2 + 3x - 2$ bestimmen (sie besteht aus zwei Elementen, den beiden Lösungen dieser Gleichung).
Mit welchen (numerischen) Methoden man Gleichungen löst, ist eine Sache für sich. Bei reellen Funktionen haben wir meist keine oder endlich viele oder auch abzählbar unendlich viele Lösungen (z.B. von $\sin(x) = 0$).
Richtig interessant wird es, wenn wir *eine* Gleichung mit *zwei* Unbekannten lösen wollen. Dann haben wir es mit Funktionen $f : \mathbb{R}^2 := \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (x, y) \mapsto f((x, y))$ von *zwei* unabhängigen Variablen zu tun, und

$$A := \{(x, y) \in \mathbb{R}^2 : f((x, y)) = 0\}$$

kann ein sehr interessantes Gebilde sein. Für eine in x und y quadratische Funktion $(x, y) \mapsto f((x, y)) = a_0 + a_1x + a_2y + a_3x + a_4x^2 + a_5y^2$ haben wir es mit einem *Kegelschnitt* zu tun, z.B. einer Ellipse oder einer Hyperbel oder einer Parabel. Auch Kreise oder Geraden oder gar Punkte können darunter fallen.
In drei Variablen x, y, z bekommt man sensationelle Bilder, siehe Abb. 5.6 für $f((x, y, z)) = x^2 + y^2 + z^2 + 2xyz - 1$.
Bemerkung: Wenn die Argumente einer Funktion n-Tupel, z.B. geordnete Paare $a = (x, y)$ sind, so ist die Schreibweise $f(a) = f((x, y))$ notwendig. In der Regel gehen einem die vielen Klammern auf den Wecker, und man schreibt kurz $f(x, y)$ oder $f(x, y, z)$.

[14] Ohne Fleiß kein Preis.

Kapitel 6

Vollständige Induktion und Rekursionen

6.1 Einführung

Induktives Denken ist das Schließen vom Besonderen auf das Allgemeine[1].
Beweise durch *vollständige Induktion* beruhen auf einer gewissen Beweistechnik. Dabei geht es um *Aussagen*, welche grundätzlich gemäß des Logikaxioms *Terium non datur* entweder *wahr* oder *falsch* sind (s. Kap. 10). Dabei hängen diese Aussagen von einer natürlichen Zahl n (zuweilen auch unter Einschluss der Null) ab, z.B. die (wahre) Aussage, dass

$$3^0 + 3^1 + 3^2 + \cdots + 3^n = \frac{3^{n+1} - 1}{2} \tag{6.1}$$

oder allgemeiner

$$1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - 1}{q - 1} \quad (q \neq 1)$$

gilt. Wie bei Abbildungen üblich, kennzeichnen wir die Abhängigkeit dieser Aussage von n dadurch, dass wir die von n abhängige Aussage (6.1) $A(n)$ nennen[2], z.B. Aussage (6.1).
Die Aussage $A(1)$ lautet dann $3^0 + 3^1 = \frac{3^2-1}{2}$. Wie man leicht nachrechnet, ist diese Aussage ($A(1)$) wahr. Ebenfalls ist $A(2)$, nämlich

$$3^0 + 3^1 + 3^2 = \frac{3^3 - 1}{2}$$

wahr. Entsprechend kann man für feste $n = 3, 4, ...$ vorgehen. Aber wie zeigt man, dass $A(n)$ *für alle* $n \in \mathbb{N}$ gilt? Der mehr oder weniger einleuchtende Trick ist ein *Induktionsschluss*: Wenn man für ein jedes n die Aussage $A(n+1)$ aus $A(n)$ folgern kann, wenn also eine Aussage für eine

[1] Das Gegenteil von Induktion die Deduktion, bei der man vom Allgemeinen auf das Einzelne schließt
[2] A ist eine Abbildung von $\mathbb{N}$ in eine Menge von Aussagen

bestimmte Zahl immer dann richtig ist, wenn sie schon für den Vorgänger dieser Zahl richtig ist, so ist $A(n)$ doch wohl für alle n richtig - vorausgesetzt, sie ist für $n = 1$ wahr. Denn wegen des Induktionsschlusses ist sie dann auch richtig für $n = 2$, dem Nachfolger von 1, dann auch für $n = 3$, dem Nachfolger von 2, usw. Das Peano-Axiom (P5) – auch Induktionsprinzip genannt – liefert die formale Grundlage für eine solche Schlussweise – man kann dies nicht beweisen, sondern nimmt es per *Axiom* als ein Charakteristikum der natürlichen Zahlen an.
Der erste Mathematiker, der einen formalen Beweis durch vollständige Induktion angab, war der italienische Geistliche Franciscus Maurolicus (1494 - 1575). Er war Abt von Messina und wurde als größter Geometer des 16. Jahrhunderts angesehen. In seinem 1575 veröffentlichten Buch „Arithmetik“ benutzte Maurolicus die vollständige Induktion unter anderem dazu, für jede natürliche Zahl n die Gültigkeit von

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

zu zeigen[3]
Den Hinweis verdanke ich einer Webseite der Uni Freiberg.

Ab Kap. 6.5 werde ich auf *Rekursionen* eingehen, die sehr eng mit dem Induktionsprinzip zusammenhängen und aus Sicht der Anwednungen fast noch wichtiger sind.
Als Beispiel nenne ich die schon in Kap. 5 erwähnte Folge

$$1, 1, 2, 3, 5, 8, 13, ...,$$

der Fibonaccizahlen. Das jeweilige Folgenglied ergibt sich ja offensichtlich durch die Summe der beiden Vorgänger. Das Bildungsgesetz in der *rekursiven Form* lautet.

$$f_{n+1} := f_n + f_{n-1}, n = 1, 2, ..., \ f_0 := 0, f_1 := 0.$$

Es gibt noch einfachere rekursive Bildungsgesetze wie

$$a_{n+1} = q \cdot a_n, n = 0, 1, 2, ..., \ a_0 := 1,$$

das in expliziter Form durch die **geometrische Folge** $a_n := q^n$ erfüllt wird.
Ferner gibt es schöne Anwendungen auf „Schneeflockenkurven“, auf das Spiel „Turm von Hanoi„ und auf „Hypothekendarlehen“. Diese Anwendungen werden in der Vorlesung wahrscheinlich nur skizziert, sind also eher zum „Selbststudium“ gedacht.

6.2 Das Summensymbol

Weil das **Summenzeichen** $\sum$ (der griechische Buchstabe Sigma) bei den Beispielen für vollständige Induktion häufiger vorkommen wird, schiebe ich einen entsprechenden Abschnitt ein, der auch unabhängig von diesem Kapitel wichtig ist.

[3]Schüler kann diese Aussage faszinieren. Es gibt eine ganz einfache geometrische Erklärung für diesen Sachverhalt, indem man im n-ten Schritt an ein Quadrat oben und rechts $(2n + 1)$ kleine Quadrate anfügt.

Will man die ersten n natürlichen Zahlen addieren, also $1+2+\cdots+n$ berechnen, so schreibt man unter Zuhilfenahme des **Summensymbols** $\sum$ kürzer

$$1+2+\cdots+n =: \sum_{j=1}^{n} j.$$

Für die Summe der ersten n Quadratzahlen schreibt man kurz

$$1^2+2^2+\cdots+n^2 =: \sum_{j=1}^{n} j^2.$$

Dabei heißt j der **Laufindex** (oder Laufvariable, Zählvariable), er „läuft“ von $j=1$ bis zu einem $j=n$, wobei n beliebig ist.
Wir werden mit Hilfe des Prinzips der vollständigen Induktion beweisen, dass *für alle* $n \in \mathbb{N}$

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}, \quad \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Allgemein wird definiert

$$\sum_{j=1}^{n} a_j := a_1 + a_2 + \cdots + a_n$$

bei Summen mit *einfach indizierten* reellen Summanden a_j.
Auch die beiden in der Einführung erwähnten Aussagen hätte man mit Hilfe des Summensymbols kürzer schreiben können:

$$\sum_{j=0}^{n} q^j = \frac{q^{n+1}-1}{q-1}$$

und

$$\sum_{j=1}^{n} (2j-1) = n^2.$$

Man kann aber auch über allgemeinere Indexmengen summieren. Denken wir z.B. an eine rechteckige Zahlen-Tabelle mit m Zeilen und n Spalten. Bezeichnet man die Zahl in der i-ten Zeile und j-ten Spalte mit a_{ij}, so erhält man doppelt indizierte Größen. Durch

$$S := \sum_{i=1,\ldots m, j=1,\ldots,n} a_{ij}$$

werden alle Tabellenwerte aufaddiert[4], ohne dass man etwas über die Reihenfolge bei der Addition aussagt. Bezeichnet man mit $s_i := \sum_{j=1}^{n} a_{ij}$ die Summe der Einträge in der i-ten Zeile,

[4] Die Summe erstreckt sich über alle Indexpaare (i,j).

so gilt offensichtlich (*zeilenweise Addition*)

$$S = \sum_{i=1}^{m} s_i = \sum_{i=1}^{m} \big(\sum_{j=1}^{n} a_{ij} \big).$$

Analog gilt mit $s^j := \sum_{i=1}^{m} a_{ij}$ – der Summe der Einträge in der j-ten Spalte[5] –, dass (*spaltenweise Addition*)

$$S = \sum_{j=1}^{m} s^j = \sum_{j=1}^{m} \big(\sum_{i=1}^{n} a_{ij} \big).$$

Es gilt also

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij},$$

d.h. in einer „Doppelsumme“ kann die Reihenfolge der Summation umgekehrt werden. Die Klammern können wir weglassen, da es kein Missverständnis geben kann.
Ein anderes Beispiel: A sei mal wieder die Menge aller HörerInnen dieser Vorlesung. Jedem $a \in A$ werde eine Zeit $T(a)$ zugeordnet, die sie(er) für das letzte Übungsblatt aufgewendet hat (eine Funktion!). Dann ist

$$T := \sum_{a \in A \text{ ist männlich}} T(a)$$

die Gesamtarbeitszeit aller männlichen Hörer. Es ist sinnvoll zu definieren[6], dass $T = 0$, wenn es keine männlichen Hörer gibt. Allgemein setzt man fest:

$$\sum_{a \in \emptyset} f(a) := 0$$

für irgendeine Funktion $f : A \to \mathbb{R}$.
Dass eine solche Setzung sinnvoll ist, erkennt man z.B. an der Formel $\sum_{j=1}^{n} (2j - 1) = n^2$, die jetzt auch für $n = 0$ richtig ist!

Die Verwendung des Summenzeichens muss eingeübt werden. Verwirrend kann z.B. die Aussage $\sum_{j=1}^{4} 1 = 4$ sein, weil der Laufindex doch gar nicht unter dem Summenzeichen auftritt! Sie werden aber $\sum_{j=1}^{4} a_j = a_1 + a_2 + a_3 + a_4$ einsehen. Nun setzen Sie einfach $a_j := 1$ für alle j.

[5] Das j in s^j ist ein oberer Index. Diese Schreibweise dient der Unterscheidnung von s_j, um Zeilensummen und Spaltensummen auseinanderzuhalten.

[6] Man darf nicht fragen, ob soetwas richtig ist, sondern nur, ob eine solche Vereinbarung sinnvoll ist.

6.3 Peano-Axiome

Wahrscheinlich glauben Sie zu wissen, was natürliche Zahlen sind. Aber es wird Ihnen nicht gelingen, diese befriedigend zu definieren. Hier behilft sich die Mathematik mit *Axiomen*[7], die die wesentlichen Eigenschaften eines Begriffs festlegen. Weitere Eigenschaften werden sodann aus den Axiomen gefolgert. Die folgende Axiome regeln, was man unter natürlichen Zahlen zu verstehen hat.

Definition 6.1 (Peano–Axiome)**.** *G. Peano 1858 – 1932*
Sei eine Menge N mit folgenden Eigenschaften gegeben:

(P1) $1 \in N$

(P2) *Zu jedem $x \in N$ gibt es einen Nachfolger $x' \in N$.*

(P3) *1 ist kein Nachfolger.*

(P4) $\forall x, y \in N : x \neq y \Longrightarrow x' \neq y'$. *(verschiedene Zahlen haben verschiedene Nachfolger)*

(P5) *Sei $U \subset N$ mit $1 \in U \ \wedge \ (x \in U \Longrightarrow x' \in U)$. Dann ist $U = N$.*

Dann heißt N die Menge der natürlichen Zahlen und wird – wie Sie schon wissen – mit $\mathbb{N}$ bezeichnet.

Bemerkungen: 1) Häufig wird die Zahl 0 zu den natürlichen Zahlen gezählt. In diesem Fall gelten (P1) – (P5) analog, wenn man 1 durch 0 ersetzt.
2) In (P2) – (P4) wird die Existenz einer injektiven Abbildung (*Nachfolgerfunktion*) verlangt ($x \mapsto x'$), die wegen (P3) jedoch nicht surjektiv ist. Jetzt kann gefolgert werden, dass es unendlich viele natürliche Zahlen gibt. Denn wenn $\mathbb{N}$ endlich wäre, hätte man eine injektive, aber nicht surjektive Nachfolgerabbildung von $\mathbb{N}$ nach $\mathbb{N}$. Eine solche kann es aber nicht geben.
3) Die Nachfolgerfunktion $x \mapsto x'$ kann als Addition von 1 interpretiert werden: $x' = x + 1$.
4) (P5) ist das sogenannte *Induktionsprinzip*.

6.4 Prinzip der vollständigen Induktion

Mit Hilfe von (P5) (Induktionsprinzip) kann man gewisse Aussagen über natürliche Zahlen beweisen. Hierzu nennen wir eine Menge $U \subset \mathbb{N}$ **induktive Menge**, wenn sie die beiden Voraussetzungen in (P5)

- $1 \in U$
- $n \in U \Longrightarrow n' = n + 1 \in U$

[7] Axiome sind nicht beweisbare, häufig auch plausible Aussagen, die man als wahr annimmt, um weitere Eigenschaften hieraus folgern zu können. Ein klassisches Beispiel hierfür, das auch in die Schulmathematik Eingang findet, ist die axiomatische Geometrie, die auf EUKLID (325-265 v.Chr.) zurückgeht.

erfüllt. Dann besagt (P5) nichts anderes als: **„Eine induktive Menge U stimmt mit $\mathbb{N}$ überein“.**
Wir demonstrieren dies an einem Beispiel: Wir wollen beweisen, dass für alle $n \in \mathbb{N}$ gilt

$$s_n := \sum_{j=1}^{n} j = \frac{n(n+1)}{2}. \tag{6.2}$$

Wir nennen die von n abhängige Aussage in (6.2) wie in der Einleitung $A(n)$ und betrachten die Menge $U := \{n \in \mathbb{N} : A(n) \text{ ist wahr}\}$[8]. Die von C.F. Gauss als 10-jähriger gefundene Aussage lässt sich jetzt auch so kurz und knapp formulieren: $U = \mathbb{N}$.
Dies ist wegen des Induktionprinzips richtig, wenn U eine induktive Menge ist. Dass $1 \in U$ ist (**Induktionsanfang**), ist offensichtlich, da die Aussage $A(1)$ wahr ist; denn offensichtlich gilt $\sum_{j=1}^{1} j = \frac{1\cdot(2)}{2}$. Jetzt fehlt noch der **Induktionsschluss**, dass mit $n \in U$ auch dessen Nachfolger $n' = n + 1 \in U$. Wenn wir also $A(n+1)$ unter Benutzung von $A(n)$ zeigen können, sind wir fertig. Das geht so: $A(n+1)$ lautet

$$s_{n+1} := \sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

Nun ist $s_{n+1} = s_n + (n+1)$. Da $n \in U$ (**Induktionsannahme**), gilt $s_n = \frac{n(n+1)}{2}$. Damit haben wir

$$s_{n+1} = s_n + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)}{2} + \frac{2(n+1)}{2},$$

und man erhält sofort $s_{n+1} = \frac{(n+1)(n+2)}{2}$. Was zu zeigen war.

Das abstrakte Prinzip geht also so: Man will eine von einer natürlichen Zahl n abhängige Aussage $A(n)$ *für alle* $n \in \mathbb{N}$ beweisen. Wenn man dann den **Induktionsanfang** $A(1)$ beweisen kann und wenn man aus der **Induktionsvoraussetzung** $A(n)$ *für ein beliebiges* n folgern kann, dass dann auch $A(n+1)$ gilt, hat man wegen (P5) für $U := \{n \in \mathbb{N} : A(n) \text{ ist wahr}\}$ gezeigt, dass $U = \mathbb{N}$, d.h., dass $A(n)$ für alle $n \in \mathbb{N}$ gilt.
Dabei ist die einzige mathematische Idee die, dass man bei dem Nachweis von $A(n+1)$ irgendwie auf $A(n)$ zurückgreifen muss, man muss $A(n)$ benutzen. Dies geschieht mit einer Idee, die ich **Induktionsschlüssel** nenne, welcher „das Tor zu $A(n+1)$ mit Hilfe von $A(n)$ aufschließt“.
Schauen wir uns als Beispiel noch einmal den Beweis von (6.2) an. Der Induktionsschlüssel ist die „Erkenntnis“, dass $s_{n+1} = s_n + (n+1)$. Denn dann kann wegen der Induktionsannahme für s_n der Wert $s_n = \frac{n(n+1)}{2}$ eingesetzt werden. Die nächsten Schritte sind „Rechenkram“.
Schwierigkeiten macht die Unterscheidung zwischen der eigentlichen mit dem Induktionsprinzip zu beweisende Aussage „Es gilt $A(n)$ **für alle** n“ und der Induktionsannahme „Es gelte $A(n)$

[8] Wieder einmal ist die geschickte Benennung von entscheidender Bedeutung. Für gegebenes n ist $A(n)$ eine Aussage, die entweder wahr oder falsch ist.

Abbildung 6.1: Dominos

für ein n“ sowie dem Induktionsschluss „Aus $A(n)$ folgt $A(n+1)$“. Die letzte Aussage lautet z.B. für $n = 9$: „Aus $A(9)$ folgt $A(10)$“.

Etwas allgemeiner (und schematischer):
Eine Aussage $A(n)$ soll für alle natürliche Zahlen $n \geq n_0$ bewiesen werden, wobei n_0 ebenfalls eine natürliche Zahl ist.

1)	*Induktionsanfang*:	Man beweist die Behauptung für n_0: $A(n_0)$ ist richtig.
2)	*Induktionsannahme*:	Die Behauptung wird für ein $n \in \mathbb{N}$ als richtig angenommen: $A(n)$ sei richtig.
3)	*Induktionsschluss*:	Man beweist, dass unter der Annahme $A(n)$ auch $A(n+1)$ richtig ist.

Nach dem Induktionsprinzip gilt die Aussage $A(n)$ für alle natürlichen Zahlen $n \geq n_0$. Die Idee, die dieser Methode zugrundeliegt, ist denkbar einfach: Nach 1) ist zunächst $A(n_0)$ richtig. Wendet man 3) auf den Fall $n = n_0$ an, hat man $A(n_0+1)$ bewiesen. Jetzt folgt aus 3) für den bewiesenen Fall $n = n_0 + 1$ die Gültigkeit von $A(n_0+2)$, *usw*, (Dominoprinzip!, s. Abb. 6.1). Das Induktionsprinzip ist sozusagen eine Rechtfertigung für das „usw“.

Analog zu der Formel

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

lassen sich auch die folgenden Summenformeln beweisen (zum Teil in den Übungen):

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}\,, \qquad \sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4}$$

Bemerkenswert an diesen drei Formeln ist, dass man auf die erste recht einfach kommen kann (so hat Gauss wahrscheinlich als 10-jähriger gedacht): Man addiere den ersten und den letzten Summanden, den zweiten und den vorletzten etc – jedes Mal ergibt dies $n+1$. Bei geradem n gibt es genau $n/2$ solcher Summen und man erhält die gewünschte Formel. Wenn n ungerade ist, behält man nach $(n-1)/2$ solcher Additionen nur noch eine Zahl nach, nämlich $(n+1)/2$,

so dass sich insgesamt ergibt:

$$(n+1)\cdot\frac{n-1}{2}+\frac{n+1}{2}=\frac{n(n+1)}{2}.$$

Man sieht: der Beweis klappt auch ohne vollständige Induktion. Das ist bei den anderen beiden Formeln anders!

6.4.1 Beispiele

Satz 6.2 (Geometrische Summenformel)**.** *Sei $q \neq 1$ eine beliebige reelle Zahl. Dann gilt*

$$\sum_{j=0}^{n} q^j = \frac{q^{n+1}-1}{q-1}$$

Beweis: Durch vollständige Induktion, Kurzform:
1) $n=0:\quad \sum\limits_{j=0}^{0} q^j = q^0 = 1 = \frac{q^1-1}{q-1}$. Dies ist offensichtlich richtig.

2) $n \mapsto n+1:$ Beachtet man $\sum\limits_{j=0}^{n+1} q^j = \sum\limits_{j=0}^{n} q^j + q^{n+1}$, so hat man den Induktionsschlüssel in der Hand. Er erlaubt die Benutzung der Induktionsannahme und führt zu

$$\sum_{j=0}^{n+1} q^j = \frac{q^{n+1}-1}{q-1}+\frac{q^{n+1}(q-1)}{q-1}=\frac{q^{n+1}-1+q^{n+2}-q^{n+1}}{q-1}=\frac{q^{n+2}-1}{q-1}$$

∎

Satz 6.3 ($|PotM| = 2^{|M|}$)**.** *Ist M eine endliche Menge mit $n := |M|$, so hat die Potenzmenge von M genau 2^n Elemente.*

Beweis: Wir können den Induktionsanfang sogar schon bei $n_0 = 0$ ansetzen: Dann ist M die leere Menge, deren Potenzmenge genau ein Element ($1 = 2^0$) besitzt, nämlich die leere Menge. Nun sei $|M| = n+1$. Induktionsschlüssel: Wir greifen irgendein Element $m' \in M$ heraus und betrachten $M' := M \setminus \{m'\}$. Nun gibt es zwei Sorten von Teilmengen von M, solche *mit* und solche *ohne* m'. Von beiden Sorten gibt es genau so viele, wie es Teilmengen von M' gibt. Da $|M'| = n$, können wir die Induktionsannahme anwenden! Der Induktionsschlüssel greift! Wir wissen auf Grund der Induktionsannahme, dass $|PotM'| = 2^n$. Von beiden Sorten von Teilmengen von M gibt es genau so viele, wie es Teilmengen von M' gibt, also 2^n Stück. Damit besteht $PotM$ aus $2^n + 2^n = 2^{n+1}$ Elementen. ∎

Man kann auch Ungleichungen[9] mit Hilfe des Prinzips der vollständigen Induktion beweisen:

[9] Ungleichungen sind auch ein Thema der Analysis. Da das Rechnen mit ihnen erfahrungsgemäß Probleme macht, werde ich die nächsten beiden Beispiele in der Vorlesung nur kurz skizzieren.

