

LEHRBUCH

Rudolf Berghammer

# Mathematik für Informatiker

Grundlegende Begriffe und Strukturen



Springer Vieweg

---

# Mathematik für Informatiker

---

Rudolf Berghammer

# Mathematik für Informatiker

Grundlegende Begriffe und Strukturen



Springer Vieweg

Rudolf Berghammer  
Institut für Informatik  
Universität Kiel  
Kiel, Deutschland

ISBN 978-3-658-06287-3  
DOI 10.1007/978-3-658-06288-0

ISBN 978-3-658-06288-0 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;  
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg  
© Springer Fachmedien Wiesbaden 2014  
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Ein-speicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Gedruckt auf säurefrei und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media.  
[www.springer-vieweg.de](http://www.springer-vieweg.de)

# **Einleitung**

Viele der modernen Wissenschaften sind ohne die Verwendung mathematischer Methoden und Techniken nicht mehr denkbar. Dies trifft auch auf die Informatik zu. Insbesondere gilt dies natürlich für ihr Teilgebiet „theoretische Informatik“. Eine Reihe von Themen der theoretischen Informatik sind so mathematisch, dass es oft sehr schwer fällt, eine klare Trennlinie zwischen der Mathematik und der theoretischen Informatik zu ziehen. Aber auch die sogenannte praktische oder angewandte Informatik benutzt sehr häufig Mathematik als Hilfsmittel, etwa bei der Speicherung von Daten, wo modulares Rechnen oft hilfreich ist, oder bei der Datenverschlüsselung, die wesentlich auf Ergebnissen aus der Algebra und der Zahlentheorie aufbaut, oder der Computergrafik, die viel mit Geometrie zu tun hat, oder den logischen Schaltungen, deren mathematische Grundlage die Theorie der sogenannten Booleschen Algebren ist.

Noch vor ungefähr zehn Jahren war die Informatikausbildung in Bezug auf Mathematik-Vorlesungen oft sehr ähnlich oder sogar identisch zur Ausbildung von Studierenden der Mathematik. Auf die höhere Schule (etwa ein Gymnasium) aufbauend wurde damals im Rahmen von Vorlesungen von den Lehrenden demonstriert, wie man in der Mathematik vorgeht, insbesondere Begriffe einführt, Aussagen (als Lemmata, Sätze, Theoreme usw.) formuliert und diese dann beweist. Die Techniken des Beweisens und die ihnen zugrundeliegenden logischen Gesetze wurden jedoch in der Regel nur knapp diskutiert. Man glaubte, auf eine gewisse Schulvorbildung aufbauend, dass sich durch das Demonstrieren von Beweisen in Vorlesungen und das Selberfinden solcher in Übungen und im Rahmen von Hausaufgaben mit der Zeit das Gefühl dafür entwickelt, was ein mathematischer Beweis ist und wie man ihn zusammen mit der zu beweisenden Aussage so aufschreibt, dass beides zusammen als bewiesener Satz der Mathematik akzeptiert wird. Auch wurde nur sehr wenig auf das konkrete Hinschreiben von Aussagen eingegangen, d.h. auf all die notationellen Besonderheiten und Abkürzungen, die von Mathematik betreibenden Personen zu Vereinfachungszwecken normalerweise verwendet werden, sich aber von Person zu Person und von Fach zu Fach manchmal deutlich unterscheiden können.

Diese traditionelle Vorgehensweise führte an der Christian-Albrechts-Universität zu Kiel bei den Informatikstudierenden zu immer größeren Problemen. Deshalb wurde vor einigen Jahren im Kieler Institut für Informatik in Zusammenarbeit mit dem Mathematischen Seminar ein neuer drei-semestrigler Zyklus von Einführungs-Vorlesungen in die Mathematik für Informatikstudierende entworfen. Er soll den Übergang von der höheren Schule zum Studium an einer wissenschaftlichen Hochschule sanfter gestalten. Dieser Text basiert auf der ersten Vorlesung des Zyklus. In ihm wird sehr viel Wert auf die grundlegenden Begriffe der Mathematik gelegt sowie auf ihre Techniken und Vorgehensweisen und auch auf ihre Sprache – und dies alles in möglichst verständlicher aber auch präziser Weise und mit detaillierten Beweisen. Es muss an dieser Stelle aber unbedingt darauf hingewiesen werden, dass vieles, was in Vorlesungen an mündlichen Hinweisen, an Bildern, an erläuternden zusätzlichen Rechnungen, an Fragen und sonstigen Interaktionen geschieht, nicht durch einen Text in Buchform darstellbar ist. Ein begleitendes Lehrbuch ersetzt also in der Regel nicht den Besuch einer Vorlesung. Es unterstützt ihn nur; der Besuch einer Vorlesung ist insbesondere am Anfang des Studiums immer noch sehr wesentlich für das Verstehen dessen, was unterrichtet wird. Gleches gilt auch für die normalerweise Vorlesungen beglei-