Satz 6.4. *Es gilt $2^n > n^2$ für alle natürlichen Zahlen $n \geq n_0 := 5$.*

Beweis: Durch vollständige Induktion, Kurzform:
1) $n_0 = 5$: $2^5 = 32 > 25 = 5^2$.
2) $n \mapsto n+1$:
Der Induktionsschlüssel lautet $2^{n+1} = 2 \cdot 2^n$. Nach Induktionsannahme ist $2^n > n^2$, also gilt $2^{n+1} = 2 \cdot 2^n > 2 \cdot n^2$, da eine Ungleichung bestehen bleibt, wenn man beide Seiten mit einer positiven Zahl multipliziert. Ferner gilt: $2 \cdot n^2 = n^2 + n^2 = n^2 + n \cdot n > n^2 + 3n = n^2 + 2n + n > n^2 + 2n + 1 = (n+1)^2$. Bei dem ersten $>$-Zeichen der letzten Kette wurde von $n \cdot n > 3n$, also von $n > 3$ Gebrauch gemacht. ∎

Bemerkung: Satz 6.4 ist zwar auch für $n = 1$ richtig, nicht aber für $n = 2, 3, 4$. (Was wäre, falls in dem Satz $>$ durch $\geq$ ersetzt worden wäre?)

Wir beenden diesen Abschnitt mit dem Beweis einer Aussage, die uns später in der Analysis Dienste leisten wird.

Satz 6.5 (Bernoullische Ungleichung)**.** *Jakob Bernoulli, 1654–1705*
Für alle reellen Zahlen $b \geq -1$ und alle $n \in \mathbb{N}$ gilt

$$(1+b)^n \geq 1 + nb$$

Beweis: Durch vollständige Induktion, Kurzform:
$n = 1$: $(1+b)^1 \geq 1 + 1 \cdot b$.
$n \to n+1$: Wegen $b \geq -1$ gilt $1 + b \geq 0$. Es folgt nach Induktionsannahme $(1+b)^{n+1} = (1+b)^n(1+b) \geq (1+nb)(1+b)$, wobei auch von Rechenregeln für Ungleichungen Gebrauch gemacht wurde[10]. Nun ist $(1+nb)(1+b) = 1+(n+1)b+nb^2$. Da $nb^2 \geq 0$ gilt, folgt $(1+b)^{n+1} \geq 1+(n+1)b$. ∎

Finden Sie heraus, wo der Induktionsschlüssel steckt!

Bemerkung: Für $n \geq 2$ und $b \neq 0$ gilt sogar die strenge Ungleichung $(1+b)^n > 1 + nb$.

6.5 Rekursionen

Angenommen, in jeder Minute verdoppelt sich die Anzahl gewisser Bakterien. Dies nennen wir ein *Wachstumsgesetz*. Zu Beginn gebe es $B_0 \in \mathbb{N}$ Bakterien. Sei B_n die Anzahl der Bakterien nach n Minuten. Dann erhalten wir auf Grund des Wachstumsgesetzes die Formel

$$B_{n+1} = 2 \cdot B_n, \quad n \in \mathbb{N}. \tag{6.3}$$

Eine solche Beziehung heißt (einstufige) **Rekursion**: Man kann aus dieser Beziehung die Größe von B_{n+1} nicht direkt ablesen, man kann sie nur ermitteln, wenn man auf B_n zurückgreift. Ganz

[10] Wenn $c > 0$ folgt aus $a \geq b$, dass $ca \geq cb$.

ähnlich wie bei dem Induktionsschluss der vollständigen Induktion. Nun kann man $B_n = 2B_{n-1}$ benutzen, so lange, bis man bei B_0 gelandet ist. Man kann auch bei B_0 anfangen und $(n+1)$-mal mit 2 multiplizieren, bis man bei B_{n+1} angelangt ist. Nun, bei dieser einfachen Rekursion (6.3) kennt man die „Lösung“: es gilt $B_n = 2^n B_0$. Wer dies nicht glaubt, kann diese Formel mit vollständiger Induktion nach n beweisen: Für $n = 0$ ist sie offensichtlich richtig. Nun gelte (Induktionsannahme) $B_n = 2^n B_0$. Dann folgt aus (6.3) $B_{n+1} = 2B_n = 2 \cdot 2^n B_0 = 2^{n+1} B_0$, was zu zeigen war.

Es gibt aber auch Rekursionen, die man nicht so leicht „lösen“ kann:

$$x_{n+1} = 3x_n(1 - x_n), \quad n \in \mathbb{N}, \quad x_0 = 0.5.$$

Versuchen Sie es mal! Dennoch kann eine solche Rekursion benutzt werden, um für ein gegebenes n die Zahl x_n zu berechnen. Wenn z.B. $n = 5$, kann man nach und nach $x_1 = 3x_0(1-x_0) = 0.75$, $x_2 = 3x_1(1 - x_1) = 9/16$, $x_3 = 3x_2(1 - x_2) =$????,.... berechnen – am besten mit Hilfe eines Computer-Programms.

6.5.1 Rekursive Definitionen

Die Potenz a^n mit $n \in \mathbb{N}$ ist durch $a^n = a \cdot a \cdots a$ (n-mal) definiert. Man kann aber auch eine elegantere *rekursive Definition* benutzen:

$$a^0 := 1, \quad a^{n+1} := a^n \cdot a.$$

Unter der Induktionsannahme, man wüsste schon, was a^n ist, wird a^{n+1} mit Hilfe von a^n definiert!

Ein weiteres Beispiel (*Definition von* $n!$, sprich n Fakuktät):

$$0! = 1, \quad (n+1)! = (n+1) \cdot n!$$

Man erkennt sofort, dass

$$n! = 1 \cdot 2 \cdots (n-1) \cdot n$$

das Produkt der ersten n natürlichen Zahlen.

Wir werden im Kap. 7 über *Kombinatorik* auf weitere Rekursionen, z.B. in Bezug auf die Binomialkoeffizienten $\binom{n}{k}$ (sprich n über k), zu sprechen kommen, letzteres im Zusammenhang mit dem *Pascal'schen Dreieck*.

6.5.2 Schneeflockenkurve

Startend mit einer Strecke der Länge 1 wird auf dem mittleren Drittel einer jeden Seite in jedem „Iterationsschritt“ ein neues entsprechend kleineres *gleichseitiges* Dreieck aufgesetzt. Durch

Abbildung 6.2: Kochkurve: $n = 1$

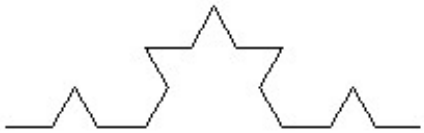


Abbildung 6.3: Kochkurve: $n = 2$

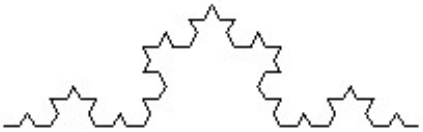


Abbildung 6.4: Kochkurve: $n = 3$

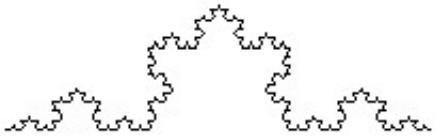


Abbildung 6.5: Kochkurve: $n = 4$

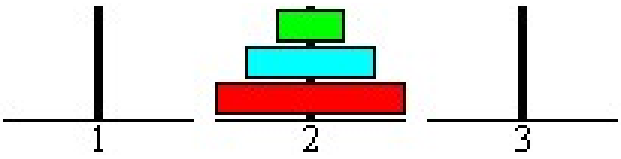


Abbildung 6.6: Turm von Hanoi mit $n = 3$ Scheiben

diesen *rekursiven Wachstumsprozess* entsteht eine Schneeflockenkurve (Kochkurve[11]). In jedem Schritt wird eine Strecke der Länge L durch 4 Strecken der Länge $L/3$ ersetzt.

Wir nennen k_n die Anzahl und s_n die Länge der Strecken nach dem n-ten Schritt. Offensichtlich gilt

$$k_{n+1} = 4k_n,\ k_0 = 1, \quad s_{n+1} = \frac{1}{3}s_n,\ s_0 = 1.$$

Daher wissen wi, dass $k_n = 4^n$ und $s_n = (1/3)^n$. Die Gesamtlänge l_n der Kochkurve beträgt also $l_n = (4/3)^n$.
Bemerkung: Es gilt $l_n = s_n^{1-D}$ mit $D = \log 4/\log 3$. D heißt die *fraktale Dimension* der Kochkurve.

6.5.3 Turm von Hanoi

Auf einem Spielbrett befinden sich drei vertikale Pfosten auf den Plätzen A, B und C, auf die Scheiben mit Löchern verschiedener Größe aufgespießt werden können. Zu Beginn des Spiels befinden sich n Scheiben der Größe nach zu einem Turm geordnet auf Position A - die unterste Scheibe hat den größten Durchmesser (dies sieht aus wie eine Pagode, ein vielstöckiger Tempelbau im fernen Osten, daher der Name „Turm von Hanoi“, s. Abb. 6.6).
Aufgabe ist es, durch mehrere Bewegungen *jeweils einer Scheibe* den ganzen Turm von A nach B zu bewegen, wobei niemals eine größere Scheibe auf einer kleineren zu liegen kommen darf. Für $n = 1$ ist die Aufgabe ganz simpel (Induktionsanfang). Nun soll man sich überlegen, wie man das Problem mit $n+1$ Steinen lösen kann, wenn man weiß, wie man es mit n Steinen löst. Dies wird eine Übungsaufgabe sein.
Hier will ich nur etwas zur „mathematischen Modellierung“ dieses Problems beitragen. Dabei ist die Benennung der 3 Pfosten durch die Buchstaben A, B und C schon sehr wichtig und nicht zu unterschätzen. Zunächst muss man sich überlegen, wie man einen einzelnen Zug *benennt*. Ich schlage X→Y vor für einen einzelnen *Zug*, eine Bewegung der obersten Scheibe auf Platz X nach Platz Y, wobei X und Y natürlich verschieden sind. Dabei sind X und Y „Platzhalter“ für die Plätze A, B und C. Beachten Sie, dass es insgesamt 6 solcher Züge gibt.
Wir können einen Zug auch mit $Z := X \to Y$ bezeichnen.
Beispiel: Eine Lösung für $n = 3$ besteht dann aus folgenden 7 Zügen $Z_j, j = 1, 2, ..., 7$: $Z_1 := A \to B, Z_2 := A \to C, Z_3 := B \to C, Z_4 := A \to B, Z_5 := C \to A, Z_6 := C \to B, Z_7 := A \to$

[11] Helge Koch 1906

B. Überzeugen Sie sich!
Allgemein: Führt man nacheinander m Züge durch, so erhält man eine *Zugfolge der Länge* m. Diese kann man als m-Tupel von Zügen $F := (Z_1, Z_2, ..., Z_m)$ notieren, wobei die Züge von links nach rechts abgearbeitet werden. Jede Komponente Z_j ist also ein Zug der Form $X \to Y$. Zwei Zugfolgen F_1 und F_2 können jetzt hintereinander ausgeführt werden, die neue Zugfolge werde mit (F_1, F_2) notiert, wobei zuerst die Zugfolge F_1, dann die Zugfolge F_2 ausgeführt wird. Man muss natürlich darauf achten, dass die Zugfolge korrekt ist, d.h., dass niemals eine größere Scheibe auf einer kleineren zu liegen kommt.

Für $n = 3$ war ja

$$(Z_1, Z_2, ..., Z_7) := (A \to B, A \to C, B \to C, A \to B, C \to A, C \to B, A \to B) \tag{6.4}$$

ein Lösung!
Das Problem ist für allgemeines n gelöst, wenn man eine von n, X und Y abhängige Zugfolge $F(n, X, Y)$ angeben kann (das ist jetzt schon ganz schön abstrakt und schwierig!), die einen n-Turm von Platz X nach Y transportiert, wobei X, Y für einen der drei Plätze A, B oder C stehen. Dabei ist Z der dritte von X und Y verschiedene Platz. Beispielsweise ist

$$F(1, X, Y) = X \to Y, \quad F(2, X, Y) = (X \to Z, X \to Y, Z \to Y),$$

wobei Z der dritte Platz neben X und Y ist, während der Fall $n = 3$ schon komplizierter ist:

$$F(3, X, Y) = (X \to Y, X \to Z, Y \to Z, X \to Y, Z \to X, Z \to Y, X \to Y).$$

Ein Vergleich mit (6.4) gelingt, wenn Sie X durch A, Y durch B und Z durch C ersetzten. Im Grunde ist F eine Funktion, die den 3 Variablen n (eine Zahl), sowie X und Y (zwei von den drei Plätzen A, B oder C) eine Zugfolge zuordnet, die auf korrekte Weise den n-Turm von Platz X nach Platz Y transportiert.
Der Witz ist nun, dass man $F(n + 1, A, B)$ *rekursiv* mit Hilfe von $F(n, X, Y)$ mit X,Y =A, B oder C ausdrücken kann. Man kann also *induktiv* eine Strategie definieren. Die Antwort ist simpel:

$$F(n + 1, A, B) = (F(n, A, C), A \to B, F(n, C, B)), \tag{6.5}$$

in Worten: Um einen $(n + 1)$-Turm von A nach B zu transportieren, bewege man zunächst die obersten n Scheiben von A nach C — mittels der Zugfolge $F(n, A, C)$. Dann lege man die letzte (und größte) Scheibe von A nach B — dies ist der Zug $A \to B$. Dann bewege man den n-Turm von C nach B (mittels der Zugfolge $F(n, C, B)$).
Überzeugen Sie sich von dieser Rekursion für $n = 3$:

$$F(3, A, B) = (F(2, A, C), A \to B, F(2, C, B)).$$

Jetzt kann man auch ganz leicht klären, wieviel Einzelzüge für das n-Turm-Hanoi-Spiel notwendig sind: Nenne diese Anzahl K_n. Dann besagt die Rekursion (6.5), dass

$$K_{n+1} = 2K_n + 1.$$

Da $K_1 = 1$, kann man ganz leicht $K_n = 2^n - 1$ nachweisen.

Sie können das Spiel online spielen: Turm von Hanoi online (Sachsen-Freizeit) oder auch Turm von Hanoi online (Online Spiele bei der blinden Kuh)

6.5.4 Hypotheken

Wenn Sie Glück haben, werden Sie sich eines Tages beim Kauf einer Eigentumswohnung oder gar eines Hauses mit diesem Thema beschäftigen müssen.
Hypotheken sind nichts anderes als Darlehen der Bank, die durch eine Immobilie abgesichert sind. Die Höhe dieses Darlehens sei X Euro, der vereinbarte Zinssatz sei p (nicht in Prozent, sondern als Anteil aus $[0, 1]$), es werde mit 1% getilgt. Ich nehme der Einfachheit halber an, dass Zahlungen im Rhythmus von einem Jahr fällig werden (in der Realität werden monatliche Zahlungen geleistet). p entspricht also dem Zinssatz per anno, der zur Zeit bei einer 10-jährigen Laufzeit zwischen $p = 0,03\,(3\%)$ und $p = 0,05\,(5\%)$ liegt.
Nach einem Jahr sind also $Z_1 := p \cdot X$ Euro Zinsen und $T_1 := 0,01 \cdot X$ Euro Tilgung, zusammen $B := (p + 0,01)X$ zu leisten [12]. Nach einem Jahr beträgt die Restschuld nur noch $X_1 := X - T_1 = (1 - 0,01)X$. Jetzt sind nach einem weiteren Jahr nur noch $Z_2 := p \cdot X_1$ Zinsen fällig. Damit die Gesamtzahlung konstant $=B$ bleibt, wird jetzt $T_2 := B - Z_2$ getilgt, die neue Restschuld beträgt $X_2 := X_1 - T_2$.
Vor Ablauf des n-ten Jahres sei die Restschuld X_{n-1}. Dann wird an Zinsen $Z_n := p \cdot X_{n-1}$ gezahlt und $T_n := B - Z_n$ getilgt. Die neue Restschuld beträgt $X_n := X_{n-1} - T_n = X_{n-1} + Z_n - B$, also

$$X_n = (1 + p)X_{n-1} - B, n = 1, 2, 3, ..., N,$$

wenn N die Laufzeit der Hypothek ist.

[12] Bei monatlichen Zahlungen $B := \frac{p+0,01}{12}X$.

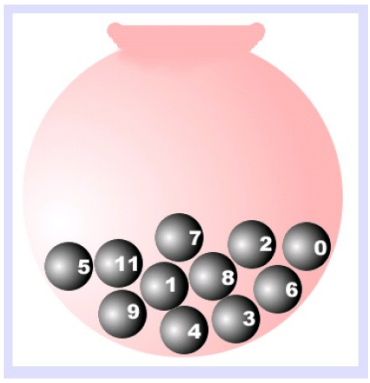
Kapitel 7

Kombinatorik

„Man kennt das doch: Der Trainer kann noch soviel warnen, aber im Kopf jeden Spielers sind 10% weniger vorhanden und bei 11 Mann sind das schon 110 %“ (Werner Hansch, Fußball-WM 2002)

7.1 Einführung

Es gibt vier Grundaufgaben der Kombinatorik, die gerne mit **Urnenmodellen** beschrieben werden. Die Urne enthält dabei n (verschiedene) Kugeln, es wird k-mal eine Kugel aus der Urne gezogen. Man unterscheidet, ob eine gezogene Kugel vor dem nächsten Zug wieder zurückgelegt wird oder nicht (in diesem Fall muss $k \leq n$ gelten, und alle gezogenen Kugeln sind verschieden) und ob die Reihenfolge (Anordnung) der Ziehungsergebnisse eine Rolle spielt oder nicht. In der Kombinatorik geht es um die ausschließlich von n und k abhängigen **Anzahl** der verschiedenen Ziehungsergebnisse, es soll also (richtig!) *gezählt* werden. Es gibt vier Grundaufgaben, nämlich „Mit zurücklegen, mit Anordnung“ (s. Kap. 7.2), „Ohne zurücklegen, mit Anordnung“ (s. Kap. 7.3), „Ohne zurücklegen, ohne Anordnung“ (s. Kap. 7.4) sowie „Mit zurücklegen, ohne Anordnung“ (s. Kap. 7.5). Daher wird es vier Formeln geben, unter ihnen sind die überall in



der Mathematik präsenten **Binomialkoeffizienten** $\binom{n}{k}$.
Die Kombinatorik spielt eine wichtige Rolle in der Wahrscheinlichkeits-Rechnung. Aber nur dann, wenn alle Ziehungsergebnisse gleichwahrscheinlich sind. Das ist bei kombinatorischen Aufgaben vom Grundtyp des Kap. 7.5 nicht der Fall. Daher wird dieser Abschnitt in der Vorlesung nur kurz behandelt – obwohl er der mathematisch reizvollste und schwierigste Fall ist.
Man kann durch eine solche Klassifizierung der Kombinatorik in vier Grundaufgaben den Eindruck haben, man könnte alle kombinatorischen Aufgaben auf ein Grundschema reduzieren und formalisieren. Das ist nur sehr bedingt der Fall, insbesondere, wenn in der „Textaufgabe“ gar keine Urnen, geschweige denn Kugeln, vorkommen. Wenn z.B. 5 Fußballspieler 8 Tore schießen und man nach der Anzahl der möglichen Torschützenlisten fragt, mag es hilfreich, aber auch ein wenig komisch sein, sich die Spieler als Kugeln in einer Urne vorzustellen, die von den geschossenen Toren „gezogen“ und danach wieder in die Urne zurückgelegt werden.

Die Urne sollte man mit einer *Menge* $A = \{a_1, ..., a_n\}$ (von n *verschiedenen* Elementen) identifizieren. Man kann sich den Index j von a_j als Zahl vorstellen, die eine Kugel beschriftet, was der Menge $A = \{1, 2, ..., n\}$ entspricht. Jeder Urnenzug entspricht dann dem Ziehen einer Zahl zwischen 1 und n. Das Ergebnis von k Zügen ist mathematisch nicht ganz einfach zu beschreiben. Am einfachsten ist der Fall „mit Zurücklegen und unter Einbeziehung der Reihenfolge“. Dann kann man das Ziehungsergebnis mit einem *k-Tupel* aus dem *kartesischen Produkt* $A^k := A \times A \times \cdots \times A$ identifizieren, d.h. jedes Ziehungsergebnis kann man durch genau ein k-Tupel aus A darstellen. Für $k = 2$ spricht man auch von einem *geordneten Paar*, für $k = 3$ von einem *Tripel*. Ein k-Tupel hat k *Komponenten*, von denen einige auch gleich sein können, alle aber in A liegen sollen. Siehe auch Kap. 3.3.5.
Ein Ziehungsergebnis ohne Berücksichtigung der Anordnung zu beschreiben, ist nicht ganz so offensichtlich. Eine Möglichkeit ist es, sich zu notieren, wie oft ein Element von A gezogen wurde: So setze man k_j für die Anzahl der Züge, mit denen das Element a_j (oder j) gezogen wird ($j = 1, 2, ..., n$). Dann repräsentiert das n-Tupel $(k_1, k_2, ..., k_n)$ mit $k_1 + k_2 + \cdots + k_n = k$ ein Ziehungsergebnis.

Neben dem Urnenmodell gibt es eine weitere Veranschaulichung der Grundaufgaben. Hier wird die Menge A mit n durchnummerierten *Plätzen* identifiziert, die für eine oder mehrere „Kugeln“ Platz haben. Durch jeden der k Züge wird bestimmt, an welchen Platz eine Kugel gelegt wird. „Mit zurücklegen“ bedeutet jetzt, dass einem Platz mehrere Kugeln zugelost werden können. Spielt die Anordnung eine Rolle, muss die Nummer des Zuges auf der platzierten Kugel notiert werden. Ich nenne dieses Modell das „Platz-Anordnungs-Modell“ im Gegensatz zum „Urnenmodell“.