tenden Übungen. Ihre Präsenzaufgaben dienen hier dazu, unter Anleitung eines Tutors zu lernen, wie man mathematische Probleme löst. Darauf aufbauende Hausaufgaben geben der Studentin oder dem Studenten die Möglichkeit, zu zeigen, was sie bzw. er ohne Anleitung zu leisten im Stande ist. Dem Lehrenden (also in der Regel der Professorin oder dem Professor) geben sie die Möglichkeit, die Leistungsfähigkeit und den Lernerfolg der Studierenden zu kontrollieren.

Hier ist eine kurze Zusammenfassung des Inhaltes. Im ersten Kapitel wird die Sprache der Mengenlehre eingeführt. Alle Beweise werden hier noch in der Umgangssprache geführt, wobei als Logik „der gesunde Menschenverstand“ benutzt wird. Diese Art der Beweisführung in einer natürlichen Sprache und mit nur wenigen logischen Symbolen (wie Quantoren und Implikationspfeilen) war früher durchaus üblich. Die Logik als ein Mittel zum Formulieren und Beweisen von mathematischen Aussagen ist der Inhalt von Kapitel 2. Bevor auf das Beweisen selber im Detail in Kapitel 4 eingegangen wird, werden in Kapitel 3 noch allgemeine Produkte behandelt, sowie, darauf aufbauend, Konstruktionen von Informatik-Datenstrukturen. Dieses Kapitel wurde eingeschoben, damit Mathematik auch mit Hilfe von anderen Objekten als den von der Schule her bekannten Zahlen betrieben werden kann. Bei der Vorstellung der Beweistechniken in Kapitel 4 wird das zugrundeliegende Prinzip jeweils erklärt. Dann werden einige Anwendungen demonstriert. Dabei wird auch erklärt, wie man formal und logisch korrekt vorzugehen hat, wenn man nicht geübt ist, und welche Formulierungen „altgedienter und erfahrener Mathematiker“ genau genommen welchen logischen Formeln entsprechen. Insbesondere die oft unterdrückten Allquantoren sorgen hier bei einer Anfängerin oder einem Anfänger oft für Schwierigkeiten. Die beiden zentralen Konzepte der Funktionen und Relationen werden schon im ersten Kapitel eingeführt. Dies geschieht aber sehr knapp. Der einzige Zweck, sie so früh einzuführen, ist, sie für Beispiele in den folgenden drei Kapiteln bereitzustellen. In den beiden Kapiteln 5 und 6 werden diese Begriffe nun im Detail behandelt. Kapitel 5 ist den Funktionen gewidmet und Kapitel 6 den Relationen. Von den Relationen ist es nur ein kleiner Schritt zu den gerichteten Graphen. Der ungerichteten Variante dieser mathematischen Struktur ist das vorletzte Kapitel 7 des Skriptums zugeordnet. Da ungerichtete Graphen oft auch benutzt werden können, um kombinatorische Fragestellungen zu verdeutlichen, etwa die Anzahl von Zugmöglichkeiten bei Spielen, geschieht die Einführung in die Theorie der ungerichteten Graphen zusammen mit der Einführung in die elementare Kombinatorik. Das letzte Kapitel 8 stellt schließlich einen Einstieg in die grundlegendsten mathematischen Strukturen der Algebra dar. Dies geschieht aber unter einem sehr allgemeinen Blickwinkel. Ich hoffe, dass dadurch die Verwendung allgemeiner mathematischer Strukturen gut vorbereitet wird.