Als Vorstufe der „Zählkunst“ kann man die *Summenregel*

$$|A \cup B| = |A| + |B| \quad \text{für disjunkte } A, B$$

und die *Produktregel* aus Kap. 3.3.5 (s. Abb. 7.1 und 7.2)

$$|A \times B| = |A| \cdot |B|$$

Abbildung 7.1: Produktregel: 3 Blusen, 4 Röcke

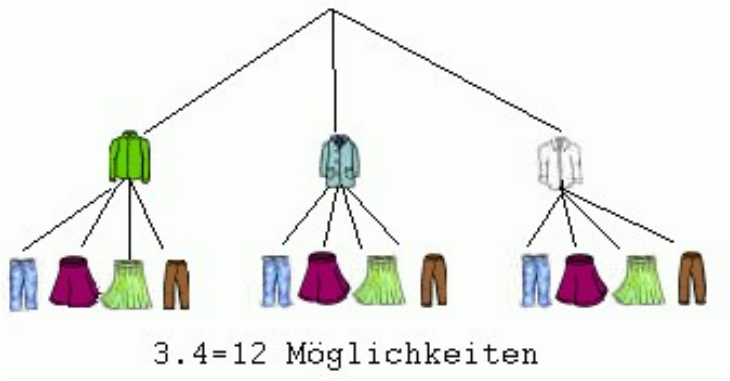


Abbildung 7.2: Entscheidungsbaum zur Produktregel: 3 Blusen, 4 Röcke

ansehen.

In den folgenden Abschnitten werden die vier Grundtypen der Kombinatorik behandelt.

Internet:
Kombinatorik[1] (Mathe Prisma Uni Wuppertal)
Anzahlen[2] (E. Prisner TU Cottbus)

7.2 Mit zurücklegen, mit Anordnung

Seien k und n natürliche Zahlen. Wie viele k-Tupel $(b_1, b_2, ..., b_k)$ mit Komponenten $b_j \in A = \{a_1, a_2, ..., a_n\}, j = 1, 2, ..., k$, gibt es?
Die Antwort lautet

[1] http://www.MathePrisma.uni-wuppertal.de/Module/Kombin/index.htm
[2] http://www.math.tu-cottbus.de/INSTITUT/lsgdi/DM/Anzahlen.html.

$$n^k \tag{7.1}$$

Der Beweis dieser Formel folgt aus der Produktregel, da A^k die Menge aller Ziehungsergebnisse ist und $|A^k| = |A|^k = n^k$ gilt. Dabei steht $|X|$ für die Anzahl der Elemente der (endlichen) Menge X. Man kann diese Formel aber auch direkt einsehen (so, wie man die Produktregel beweist):
Für die 1. Komponente (Zug) b_1 gibt es n Möglichkeiten – jedes Element aus A ist denkbar. Für die 2. Komponente gibt es ebenfalls n Möglichkeiten, macht $n^2 = n \cdot n$ Möglichkeiten, da jedes Ergebnis des 1. Zuges mit jedem Ergebnis des 2. Zuges kombiniert werden kann, usw. Hier kommt eigentlich ein Induktionsschluss (nach k) zum Tragen, beschrieben durch die Rekursion

$$n^{k+1} = n^k \cdot n.$$

7.2.1 Beispiele

1. Ein Alphabet enthalte n Zeichen. Wie viele (nicht notwendig sinnvolle) Worte der Länge k kann man aus ihnen bilden? Hier spielt die Reihenfolge offensichtlich eine Rolle, und die Zeichen (Buchstaben) können mehrfach auftreten[3].

2. Auf wie viele Weisen kann man k verschiedene Geschenke auf n Personen verteilen? (Wichtig ist hier *verschieden*, weil dies die Anordnung der Ergebnisse notwendig macht)[4].

3. Sei $|A| = k, |B| = n$. Wie viele Abbildungen $f : A \to B$ gibt es?[5]

4. Wie viele k-stellige Telefonnummern gibt es?[6]

5. Wie viele verschiedene Informationen kann man mit k Bits darstellen?

   Ein Bit ist die Information für „an-aus“, „0 oder 1“, „ja-nein“, etc. Durch k Bits kann eine Dualzahl mit k Stellen dargestellt werden. Jede Stelle „zieht“ ein Bit ($n := 2$). Also ist die Antwort 2^k.

7.3 Ohne zurücklegen, mit Anordnung

Wie viele k-Tupel $(b_1, b_2, ..., b_k)$ gibt es, deren Komponenten $b_j \in A$ alle verschieden sind? Hier muss offensichtlich $k \leq n$ gelten.
Die Antwort lautet

[3] Die Urne enthält n Buchstaben. Für jede Position des Wortes wird ein Buchstabe „gezogen“.
[4] Die Urne enthält die Personen. Jedes Geschenk „zieht“ eine Person.
[5] Jedes Element $a \in A$ „zieht“ ein „Bild“ $f(a)$.
[6] Jede Stelle der Telefonnumer „zieht“ eine der $n := 10$ Ziffern.

$$(n)_k := n \cdot (n-1) \cdots (n-k+1) \tag{7.2}$$

Für die 1. Komponente gibt es n Möglichkeiten, für die 2. te nur noch $n-1$, für die letzte schließlich noch $n-k+1$ Möglichkeiten.

7.3.1 Permutationen

Ist $k = n$, so haben wir mit jedem Ziehungsergebnis eine **Permutation** der Menge A. Es gibt $n!$ (sprich n Fakultät) Permutationen einer n-elementigen Menge A. Wir hatte $n!$ schon im Kap. 6.5.1 kennen gelernt.
Es ist einfacher und index-sparend, die Menge $A = \{a_1, ..., a_n\}$ mit der Menge $A = \{1, 2, ..., n\}$ gleich zu setzen. Eine Permutation ist zum einen dadurch beschrieben, dass man festlegt, welche dieser Zahlen als erste, zweite,...., letzte (n-te) gezogen wird. In diesem Sinn ist $(4, 2, 1, 3)$ eine Permutation für $n = 4$: Die 4 wurde als erste, die 2 als zweite, die 1 als dritte und die 3 als letzte Zahl gezogen. Man kann es aber auch anders sehen – dies wird unsere „offizielle“ Sichtweise sein: Wenn man die Zahlen 1,2,3,4 permutiert, will man wissen, an welche Position die 1, die 2, etc. kommt. Jede Position kommt genau einmal vor, in obigem Fall kann man die Permutation auch durch (3,2,4,1) beschreiben, da die 1 an Position 3, die 2 an Position 2, die 3 an Position 4 und die 4 an Position 1 steht. Diese Sichtweise ist die einer *Abbildung*, genauer einer *Bijektion* von A. Diese ist dadurch festgelegt, dass man weiß, wohin $a_1 = 1$, wohin $a_2 = 2$,..., und wohin $a_n = n$ abgebildet wird. Die erstgenannte Darstellung beschreibt nacheinander die Bilder von 1,2,3,4 unter der *Umkehrabbildung*. Wir fassen zusammen:

Definition 7.1. *Eine Permutation der endlichen Menge $A = \{1, ..., n\}$ ist eine bijektive Abbildung $p : A \to A$. Sie wird mit $(p(1), p(2), ..., p(n))$ bezeichnet.*

Es ist also klar, dass es $n!$ Bijektionen einer n-elementigen Menge gibt.

Wir schreiben auch:

$$(n)_k = n(n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!}. \tag{7.3}$$

7.3.2 Beispiele

1. Wie viele Worte der Länge k eines n-elementigen Alphabets kann man bilden, wenn die Buchstaben des Wortes alle verschieden sein sollen?

2. Eine Großküche kann n Gerichte kochen. Es soll ein Speiseplan für eine Woche aufgestellt werden, wobei kein Gericht mehrfach vorkommen darf. Wie viele Speisepläne gibt es?

3. 6 LäuferInnen kommen nacheinander ins Ziel. Wie viele mögliche Reihenfolgen gibt es?

4. Beim Pferdetoto muss man die Reihenfolge der ersten drei Pferde voraussagen. Wie viele Möglichkeiten gibt es bei 15 Pferden?

5. Sei $|A| = k, |B| = n$ und $n \geq k$. Wie viele injektive Abbildungen $f : A \to B$ gibt es?

7.4 Ohne zurücklegen, ohne Anordnung

Das Ziehungsergebnis kann als k-elementige Teilmenge der n-elementigen Menge A beschrieben werden. Wieder muss $k \leq n$ gelten.
Somit ist die Frage nach der Anzahl der verschiedenen Ziehungsergebnisse gleichbedeutend mit der Frage nach der Anzahl von k-elementigen Teilmengen einer n-elementigen Menge.
Antwort: **Binomialkoeffizient**

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{7.4}$$

Wir formulieren:

Satz 7.2. *Es gibt* $\binom{n}{k}$ *k-elementige Teilmengen einer n-elementigen Menge.*

Beweis: Mit Berücksichtigung der Anordnung wäre die Antwort wegen (7.3) $\frac{n!}{(n-k)!}$. Eine k-elementige Menge kann man auf $k!$ Weisen anordnen. Daher können je $k!$ Möglichkeiten der Ergebnisse *mit* Anordnung zu einem Ergebnis *ohne* Anordnung zusammengefasst werden, und wir erhalten obige Formel[7].
Eine andere Sicht- und Herleitungsweise: Es gibt $n!$ Permutationen von A. Sei $A_k \subset A$ eine k-elementige Teilmenge. Betrachten wir alle Permutationen $(p_1, ..., p_n)$ von A, deren ersten k Einträge $p_1, ..., p_k$ die Menge A_k bilden, so gibt es hiervon $k!(n-k)!$, da wir die k Elemente von A_k und die $(n-k)$ ihres Komplements $\overline{A_k}$ noch beliebig permutieren können. Also ergeben $\frac{n!}{k!(n-k)!}$ Permutationen jeweils verschiedene Mengen A_k. ∎

7.4.1 Beispiele:

1. Wie viele Spielpaarungen gibt es bei es bei n Mannschaften? $(k = 2)$

2. Der Vorstand eines Vereins mit n wählbaren Mitgliedern besteht aus k Personen. Wie viele verschiedene Vorstände gibt es?

[7] Bezeichnet man mit $b(n, k)$ die gesuchte Formel, so haben wir $\frac{n!}{(n-k)!} = k!b(n, k)$.

3. Beim Elfmeterschießen werden 5 Spieler ausgesucht. Wie viele Möglichkeiten hat der Trainer? (Wenn es nicht auf die Reihenfolge ankommt). Werden die Schützen inkl. Reihenfolge benannt, ist es ein Problem aus Abschnitt 7.3.

4. Wie viele Möglichkeiten gibt es, 6 Zahlen aus 49 (Lotto) auszulosen? Antwort: $\binom{49}{6} = 13983816$

5. Aus einer Bibliothek mit n Büchern kann man k Bücher auswählen.

6. Wieviele Möglichkeiten gibt es, 12 Plätze mit 4 roten, 3 gelben und 5 blauen Steinen zu belegen?

   Antwort:
   $$\binom{12}{4} \cdot \binom{8}{3} = 27720.$$

   Dieses Beispiel kann verallgemeinert werden: In einer Urne sind k_1 Kugeln vom „Typ 1“, ..., k_m Kugeln vom „Typ m“. Auf wie viele Weise kann man diese anordnen? Antwort:
   $$\frac{n!}{k_1!k_2!\cdots k_m!}, \quad n = k_1 + k_2 + \cdots + k_m.$$

   Bei dem Beweis dieser Formel hilft das „Platz-Anordnungs-Modell“ aus der Einführung.

Internet:
Applet Binomialkoeffizient[8] (JUMBO Biometrie Uni Münster)

7.4.2 Merkenswertes zu Binomialkoeffizienten

Alle nachfolgenden Aussagen können kombinatorisch verstanden werden.

Satz 7.3.
$$\binom{n}{k} = \binom{n}{n-k}$$

Kombinatorischer **Beweis:** Mit jeder Teilmenge ist auch ihr Komplement festgelegt. Also gibt es genau so viele k-elementige wie $(n-k)$-elementige Teilmengen der n-elementigen Menge A. Noch einfacher ist es, die Formel (7.4) direkt zu benutzen. ∎

Satz 7.4.
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

[8] http://medweb.uni-muenster.de/institute/imib/lehre/skripte/biomathe/bio/script5.html#5.4

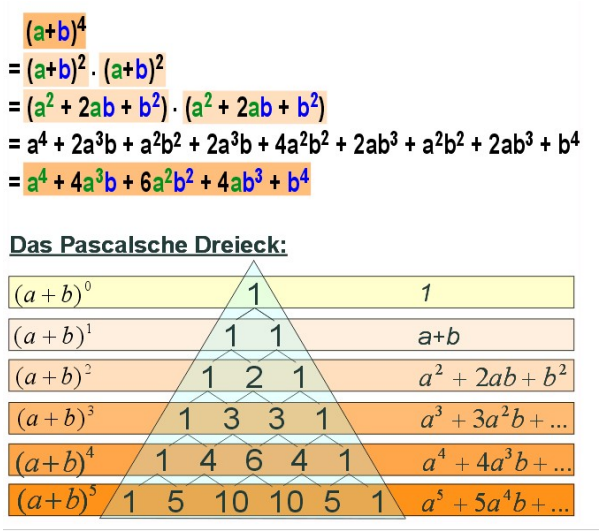


Abbildung 7.3: Pascal'sches Dreieck und Binomischer Lehrsatz

[9]

Beweis: Die linke Seite ist gleich der Anzahl *aller* Teilmengen von A, also gleich der Anzahl der Elemente der Potenzmenge von A. Diese enthält $2^{|A|}$ Elemente – das hatten wir mit vollständiger Induktion bewiesen. Auch letzteres ist ein kombinatorisches Resultat, da eine Teilmenge von A durch eine 0-1-Belegung eines jeden Elementes von A gekennzeichnet ist – 0, falls das Element nicht zur Teilmenge gehört und sonst 1.
Man kann diese Formel auch direkt aus der *binomischen Formel* (7.6) ableiten, wenn man dort $a = 1 = b$ setzt. ∎

Beispiel: In der Blindenschrift bedient man sich der sogenannten Brailleschen Zelle. Sie besteht aus 6 Punkten. Dieses Schema dient dazu, durch Durchdrücken eines oder mehrerer Punkte verschiedene Zeichen zu erzeugen, die der Blinde mit den Fingerspitzen abtastet. Wie viele Zeichen gibt es? Antwort: $\sum_{k=1}^{6} \binom{6}{k} = 2^6 - 1 = 63$.

Satz 7.5 (Formel des Pascal'schen Dreiecks)**.** *(Blaise Pascal 1623-1662), Abb. 7.3*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \tag{7.5}$$

Beweis: Zeichne ein Element von A aus und zähle die k-elementigen Teilmengen von A, denen dieses ausgezeichnete Element angehört (davon gibt es $\binom{n-1}{k-1}$) und die, wo dies nicht der Fall ist (davon gibt es $\binom{n-1}{k}$). ∎

Satz 7.6 (Binomischer Lehrsatz)**.**

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{7.6}$$

Beweis: Dieser Satz folgt aus rein kombinatorischen Betrachtungen. Hierzu verwenden wir einen Trick und schreiben

$$(a+b)^n = (a_1+b_1)(a_2+b_2)\cdots(a_n+b_n)$$

mit $a_1 = a_2 = \cdots = a_n := a$ und $b_1 = b_2 = \cdots = b_n := b$. Dieses Produkt berechnen wir mit dem üblichen „Ausmultiplizieren“. Für $n = 4$ entstehen so z.B. – u.a. – die Produkte $a_1a_2b_3a_4 = a^3b, b_1a_2b_3a_4 = a^2b^2$. Bei festem k fassen wir nunmehr alle Produkte zusammen, die k-mal den Faktor a und damit $(n-k)$-mal den Faktor b enthalten. Wie viele solcher Produkte gibt es? Nun, wir müssen aus der Indexmenge $\{1, 2, ..., n\}$ der $a_j, j = 1, ..., n$ eine k-elementige Teilmenge auswählen. Das geht auf $\binom{n}{k}$ Weisen! Also führt diese Zusammenfassung auf den Ausdruck $\binom{n}{k}a^kb^{n-k}$. Die Summe all dieser Terme führt dann auf den rechten Ausdruck in (7.6). ∎
Formal einfacher ist ein Beweis per vollständiger Induktion. Versuchen Sie es!

7.5 Mit zurücklegen, ohne Anordnung

Dies ist der komplizierteste Fall.
Antwort:

$$\binom{n+k-1}{k}$$

oder auch

$$\binom{n+k-1}{n-1}.$$

Für $k = 2$ ergeben sich $n(n+1)/2$ Möglichkeiten.
Das Ziehungsergebnis ist durch ein n-Tupel $(h_1, ..., h_n)$ mit $h_j \in \mathbb{N}_0$ und $h_1 + h_2 + \cdots + h_n = k$ gegeben. Dabei gibt h_j an, wie oft a_j gezogen wurde. Dies kann durch das „Platz-Anordnungs-Modell“ beschrieben werden: Jeder j-te Platz erhält als Ziehungsergebnis die Anzahl der „Treffer“ h_j, etwa durch h_j Kreuze.

7.5.1 Beispiele

1. Es gibt k Personen und n Parteien. Jede Person hat genau eine Stimme. Wie viele Stimmenverteilungen gibt es?

   Hier ist wieder das „Platz-Anordnungs-Modell“ hilfreich. Die n Parteien sind die Plätze. Jede WählerIn ergibt einen Strich bei der gewählten Partei. Am Ende zählt man bei jeder Partei die Anzahl der Striche.

2. n Fußballspieler erzielen in einer Partie k Tore. Wie viele mögliche Torschützenverteilungen gibt es?

   Auch hier ist das „Platz-Anordnungs-Modell“ nützlich. Die n Spieler sind die „Plätze“. Bei jedem Tor wird bei dem jeweiligen Torschützen ein Strich gemacht.

7.5.2 Zur Herleitung der Formel

Der Trick bei der kombinatorischen Behandlung ist die Zurückführung auf eine k-fache Ziehung aus einer Urne mit $n+k-1$ Kugeln *ohne Zurücklegen* und ohne Berücksichtigung der Reihenfolge. Bleiben wir einmal beim Fußballspiel, wobei a_j (bzw. j) der Name (die Nummer) des j-ten Spielers sei. Wir legen gedanklich die $n+k-1$ Kugeln nebeneinander, von denen wir die k gezogenen Kugeln durch Kreuze *markieren*. Die nichtmarkierten $n-1$ Kugeln beschriften wir mit den Namen a_1 bis a_{n-1} (bzw. den Nummern $1, 2, ..., n-1$). Sie entsprechen den Fußballspielern (bis auf einen). Die erste unmarkierte Kugel rechts einer markierten Kugel gibt den Namen (bzw. die Nummer) des Spielers an, der soviele Tore geschossen hat, wie es links von ihm markierte Kugeln gibt. Die rechtsaußen befindlichen Kreuze „gehören“ dem n-ten Spieler. So hat Spieler Nr. 1 kein Tor geschossen, wenn die erste Kugel unmarkiert bleibt, Spieler Nr. n hat j Tore geschossen, wenn die letzten j Kugeln markiert sind. Gibt es viele Spieler und wenig Tore, sind die markierten Kugeln in der Minderzahl.

Eine gleichwertige Beschreibung: Allgemein besteht ein Ziehungsergebnis aus einer Zuordnung, die jeder der n Kugeln eine gewisse Trefferzahl $h_j, j = 1, 2, ..., n$ zuordnet. Das gesamte Ziehungsergebnis besteht dann aus einem n-Tupel $(h_1, ..., h_n)$. Dieses können wir notieren, indem wir aus einer abstrakten Urne $K = \{1, 2, ..., n+k-1\}$ mit $n+k-1$ Kugeln k Kugeln ohne Zurücklegen ziehen. Jede solcher gezogenen Kugeln *markieren* wir und legen die $n+k-1$ Kugeln danach der Reihe nach in eine waagerechte Linie. Die $n-1$ nicht markierten Kugeln beschriften wir mit $a_1, ..., a_{n-1}$ und fügen ganz rechtsaußen eine Kugel mit der Beschriftung a_n hinzu. Nun deuten wir das Ergebnis, indem wir nebeneinanderliegende markierte Kugeln bzw. ihre Anzahl auf den ersten unmarkierten rechten Nachbarn beziehen.

Grundsätzlich ist es gleich, ob wir k Kugeln oder die verbliebenen $n-1$ Kugeln markieren (Auch „Nichtmarkierung“ ist eine Markierung). Bei dem Beispiel mit den Fußballspielern wird i.a. $k < n$ sein, so dass es naheliegend ist, hier k Kugeln zu markieren. Bei dem Parteienbeispiel ist jedoch $n < k$, und n ist sogar sehr viel kleiner als k, wir markieren $n-1$ Kugeln, die wir als „Trennkugeln“ deuten werden. Die Anzahl der linksaußen liegenden unmarkierten Kugeln gibt dann an, wie viele Stimmen die Partei Nr. 1 erhalten hat. Die Anzahl der rechts der ersten markierten Kugel („Trennkugel“) liegenden unmarkierten Kugeln gibt sodann die Anzahl der Stimmen für Partei Nr. 2 an, während die Anzahl der unmarkierten rechtsaußen liegenden Kugeln die Anzahl der Stimmen der Partei Nr. n bestimmt. Hier „trennen“ die $n-1$ markierten („Trenn-“) Kugeln die einzelnen Parteien. Da $\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$ gilt, hat man also $n-1$ Kugeln gezogen, deren Nummern die Lage der „Trennkugeln“ bestimmen.

Beispiel: $n = 5, k = 100$. Die Urne enthält $n+k-1 = 104$ Kugeln mit den Nummern 1,2,...,104. Es werden $n-1 = 4$ Kugeln mit den Nummern 7, 11, 83, 101 gezogen. Dann hat Partei Nr. 1 sechs Stimmen, Partei Nr. 2 drei, Partei Nr. 3 einundsiebzig, Partei Nr. 4 siebzehn und Partei Nr. 5 drei Stimmen.

Internet:
Verständnistest der vier Grundaufgaben[10] (Mathe Prisma),
Arbeitsblatt Kombinatorik (Aufgaben[11] (Mathe-Prisma),
Einführung in die Stochastik – die kombinatorischen Grundaufgaben (learn: line NRW)

[10] http://www.MathePrisma.uni-wuppertal.de/Module/Kombin/schluss.htm
[11] http://www.MathePrisma.uni-wuppertal.de/Module/Kombin/Aufgaben.htm

Kapitel 8

Gruppen

8.1 Einführung

Sie haben schon in Kap. 5 über Funktionen, genauer in Kap. 5.2.3 den Begriff *binäre (zweistellige) Verknüpfung auf einer Menge A* kennengelernt. Darunter versteht man eine Abbildung $F : A \times A \to A$. Die wichtigsten Beispiele hierfür sind Addition und Multiplikation auf $A := \mathbb{R}$, der Menge der reellen Zahlen, also die Abbildungen $F : \mathbb{R}^2 \to \mathbb{R}$, die durch $F(x, y) := x + y$ bzw. $F(x, y) := x \cdot y$ definiert sind.
Etwas weniger vertraut und gewöhnungsbedürftig ist die Verknüpfung „Verkettung“ von zwei Abbildungen f und g mittels $f \circ g$, etwa von zwei Bijektionen f und g einer Menge B. In diesem Fall ist A die Menge aller Bijektionen von B und $F(f, g) = f \circ g$[1]. F ist also eine Abbildung von $A \times A$ nach A, wobei A eine Menge von speziellen Abbildungen (auf B) ist — das ist schon etwas gewöhnungsbedürftig.
Immer wieder kamen *logische* Verknüpfungen von *Aussagen* vor, ohne dass wir dies bisher ganz streng präzisiert haben: Zwei Aussagen A und B können durch *und* oder auch durch *oder* miteinander verknüpft werden und ergeben so wieder eine neue Aussage. Hier haben wir es mit einer binären Verknüpfung auf einer Menge von Aussagen zu tun. Genaueres erfahren Sie in Kap. 10.
Gruppen sind nichts anderes als Mengen G zusammen mit einer Verknüpfung auf G, die gewisse Eigenschaften haben, welche zum Begriff des *neutralen Elements* von G und den des *Inversen* eines Elements $g \in G$ führen. Das Konzept von Gruppen ist fast ebenso fundamental wie das von Mengen. Spätere Begriffe wie *Körper* (bei der Einführung von reellen und komplexen Zahlen) oder *Vektorraum* (in der Linearen Algebra) bauen auf dem Begriff „Gruppe“ auf. Aber auch die *Symmetrie* geometrischer Objekte kann man sehr elegant mit Hilfe ihrer *(Symmetrie-) Gruppen* beschreiben.
Dieses Kapitel hat aber auch einen Selbstzweck: wieder kann das formale, abstrakte Schließen trainiert werden.

[1] Ich hätte auch $F(x, y) = x \circ y$ schreiben können, wobei dann aber x und y Bijektionen von B sein müssen. Es ist jedoch üblich – aber nicht zwingend – Abbildungen mit $f, g, h, ...$ zu bezeichnen.

Wir werden als wichtigste Beispiele Gruppen von Zahlenmengen ($\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$), auch von denjenigen Mengen, die bei der *Rechnung mit Resten* vorkommen, behandeln sowie die *Symmetriegruppen* von geometrischen Objekten streifen.

8.2 Verknüpfungen

Wie schon in der Einführung dargestellt, geht es bei den Gruppen um Mengen mit einer binären (zweistelligen) Verknüpfung. Diese Verknüpfung $F : G \times G \to G$ stellen wir durch ein *Verknüpfungssymbol* $\star$ oder $\circ$ oder $\oplus$ oder $+$ oder $\cdot$ dar, zunächst einmal durch $\star$, wobei man $g \star h$ an Stelle von $F(g, h)$ schreibt. Wir sprechen *„g Stern h“* oder allgemeiner *„g verknüpft mit h“*.
Die Schreibweise $F(g, h)$ ist formal nicht korrekt: F wird auf das Paar $(g, h) \in G \times G$ angewendet. Richtig muss es $F((g, h))$ heißen. Wir werden aber auf ein Klammerpaar verzichten!
Die einzige Eigenschaft einer solchen Verknüpfung ist, dass für alle $g, h \in G$ das Element $g \star h$ definiert ist und wieder in G liegt. In diesem Fall benutzen wir die Notation $(G, \star)$ und nennen $(G, \star)$ ein **Gruppoid**.
Wenn eindeutig klar ist, welche zweistellige Verknüpfung $\star$ gemeint ist, soll in Zukunft statt von $(G, \star)$ kürzer nur vom Gruppoid G die Rede sein.
In diesem Sinne sind $(\mathbb{N}, +)$ und $(\mathbb{R}, \cdot)$ Gruppoide, während $(\mathbb{N}, -)$ kein Gruppoid ist, da die Differenz $m - n$ zweier natürlicher Zahlen m und n negativ, also keine natürliche Zahl sein kann.
Weitere Beispiele für Gruppoide sind $(PotM, \cup)$ oder $(PotM, \cap)$ oder $(Abb(\mathbb{R}, \mathbb{R}), \circ)$, wobei $Abb(\mathbb{R}, \mathbb{R})$ die Menge aller reellen Funktionen und $\circ$ das Verkettungssymbol für Abbildungen ist.
Für endliche Mengen G kann man ein Gruppoid durch eine **Verknüpfungstafel** darstellen:

$\star$	a	b	c	$\cdots$
a				
b			X	
c				
$\vdots$				

An der Stelle X wird das Ergebnis $b \star c$ eingetragen usw.

8.3 Das Rechnen mit Resten

Einen kleinen ersten Einstieg haben Sie in Kap. 2.3 kennengelernt. Sie erinnern sich: $m \bmod n = r$ bedeutet, dass r der Rest ist, wenn man m durch n teilt. Als Reste kommen hierbei nur Zahlen aus

$$\mathbb{Z}_n := \{0, 1, ..., n-1\}$$

in Frage. Dass *mod* (sprich „modulo“) zunächst eine binäre Verknüpfung auf $\mathbb{N}$, ja auf $\mathbb{Z}$ ist, interessiert uns weniger. Vielmehr führen wir auf $\mathbb{Z}_n$ die beiden Verknüpfungen $+_n$ und $\cdot_n$ durch

$$r +_n s := (r + s) \bmod n, \quad r \cdot_n s := (r \cdot s) \bmod n.$$

ein. Z.B. ist $6 +_8 4 = 2$ und $6 \cdot_8 4 = 0$.
Auf diese Weise erhalten wir natürlich zwei Gruppoide $(\mathbb{Z}_n, +_n)$ und $(\mathbb{Z}_n, \cdot_n)$, die sich nur in ihrer Verknüpfung unterscheiden.
Beispiele: Gesucht sind die Verknüpfungstafeln der Gruppoide $(\mathbb{Z}_4, \cdot_4)$ und $(\mathbb{Z}_4, +_4)$

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2			0	
3			2	1

$+_4$	0	1	2	3
0				
1				
2			0	1
3				2

Diese Tafeln werden in Vorlesung und/oder Übungen ergänzt.

Es zeigt sich, dass man bei allen „normalen“ Rechnungen mit anschließender modulo-Bildung $\bmod n$ auch bei jedem Zwischenschritt schon hätte zu den Resten übergehen können. Zum Beispiel:

$$(3 \cdot 7 \cdot 11) \bmod 5 = ((3 \bmod 5) \cdot (7 \bmod 5) \cdot (11 \bmod 5)) \bmod 5 = (3 \cdot 2 \cdot 1) \bmod 5 = 1$$

oder auch

$$(3 \cdot 7 \cdot 11) \bmod 5 = ((21 \bmod 5) \cdot 11) \bmod 5 = 11 \bmod 5 = 1.$$

Dasselbe gilt, wenn man die Multiplikation durch die Addition ersetzt. Wir formulieren diesen Sachverhalt durch einen

Satz 8.1. *Wenn $n \in \mathbb{N}$ und[2] $r, s \in \mathbb{N}_0$, so gilt*

$$(r + s)\ mod\, n = ((r\ mod\, n) + (s\ mod\, n))\ mod\, n,$$

$$(r \cdot s)\ mod\, n = ((r\ mod\, n) \cdot (s\ mod\, n))\ mod\, n.$$

Wie beweist man diesen Satz? Hier hilft die Definition 4.2 von *kongruent* in Kap. 4: Zwei ganze Zahlen r, s heißen **kongruent modulo** einer natürlichen Zahl n : $\Longleftrightarrow$ n teilt $r - s$ bzw. (hiermit äquivalent) r und s haben bei Division durch n denselben **Rest**. Diese Relation, von der wir wissen, dass sie eine Äquivalenzrelation ist, nennen wir **Kongruenzrelation** bzgl n. Genauer: Die *Kongruenzrelation modulo* n, genannt R_n, ist durch

$$(r, s) \in R_n : \Longleftrightarrow \quad n \text{ teilt } (r - s)$$

[2] n darf nicht Null sein, wohl aber r und s.

definiert.
Jetzt besagt die erste Behauptung des Satzes, dass $r+s$ kongruent zu $(r \bmod n)+(s \bmod n)$ modulo n ist, d.h., dass n den Ausdruck $r+s-(r \bmod n)-(s \bmod n) = r-(r \bmod n)+s-(s \bmod n)$ teilt. Das ist richtig, wenn n beide Summanden, $r-(r \bmod n)$ und $s-(s \bmod n)$ teilt, was wiederum wahr ist, da n stets $m-(m \bmod n)$ für alle $m \in \mathbb{N}_0$ teilt, wie man sofort aus der Existenz von $q \in \mathbb{N}_0$ mit $m = q \cdot n + (m \bmod n)$ schließen kann (Definition des Restes). ∎

8.4 Neutrales Element, Inverse

Definition 8.2. *Gegeben sei ein Gruppoid $(G, \star)$. Ein Element $e \in G$ heißt* **neutrales Element** *oder auch* **Einselement**, *wenn $g \star e = e \star g = g$ für alle $g \in G$.*

Beispiele: In $(\mathbb{R}, +)$ ist $e = 0$ das neutrale Element, während die „Eins“ ($e = 1$) das neutrale Element in $(\mathbb{R}, \cdot)$ ist.
Nun schauen wir uns die Gruppoide $(PotM, \cup)$, $(PotM, \cap)$ und $(Abb(\mathbb{R}, \mathbb{R}), \circ)$ an. Gibt es hier neutrale Elemente und welche könnten es sein? Im ersten Fall ist es die leere Menge, im zweiten Fall M, im dritten Fall die **Identität**[3], das ist die Abbildung f, die $f(x) = x$ für alle x erfüllt, also alles so lässt, wie es ist.
In $(\mathbb{Z}_n, +_n)$ ist 0 das neutrale Element, in $(\mathbb{Z}_n, \cdot_n)$ ist $e = 1$ neutrales Element.
Es ist nicht schwer einzusehen, dass es in einem Gruppoid höchstens ein neutrales Element geben kann: Wenn es ein weiteres e' gäbe mit $g = g \star e' = e' \star g$ für alle g, könnte man hier auch $g = e$ setzen und erhält $e = e \star e'$. Da aber auch e ein Einselement ist, gilt $e \star e' = e'$, insgesamt also $e' = e$.

8.4.1 Inverse

Definition 8.3. *In einem Gruppoid $(G, \star)$ mit neutralem Element e heißt $h \in G$* **invers zu** *$g \in G$ (oder* **Inverses von** *g), wenn $g \star h = e$ und $h \star g = e$ gilt.*

Aus dieser Definition folgt sofort, dass das Inverse des Inversen von g wieder g selbst ist. Oder anders ausgedrückt: Wenn h zu g invers ist, so auch g zu h.
Beispiele: In $(\mathbb{R}, +)$ ist $-x$ invers zu $x \in \mathbb{R}$, in $(\mathbb{R}^\star, \cdot)$ mit $\mathbb{R}^\star := \mathbb{R} \setminus \{0\}$ ist $1/x$ invers zu x. In $(PotM, \cup)$ besitzt nur die „Null“ $\emptyset$ ein Inverses. In $(PotM, \cap)$ besitzt nur M selbst ein inverses Element, nämlich sich selbst, in $(Abb(\mathbb{R}, \mathbb{R}), \circ)$ besitzen nur die Bijektionen f inverse Elemente, nämlich ihre Umkehrabbildungen f^{-1}.
Die obige Bemerkung über das Inverse des Inversen liest sich jetzt so: $-(-x) = x$, $1/(1/x) = x$, $(M^c)^c = M$, $(f^{-1})^{-1} = f$.

Besonders interessant ist das Beispiel $(\mathbb{Z}_n^\star, \cdot_n)$ wobei $\mathbb{Z}_n^\star$ aus $\mathbb{Z}_n$ entsteht, indem man $\mathbb{Z}_n$ der Null beraubt. Dass man die Null auslässt, liegt daran, dass die Null niemals ein Inverses bzgl.

[3] Die Identität ist in $Abb(X, X)$ mit irgendeinem X definiert.

der Multiplikation besitzt. Aber auch andere Elemente müssen kein inverses Element besitzen: So z.B. $m = 6 \in \mathbb{Z}_8$. Wegen $6 \cdot_8 4 = 0$ kann solch ein Element nicht existieren (s.u.). Man kann aber auch alle „Kandidaten“ aus $\{1, 2, 3, 4, 5, 6, \}$ durchgehen – man findet kein Inverses von 6. Hier gilt der

Satz 8.4. *$m \in \mathbb{Z}_n^\star$ besitzt genau dann ein inverses Element bzgl. der Multiplikation $\cdot_n$, wenn m und n* **teilerfremd** *sind, d.h., wenn der* **größte gemeinsame Teiler** *von m und n Eins ist.*

Beweis: Wir haben es mit zwei Aussagen zu tun: Die Aussage, dass m ein Inverses m' in $\mathbb{Z}_n$ besitzt – diese Aussage nennen wir **A** – und die Aussage, dass m und n teilerfremd sind – diese Aussage nennen wir **B**.
Wir müssen zwei Aussagen zeigen: $\mathbf{A} \Longrightarrow \mathbf{B}$ (wenn **A**, dann **B**) und $\mathbf{B} \Longrightarrow \mathbf{A}$[4].
Wir beginnen mit $\mathbf{A} \Longrightarrow \mathbf{B}$: Wir können also gemäß **A** annehmen, dass m ein Inverses $m' \in \mathbb{Z}_n$ besitzt. Dann gilt

$$(m \cdot m') \bmod n = 1,$$

d.h. es gibt ein $q \in \mathbb{N}_0$ mit $m \cdot m' = q \cdot n + 1$. Dann können m und n aber keinen gemeinsamen Teiler $r \geq 2$ haben!
Ein logisch gleichwertiger Beweis für diese Richtung ist **Nicht B** $\Longrightarrow$ **Nicht A**[5].
Also nehmen wir an, dass m und n einen gemeinsamen Teiler $r \geq 2$ haben. Nun ist die Aussage A äquivalent zu $\exists q \in \mathbb{N}_0$ mit $m \cdot m' = q \cdot n + 1$. Nun teilt r sowohl m als auch n, also auch $m \cdot m'$ und damit $q \cdot n + 1$ sowie $q \cdot n$. Also teilt r zwei benachbarte Zahlen. Widerspruch zur Aussage A. Also ist A falsch.

Die fehlende Richtung „$\mathbf{B} \Longrightarrow \mathbf{A}$“ ist nicht sehr einfach zu zeigen. Hierzu benötigt man den *verallgemeinerten Euklidischen Algorithmus*, den wir evtl. später behandeln werden – wie auch den *Euklidischen Algorithmus* zur Berechnung des *größten gemeinsamen Teilers* $ggT(m, n)$ zweier Zahlen m und n. ∎

Jetzt können wir aus dem letzten Satz eine Folgerung ziehen:

Korollar 8.5. *Ist $p \in \mathbb{N}$ eine Primzahl, so hat jedes Element in $(\mathbb{Z}_p^\star, \cdot_p)$ ein Inverses.*

Beispiel: $p = 7$. Das Inverse von 4 ist 2, das von 6 ist 6 selbst.
Später werden wir sehen, dass dieser Satz $(\mathbb{Z}_p^\star, \cdot_p)$ zur Gruppe und $(\mathbb{Z}_p, +_p, \cdot_p)$ zu einem Körper macht.

[4] $\Longrightarrow$ ist eine zweistellige Verknüpfung auf einer Menge von Aussagen. In der Aussagenlogik (s. Kap. 10.3) fasst man diese beiden Aussagen zu $\mathbf{A} \Longleftrightarrow \mathbf{B}$ zusammen.

[5] Diese Gleichwertigkeit ist ein Gesetz der Aussagenlogik, s. Satz 10.3. Dabei ist **Nicht A** – auch $\overline{A}$ genannt (s. Kap. 10.2) – die Aussage „**A** gilt nicht“. „Wenn es regnet, ist die Straße nass“ ist gleichwertig mit „Ist die Straße nicht nass, regnet es nicht“.

8.5 Assoziativität und Kommutativität

Definition 8.6. *Eine Verknüpfung $\star$ für ein Gruppoid $(G, \star)$ ist* **assoziativ**, *wenn sie das* **Assoziativgesetz**

$$(u \star v) \star w = u \star (v \star w) \text{ für alle } \quad u, v, w \in G \tag{8.1}$$

erfüllt.

In einem solchen Fall kommt es nicht darauf an, in welcher Reihenfolge man verknüpft und man kann auch $u \star v \star w$ ohne jede Klammer schreiben! Das gleiche gilt für „Produkte“ mit endlich vielen Faktoren: Bei der Berechnung von $g_1 \star g_2 \star \cdots \star g_n$ kommt es nicht auf die Reihenfolge an, mit der man verknüpft!

In unseren Beispielen $(\mathbb{R}, +), (\mathbb{R}, \cdot), (PotM, \cup), (PotM, \cap), (\mathbb{Z}_n, +_n), (\mathbb{Z}_n, \cdot_n), (Abb(\mathbb{R}, \mathbb{R}), \circ)$ gilt das Assoziativgesetz. In $(\mathbb{R}, -)$ gilt das Assoziativgesetz nicht!

Satz 8.7. *Wenn in einem Gruppoid das Assoziativgesetz gilt und $g, h \in G$ Inverse g', h' besitzen, so besitzt auch $g \star h$ ein Inverses. Dieses ist gleich $h' \star g'$.*

Bemerkung: Man beachte, dass sich die Reihenfolge bei der Verknüpfung umdreht. Dies Prinzip kennen Sie von der Verkettung von Abbildungen: $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ (vgl. Satz 5.11), welches Sie sich sehr leicht merken können: Wenn Sie morgens erst die Strümpfe und dann die Schuhe anziehen, geht es abends beim Ausziehen anders herum: erst die Schuhe, dann die Strümpfe[6].
Beweis: Zu zeigen ist $(g \star h) \star (h' \star g') = e$. Wegen der Assoziativität von G kommt es nicht auf das Setzen der Klammern an:

$$(g \star h) \star (h' \star g') = g \star (h \star h') \star g' = g \star e \star g' = g \star g' = e.$$

∎

Definition 8.8. *Eine Verknüpfung $\star$ für ein Gruppoid $(G, \star)$ ist* **kommutativ**, *wenn es das* **Kommutativgesetz**

$$u \star v = v \star u \text{ für alle } \quad u, v \in G \tag{8.2}$$

erfüllt.

In unseren Beispielen $(\mathbb{R}, +), (\mathbb{R}, \cdot), (PotM, \cup), (PotM, \cap), (\mathbb{Z}_n, +_n), (\mathbb{Z}_n, \cdot_n), (Abb(\mathbb{R}, \mathbb{R}), \circ)$ gilt das Kommutativitätsgesetz – mit einer Ausnahme: **Die Verkettung von Abbildungen ist keine kommutative Verknüpfung**. Es ist sogar die Regel, dass für zwei Abbildungen $f, g \in Abb(\mathbb{R}, \mathbb{R})$ gilt

$$f \circ g \neq g \circ f.$$

Beispiele: $f : x \mapsto x^2, \quad g : x \mapsto x + 1$. Dann ist $f(g(x)) = (x+1)^2 = x^2 + 2x + 1$, aber $g(f(x)) = x^2 + 1$. Ganz offensichtlich sind die beiden Abbildungen $f \circ g$ und $g \circ f$ verschieden[7]!

[6] Dieses Beispiel stammt von meinem Kollegen Ch. Schweigert.
[7] Nur für $x = 0$ ergeben sie denselben Wert.

8.6 Gruppen

Definition 8.9. *Ein Gruppoid $(G, \star)$ ist eine* **Gruppe**, *falls die Verknüpfung assoziativ ist, falls es ein neutrales Element gibt und falls jedes Element $g \in G$ ein Inverses besitzt.*
Die Gruppe heißt **abelsch**, *wenn die Verknüpfung kommutativ ist.*

Unsere Beispiele: $(\mathbb{R}, +)$ ist eine (abelsche) Gruppe, $(\mathbb{R}, \cdot)$ nicht (Null besitzt kein Inverses), wohl aber $(\mathbb{R}^\star, \cdot)$ (ist auch abelsch), $(PotM, \cup)$ ist keine Gruppe, $(PotM, \cap)$ ebenfalls nicht (es gibt keine Inverse), $(\mathbb{Z}_n, +_n)$ ist eine (abelsche) Gruppe, $(\mathbb{Z}_n^\star, \cdot_n)$ nur, wenn n eine Primzahl ist. $(Abb(\mathbb{R}, \mathbb{R}), \circ)$ ist keine Gruppe, da nicht alle Abbildungen ein Inverses besitzen. Aber alle Bijektionen einer Menge X mit der Verkettung $\circ$ als Verknüpfung bilden eine Gruppe, insbesondere bilden alle Permutationen (s. Kap. 7.3.1) S_n der Zahlen 1,2,...,n eine Gruppe. Sie heißt **n-te symmetrische Gruppe** S_n.