Ich habe mich in diesem Text dazu entschieden, Mengen vor der formalen mathematischen Logik zu behandeln. Dies hat den Vorteil, dass dadurch die in der Mathematik immer wieder verwendeten logischen Verknüpfungen und deren Grundeigenschaften gut herausgearbeitet werden können. Weiterhin kann man durch das Vorgehen demonstrieren, dass durchaus auch in der Umgangssprache logisch argumentiert werden kann, vorausgesetzt man drückt sich präzise aus. Schließlich stehen durch die Mengen bei der Einführung einer formalen logischen Sprache genügend viele mathematische Objekte zur Formulierung von Beispielen zur Verfügung, und man kann auch sofort die in der mathematischen Praxis normalerweise verwendeten Kurzschreibweisen erklären. Nachteilig an der Vorgehenswei-

se ist, dass die Logik des gesunden Menschenverstandes vielleicht doch nicht von allen Menschen in derjenigen Präzision verstanden und angewendet wird, wie es für Mathe-matik notwendig ist. Auch lassen umgangssprachliche Argumentationen die verwendeten Schlüsse oft nicht so deutlich erkennen wie Regelanwendungen in der formalen logischen Sprache. Deswegen gibt es viele Mathematikbücher, in denen die Sprache der Logik vor der Sprache der Mengenlehre behandelt wird. Teilweise werden diese beiden Grundpfeiler der Mathematik auch verschränkt eingeführt.

Mit Ausnahme von Kapitel 4 endet jedes Kapitel mit einem kurzen Abschnitt und dann einer Reihe von Übungsaufgaben. Diese speziellen Abschnitte vor den Übungsaufgaben sind für das weitere Vorgehen im Stoff nicht wesentlich, aber hoffentlich hilfreich. Sie runden nämlich unter bestimmten Blickwinkeln die einzelnen Themen in informeller Weise ab und zeigen auch auf, wo und wie die Themen in späteren Studienabschnitten wieder aufgegriffen werden. Der entsprechende Abschnitt von Kapitel 4 ist dem Finden von Beweisen gewidmet. Dies geschieht durch das Aufzeigen von Vorgehensweisen, die helfen können, einen Beweis zu finden. Sie werden mittels vieler Beispiele verdeutlicht, und das macht den Abschnitt im Vergleich zu den anderen ergänzenden Abschnitten wesentlich umfang-reicher.

Der vorliegende Text basiert auf einem handschriftlichen Manuskript von mir, das von E. Lurz im Wintersemester 2010/2011 in L<sup>A</sup>T<sub>E</sub>X gesetzt wurde und das ich anschließend weiter entwickelte. Die Gliederung und Stoffauswahl zur Vorlesung erfolgte in enger Zusammenarbeit mit Kollegen des Instituts für Informatik, insbesondere mit Herrn A. Srivastav. Bei der Weiterentwicklung des Texts wurde ich von Frau B. Langfeld, Frau I. Stucke und den Herren N. Danilenko und L. Kliemann unterstützt, bei denen ich mich, wie auch bei Herrn Srivastav, sehr herzlich bedanke. Auch bedanken möchte ich mich bei C. Giessen, L. Kuhlmann, S. Reif, C. Robenek, C. Roschat und G. Schmidt für das Lesen von Vorver-sionen und Verbesserungshinweise. Ich bedanke mich schließlich noch sehr herzlich beim Verlag Springer Vieweg, insbesondere bei Frau Sybille Thelen, für die sehr angenehme Zusammenarbeit, sowie bei meiner Frau Sibylle für ihre Unterstützung und Hilfe.

Kiel, im Juli 2014

Rudolf Berghammer.