Eine Gruppe $(G, \star)$ heißt **endlich**, wenn G endlich viele Elemente besitzt. Ihre Anzahl $|G|$ heißt **Ordnung** der Gruppe. Welche endlichen Gruppen kennen wir schon? $(\mathbb{Z}_n, +_n)$ hat die Ordnung n, $(\mathbb{Z}_p^\star, \cdot_p)$ (für eine Primzahl p) ist eine Gruppe der Ordnung $p-1$, die Permutationsgruppe S_n hat die Ordnung $n!$.
Die kleinste Gruppe G besteht nur aus einem einzigen Element x, das mit sich selbst verknüpft wieder x ergeben muss ($x \star x = x$). Eine Gruppe $G = \{a, b\}$ mit zwei Elementen gibt es auch. Für die zugehörige Verknüpfungstafel gibt es nur eine Möglichkeit, wenn man a als neutrales Element auswählt:

$\star$	a	b
a	a	b
b	b	a

Gilt das Assoziativgesetz? Es sind acht Gleichungen zu untersuchen:

$$\begin{array}{llll} a(aa) = (aa)a & a(ab) = (aa)b & a(ba) = (ab)a & a(bb) = (ab)b \\ b(aa) = (ba)a & b(ab) = (ba)b & b(ba) = (bb)a & b(bb) = (bb)b \end{array}$$

Nach Erledigung dieser Fleißaufgabe wissen wir: $(G, \star)$ ist eine Gruppe.
Man erkennt, dass $(\mathbb{Z}_2, +_2)$ dieselbe Verknüpfungstafel besitzt, wenn man $a := 0, b := 1$ setzt. Auch die Gruppe $(\mathbb{Z}_3^\star, \cdot_3)$ besitzt dieselbe Verknüpfungstafel, wenn $a := 1, b := 2$. Man spricht davon, dass diese Gruppen *isomorph* sind – ein Begriff, auf dessen genaue Definition ich hier verzichte.

Nun betrachten wir in Gruppen $(G, \star)$ **Gleichungen** der Form $a \star x = b$. Genauer:

Satz 8.10. *Zu gegebenen $a, b \in G$ gibt es genau eine* **Lösung** *$x \in G$ von $a \star x = b$. Diese lässt sich als $x = a' \star b$ darstellen, wenn a' das Inverse von a ist.*

Der **Beweis** ist einfach, aber man muss genau aufpassen, wie argumentiert wird: Aus $a \star x = b$ folgt $a' \star (a \star x) = a' \star b$, indem man die Gleichung von links mit dem Inversen a' von a

„multipliziert“. Nun gilt nach dem Assoziativgesetz $a' \star (a \star x) = (a' \star a) \star x = e \star x = x$, wenn e das neutrale Element in G ist. Wir haben also gezeigt, dass $x = a' \star b$, wenn es denn eine Lösung x gibt. Immerhin: Mehr als eine Lösung kann es nicht geben.
Nun müssen wir noch zeigen, dass $x = a' \star b$ wirklich eine Lösung von $a \star x = b$ ist. Setzen wir also ein. Dann muss also gezeigt werden, dass $a \star (a' \star b) = b$. Wieder wenden wir das Azzoziativgesetz an und wir erhalten: $a \star (a' \star b) = (a \star a') \star b = e \star b = b$, da $a \star a' = e$ das neutrale Element ergibt. ∎

In Gruppen $(G, \star)$ können wir auch *Potenzen* definieren: so ist

$$g^n := g \star \cdots \star g \text{ (n-mal)}.$$

Wir schließen diesen kleinen Ausflug in die Gruppentheorie mit einem fundamentalen

Satz 8.11. *Ist die Gruppe $(G, \star)$ mit Einselement e endlich, so gilt*

$$g^{|G|} = e \text{ für alle } g \in G.$$

Beweis-Skizze: Sei $g \in G$ beliebig. Da G endlich, muss es zwei Potenzen g^m und g^n mit $m < n$ geben, die übereinstimmen: $g^m = g^n$. Multiplizieren wir diese Identität mit $(g')^m$, wobei g' das Inverse von g ist, so folgt $e = g^{n-m}$. Es gibt also ein kleinstes $r \in \mathbb{N}$ mit $g^r = e$, und die r Elemente $g^0 = e, g, g^2, ..., g^{r-1}$ sind alle (paarweise) verschieden. Wir sind fertig, wenn r ein Teiler von $|G|$ ist. Das ist nicht ganz so leicht zu zeigen: Man führt eine von g abhängige Äquivalenzrelation $\sim_g$ auf G ein durch

$$g_1 \sim_g g_2 :\Longleftrightarrow \exists j : g_1 = g_2 \star g^j.$$

Jede Äquivalenzklasse hat r Elemente der Form $g_1, g_1 \star g, ..., g_1 \star g^{r-1}$, G ist die disjunkte Vereinigung aller Äquivalenzklassen, s. Kap. 4.4.1. Also ist $|G| = m \cdot r$, wenn es m Äquivalenzklassen gibt. ∎

8.7 Gruppen in der Geometrie

Wir betrachten ein gleichseitiges Dreieck, Abb. 8.1. Drehen wir es um eine Achse, die senkrecht auf dem Dreieck steht und durch den Dreiecksmittelpunkt M geht, so führen Drehungen um 120 Grad und 240 Grad das Dreieck in sich über, aber natürlich auch die „Drehung“ um 0 Grad, die Identität. Diese drei Drehungen sind Abbildungen der Ebene in sich, die man verketten kann. Nennen wir sie δ_0 (Identität), δ_1 (Drehung um 120 Grad) und δ_2 (Drehung um 240 Grad), so erhalten wir eine Gruppe $G = \{\delta_0, \delta_1, \delta_2\}$ mit der Verkettung als Verknüpfung. Diese ist abelsch, ihre Verknüpfungstafel sieht genauso aus, wie die von $(\mathbb{Z}_3, +_3)$. Zu beachten ist nur, dass eine Drehung um 360 Grad als Abbildung nichts anderes als die Identität ist. Insofern ist δ_2 das Inverse von δ_1 und umgekehrt.

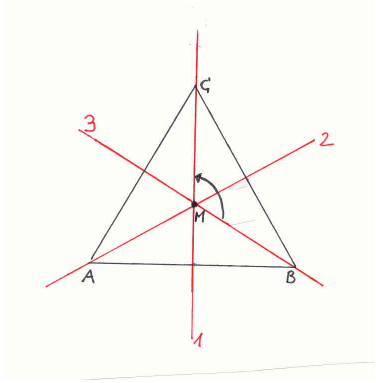


Abbildung 8.1: Zur Diedergruppe D_3

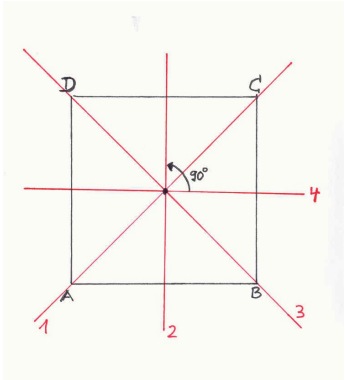


Abbildung 8.2: Zur Diedergruppe D_4

Nun betrachten wir zusätzlich die drei Spiegelungen σ_1, σ_2 und σ_3 an den drei Mittelsenkrechten (in Abb. 8.1 die Geraden mit den Nummern 1, 2 und 3). Wieder betrachten wir die Verkettung als Verknüpfung. Verknüpft man zwei Spiegelungen miteinander, erhält man eine Drehung, verknüpft man eine Drehung mit einer Spiegelung, so erhält man eine Spiegelung. Jede Spiegelung ist zu sich selbst invers (**selbstinvers**). Man erhält eine Gruppe $D_3 = \{\delta_0, \delta_1, \delta_2, \sigma_1, \sigma_2, \sigma_3\}$, eine sogenannte *Diedergruppe*.
Diese Gruppe ist nicht abelsch: so gilt $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$. Überzeugen Sie sich, indem Sie sich überlegen, welches die jeweiligen Bildpunkte der Ecken A, B oder C sind!

Ganz analog kann man ein Quadrat betrachten, s. Abb. 8.2. Hierzu gibt es vier Drehungen um 0, 90, 180 und 270 Grad, die die vierelementige Drehgruppe des Quadrates bilden. Diese ist im wesentlichen dieselbe wie $(\mathbb{Z}_4, +_4)$. Nun gibt es noch vier Spiegelungen, die ein Quadrat auf sich selbst abbilden, zwei spiegeln an den Diagonalen (1 und 3), zwei an den „Mittelsenkrechten“ (2 und 4). Man erhält eine nicht abelsche 8-elementige Diedergruppe D_4.

Bemerkungen:

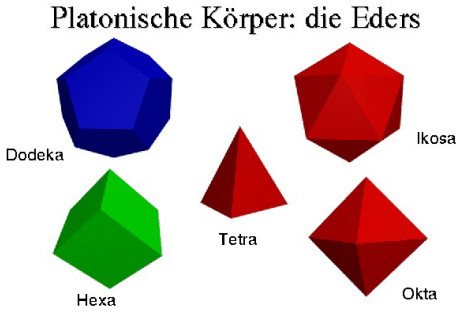


Abbildung 8.3: Die 5 platonischen Körper

- Immer wieder bin ich dem gedanklichen Fehler begegnet, die Ecken des Dreiecks oder des Quadrats seien die Gruppenelemente der Diedergruppen. Die Gruppenelmente sind vielmehr Abbildungen in Form von Drehungen und Spiegelungen, die auf die Eckpunkte angewendet werden können.

- Ist F irgend eine geometrische „Figur“ in der Ebene oder im Raum (Dreieck, Viereck, Würfel, Tetraeder), so kann man alle *Bewegungen*[8] betrachten, die F auf sich abbilden. Diese bilden die *Symmetriegruppe* der Figur F. Die Symmetriegruppe des gleichseitigen Dreiecks und die des Quadrates haben wir kennengelernt. Sie hat 6 bzw. 8 Elemente. Die Gruppe eines Rechtecks[9] hat 4 Elemente (sie ist abelsch!), die des Tetraeders hat 24 Elemente[10], aber die des Würfels hat schon 48 (!) Elemente, davon alleine 24 Drehungen, siehe Geometrische Gruppentheorie (Rosebrock).

Solche Fragen gehören in den Bereich von *Symmetrien*. Zur mathematischen Allgemeinbildung zählt dabei die Kenntnis der 5 platonischen Körper, s. Abb. 8.3.
Das lateinische Wort „eder“ bedeutet „Seite (Fläche)“. Ein *Oktaeder* ist ein *8-Flächner*, ein *Ikosaeder* ein *20-Flächner*.
Platonische Körper sind vollkommen regelmäßige Körper. Ihre Oberflächen bestehen aus gleich großen, gleichseitigen und gleichwinkligen Vielecken. In jeder Ecke eines platonischen Körpers stoßen genau gleich viele Flächen aneinander. Sie sind Spezialfälle *konvexer Polyeder*, für die die *Euler'sche Poyederformel*

$$E + F - K = 2$$

gilt, wobei E, F und K die Anzahl der Ecken, der Seitenflächen bzw. der Kanten ist. Auch wenn es nichts mit *Gruppen* zu tun hat, möchte ich erwähnen, dass man den Euler'schen Polyedersatz relativ einfach mit vollständiger Induktion beweisen kann, wenn man sich das Polyeder durch

[8] Spiegelungen, Drehungen und Verkettungen von diesen. Näheres im Kapitel über Lineare Algebra.
[9] vorausgesetzt, es handelt sich nicht um ein Quadrat.
[10] Sie ist i.W. gleich der Permutationsgruppe S_4.

Entfernen einer Seitenfläche nach Dehnungen und Streckungen so auf einen Tisch „geplättet“ vorstellt, dass sich keine Kanten überschneiden. Siehe Beweis der Eulerschen Polyederformel und
RAN - Fußball einmal anders.

Kapitel 9

Die Körper der reellen und komplexen Zahlen

9.1 Einführung

In Kap. 2 hatten Sie einen ersten Zugang zu Zahlen kennengelernt. Dieser Zugang soll hier vertieft werden. Wir lernen den Begriff eines *Körpers* kennen – das ist eine Menge, in der sowohl „addiert“ als auch „multipliziert“ werden kann — mit verbindenden *Distributivgesetzen*. In diesem Sinne sind die rationalen Zahlen ($\mathbb{Q}$) und die reellen Zahlen ($\mathbb{R}$) Körper, sogar *angeordnete Körper*, in dem eine $<$-Beziehung (eine *Ordnungsrelation*, s. Def. 4.5) definiert ist. Die zugehörigen Axiome legen die Grundlage für das auch in der Schule wichtige *Rechnen mit Ungleichungen*.
Die reellen Zahlen unterscheiden sich von den rationalen Zahlen dadurch, dass für sie ein *Vollständigkeitsaxiom* (Kap. 9.4) gilt: die reellen Zahlen bilden ein „lückenloses“ Kontinuum. Durch „Ausfüllen“ der bei rationalen Zahlen noch vorhandenen Lücken durch irrationale Zahlen werden die reellen Zahlen so „mächtig“, dass sie — im Gegensatz zu den rationalen Zahlen — nicht mehr abzählbar sind (Kap. 9.5): die Menge $\mathbb{R}$ ist *überabzählbar*. Die auf G. Cantor zurückgehenden Beweise sowohl für die Abzählbarkeit von $\mathbb{Q}$ (Satz 9.11) wie auch für die Überabzählbarkeit von $\mathbb{R}$ (Satz 9.12) sind ausgesprochen elegant und werden hier wiedergegeben.
Sie lernen auch weitere Körper kennen wie den Erweiterungskörper $K_{\sqrt{2}} := \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ — den kleinsten Körper der sowohl alle rationalen Zahlen als auch die irrationale Zahl $\sqrt{2}$ enthält.
Zum Schluss (Kap. 9.6) werden die *komplexen Zahlen* $\mathbb{C}$ in Fortführung von Kap. 2 eingeführt. Jede komplexe Zahl z hat einen reellen Real- und einen reellen Imaginärteil. Nur, wenn letzterer Null ist, handelt es sich um eine reelle Zahl. In diesem Sinne sind reelle Zahlen auch spezielle komplexe Zahlen. Man kann in $\mathbb{C}$ eine Addition und Multiplikation so einführen, dass $\mathbb{C}$ ebenfalls zum Körper wird. Die Multiplikation wird geometrisch mit Hilfe von Polarkoordinaten interpretiert.

Die Nützlichkeit von komplexen Zahlen in den Anwendungen kann nur erahnt werden: so haben quadratische Gleichungen $x^2 + px + q = 0$ stets zwei Nullstellen (eventuell auch nicht-reelle), für die die *Vieta'schen Wurzelsätze* gelten.
Als letztes geben wir einige Hinweise zur „schönsten Formel" der Mathematik, s. Abb. 9.9.

In der Vorlesung kann nicht alles behandelt werden. Die nicht behandelten Teile werden in kleinen Fonts wiedergegeben. Sie sind für die anstehenden Prüfungen irrelevant, sollen die interessierte LeserIn aber Orientierungshilfe geben.

9.2 Körper

Im Folgenden bezeichnen wir mit $\mathbb{K}$ entweder die Menge $\mathbb{R}$ der reellen Zahlen oder die Menge $\mathbb{Q}$ der rationalen Zahlen, da diese beiden Mengen viele gemeinsame Eigenschaften haben — auf den wesentlichen Unterschied kommen wir noch zu sprechen.
Zunächst stellen wir fest, dass es sich bei $(\mathbb{K}, +)$ um eine abelsche Gruppe handelt, siehe Def. 8.9, mit der Null als neutralem Element. Aber auch die Multiplikation ist eine gängige Verknüpfung. Mit $\mathbb{K}^\star := \mathbb{K} \setminus \{0\}$ ist $(\mathbb{K}^\star, \cdot)$ ebenfalls eine abelsche Gruppe — mit der Eins als neutralem Element.
Das nun folgende *Distributivgesetz* ist eine „Rechenregel", die sich auf das Zusammenspiel beider Verknüpfungen bezieht und die *Körper*-Eigenschaft von $\mathbb{K}$ definiert.

Definition 9.1. *Es sei K eine Menge mit den beiden Verknüpfungen $+$ und $\cdot$. Es sei $(K, +)$ eine abelsche Gruppe mit neutralem Element Null (0). Sei $K^\star := K \setminus \{0\}$ und $(K^\star, \cdot)$ ebenfalls eine abelsche Gruppe mit neutralem Element Eins (1). Wenn dann noch das* **Distributivgesetz**

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

für alle $a, b, c \in K$ gilt, so heißt $(K, +, \cdot)$ ein **Körper**[1].

In diesem Sinne sind sowohl $\mathbb{Q}$ als auch $\mathbb{R}$ *Körper*. In Kap. 9.6 werden wir noch einen weiteren Körper kennenlernen, nämlich den der *komplexen Zahlen* $\mathbb{C}$.

Es gibt unendlich viele Körper „zwischen" $\mathbb{Q}$ und $\mathbb{R}$, einen werden werden wir vielleicht in den Übungen kennenlernen:

$$K_{\sqrt{2}} := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\},$$

den kleinsten Körper, der $\mathbb{Q}$ und $\sqrt{2}$ enthält. Solche „Erweiterungskörper" spielen bei „Konstruktionen mit Zirkel und Lineal" und speziell auch bei der „Quadratur des Kreises" (Kap. 9.4.2) eine Rolle.

Es gibt auch endliche Körper, der kleinste ist $K := \{0, 1\}$, er besteht aus nur zwei Elementen[2].

[1] Genauer: ein *kommutativer* Körper. Es gibt auch *nichtkommutative* Körper, bei denen die Multiplikation nicht kommutativ ist. Das bekannteste Beispiel hierfür ist der Körper der Quaternionen.

[2] Wie müssen Addition und Multiplikation definiert werden?

Auch $(\mathbb{Z}_p, +_p, \cdot_p)$ ist ein Körper, wenn p eine Primzahl. Diesen haben Sie schon in Kap. 8, siehe Korollar 8.5, kennengelernt.

Erinnern Sie sich, wo Ihnen schon Distributivgesetze begegnet sind? In Kap. 3.3.4 (Rechenregeln für Mengen), Satz 3.5

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

$\cup$ entspricht der Addition, $\cap$ der Multiplikation. Da $(PotM, \cup)$ keine abelsche Gruppe ist (es gibt keine Inversen, s. Kap. I.8.6), haben wir es hier nicht mit einem Körper zu tun.

Wir notieren einfache Aussagen, die für $\mathbb{K} = \mathbb{R}$ und $K = \mathbb{Q}$ vertraut sind, hier aber für beliebige Körper K gezeigt werden sollen – als Übung für formales (abstraktes) Schließen. Beachten Sie erneut die beiden Bedeutungen des Minus-Zeichens **-**: zum einen bezeichnet **-** das Subtrahieren als Verknüpfung, zum anderen ist $-a$ das *additive Inverse* von a. Ersteres hat natürlich mit dem zweiten zu tun: es ist $a - b = a + (-b)$ — auf diese Weise kann die Subtraktion auf die Addition zurückgeführt werden. Ganz entsprechend ist $a/b = a \cdot b^{-1}$, wobei b^{-1} das *multiplikative Inverse* von b ist — die Division wird auf diese Weise auf die Multiplikation zurückgeführt[3].

Satz 9.2. *Sei $(K, +, \cdot)$ ein Körper. Seien $a, b \in K$, $c \in K^\star$ beliebig. Dann gelten*

1) $0 \cdot a = 0$
2) $-(-a) = a, \qquad (c^{-1})^{-1} = c$
3) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
4) $(-a) \cdot (-b) = a \cdot b$

Beweis:
1): Es ist $0 \cdot a = (0 + 0) \cdot a$, da $0 + 0 = 0$. Nun kann man das Distributivgesetz und das Kommunikativgesetz anwenden: $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. In abelschen Gruppen $(K, +)$ gilt $x + x = x$ aber nur, wenn $x = 0$.
2): Dies folgt — wie in Kap. I.8.4.1 ausgeführt — aus den Gruppeneigenschaften von $(K, +)$ und $(K^\star, \cdot)$.
3): Wir zeigen, dass $a \cdot (-b)$ das additive Inverse von $a \cdot b$ ist, d.h. dass $a \cdot (-b) + a \cdot b = 0$. Auch hier kann man das Distributivgesetz und Teil 1) unserer Aussage anwenden: $a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot 0 = 0$. Damit ist $a \cdot (-b) = -a \cdot b$ gezeigt. Der mittlere Teil der Aussage 3) folgt ganz analog, wenn man die Kommutativität von $(K, \cdot)$ ausnutzt: $(-a) \cdot b = b \cdot (-a)$. Nun haben wir eben gerade gezeigt, dass $b \cdot (-a) = -(b \cdot a)$ – man muss nur die Rollen von a und b vertauschen. Wegen $b \cdot a = a \cdot b$ folgt der Rest.
4) s. Übungen. ∎

[3] Überlegen Sie einmal, wie man die Rechenregel „Zwei Brüche werden dividiert, indem ich den ersten Bruch mit dem Kehrwert des zweiten multipliziere“, begründet.

9.3 Angeordnete Körper

Wir haben uns die reellen Zahlen auf einem *Zahlenstrahl* angeordnet vorgestellt. Diese Vorstellung ist mit einer *Anordnung* von Zahlen verbunden, genauer: es ist eine Relation $<$ (in Worten „kleiner“) mit den folgenden Eigenschaften gegeben:

$(A1)$ für alle $(a,b) \in K \times K$ gilt genau eine der Möglichkeiten $a < b$ oder $a = b$ oder $b < a$

$(A2)$ $a < b$ und $b < c \Longrightarrow a < c$ für alle $a, b, c \in K$

$(A3)$ $a < b \Longrightarrow a + c < b + c$ für alle $a, b, c \in K$

$(A4)$ $a < b$ und $0 < c \Longrightarrow a \cdot c < b \cdot c$ für alle $a, b, c \in K$

Bemerkung: Für einen beliebigen Körper K stellen (A1)-(A4) sogenannte **Anordnungsaxiome** dar, die den Körper zu einem *angeordneten Körper* machen, wenn auf ihm eine Relation $<$ mit den Eigenschaften (A1=-(A4) gegeben ist. Dass in diesem Sinne sowohl $\mathbb{Q}$ als auch $\mathbb{R}$ angeordnete Körper sind, wird nicht bewiesen, sondern die Axiome (A1)-(A4) werden unterstellt.

Wie bei reellen Zahlen üblich, vereinbaren wir die Verwendung der $>$-Relation durch

$$a > b :\Longleftrightarrow b < a.$$

Für uns sind (A1)-(A4) wohlbekannte *Rechenregeln* für das Rechnen mit *Ungleichungen*. Man beachte bei (A4) die Bedingung, dass $c > 0$ ist (Merkregel: „Ungleichungen kann man mit positiven Zahlen multiplizieren“). Ohne diese Bedingung ist die Schlussfolgerung falsch. (A2) ist nichts anderes als die Transitivität der $<$-Relation, aus (A1) folgt ihre Antisymmetrie. Die $\leq$-Relation ist dann eine Ordnungsrelation. Vgl. Kap. I.4.3.
Nun kann man aus (A1)-(A4) weitere Rechenregeln ableiten:

Satz 9.3. *Sei $(K, +, \cdot, <)$ ein angeordneter Körper.*
Für alle $a, b, c, d \in K$ gilt:

1) $a < b$ *und* $c < d \implies a + c < b + d$
2) $a < b$ *und* $c < 0 \implies ac > bc$
3) $0 < 1$
4) $0 < a < b \implies 0 < b^{-1} < a^{-1}$

Die Aussagen scheinen für die Körper $K \setminus \mathbb{R}$ und $\mathbb{Q}$ klar, jedenfalls sind Sie Ihnen wahrscheinlich vertraut. Besonders wichtig sind die Regeln 2) und 4). Erstere ist die Merkregel: „Eine Ungleichung wird durch Multiplikation beider Seiten mit einer negativen Zahl umgekehrt“. Letztere sollte man sich so merken: „Invertiert man zwei positive Zahlen a und b zu $\frac{1}{a}$ und $\frac{1}{b}$, so wird die kleinere zur größeren und umgekehrt“.
Beweis:
Ich gebe hier einen Beweis, der nur die Rechenregeln für einen angeordneten Körper benutzt. Daher wollen wir ganz genau argumentieren und uns immer klar machen, welche der Eigenschaften (z.B. die

Axiome (A1)-(A4)) von K wir nutzen. Es soll hier das *formale Schließen* auf Grund von vorgegebenen Regeln geübt werden.
1) Aus $a < b$ folgt mit (A3) $a + c < b + c$. Genauso folgt $c + b < d + b$ aus $c < d$. Aus der Transitivität der Ordnungsrelation $<$ folgt dann die Behauptung, sofern $b + c = c + b$ — dies ist jedoch richtig, da $(K, +)$ eine abelsche Gruppe, die Addition also kommutativ ist.
2) Zunächst folgt aus $c < 0$, dass $c' := -c > 0$ (Da $c' \neq 0$ käme sonst nur $c' < 0$ in Frage. Wegen Teil 1) folgt dann $0 = c + c' < 0$). Wenn wir (A4) mit c' an Stelle von c anwenden, folgt $a \cdot (-c) < b \cdot (-c)$. Wegen Teil 3) von Satz 9.2 ist $a \cdot (-c) = -a \cdot c$ und $b \cdot (-c) = -b \cdot c$, also gilt $-a \cdot c < -b \cdot c$. Nun addiere auf beiden Seiten $a \cdot c + b \cdot c$ und nutze die Gruppeneigenschaft von $(K, +)$ aus, wie z.B. $-a \cdot c + a \cdot c + b \cdot c = 0 + b \cdot c = b \cdot c$. Dann folgt $b \cdot c < a \cdot c$ oder umgestellt $a \cdot c > b \cdot c$.
3) Es kann wegen (A1) und $1 \neq 0$ nur $1 < 0$ oder $1 > 0$ gelten. Wäre $1 < 0$, so multiplizieren wir diese Ungleichung mit 1. Wegen des eben bewiesenen Teils 2) dreht sich das Vorzeichen um, es folgt $1 \cdot 1 > 1 \cdot 0$. Mit $1 \cdot 1 = 1$ und $1 \cdot 0 = 0$ (letzteres folgt aus Teil 1 von Satz 9.2) folgt sofort ein Widerspruch.
4) Zunächst zeigt man, dass $a^{-1} > 0$ und $b^{-1} > 0$ (Aufgabe!!). Dann multipliziere man die Ungleichung mit $a^{-1} \cdot b^{-1}$. ∎

Man kann noch mehr Regeln ableiten, z.B. $-1 < 0$ und somit $a > 0 \Longrightarrow -a < 0$.

Wie schon zuvor sei der Körper $\mathbb{K}$ stets $\mathbb{R}$ oder $\mathbb{Q}$, auch wenn die folgende Definitionen und Aussagen in einem beliebigen angeordneten Körper sinnvoll sind und gelten. Bemerken möchte ich schon jetzt, dass der später eingeführte Körper $\mathbb{C}$ der komplexen Zahlen *kein* angeordneter Körper ist.

Zunächst gebe ich Rechenregeln für Ungleichungen mit der Relation $\leq$ ohne Beweis an. Dabei schreibt man $a \leq b$, wenn entweder $a < b$ oder $a = b$ gilt.
Ab jetzt schreibe ich wie üblich kurz ab an Stelle von $a \cdot b$.

Satz 9.4. *Seien $a, b, c, d \in K$. Dann gelten die Regeln*

1)	$a \leq b$ *und* $b \leq c$	$\Longrightarrow$	$a \leq c$	$(vgl.(A2))$
2)	$a \leq b$ *und* $c \leq d$	$\Longrightarrow$	$a + c \leq b + d$	$(vgl. Satz 1.3, 1.)$
3)	$a \leq b$ *und* $c > 0$	$\Longrightarrow$	$ac \leq bc$	$(vgl.(A4))$
4)	$a \leq b$ *und* $c < 0$	$\Longrightarrow$	$ac \geq bc$	$(bgl. Satz 1.3, 2.)$

9.3.1 Betragsfunktion und Dreiecksungleichung

Eine ganz wichtige Funktion von $\mathbb{K}$ nach $\mathbb{K}$ ist die **Betragsfunktion**, die folgendermaßen definiert ist:

Definition 9.5.

$$|a| := \begin{cases} a & falls \quad a \geq 0 \\ -a & falls \quad a < 0 \end{cases} \qquad \textit{ist der (}\textbf{Absolut-)Betrag}\textit{ von } a.$$

Beispiel: $|-5| = -(-5) = 5$

Im nachfolgenden Satz ist die **Dreiecksungleichung**

$$|a+b| \;\leq\; |a|+|b| \tag{9.1}$$

ein zentrales Hilfsmittel der Analysis. Diesen Namen kann man in diesem Zusammenhang nicht so leicht verstehen. Ich versuche es aber:
Eine *„echte" Dreiecksungleichung* der Form, dass *eine Seite in einem Dreieck niemals länger ist als die Summe der Längen der anderen beiden Seiten* ist offensichtlicher. Nennen wir die Ecken eines Dreiecks X, Y und Z und bezeichnen wir mit $d(X,Y)$ den Abstand von X zu Y (d=*Distanz*), so liest sich unsere „echte" Dreiecksungleichung so:

$$d(X,Y) \leq d(X,Z) + d(Z,Y). \tag{9.2}$$

Auf der Zahlengeraden ist $|x-y|$ gerade der Abstand von x zu y. Mit $d(x,y) := |x-y|$ liest sich (9.2) wie eine „entartete[4]" Dreiecksungleichung:

$$|x-y| \leq |x-z| + |z-y|.$$

Diese geht nun in (9.1) über, wenn man $a := x-z, b := z-y$ setzt (wegen $a+b = x-z+z-y = x-y$)!

Satz 9.6. *Seien $a, b \in K$. Dann gelten*

1) $|a| \geq 0$. *Es ist* $|a| = 0 \iff a = 0$
2) $|a\,b| \;=\; |a|\,|b|$
3) $|\frac{a}{b}| \;=\; \frac{|a|}{|b|}$ *falls* $b \neq 0$
4) $|a+b| \;\leq\; |a|+|b|$ *(sogenannte Dreiecksungleichung)*
5) $|a-b| \;\geq\; |a|-|b|$

Wir beschränken uns beim **Beweis** auf die *Dreiecksungleichung*:
Für $x \in \mathbb{K}$ gilt stets $x \leq |x|$ und $-x \leq |x|$. Damit folgt $a+b \leq |a|+|b|$ und $-(a+b) = (-a)+(-b) \leq |a|+|b|$.

$a+b \geq 0 \Longrightarrow |a+b| = a+b \leq |a|+|b|$
$a+b < 0 \Longrightarrow |a+b| = -(a+b) \leq |a|+|b|$ ∎

Mit Hilfe vollständiger Induktion kann man die Dreiecksungleichung auf n Summanden ausdehnen. Mit den bisherigen Voraussetzungen gilt:

Satz 9.7. $\left|\sum_{j=1}^{n} a_j\right| \leq \sum_{j=1}^{n} |a_j|$ *für $a_j \in K$*

[4] Alle Punkte liegen auf einer Geraden!

9.4 Vollständigkeit der reellen Zahlen

In diesem Abschnitt soll der Versuch gemacht werden, Ihnen das Wesen der reellen Zahlen näher zu bringen. Ich unterstelle, dass Sie die natürlichen, ganzen und rationalen Zahlen „begriffen“ haben. Auch die Vorstellungen von rationalen Zahlen auf einem Zahlenstrahl dürfte gelingen: Man markiere den Nullpunkt und den Punkt 1 rechts von 0. Dann kann man jede positive rationale Zahl $\frac{p}{q}$ konstruieren, indem man die Strecke $\overline{01}$ in q gleichlange Strecken unterteilt und die Strecke der Länge $\frac{1}{q}$ insgesamt p-mal nach rechts abträgt. Die negativen rationalen Zahlen werden analog nach links abgetragen.
Dass $\mathbb{Q}$ ein angeordneter Körper ist, kann leicht eingesehen werden. Dabei ist es wichtig, dass zwischen zwei rationalen Zahlen immer noch unendlich viele rationale Zahlen liegen[5]. Dennoch gibt es noch „unendlich kleine Lücken“ zwischen rationalen Zahlen: Wir wissen, dass die Diagonale eines Einheitsquadrates die Länge $\sqrt{2}$ hat — keine rationale Zahl, wie wir gleich zu Beginn in Kap. 2 gesehen haben. Trägt man diese Diagonale auf dem Zahlenstrahl von 0 ausgehend nach rechts ab, so trifft man keine rationale Zahl — es gibt also Lücken!
Wieviele solche Lücken gibt es nun? Intuitiv wollen wir die reellen Zahlen so beschreiben, dass sie die Zahlengerade lückenlos lassen.
Wir folgen hier einem Zugang von Dedekind (1831-1916), der einen **Dedekindschen Schnitt** eines angeordneten Körpers K einführte: Dies sind zwei nichtleere, disjunkte Mengen A und B mit $A \cup B = K$ (D.h., dass jede Zahl aus K entweder in A oder in B liegt.) und mit $a < b$, wenn $a \in A$ und $b \in B$. Einen Dedekindschen Schnitt bezeichnen wir mit dem Symbol $(A|B)$. Man nennt eine Zahl t **Trennzahl** von $(A|B)$, wenn $a \leq t \leq b$ für alle $a \in A$ und $b \in B$.
Nun betrachten wir den folgenden Dedekindschen Schnitt von $K = \mathbb{Q}$, der $\sqrt{2}$ als Trennzahl hat: B sei die Menge aller positiven rationalen Zahlen, deren Quadrat > 2, A die anderen rationalen Zahlen. Sie ahnen schon: die Aussage, dass $\sqrt{2}$ irrational ist, lautet jetzt: *Es gibt keine rationale Trennzahl.* Dies wollen wir jetzt beweisen — wie schon häufig durch einen indirekten Beweis[6]. Wir nehmen also an, es gäbe eine rationale Trennzahl $t = \frac{p}{q}$. Dann muss $t \in A$ oder $t \in B$ gelten. Ich nehme $t \in A$ an. Klar, dass t dann die größte Zahl in A ist, da $a \leq t$ für alle $a \in A$ für eine Trennzahl gilt. Es gilt also $\frac{p^2}{q^2} < 2$ und aus $\frac{r}{s} \in A$ bzw. aus $\frac{r^2}{s^2} < 2$ folgt dann stets $\frac{r}{s} \leq \frac{p}{q}$. Die Idee für den angestrebten Widersprcuh ist einfach: Wir addieren eine *hinreichend kleine* positive rationale Zahl $\frac{1}{n}$ (mit hinreichend großem $n \in \mathbb{N}$) zu $\frac{p}{q}$ hinzu, erhalten $\frac{r}{s} := \frac{p}{q} + \frac{1}{n}$ und wählen dabei n so groß („hinreichend groß“) bzw. $\frac{1}{n}$ so klein („hinreichend klein“), dass immer noch $(\frac{r}{s})^2 < 2$. Schließlich muss es doch noch ausreichend „Luft“ zwischen $t^2 = (\frac{p}{q})^2$ und 2 geben! Wenn dies gelingt, erhalten wir einen Widerspruch, weil es dann Zahlen in A gibt, die größer als die Trennzahl t sind!
Dass dies für ein hinreichend großes $n \in \mathbb{N}$ tatsächlich gelingt, zeigen wir jetzt: Ziel ist die Ungleichung $(\frac{p}{q}+\frac{1}{n})^2 < 2$, ausmultipliziert $(\frac{p}{q})^2+\frac{1}{n}(2\frac{p}{q}+\frac{1}{n}) < 2$ bzw. $\frac{1}{n}(2\frac{p}{q}+\frac{1}{n}) < c := 2-(\frac{p}{q})^2$. Nach Voraussetzung ist $c > 0$. Die letzte Ungleichung ist erst recht richtig, wenn das zweite $\frac{1}{n}$ durch 1 ersetzt werden kann, wenn also $\frac{1}{n}(2\frac{p}{q} + 1) < c$ oder (gleichwertig) wenn $\frac{1}{n} < c' := \frac{c}{2\frac{p}{q}+1}$. Nun ist c' ebenfalls eine positive rationale Zahl. Dies kann in der Tat durch ein $\frac{1}{n}$ unterboten werden, man muss für n nur den Nenner von c' nehmen!

[5] In einem angeordneten Körper folgt aus $a < b$, dass $a < \frac{a+b}{2} < b$.

[6] Im Beweis müssen wir von der Definition von t als Trennzahl der Mengen A und B ausgehen, nicht von der Definition von $\sqrt{2}$ als Lösung von $t^2 = 2$.

Die Annahme, dass die Trennzahl t zu B gehört, wird genauso zum Widerspruch geführt. Also ist die Trennzahl (wenn es sie denn gibt!) unseres speziellen Dedekindschen Schnittes keine rationale Zahl. ∎

Nun formulieren wir ein Axiom, das uns die Menge der reellen Zahlen „erschließt“:

Definition 9.8. *(Vollständigkeitsaxiom)*
Ein angeordneter Körper $(K, +, \cdot)$ heißt vollständig : $\Longleftrightarrow$ *Jeder Dedekindsche Schnitt von K hat genau eine Trennzahl $t \in K$.*

Der obige längliche Beweis führt jetzt offensichtlich zu

Satz 9.9. *Der Körper $\mathbb{Q}$ der rationalen Zahlen ist nicht vollständig.*

Jetzt haben wir unser Ziel erreicht, die reellen Zahlen sind eindeutig durch Axiome festgelegt: *Die reellen Zahlen bilden den (einzigen) vollständigen, angeordneten Körper.* Diesen kann man aus $\mathbb{Q}$ durch Vervollständigung gewinnen, indem man jede irrationale Zahl durch einen Dedekindschen Schnitt von $\mathbb{Q}$ gewinnt. Genauer:
In beliebiger Nähe einer reellen Zahl x finden sich stets rationale Zahlen $< x$ und $> x$.

9.4.1 Algebraische und transzendente Zahlen

Diese Einführung der reellen Zahlen mit Hilfe des Vollständigkeitsaxioms erscheint Ihnen sicher etwas unheimlich. Wissen Sie jetzt wirklich, was reelle Zahlen sind? Sind Sie überrascht, wenn sich herausstellt, dass es viel, viel mehr[7] irrationale als (abzählbar viele) rationale Zahlen gibt?
Wenn Sie glauben zu wissen, was rationale Zahlen sind, müssen Sie also mehr über irrationale Zahlen wissen. $x := \sqrt{2}$ haben wir schon als irrational erkannt — als Lösung der quadratischen Gleichung $x^2 - 2 = 0$. Entsprechend sind alle Wurzeln $\sqrt{n}$ irrational, wenn $n \in \mathbb{N}$ keine Quadratzahl ist. Es handelt sich um Lösungen der Gleichung $x^2 - n = 0$. Dies ist ein Beispiel einer *algebraischen Gleichung.* Weitere Beispiele sind $x^3 - 2 = 0$ oder $x^{17} - 2x^3 + 5 = 0$. *Algebraische Zahlen* sind gerade die Lösungen algebraischer Gleichungen[8]. Viele irrationale Zahlen sind algebraisch[9], aber noch viel, viel mehr[10] sind nicht algebraisch — auch *transzendent* genannt. Hierzu zählen die Kreiszahl π und die Eulersche Zahl e.
Die algebraischen Zahlen bilden ebenfalls einen Körper. Aber es gibt noch sehr viele andere Körper „zwischen“ $\mathbb{Q}$ und $\mathbb{R}$. Z.B. der Körper $K_{\sqrt{2}} := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Aufgabe: Warum sind rationale Zahlen algebraisch? Welcher (ganz einfachen) algebraischen Gleichung genügen sie?

---

[7] überabzählbar viele!

[8] Allgemein ist eine solche Gleichung von der Form $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$ mit ganzzahligen Koeffizienten $a_j \in \mathbb{Z}$.

[9] aber auch nur abzählbar viele!

[10] überabzählbar viele!

9.4.2 Quadratur des Kreises

Sogar Politiker sprechen zuweilen von der „Quadratur des Kreises“, die ja bekanntermaßen nicht gelingen kann, wenn die Politik mit einem unlösbar erscheinenden Problem konfrontiert wird. Aber kaum jemand weiß, was man unter der Quadratur des Kreises wirklich versteht: Wenn man mit Hilfe von Zirkel und Lineal zu einem Kreis ein flächengleiches Quadrat konstruieren kann, so ist die Quadratur des Kreises gelungen. Dass dies nicht gelingen kann, liegt an der Transzendenz der Kreiszahl π. Irrationalität alleine reicht nicht aus. Die Fläche eines Kreises mit Radius $r = 1$ ist ja $\pi = r^2\pi$. Ein Quadrat gleich großer Fläche hat die Kantenlänge $x := \sqrt{\pi}$. Die Quadratur des Kreises heißt also, zu einer Strecke der Länge 1 mit Hilfe von Zirkel und Lineal eine Strecke der Länge $x = \sqrt{\pi}$ zu konstruieren.
Nun kann man zeigen (Übungen!), dass $\sqrt{a}$ für $a > 0$ genau dann konstruierbar ist, wenn es die Zahl a ist. Daher gelingt die Quadratur des Kreises genau dann, wenn π konstruierbar ist. Das ist jedoch nicht der Fall, weil π transzendent ist und weil alle konstruierbaren Zahlen algebraisch sind (aber nicht umgekehrt!).
Mehr hierzu in den Übungen.

Der mathematische Beweis, dass die Quadratur des Kreises unmöglich ist, hat viele „Freigeister“ nicht daran gehindert, Jahre an Arbeit in dieses Problem zu stecken. Die Nutzlosigkeit dieser Arbeit hat den Term „Quadratur des Kreises“ als Metapher bekannt gemacht, wo er einfach als ein Synonym für ein Unterfangen, das von vorherein zum Scheitern verurteilt ist, benutzt wird.

Eine weitere geometrische Unmöglichkeit ist die Drittelung eines Winkels mit Zirkel und Lineal. Auch, dass es keine geschlossene Formel zur Berechnung der Nullstellen von Polynomen fünften oder höheren Grades gibt, die nur mit den vier Grundrechenarten und Wurzelziehen auskommt, passt in diese Thematik, die unter dem Namen Galoistheorie[11] zusammengefasst wird — ein Teilgebiet der Algebra.
Quadratur des Kreises, Drittelung eines Winkels sowie die Konstruktion eines Würfels mit doppeltem Volumen sind klassische Probleme des antiken Griechenlands. Sie konnten erst im 19. Jhd (u.a. mit Hilfe von Galois) auf algebraische Weise gelöst werden. Dabei haben (Erweiterungs-) Körper eine besondere Bedeutung.
Eine präzise Erörterung dieser Fragen würde den Rahmen dieser Vorlesung sprengen.

9.5 (Über-) Abzählbarkeit

In diesem Abschnitt geht es um die *Mächtigkeit* von $\mathbb{Q}$ und von $\mathbb{R}$, die wir schon mit den Termen *abzählbar* und *überabzählbar* ansprachen.
Sie erinnern sich (vielleicht): Zwei Mengen A und B heißen gleichmächtig, wenn es eine Bijektion $f : A \to B$ gibt, s. Def. 5.12. Wir haben die Gleichmächtigkeit durch $|A| = |B|$ notiert. Bei endlichen Mengen ist keiner verwirrt: Zwei endliche Mengen sind genau dann gleichmächtig, wenn sie gleich viele Elemente besitzt — in diesem Fall ist ja $|A|$ auch gerade die Anzahl der Elemente von A.
Wir hatten aber schon gesehen, dass die „unendlichen“ Mengen $\mathbb{N}$ und $\mathbb{Z}$ gleichmächtig sind, obwohl es fast doppelt so viele ganze wie natürliche Zahlen zu geben scheint, s. Kap. 5.2.7. Im

[11] Evariste Galois, 1811-1832, wurde nur 20 Jahre alt. Er starb in einem Duell.