# Inhalt

|   |            |
|---|------------|
| <b>Einleitung</b>   | <b>v</b>   |
| <b>1 Mengentheoretische Grundlagen</b>                              | <b>1</b>   |
| 1.1 Der Cantorsche Mengenbegriff . . . . .                          | 1          |
| 1.2 Einige Konstruktionen auf Mengen . . . . .                      | 7          |
| 1.3 Potenzmengen und Kardinalitäten . . . . .                       | 15         |
| 1.4 Relationen und Funktionen . . . . .                             | 20         |
| 1.5 Einige Ergänzungen zum Funktionsbegriff . . . . .               | 27         |
| 1.6 Übungsaufgaben . . . . .  | 30         |
| <b>2 Logische Grundlagen</b>  | <b>33</b>  |
| 2.1 Sprache und Ausdrucksweise der Mathematik . . . . .             | 33         |
| 2.2 Grundlagen der Aussagenlogik . . . . .                          | 35         |
| 2.3 Grundlagen der Prädikatenlogik . . . . .                        | 44         |
| 2.4 Die Grenzen des naiven Mengenbegriffs . . . . .                 | 54         |
| 2.5 Übungsaufgaben . . . . .  | 56         |
| <b>3 Allgemeine direkte Produkte und Datenstrukturen</b>            | <b>59</b>  |
| 3.1 Tupel, Folgen und Familien . . . . .                            | 59         |
| 3.2 Lineare Listen . . . . .  | 64         |
| 3.3 Knotenmarkierte Binäräbäume . . . . .                           | 70         |
| 3.4 Zur induktiven Definition von Mengen . . . . .                  | 76         |
| 3.5 Übungsaufgaben . . . . .  | 78         |
| <b>4 Mathematische Beweise</b>                                      | <b>81</b>  |
| 4.1 Direkte Beweise . . . . .                                       | 81         |
| 4.2 Indirekte Beweise . . . . .                                     | 83         |
| 4.3 Beweise durch Widerspruch . . . . .                             | 85         |
| 4.4 Induktionsbeweise . . . . .                                     | 90         |
| 4.5 Einige Hinweise zum Finden von Beweisen . . . . .               | 99         |
| 4.6 Übungsaufgaben . . . . .  | 110        |
| <b>5 Spezielle Funktionen</b>                                       | <b>113</b> |
| 5.1 Injektivität, Surjektivität und Bijektivität . . . . .          | 113        |
| 5.2 Kardinalitätsvergleich von Mengen . . . . .                     | 126        |
| 5.3 Wachstum spezieller Funktionen . . . . .                        | 134        |
| 5.4 Einige Bemerkungen zur Berechenbarkeit von Funktionen . . . . . | 144        |
| 5.5 Übungsaufgaben . . . . .  | 146        |
| <b>6 Spezielle Relationen und gerichtete Graphen</b>                | <b>149</b> |
| 6.1 Äquivalenzrelationen und Partitionen . . . . .                  | 149        |
| 6.2 Ordnungsrelationen und geordnete Mengen . . . . .               | 158        |
| 6.3 Grundbegriffe gerichteter Graphen . . . . .                     | 172        |
| 6.4 Einige Bemerkungen zu mehrstelligen Relationen . . . . .        | 185        |
| 6.5 Übungsaufgaben . . . . .  | 186        |

|   |            |
|---|------------|
| <b>7 Elementare Kombinatorik und ungerichtete Graphen</b>                 | <b>189</b> |
| 7.1 Fakultäten und Binomialkoeffizienten . . . . .                        | 189        |
| 7.2 Grundbegriffe ungerichteter Graphen . . . . .                         | 202        |
| 7.3 Dünne ungerichtete Graphen . . . . .                                  | 211        |
| 7.4 Einige Variationen des Graphenbegriffs . . . . .                      | 220        |
| 7.5 Übungsaufgaben . . . . .  | 222        |
| <b>8 Grundbegriffe algebraischer Strukturen</b>                           | <b>225</b> |
| 8.1 Homogene algebraische Strukturen . . . . .                            | 225        |
| 8.2 Strukturerhaltende Funktionen . . . . .                               | 236        |
| 8.3 Unterstrukturen . . . . .   | 243        |
| 8.4 Produkt- und Quotientenstrukturen . . . . .                           | 249        |
| 8.5 Der Körper der komplexen Zahlen . . . . .                             | 258        |
| 8.6 Einige Bemerkungen zu allgemeinen mathematischen Strukturen . . . . . | 266        |
| 8.7 Übungsaufgaben . . . . .  | 270        |
| <b>9 Einige Literaturhinweise</b>   | <b>273</b> |
| <b>Index</b>  | <b>277</b> |

# 1 Mengentheoretische Grundlagen

Die Mengenlehre ist ein Teilgebiet der Mathematik. Sie wurde vom deutschen Mathematiker Georg Cantor (1845-1918) etwa zwischen 1870 und 1900 begründet. Heutzutage baut die gesamte moderne und wissenschaftliche Mathematik, wenn sie formal axiomatisch betrieben wird, auf der axiomatischen Mengenlehre auf. Für Anfänger in der Mathematik ist ein **axiomatischer** Mengenbegriff sehr schwer zu verstehen. Deshalb wählen wir in diesem Kapitel einen, wie man sagt, **naiven** Zugang zu Mengen. Man spricht in diesem Zusammenhang auch von naiver Mengenlehre.