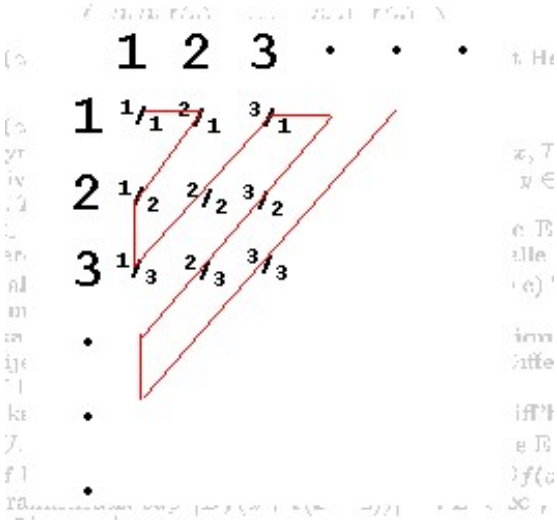


Abbildung 9.1: Übungsaufgabe 26

Sinne dieser „Gleichmächtigkeit“ gibt es auch genauso viele natürliche Zahlen wie Quadratzahlen[12].
Klar, dass es unendlich viele natürliche Zahlen gibt. Klar ist auch, dass es mehr rationale als natürliche und mehr reelle als rationale Zahlen gibt.
Ein keineswegs sofort einsichtiges Resultat ist, dass $\mathbb{N}$ und $\mathbb{Q}$ gleichmächtig sind, kurz, dass $|\mathbb{Q}| = |\mathbb{N}|$ gilt. Wir sagen, dass $\mathbb{Q}$ gemäß der nachfolgenden Definition *abzählbar* ist:

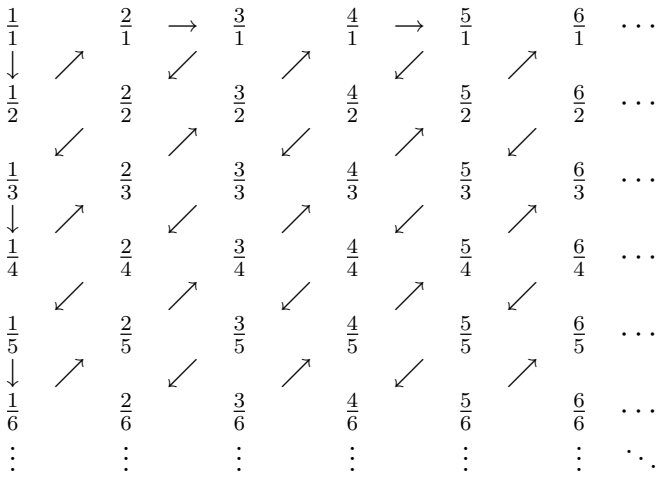
Definition 9.10. *Eine Menge M heißt* **abzählbar** *genau dann, wenn M endlich ist oder gleichmächtig zu $\mathbb{N}$ ist. Letzteres bedeutet die Existenz einer Bijektion $f : \mathbb{N} \to M$. Wir sprechen dann auch von* **abzählbar unendlichen** *Mengen M.*
Eine Menge M heißt **überabzählbar**, *falls M nicht abzählbar ist.*

Ist M abzählbar unendlich, so kann man die Elemente von M mit Hilfe einer Bijektion $f : \mathbb{N} \to M$ *durchnummerieren*: Zu jedem $m \in M$ gibt es genau eine *Nummer* j mit $m = f(j)$ — man kann M *abzählen*.

Satz 9.11. *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.*

Beweis: Wir geben eine Bijektion $f : \mathbb{N} \to \mathbb{Q}^+$ an, wobei $\mathbb{Q}^+$ die Menge der *positiven* rationalen Zahlen ist.
Wir machen dies mit dem sog. *Cantorschen Diagonalverfahren* und ordnen die Elemente aus $\mathbb{Q}^+$ in dem folgenden Schema[13] an. Wir folgen bei der Nummerierung der Elemente von $\mathbb{Q}^+$ (dies entspricht einer Bijektion $\mathbb{N} \to \mathbb{Q}^+$) den Pfeilen des Schemas. Dabei überspringen wir alle Zahlen, die in der Nummerierung schon einmal (in anderer Darstellung) aufgetreten sind.

[12] Welche ist die zugehörige Bijektion?
[13] In Aufgabe 26 wurde in einem ganz analogen Sinne auf Abb. 9.1 Bezug genommen.



Auf diese Art erhält man eine bijektive Abbildung $f : \mathbb{N} \to \mathbb{Q}^+$, nämlich
$f(1) = 1$, $f(2) = \frac{1}{2}$, $f(3) = 2$, $f(4) = 3$, $f(5) = \frac{1}{3}$, $f(6) = \frac{1}{4}, \ldots$.
Hieraus kann man dann nach folgendem Schema eine Abzählung von ganz $\mathbb{Q}$, also den positiven und negativen ganzen Zahlen sowie die Zahl Null, gewinnen: 0, $f(1)$, $-f(1)$, $f(2)$, $-f(2)$, $f(3)$, $-f(3), \ldots$. ∎

Analog zum letzten Beweis können wir auch die Abzählbarkeit von Mengen wie $\mathbb{Q} \times \mathbb{Q}$ nachweisen. Die endliche Vereinigung von abzählbaren Mengen ist ebenfalls abzählbar. Es gibt aber auch Mengen, die überabzählbar, also viel „mächtiger“ als die Menge $\mathbb{N}$ der natürlichen Zahlen sind:

Satz 9.12. *Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.*

Beweis:
Wir zeigen, dass bereits das Intervall $J := [0, 1) := \{x \in \mathbb{R} : 0 \leq x < 1\}$ überabzählbar ist. Dabei nutzen wir aus, dass man jede reelle Zahl $x \in J$ als *unendlichen Dezimalbruch* (s. Kap. **??** darstellen kann:

$$x = 0.z_1 z_2 z_3 z_4 ...., \; 0 \leq z_j \leq 9.$$

Die Ziffer z_j ist die j-te Stelle des Dezimalbruchs, die j-te Stelle „nach dem Komma“. Zwei unendliche Dezimalbrüche können dieselbe Zahl x darstellen, z.B. $x = 0.2$ und $x = 0.1999999.... = 0.1\overline{9}$. Wir legen uns darauf fest, nur solche Dezimalbrüche zu wählen, für die ab einer Ziffer nicht nur Neunen auftreten. Dadurch ist die Dezimalbruchdarstellung eindeutig. Bei endlichen Dezimalbrüchen denken wir uns unendlich viele Nullen als Ziffern drangehängt. Diese Veranschaulichung von reellen Zahlen als unendliche Dezimalbrüche zeigt sehr schön, dass die Eigenschaft „rational“ eher „reiner Zufall“ ist: Stellen Sie sich vor, Sie erzeugen eine reelle Zahl durch Auslosung der unendlich vielen Ziffern z_j. Was für ein Zufall, wenn irgendwann nur noch Nullen verlost werden oder wenn sich Ziffernfolgen immer wiederholen!

Jetzt führen wir einen *indirekten Beweis* (wie auch in den ersten beiden Beweisen von Satz 2.1 und Satz 2.2) d.h. wir nehmen an, dass der Satz falsch ist und konstruieren einen Widerspruch.

Sei also $J = [0,1)$ abzählbar. D.h., dass man jedem $x \in J$ genau eine „Nummer“ $j = f(x)$ zuordnen kann, wobei $f : J \to \mathbb{N}$ eine Bijektion ist, — die es ja geben muss, wenn J abzählbar ist. Wir sprechen daher von der ersten, zweiten, dritten,..., j-ten Zahl r_j in J. Alle diese Zahlen r_j können wir als unendliche Dezimalbrüche darstellen:

$$\begin{array}{lcll} r_1 & = & 0.s_{11}s_{12}s_{13}s_{14}s_{15} & \dots \\ r_2 & = & 0.s_{21}s_{22}s_{23}s_{24}s_{25} & \dots \\ r_3 & = & 0.s_{31}s_{32}s_{33}s_{34}s_{35} & \dots \\ r_4 & = & 0.s_{41}s_{42}s_{43}s_{44}s_{45} & \dots \\ \vdots & & & \ddots \end{array}$$

Allgemein:

$$r_j = 0.s_{j1}s_{j2}s_{j3}s_{j4}s_{j5} \quad \dots$$

Dies ist ein gutes Beispiel dafür, dass eine Doppelindizierung ausgesprochen sinnvoll ist: Wir haben eine j-te Zahl r_j und wir haben eine k-te Nachkommastelle $s_{jk} \in \{0,1,2,\dots,9\}$ von r_j. Wir konstruieren jetzt eine Zahl $r \in J$, indem wir nach und nach die „Nachkommastellen“ $z_1, z_2, z_3, \dots$. in

$$r = 0.z_1z_2z_3\dots$$

festlegen. Wir wählen einfach das z_j so, dass „nur“ $z_j \neq s_{jj}, j = 1,2,\dots$. erfüllt ist. Wir sorgen dabei dafür, dass nicht alle $z_j = 9$ ab einer bestimmten Stelle sind. Das ist kein Problem, weil wir für die Wahl von z_j ganze 9 Möglichkeiten haben! Auswahl in Hülle und Fülle!
Nun — und das ist der Clou — muss die so konstruierte Zahl r ja auch eine „Nummer“ tragen. Sagen wir die Nummer k. Dann muss aber $r_k = s_{kk}$ sein — im *Widerspruch* zur Konstruktion von r! ∎

Diese Beweisführung geht auch auf G. Cantor zurück. Raffiniert, nicht wahr? Wenn Sie den Beweis selbst frei führen können, bin ich mit Ihnen sehr zufrieden.

Ich bin mir bewusst, dass es eine ziemliche Herausforderung an Sie ist, sich die letzten beiden Sätze zu erschließen. Vielleicht „hänge ich Sie ab“, wenn ich die Frage aufwerfe, ob es Mengen gibt, die noch mächtiger sind als $\mathbb{R}$. Die Antwort ist ja: die Potenzmenge $Pot\mathbb{R}$ ist nicht gleichmächtig mit $\mathbb{R}$, da man mit einem wunderbar eleganten Beweis zeigen kann:

Satz 9.13. *Für alle Mengen M gibt es keine Bijektion $f : M \to PotM$.*

Man kann also $|M| < |PotM|$ schreiben.
Beweis: Wieder führen wir den Beweis durch Widerspruch. Nehmen wir an, es gebe eine solche Bijektion $f : M \to PotM$. Für $m \in M$ ist $f(m)$ eine Teilmenge von M. Jetzt betrachten wir

$$A := \{m \in M : m \notin f(m)\},$$

die Menge aller $m \in M$, für die m nicht in $f(m)$ liegt. Eine verrückte Konstruktion! Sie zahlt sich aber aus: Da A selbst eine Teilmenge von M ist ($A \in PotM$), wird A ebenfalls von genau

Abbildung 9.2: aleph als hebräischer Buchstabe

einem „f-Pfeil“ getroffen: Es gibt genau ein $m' \in M$ mit $f(m') = A$, da f eine Bijektion ist. m' ist das Urbild von A unter f.
Nun stellen wir die Frage, ob $m' \in A$ oder nicht. Wäre $m' \in A$, so ergäbe sich aus der Definition von A, dass $m' \notin f(m') = A$. Ein Widerspruch. Also kann nur $m' \notin A$ gelten. Das bedeutet aber gerade, dass $m' \in f(m') = A$. Ein Widerspruch. Es kann weder $m' \in A$ noch $m' \notin A$ gelten. Die Annahme ist falsch. Der Satz ist bewiesen. ∎

9.5.1 Der Begriff Unendlich

Dass es **unendlich** viele natürliche Zahlen gibt, machen wir uns dadurch klar, dass es ja keine größte Zahl gibt: wir können immer noch um Eins erhöhen. Ist *Unendlich* nun so etwas wie eine Zahl? Die Mathematik kennt hierfür das Symbol ∞. Wenn man hiermit $|\mathbb{N}| = \infty$ oder auch $|\mathbb{R}| = \infty$ schreibt, wird nicht deutlich, dass $|\mathbb{N}| < |\mathbb{R}|$. Um diese Unterscheide zu erfassen, führt man *Kardinalzahlen* ein, die die Mächtigkeit von unendlichen Mengen messen. Dabei verwendet man den ersten hebräischen Buchstaben **aleph** (s. Abb. 9.2), indem man $|\mathbb{N}| = |\mathbb{Q}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0, |\mathbb{R}| = \aleph_1, |Pot\mathbb{R}| = \aleph_2, ...$ schreibt. Dies geht wie schon die Mengenlehre selbst auf Georg Cantor zurück.
Für SchülerInnen ist der Begriff *unendlich* natürlich etwas mystisch. Ist das Weltall unendlich groß? Gibt es unendlich viele Mücken? Unendlich viele Atome?
Kann man mit unendlich rechnen? Gilt $\frac{1}{0} = \infty$? Wie ist es mit $\infty + \infty = \infty$? Wenn man von der Menge $\mathbb{N}$ alle geraden Zahlen „abzieht“, bleiben alle ungeraden Zahlen nach, die immer noch gleichmächtig zu $\mathbb{N}$ sind. Denken Sie an das *Hilberthotel* und den ankommenden *Hilbertbus*. Siehe auch Hilberts Hotel (Wikepedia).
Was weiß man über $0 \cdot \infty$?

Der Unendlichkeitsbegriff begegnet uns auch im „unendlich Kleinen“ und steckt im Begriff „infinitesimal“, der wiederum die Grundlage unserer modernen Analysis ist. Hier ist die berühmte Geschichte von „Achilles und die Schildkröte“ einzuordnen, die dem Philosophen Zenon von Elea (495-435 v. Chr.) zugeschrieben wird. Da die Schildkröte viel langsamer ist als Achill, der schnellste Läufer Griechenlands, bekommt sie einen Vorsprung. Nun argumentierte Zenon folgendermaßen: Wenn Achill den Punkt erreicht, von dem die Schildkröte das Wettrennen begonnen hat, ist die Schildkröte ein Stück vorangekommen. Zu dem Zeitpunkt, da Achill diese Strecke zurückgelegt hat, ist die Schildkröte wiederum ein Stück vorangekommen. Und so geht es fort ad infinitum. Also könne der schnelle Achill, so Zenons Schluss, die langsame Schildkröte niemals überholen. Aus diesem Paradox leitete Zenon die

Abbildung 9.3: Unendlich

Abbildung 9.4: Unendlich in der Kunst

Behauptung ab, unter der Voraussetzung, dass Raum und Zeit unendlich teilbar seien, könne es keine Bewegung geben.
Die mathematische Lösung des Paradoxons ist die Beobachtung, dass die Summe aller Vorsprünge einen endlichen Wert nicht überschreitet. Ist der Vorsprung anfangs 1 und ist die Schildkröte um den Faktor $q < 1$ langsamer als Achill, so beträgt der Vorsprung nur noch q, wenn Achill den Startpunkt der Schildkröte erreicht hat, danach nur noch q^2, dann q^3, etc[14]. Wenn z.B. $q = 0.0001$, so hat Achill die Schildkröte nach $\frac{1}{1-q} = 1.00010001000100$ Längeneinheiten überholt.

9.6 Komplexe Zahlen

In Kap. 2 gab es bereits einen kurzen Einstieg in *komplexe Zahlen*. Wir hatten die Gauß'sche Zahlenebene kennengelernt, deren Punkte Zahlenpaare $(a, b) \in \mathbb{R}^2$ sind. Definiert man das Produkt zweier solcher Zahlenpaare durch

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc),$$

so ergibt sich $(0, 1) \cdot (0, 1) = (-1, 0)$. Interpretiert man ein Zahlenpaar der Gestalt $(a, 0)$ als reelle Zahl a und schreibt die **imaginäre Einheit i** für $(0, 1)$, so erhalten wir

$$i^2 = -1,$$

was auch die Schreibweise $i = \sqrt{-1}$ erklärt.
Üblicherweise schreibt man nun $a+ib$ an Stelle von (a, b), wobei das +-Zeichen noch symbolisch ist und erst später als Addition verstanden werden kann. Die Multiplikation sieht jetzt so aus

$$(a + ib) \cdot (c + id) = ac - bd + i(ad + bc).$$

Die Art zu multiplizieren ist zwingend, wenn man Distributivgesetze und die Regel $i^2 = -1$ benutzt!!
a heißt der **Realteil** von $z := a + ib$ (Schreibweise: $a = \Re z$) und b der **Imaginärteil** von z (Schreibweise: $b = \Im z$). Ist letzterer Null, so schreibt man $z = a$ an Stelle von $a + i0$ und behandelt $z = a$ als eine reelle Zahl. Nennt man $\mathbb{C}$ die Menge aller **komplexer Zahlen** $a + ib$, so gilt $\mathbb{R} \subset \mathbb{C}$. Ist $a = 0$, so schreibt man $z = ib$ an Stelle von $z = 0 + ib$ und nennt $z = ib$ **rein imaginär**.
Die Addition reeller Zahlen kann auf komplexe Zahlen erweitert werden, indem man die Real- und die Imaginärteile addiert:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Jetzt ist es nicht schwer einzusehen, dass $(\mathbb{C}, +, \cdot)$ ein Körper[15] ist — nach $\mathbb{Q}$ und $\mathbb{R}$ ein weiterer Körper, den wir kennenlernen. Insgesamt erhält man die aufsteigende Folge

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

[14] Später lernen Sie: Für $|q| < 1$ konvergiert die geometrische Reihe $\sum_{j=0}^{\infty} q^j$ gegen $\frac{1}{1-q}$.
[15] der nicht angeordnet werden kann!

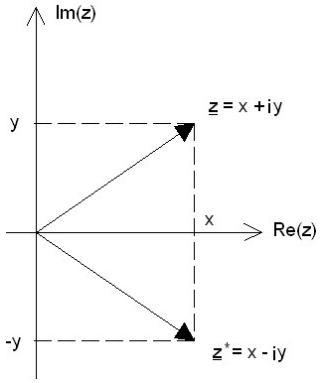


Abbildung 9.5: Komplexe Zahl z und ihre konjugierte

Wenn $\mathbb{C}$ ein Körper ist, muss $z = a + ib$ ein multiplikatives Inverses besitzen, sofern $z \neq 0$. Beachte, dass $z = 0$ nur dann gilt, wenn $a = \Re z = 0$ und $b = \Im z = 0$. Wenn man das multiplikative Inverse als $w := \frac{1}{a+ib}$ schreibt, kann man den Nenner durch Erweiterung mit $a - ib$ wegen $(a + ib)(a - ib) = a^2 + b^2$ reell machen, und man erhält

$$w = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}.$$

Definition 9.14. $\overline{z} := a - ib$ *heißt die zu* $z = a + ib$ **konjugierte Zahl**.

Beachte, dass z und $\overline{z}$ in der komplexen Zahlenebene symmetrisch zur „reellen Achse“ (der horizontalen Achse) liegen, d.h. durch Spiegelungen auseinander gewonnen werden können. Klar, dass die Konjugierte von $\overline{z}$ wieder z ist, s. Abb. 9.5, in der z' für $\overline{z}$ steht.

Definition 9.15. *Der* **Betrag** *von* $z := a + ib$ *ist*

$$|z| := \sqrt{a^2 + b^2}.$$

$|z|$ ist nichts anderes als der Abstand von z zum Ursprung in der komplexen Zahlenebene. Jetzt erhalten wir

$$z \cdot \overline{z} = |z|^2 \tag{9.3}$$

Beweis: Es ist $(a + ib)(a - ib) = a^2 + b^2$. ∎

9.6.1 Quadratische Gleichungen

Sie kennen die Lösungsformel

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

für eine quadratische Gleichung

$$x^2 + px + q = 0.$$

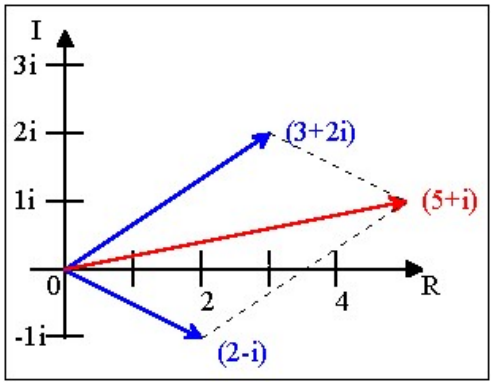


Abbildung 9.6: Addition komplexer Zahlen

Wenn die *Diskriminante* $D := \frac{p^2}{4} - q \geq 0$, so sind beide Lösungen x_1 und x_2 reell, und es gelten die VIETA'schen Wurzelsätze

$$x_1 + x_2 = -p, \quad x_1 \cdot x_2 = q.$$

Dieser Sachverhalt überträgt sich auf den Fall negativer Diskriminante $D < 0$ unter Benutzung komplexer Zahlen: Dann schreiben wir statt $\sqrt{D}$ jetzt $i\sqrt{-D}$ und erhalten statt $x_{1,2}$ die beiden (zueinander konjugiert-) komplexen Lösungen

$$z_{1,2} = -\frac{p}{2} \pm i\sqrt{q - \frac{p^2}{4}}.$$

Es gelten sogar nach wie vor die Vieta'schen Wurzelsätze

$$z_1 + z_2 = -p, \quad z_1 \cdot z_2 = q.$$

Dann gilt auch $|z_1| = |z_2| = \sqrt{q}$.

9.6.2 Polarkoordinaten und Multiplikation

Die Addition von zwei komplexen Zahlen z_1 und z_2 kann man in der komplexen Zahlenebene leicht geometrisch veranschaulichen: Man zeichne ein Parallelogramm, siehe Abb. 9.6. Ein solches Parallelogramm wird uns in ähnlicher Form auch in der Vektorrechnung begegnen.
Weniger offensichtlich ist die geometrische Veranschaulichung der Multiplikation zweier komplexer Zahlen. Hier helfen *Polarkoordinaten*: Jeder komplexen Zahl $z \neq 0$ kann man den Betrag $r := |z|$ und den Winkel φ (**Argument** von z im Bogenmaß: $0 \leq \varphi < 2\pi$) zuordnen. ϕ wird durch

$$\Re z = r\cos\varphi, \quad \Im z = r\sin\varphi$$

eindeutig festgelegt, siehe Abb. 9.7. Sind umgekehrt $r > 0$ und φ gegeben, so ist die komplexe Zahl

$$z = r(\cos\varphi + i\sin\varphi)$$

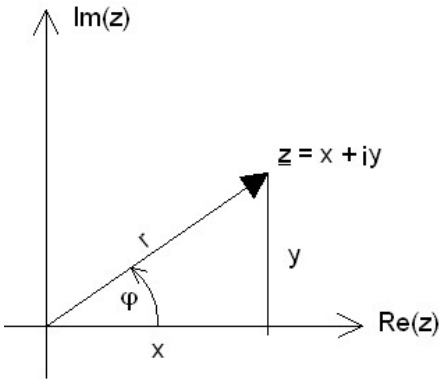


Abbildung 9.7: Polarkoordinaten

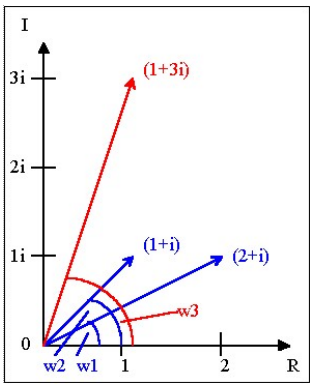


Abbildung 9.8: Multiplikation komplexer Zahlen

dadurch eindeutig festgelegt. r und φ heißen die **Polarkoordinaten** von z.
Wenn wir jetzt zwei komplexe Zahlen z_1 und z_2 miteinander multiplizieren, so können wir mit Hilfe von *Additionstheoremen*[16] für $\sin\phi$ und $\cos\phi$ das Produkt $z_1 \cdot z_2$ in Polarkoordinaten notieren:

Satz 9.16. *Mit den beiden komplexen Zahlen*

$$z_j = r_j(\cos\phi_j + i\sin\phi_j), j = 1, 2$$

gilt für ihr Produkt

$$z_1 z_2 = r_1 r_2(\cos(\phi_1 + \phi_2) + i\sin(\phi_1 + \phi_2)).$$

Bei der Multiplikation von z_1 und z_2 werden also die **Beträge multipliziert und die Winkel addiert**! In Abb. 9.8 werden die beiden komplexen Zahlen $2+i$ und $1+i$ mit den Winkeln $w1$ und $w2$ multipliziert: $(1+i)(2+i) = 1+3i$

[16] $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$ und $\sin(\alpha+\beta) = \cos\alpha\sin\beta + \cos\beta\sin\alpha$.