## 1.1 Der Cantorsche Mengenbegriff

Im Jahre 1885 formulierte Georg Cantor die folgende Definition einer Menge, die immer noch als Grundlage für eine naive Mengenlehre verwendet werden kann. Dabei verwenden wir erstmals das Zeichen „□“, um das Ende eines nummerierten Textstücks anzuseigen, das durch ein Schlüsselwort (wie „Definition“, „Beispiel“ oder „Satz“) eingeleitet wird.

### 1.1.1 Definition: Menge (G. Cantor)

Unter einer **Menge** verstehen wir jede Zusammenfassung  $M$  von bestimmten wohlunterschiedenen Objekten  $m$  unserer Anschauung oder unseres Denkens (welche die „Elemente“ von  $M$  genannt werden) zu einem Ganzen. □

Aus dieser Definition ergeben sich unmittelbar die folgenden drei Forderungen.

- (1) Wir müssen eine Schreibweise dafür festlegen, wie Objekte zu einer Menge zusammengefasst werden.
- (2) Wir müssen eine Notation festlegen, die besagt, ob ein Element zu einer Menge gehört oder nicht.
- (3) Da alle Objekte wohlunterschieden sein sollen, ist für alle Objekte festzulegen, wann sie gleich sind und wann sie nicht gleich sind.

Beginnen wir mit dem ersten der obigen drei Punkte. Dies führt zur Festlegung, wie Mengen dargestellt werden. Wir starten mit der einfachsten Darstellung.

### 1.1.2 Definition: explizite Darstellung

Die **explizite Darstellung** (oder **Aufzählungsform**) einer Menge ist dadurch gegeben, dass man ihre Elemente durch Kommata getrennt in Form einer Liste aufschreibt und diese dann mit den geschweiften Mengenklammern „{“ und „}“ einklammert. Jedes Element tritt in der Liste genau einmal auf. □

Die Reihenfolge des Auftretens der Elemente bei einer expliziten Darstellung einer Menge ist irrelevant. Etwa stellen  $\{1, 2, 3\}$  und  $\{2, 1, 3\}$  die gleiche Menge dar, nämlich diejenige, welche genau aus den drei Elementen 1, 2 und 3 besteht. Explizit kann man nur Mengen mit endlich vielen Elementen darstellen. Ist die Elementanzahl zu groß, so verwendet man oft drei Punkte „...“ als Abkürzung, wenn die Gesetzmäßigkeit, die sie abkürzen,

klar ist. Zu Vereinfachungszwecken werden die drei Punkte auch verwendet, um Mengen mit nicht endlich vielen Elementen explizit darzustellen. Dies ist mathematisch aber nur dann zulässig, wenn man diese Mengen auch anders darstellen könnte und die drei Punkte wirklich nur der Abkürzung und der Verbesserung der Lesbarkeit dienen. Beispielsweise bezeichnet so  $\{0, 2, 4, 6, \dots, 48, 50\}$  die Menge der geraden natürlichen Zahlen, welche kleiner oder gleich 50 sind,  $\{0, 2, 4, 6, \dots\}$  die Menge aller geraden natürlichen Zahlen und  $\{1, 3, 5, 7, \dots\}$  die Menge aller ungeraden natürlichen Zahlen.

### 1.1.3 Beispiele: explizite Darstellungen

Hier sind einige weitere Beispiele für explizite Darstellungen von Mengen

- (1) Die Menge  $\{1, 2, 3, 4\}$  besteht aus den vier Elementen 1, 2, 3 und 4.
- (2) Die Menge  $\{0, 2, 4, 6, \dots, 98, 100\}$  besitzt, wie man leicht nachzählt, genau 51 Elemente, nämlich die geraden natürlichen Zahlen von 0 bis 100.
- (3) Die Menge  $\{\heartsuit, \spadesuit, \heartsuit, \dagger\}$  besitzt drei Elemente, von denen wiederum zwei Mengen sind, nämlich  $\{\spadesuit\}$  und  $\{\heartsuit, \dagger\}$ .  $\square$

Um die zweite in der Mathematik gebräuchliche Darstellung von Mengen festlegen zu können, brauchen wir den folgenden Begriff einer (logischen) Aussage, der auf den antiken griechischen Philosophen Aristoteles (384-323 v. Chr.) zurückgeht.

### 1.1.4 Definition: Aussage (Aristoteles)

Eine **Aussage** ist ein sprachliches Gebilde, von dem es sinnvoll ist, zu sagen, es sei wahr oder falsch. Ist sie wahr, so sagt man auch, dass sie gilt, ist sie falsch, so sagt man auch, dass sie nicht gilt.  $\square$

Etwa ist „heute regnet es“ eine Aussage in der deutschen Sprache, und „Oxford is a town in the UK“ ist eine Aussage in der englischen Sprache. Manchmal kommen in Aussagen auch Platzhalter für Objekte vor, etwa „Person  $x$  studiert Informatik“. In diesem Zusammenhang spricht man dann oft präziser von **Aussageformen**. Im Weiteren werden wir uns auf Aussagen beschränken, die mit Mathematik zu tun haben, wie  $5 < 6$  (diese Aussage ist wahr) oder „8 ist eine Primzahl“ (diese Aussage ist falsch) oder  $x < 5$  (die Wahrheit dieser Aussage hängt davon ab, was man für den Platzhalter  $x$  setzt). Am letzten Beispiel sieht man, dass es bei einer Aussageform keinen Sinn ergibt, davon zu sprechen, sie sei wahr oder falsch. Vielmehr müssen alle darin vorkommenden Platzhalter entweder durch konkrete Objekte ersetzt werden oder durch Konzepte wie „für alle …“ und „es gibt …“ gebunden werden.

Neben den Mengen bilden Aussagen und das Argumentieren mit ihnen, also die Logik, das zweite Fundament der Mathematik. Dies behandeln wir im zweiten Kapitel genauer.

Wir werden im Folgenden Aussagen verwenden, von denen aus der Umgangssprache heraus nicht unbedingt sofort klar ist, wie sie gemeint sind. Daher müssen wir uns auf eine Lesart einigen (die Formalia dazu werden in Kapitel 2 nachgereicht). Bei Aussagen mit „oder“, etwa „Anna oder Martin studieren Informatik“ meinen wir immer das sogenannte

„einschließende oder“ und nicht das „entweder ... oder“. Der Satz von eben ist damit wahr, wenn nur Anna oder nur Martin oder beide Informatik studieren, und er ist falsch, wenn sowohl Anna als auch Martin nicht Informatik studieren. Ebenfalls uneindeutig sind Aussagen mit „wenn ... dann ...“ bzw. „aus ... folgt ...“, etwa „wenn Anna Informatik studiert, dann hat sie Physik als Nebenfach“. Wenn Anna tatsächlich Informatik studiert, dann entscheidet sich die Wahrheit der Aussage ganz klar daran, welches Nebenfach sie gewählt hat. Aber wie sieht es mit dem Wahrheitswert der Aussage aus, wenn Anna gar nicht Informatik studiert? Hier müssen wir uns wieder auf eine einheitliche Lesart einigen. Wir werden solche Aussagen wie ein Versprechen oder eine Wette interpretieren, die genau dann falsch wird, wenn wir das Versprechen gebrochen haben oder die Wette verloren haben. Liest man die Aussage oben nochmal so: „Ich verspreche Dir (Ich wette mit Dir): Wenn Anna Informatik studiert, dann hat sie Physik als Nebenfach“. Sollte Anna gar keine Informatikstudentin sein, dann haben wir das Versprechen nicht gebrochen (bzw. die Wette nicht verloren), in diesem Fall ist die Aussage also wahr (und zwar ganz unabhängig davon, ob Anna Physik als Nebenfach studiert oder nicht). Eine besondere Situation liegt vor, wenn für zwei Aussagen  $A_1$  und  $A_2$  die Wahrheitswerte gleich sind, also beide wahr oder beide falsch sind und nicht  $A_1$  wahr und  $A_2$  falsch oder  $A_1$  falsch und  $A_2$  wahr ist. Dann sagt man, dass  $A_1$  genau dann gilt, wenn  $A_2$  gilt, oder, dass  $A_1$  und  $A_2$  äquivalent (oder gleichwertig) sind.