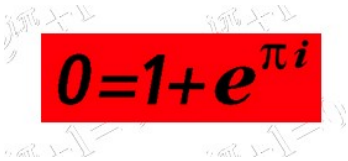


Abbildung 9.9: Schönste Formel der Mathematik

Hieraus folgt auch sofort, dass $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ für zwei komplexe Zahlen $z_j, j = 1, 2$.

Für komplexe Zahlen z vom Betrag 1 ($|z| = 1$) und Argument ϕ gilt offensichtlich

$$z = \cos\phi + i \sin\phi.$$

Multipliziert man zwei solcher komplexen Zahlen mit Argument ϕ und ψ, addieren sich einfach die Winkel (modulo 2π). n-faches Potenzieren von z führt auf

$$z^n = (\cos\phi + i\sin\phi)^n = \cos(n\phi) + i\sin(n\phi).$$

Diese Darstellung erlaubt eine explizite Angabe aller n komplexer Lösungen der Gleichung $z^n = 1$ — der sogenannten n-ten Einheitswurzeln. Diese bilden in der komplexen Zahlenebene die Ecken eines regelmäßigen n-Ecks.

9.6.3 Schönste Formel

In Kap. **??** hatte ich auf die „schönste Formel“

$$e^{i\pi} + 1 = 0$$

hingewiesen, siehe Abb. 9.9.
Diese Formel möchte ich ein klein wenig, aber nicht vollständig, entschleiern: Des Rätsels Lösung liegt in der *Euler'schen Formel*

$$e^{i\phi} = \cos\phi + i\sin\phi. \tag{9.4}$$

Man sieht sofort, dass unsere „schöne Formel“ folgt, wenn man $\phi = \pi$ setzt und $\cos\pi = -1$ und $\sin\pi = 0$ beachtet.
Zu (9.4): Nennt man die rechte Seite $E(\phi)$, so ist $E(\phi)$ eine komplexe Zahl vom Betrag 1 (da $\cos^2(\phi) + \sin^2(\phi) = 1$ gilt)[17]. Die obigen Multiplikationsregeln in Polarkoordinaten führen auf

$$E(\phi) \cdot E(\psi) = E(\phi + \psi), \quad E(0) = 1.$$

Das erinnert doch sehr an das Potenzgesetz $a^{x+y} = a^x \cdot a^y$. Alles weitere benötigt mehr Mathematik. Stichworte sind die Potenzreihendarstellungen von den Funktionen $x \mapsto e^x, x \mapsto \sin x, x \mapsto \cos x$.

[17] $E(\varphi)$ liegt also auf dem Einheitskreis.

9.6.4 Abschließende Bemerkungen

Wo liegt der „Nutzen“ der komplexen Zahlen? Nun, als erstes sollte der *Fundamentalsatz der Algebra* erwähnt werden. Er besagt, dass jede Polynomgleichung n-ten Grades immer genau n Lösungen besitzt — wenn man auch komplexe Lösungen und mehrfache Lösungen zulässt. Ein Beispiel ist die Gleichung $z^n = 1$, die für ungerade n nur eine reelle Lösung ($z = 1$) besitzt — alle anderen sind nichtreell.
Aus Sicht der Reinen Mathematik“ legen die komplexen Zahlen den Grundstein für eine wunderschöne Theorie, die *Funktionentheorie*. Hier betrachtet man Funktionen $f : \mathbb{C} \to \mathbb{C}$, speziell die *holomorphen* Funktionen.
Die wichtigsten Anwendungen der komplexen Zahlen liegen in der Physik und den Ingenieurwissenschaften, vor allem in der Signalverarbeitung, wo sie etwa bei Musikaufnahmen zum Zuge kommen. So werden harmonische Schwingungen (Töne) durch $f(t) = a\sin(\omega t + \phi)$ dargestellt, wobei ω die *Kreisfrequenz*, a die Amplitude und ϕ die *Phase* ist. In komplexer Form kann stattdessen $z(t) = Ae^{i\omega t}$ mit komplexer Amplitude geschrieben werden, in die die reelle Amplitude a und die Phase ϕ eingeht. Auch die Beschreibung von Wellen, etwa von *Sinus-Wellen* ist sehr elegant im Kalkül der komplexen Zahlen.

Kapitel 10

Aussagenlogik

10.1 Einführung

Es wurden schon mehrfach Beweise geführt und dabei *logischen Regeln* gefolgt, z.B. bei indirekten Beweisen wie von Satz 2.1 und Satz 2.2 der Regel, dass eine Aussage entweder wahr oder falsch ist. *Tertium non datur* — etwas Drittes gibt es nicht.

Kernbegriff der Logik ist der einer **Aussage**. Was aber sind genau *Aussagen*? Uns sind in den vorangegangenen Kapiteln hunderte Aussagen begegnet und Sie haben (hoffentlich) gelernt, mit ihnen intuitiv umzugehen. Wir lassen uns hier nicht auf den Versuch einer präzisen Definition ein, sondern sagen nur, dass Aussagen gewisse Dinge sind, denen das Attribut *wahr* oder *falsch* zukommt.

„Wien ist Hauptstadt Österreichs“ ist genauso eine Aussage wie *„Wien ist nicht Hauptstadt Österreichs“*. Die erste Aussage ist wahr, die zweite falsch. Auch *„es gibt unendlich viele Primzahlen“* ist eine Aussage (die von Satz 2.1). „$1+2=3$“ oder „$3 \in \mathbb{N}$“ oder „$\sum_{j=1}^{n} q^j = \frac{1-q^{n+1}}{1-q}$“ sind ebenfalls (wahre) Aussagen. Kürzen wir wieder wie in Kap. 6 die letzte Aussage mit $A(n)$ ab, so haben wir sehr wohl die beiden Aussagen „$A(n)$ gilt für ein $n \in \mathbb{N}$“ (z.B. „es gilt $A(3)$“) und – weitergehend – „Für alle $n \in \mathbb{N}$ gilt $A(n)$“ unterschieden.

Keine Aussagen sind „4+5“ oder „Haltet den Dieb!“.

Wir haben auch schon mehrfach von gewissen binären Verknüpfungen von zwei Aussagen A und B Gebrauch gemacht, die man mit „*und* “ und mit „*oder*“ bezeichnet. Abgekürzt werden sie durch die Symbole $\wedge, \vee$. Mit ihrer Hilfe kann man aus zwei Aussagen eine dritte gewinnen.

Wir werden hier diese Verknüpfungen (oder *logische Operatoren*) durch eine *Wahrheitstabelle* definieren. Ähnliches werden wir mit den Verknüpfungen „$\Longrightarrow$“ und „ $\Longleftrightarrow$ “ tun, die wir u.A. im Beweis des Satzes 8.4 des Kap. 8 verwendet haben, aber auch für eine der häufigsten Verknüpfungen, nämlich die Implikation „$\Rightarrow$“, die Sie verbal als „Aus A folgt B“ bzw. formal als „$A \Rightarrow B$“ kennengelernt haben.

10.2 Negation, Konjunktion und Disjunktion

Wir bezeichnen Aussagen mit großen lateinischen Buchstaben $A, B, \ldots..$ Der einfachste (einstellige) logische Operator ist die **Negation**, die einer Aussage A die Aussage $\overline{A}$, gesprochen „nicht A“ oder „non A“ zuordnet. Die Aussage $\overline{A}$ ist genau dann wahr, wenn die Aussage A falsch ist. Zweimaliges Verneinen von A ergibt wieder A.
Kommt Ihnen dies nicht bekannt vor? Wenn man eine *Menge* A anstelle einer *Aussage* A betrachtet, so entspricht $\overline{A}$ gerade dem *Komplement* A^c. Diese Übereinstimmung ist einleuchtend, wenn man die Menge A mit der Aussage „$a \in A$“ verbindet. Weitere Analogien s. Tab. 10.1.
In diesem Sinne entspricht die *Konjunktion* von Aussagen „$A \wedge B$“ gerade der Durchschnittbildung von Mengen, während die *Disjunktion* „$A \vee B$“ der Vereinigung von Mengen entspricht.

Wir legen im Folgenden fest (eine Art „code“):

Definition 10.1. *„falsch“ wird ausgedrückt durch „0“, „wahr“ wird ausgedrückt durch „1“.*

Jetzt definieren wir die **Konjunktion** „$A \wedge B$“ durch die folgende **Wahrheitstabelle**[1]:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Durch $\wedge$ werden also zwei beliebige Aussagen A, B zu einer neuen Aussage „$A \wedge B$“ verknüpft, die genau dann wahr ist, wenn beide Aussagen A und B wahr sind.

Die Verknüpfung $\vee$ bezeichnet man als **Disjunktion** und wird durch die folgende Tabelle gegeben:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Die durch die Verknüpfung $\vee$ aus A, B gebildete Aussage „$A \vee B$“ ist also genau dann falsch, wenn beide Aussagen A, B falsch sind.

10.3 Implikation und Äquivalenz

Die Verknüpfung „$\Rightarrow$“bildet das umgangssprachliche „wenn, dann“ nach. Wir haben von dieser Sprechweise u.A. im Beweis von Satz 8.4 Gebrauch gemacht. Sie heißt **Implikation**. Wenn man „$A \Rightarrow B$“ schreibt, nennt man die Aussage A auch die **Voraussetzung** und B die **Folgerung** der Implikation. Die *Äquivalenz* wird mit „ $\Longleftrightarrow$ “ bezeichnet und entspricht dem umgangssprachlichen „genau dann, wenn“ oder „dann und nur dann“. Implikation und Äquivalenz werden in der folgenden Tabelle definiert:

[1] Eigentlich wird hierdurch nicht die Konjunktion selbst, sondern ihre Wahrheitswerte festgelegt.

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	1
0	1	1	0
1	0	0	0
1	1	1	1

Die durch $\Rightarrow$ aus den Aussagen A und B gebildete Aussage „$A \Rightarrow B$“ ist also genau dann falsch, wenn A wahr und B falsch ist; „$A \Leftrightarrow B$“ ist genau dann wahr, wenn A und B denselben Wahrheitswert haben.

Meist irritiert bei der Implikation die Beobachtung, dass die Aussage „$A \Rightarrow B$“ schon dann wahr ist, wenn A falsch ist. Dass diese Festsetzung jedoch sinnvoll ist, erkennt man an der folgenden offensichtlich wahren Aussage:

$$\text{Für alle } x \in \mathbb{R} \text{ gilt : } \quad x < 1 \Rightarrow x < 2.$$

Die Implikation „$x < 1 \Rightarrow x < 2$“ ist danach auch richtig, wenn $x \geq 1$, schließlich ist sie ja *für alle* $x \in \mathbb{R}$ richtig, also auch für diejenigen, für die die Voraussetzung $x < 1$ falsch ist! Nennt man „$x < 1$“ die Aussage A (besser $A(x)$, m die Abhängigkeit der Aussage von x zu erfassen) und „$x < 2$“ die Aussage B (besser $B(x)$), so ist A für $x = 1.5$ falsch, B jedoch wahr, für $x = 3$ sind weder A noch B wahr – was der Richtigkeit von „$A \Rightarrow B$“ keinen Abbruch tut.

Die Implikation ist wohl die Operation, die man bei mathematischen Argumenten und bei Beweisen am häufigsten zu nutzen glaubt („Aus A folgt B“). Man sollte sich jedoch nicht einbilden, dass das logische Denken eher gelingt, wenn man die Wahrheitstabelle der Implikation im Kopf hat.
Mit einer Implikation hängen die häufig verwendeten Begriffe *notwendige Bedingung* und *hinreichende Bedingung* zusammen.

Definition 10.2. *Wenn „$A \Rightarrow B$“ wahr ist, heißt B die* **notwendige Bedingung** *für A und A die* **hinreichende Bedingung** *für B.*

Beispiele: „Wenn es regnet, ist die Straße nass“: Eine nasse Straße ist notwendig für Regen – in dem Sinne, dass eine trockene Straße bedeutet, dass es nicht regnet. Eine nasse Straße ist ein „Indiz“ für Regen. Eine nasse Straße reicht jedoch nicht aus, um auf Regen zu schließen – schließlich kann ein Wasserwagen die Straße gewässert haben. Anders ausgedrückt: Eine nasse Straße ist keine hinreichende Bedingung für Regen, da die Implikation „Wenn die Straße nass ist, dann regnet es“ falsch ist.
Andererseits ist Regen hinreichend für eine nasse Straße, aber nicht notwendig.

Die Äquivalenz „$A \Longleftrightarrow B$“ von zwei Aussagen A und B bedeutet von der Logik her, dass A und B in einem gewissen Sinne „gleich“ sind. Bei Gleichungsumformungen machen wir davon ständig Gebrauch, z.B.

$$3x + 4y = 2 \Longleftrightarrow y = \frac{2 - 3x}{4}.$$

Im Grunde enthält die Äquivalenz zwei Implikationen: „$A \iff B$“ ist gleichwertig mit der Aussage „$A \Rightarrow B$ und $B \Rightarrow A$“. Aber diese Feststellung ist auch eine logische Aussage:

$$(A \iff B) \quad \iff \quad ((A \Rightarrow B) \wedge (B \Rightarrow A))$$

Hiervon kann man sich leicht an Hand einer Wahrheitstabelle überzeugen!

10.4 Widerspruchsbeweis, Indirekter Beweis

Von welchen logischen Regeln haben wir eigentlich bisher „naiv“ Gebrauch gemacht?
Schauen wir uns noch einmal einen der ersten Sätze, den Satz 2.2, an. Die Aussage A lautet: „$x = \sqrt{2}$“, die Aussage B lautet „$x \notin \mathbb{Q}$“. Der Satz 2.2 lautet „$A \Rightarrow B$“. Wir haben einen *indirekten Beweis* geführt, indem wir $\overline{B}$ – die Negation von B – und A annahmen und hieraus $\overline{A}$ (einen *Widerspruch* zu A) folgerten. Wieso durften wir dies? Nun, „$A \Rightarrow B$“ ist nur dann falsch, wenn A wahr und B falsch ist. Wenn wir also A und $\overline{B}$ annehmen und hieraus etwas auffensichtlich falsches folgern, ist die Annahme falsch und die Implikation „$A \Rightarrow B$“. Dies ist ein **Widerspruchbeweis**. Auch Euklids Beweis für die Existenz von unendlich vielen Primzahlen ist ein Widerspruchsbeweis.
Ähnlich ist ein indirekter Beweis. Dieser beruht darauf, dass „$A \Rightarrow B$“ äquivalent zu „$\overline{B} \Rightarrow \overline{A}$“ ist – oder noch formaler: Es gilt der folgende

Satz 10.3. *Für alle Aussagen A und B gilt*

$$(A \Rightarrow B) \iff (\overline{B} \Rightarrow \overline{A}.)$$

Wir beweisen diesen Satz 10.3 mit Hilfe einer Wahrheitstafel 10.1, die alle vier Fälle für den Wahrheitsgehalt von A und B behandelt:

A	B	$\overline{A}$	$\overline{B}$	$A \Rightarrow B$	$\overline{B} \Rightarrow \overline{A}$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

(10.1)

Ein Beispiel für einen solchen indirekten Beweis ist der Beweis der Aussage „*Wenn* $2^n - 1$ *eine Primzahl ist, dann ist* n *eine Primzahl*“. Nach Satz 10.3 muss nur „*Wenn* n *keine Primzahl ist, dann ist* $2^n - 1$ *keine Primzahl*“ gezeigt werden. Das wurde in Kap.2.6.3. gezeigt.

Zuweilen wird zwischen einem indirekten Beweis und einem Widerspruchsbeweis für Aussagen der Form „$A \Rightarrow B$“ unterschieden. In letzterem Fall folgert man aus $\overline{B}$ und A zugleich eine Aussage C und $\overline{C}$ — einen Widerspruch. In diesem Sinne ist der indirekte Beweis ein Spezialfall des Widerspruchbeweises.

Tabelle 10.1: Zusammenhang zwischen Mengen und Aussagen

Menge M	$x \in M$ / $x \notin M$	Komplement	$\cap$	$\cup$	$\subset$	$=$
Aussage A	A ist wahr / falsch	Negation	$\wedge$	$\vee$	$\Rightarrow$	$\Longleftrightarrow$

Tabelle 10.2: Beweis von (10.2)

A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cup \overline{B}$
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

10.5 Mengen und Aussagen

Wenn man Mengenlehre und Aussagenlogik vergleicht, fallen große Übereinstimmungen auf. Wir halten dies in Tabelle 10.1 fest.

Diese Analogie hatten wir schon im Beweis von Satz 3.5, der Rechenregel von de Morgan für Mengen

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{10.2}$$

ausgenutzt, indem wir die Menge A mit der Aussage „$x \in A$“ identifizierten, s. Tabelle 10.2. Dieser Regel von de Morgan entspricht auch eine Äquivalenz von Aussagen der Form

$$\overline{A \wedge B} \Longleftrightarrow \overline{A} \vee \overline{B} \tag{10.3}$$

Umgangssprachlich drückt dieses Gesetz etwas aus, was alle logisch denkenden Menschen auch ohne solche formalen Regeln sofort als „wahr“ akzeptieren: „Wenn nicht zugleich A und B gelten, so ist A falsch oder B ist falsch[2]“.

Man kann allen Regeln der Mengenlehre Regeln der Aussagenlogik gegenüberstellen. So wie man mit Mengen rechnen kann, so auch mit Aussagen.

Was entspricht der leeren Menge $\emptyset$? Offensichtlich, die Aussage, die man 0 nennt, die stets falsch ist. Schließlich gilt „$A \wedge 0 \Longleftrightarrow 0$“ und „$A \vee 0 \Longleftrightarrow A$“. Wenn man mit 1 eine wahre Aussage bezeichnet, so gilt „$A \wedge 1 \Longleftrightarrow A$“ und „ $A \vee 1 \Longleftrightarrow 1$“. Ferner „$A \wedge \overline{A} \Longleftrightarrow 0$“ und „$A \vee \overline{A} \Longleftrightarrow 1$“. Nette Spielerei.

[2]Es können auch beide, A und B, falsch sein.

10.6 Quantoren

Schon in Kap. 3.2 haben wir die **Quantoren** $\forall$ („für alle“) und $\exists$ („es existiert“) kennengelernt, deren Verwendung zu neuen Aussagen führt. Z.B. die Aussage „für alle $n \in \mathbb{N}$ gilt, dass die Summe der ersten n ungeraden Zahlen n^2 ist“. Umgangsprachlich verwendet man i.a. nur das Wort „alle“, z.B. in „alle Menschen haben einen Kopf“, mathematisch: „für alle Menschen x gilt, dass x einen Kopf hat“. Oder noch formaler:

$$\forall x : (M(x) \Longrightarrow K(x)),$$

wobei die Aussage $M(x)$ für „x ist ein Mensch“ und $K(x)$ für „x hat einen Kopf“ steht.
Oder die (falsche) Aussage „es existieren zwei Zahlen $p, q \in \mathbb{N}$ mit $\sqrt{2} = \frac{p}{q}$“. Oder die (wahre) Aussage „es gibt einen Menschen, der schon einmal höher als 2,30 m gesprungen ist“. Umgangssprachlich sagt man auch „einige Menschen springen höher als 2,30 m“. Formalisiert schreibt man auch

$$\exists x : (M(x) \wedge S(x)),$$

wobei $S(x)$ für „x springt höher als 2,30m“ steht.
Komplizierter sind schon Aussagen, die diese beiden Quantoren enthalten wie

$$\forall x \in \mathbb{R}\, \exists\, y \in \mathbb{R} : 3x + 4y = 3.$$

Oder „alle Menschen haben eine Mutter“, mathematisch kompliziert: „für alle Menschen x existiert ein Mensch y, der Mutter von x ist“.

Es gibt formale Regeln, wie man Aussagen, die Quantoren enthalten, verneint. Wenn wir die Aussage „für alle x gilt die Aussage $A(x)$“ verneinen, führt dies auf „es gibt ein x mit $\overline{A(x)}$“, d.h. eine solche Aussage kann mit Hilfe eines Gegenbeispiels widerlegt werden. Schauen wir uns z.B. die Aussage „$\forall n \in \mathbb{N}$ gilt $2^n > n^2$“ an. Die Verneinung lautet „$\exists n \in \mathbb{N} : 2^n \leq n^2$“. Diese Aussage ist richtig, man nehme nur $n = 2$. Vergleiche mit Satz 6.4, der besagt, dass $2^n > n^2$ für $n > 4$ richtig ist.

Wenn wir dagegen die Aussage „ es existiert ein x, für das die Aussage $A(x)$ gilt“, verneinen, führt dies auf „für alle x gilt $\overline{A(x)}$“. Z.B. ist die Aussage „$\exists x \in \mathbb{R} : x^2 < 0$“ falsch, da deren Negation „$\forall\, x \in \mathbb{R}$ gilt $x^2 \geq 0$“ wahr ist.

10.7 Bemerkungen

Die Logik ist ein wichtiger Bestandteil der Philosophie, genauer der Erkenntnistheorie. Sie ist auch ein Grundlagengebiet der Mathematik. In den Anwendungen spielt sie im Rahmen der Boole'schen Algebra eine wichtige Rolle in der Elektrotechnik („logische Schaltungen“). So ist die Boole'sche Algebra Pflichtfach im ersten Fachsemester der Studierenden der Elektrotechnik an der TU Hamburg-Harburg.