### 1.1.5 Definition: deskriptive Mengenbeschreibung

Es sei  $A(x)$  eine Aussage, in der die Variable (Platzhalter für Objekte)  $x$  vorkommen kann, und für jedes Objekt  $a$  sei  $A(a)$  die Aussage, die aus  $A(x)$  entsteht, indem  $x$  durch  $a$  ersetzt wird. Dann bezeichnet  $\{x \mid A(x)\}$  die Menge, welche genau die Objekte  $a$  enthält, für die die Aussage  $A(a)$  wahr ist. Das Gebilde  $\{x \mid A(x)\}$  nennt man **deskriptive Darstellung** oder **deskriptive Mengenbeschreibung** oder **Beschreibungsform**.  $\square$

Es ist allgemein üblich, durch Schreibweisen wie  $A(x)$ ,  $A(x, y)$  usw. anzugeben, dass in einer Aussage Variablen vorkommen können. Mit den deskriptiven Darstellungen kann man, im Gegensatz zu den expliziten Darstellungen, auch ohne die (informellen) drei Punkte Mengen mit nicht endlich vielen Elementen formal durch endlich viele Zeichen angeben. Wir wollen dies nun an einem Beispiel zeigen.

### 1.1.6 Beispiele: deskriptive Mengenbeschreibungen

Es sei  $x$  eine Variable, die für irgendwelche natürlichen Zahlen Platzhalter sei. Dann ist beispielsweise eine Aussage  $A(x)$  gegeben durch die Formel

$$x^2 \leq 100.$$

Es gilt  $0^2 \leq 100$ , also  $A(0)$ , auch  $1^2 \leq 100$  gilt, also  $A(1)$ , usw. bis  $10^2 \leq 100$ , also  $A(10)$ . Hingegen sind die Aussagen  $A(11)$ ,  $A(12)$ ,  $A(13)$  usw. alle falsch. Also beschreibt die Mengendarstellung  $\{x \mid x \text{ ist natürliche Zahl und } x^2 \leq 100\}$  die Menge der natürlichen Zahlen von 0 bis 10. Man beachte, dass aufgrund der zusätzlichen Forderung in dieser deskriptiven Mengenbeschreibung nun  $x$  für beliebige Objekte steht.

Wieder sei nun  $x$  eine Variable, aber jetzt Platzhalter für alle ab dem Jahr 1000 lebenden Personen. Trifft die durch

„ $x$  studierte Informatik oder  $x$  studiert derzeit Informatik“

beschriebene Aussage  $A(x)$  auf Sie oder Ihre Eltern zu? Jedenfalls ist  $A(\text{Cantor})$  falsch, denn zu Cantors Lebzeiten gab es dieses Studienfach noch nicht.  $\square$

Aufgrund der eben geschilderten Einschränkungen des Platzhaltens ist es üblich, die Variablen zu typisieren, also zu sagen, für welche spezielleren Objekte sie Platzhalter sind. Wir kommen auf diesen Punkt später noch einmal zurück.

Nachdem wir den obigen Punkt (1) zufriedenstellend geklärt haben, wenden wir uns nun der Lösung von Punkt (2) zu, dem Enthaltensein in einer Menge.

### 1.1.7 Definition: Enthaltenseinssrelation

Es sei  $M$  eine Menge und  $a$  ein Objekt. Wir schreiben

- (1)  $a \in M$ , falls  $a$  zu  $M$  gehört, also ein Element von  $M$  ist.
- (2)  $a \notin M$ , falls  $a$  nicht zu  $M$  gehört, also kein Element von  $M$  ist.

Das Symbol „ $\in$ “ wird auch **Enthaltenseinssymbol** genannt und das Symbol „ $\notin$ “ seine Negation oder das **Nichtenthaltenseinssymbol**.  $\square$

Insbesondere gilt also für alle Objekte  $a$ , dass die Aussage  $a \in \{x \mid A(x)\}$  genau dann wahr ist, wenn die Aussage  $A(a)$  wahr ist. Damit wir uns im Folgenden mit den Beispielen leichter tun, erklären wir nun einige Mengen von Zahlen, die man von der weiterbildenden Schule her sicher schon kennt.

### 1.1.8 Definition: Zahlenmengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Die vier Symbole für Mengen  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  werden wie folgt festgelegt:

- (1)  $\mathbb{N}$  bezeichnet die Menge der natürlichen Zahlen, also die Menge  $\{0, 1, 2, \dots\}$ . Man beachte, dass in diesem Text (wie fast immer in der Informatik-Literatur) die Null per Definition in  $\mathbb{N}$  enthalten ist.
- (2)  $\mathbb{Z}$  bezeichnet die Menge der ganzen Zahlen, also die Menge  $\{0, 1, -1, 2, -2, \dots\}$  bestehend aus den natürlichen Zahlen und ihren Negationen.
- (3)  $\mathbb{Q}$  bezeichnet die Menge der rationalen Zahlen (der Bruchzahlen mit ganzzahligen Zählern und Nennern), also, in deskriptiver Darstellung, die Menge

$$\{x \mid \text{Es gibt } y, z \text{ mit } y \in \mathbb{Z} \text{ und } z \in \mathbb{Z} \text{ und } z \neq 0 \text{ und } x = \frac{y}{z}\}.$$

- (4)  $\mathbb{R}$  bezeichnet die Menge der reellen Zahlen.  $\square$

Die Menge der reellen Zahlen kann man nicht mehr so einfach spezifizieren wie die drei vorhergehenden Mengen von Zahlen. Wir verweisen hier auf Analysis-Bücher, in welchen normalerweise die reellen Zahlen mathematisch formal eingeführt werden, beispielsweise

durch die Forderung von geeigneten Eigenschaften oder durch ein konstruktives Vorgehen. Trotzdem werden wir die Menge  $\mathbb{R}$  im Folgenden bei Beispielen immer wieder verwenden und setzen dabei ein intuitives Verständnis reeller Zahlen voraus, wie es in der weiterbildenden Schule gelehrt wird.

Durch das Symbol „ $\in$ “ kann man bei der deskriptiven Darstellung von Mengen auch die Beschränktheit bei den zur Aussonderung zugelassenen Objekte durch das Enthaltensein in einer anderen Menge beschreiben. In Beispiel 1.1.6 können wir nun einfacher  $\{x \mid x \in \mathbb{N} \text{ und } x^2 \leq 100\}$  schreiben. Dies kürzt man normalerweise zu  $\{x \in \mathbb{N} \mid x^2 \leq 100\}$  ab. Damit wird  $x$  eine typisierte Variable in dem schon früher erwähnten Sinn. Als Verallgemeinerung des Beispiels legen wir folgendes fest.

### 1.1.9 Festlegung: deskriptive Darstellung mit Typisierung

Für alle Mengen  $M$  und alle Aussagen  $A(x)$ , in denen  $x$  eine Variable ist, stellt die deskriptive Darstellung  $\{x \in M \mid A(x)\}$  eine Abkürzung für  $\{x \mid x \in M \text{ und } A(x)\}$  dar.  $\square$

Eine Voraussetzung der Mengenlehre ist, dass alle Objekte wohlunterschieden sind. Wir schreiben  $a = b$ , falls die Objekte  $a$  und  $b$  gleich sind, und  $a \neq b$ , falls sie verschieden sind. Bei Zahlen wissen wir, was  $a = b$  und  $a \neq b$  bedeuten. Da wir nun Mengen als neue Objekte hinzubekommen haben, denn sie dürfen ja wieder in Mengen als Elemente vorkommen, müssen wir, man vergleiche mit Punkt (3) nach der Definition von Mengen, als Nächstes festlegen, was die Aussage  $M = N$  für zwei Mengen bedeutet, also wann sie wahr und wann sie falsch ist. In der folgenden Definition führen wir, neben  $M = N$ , für Mengen noch drei weitere Aussagen  $M \subseteq N$ ,  $M \neq N$  und  $M \subset N$  ein.

### 1.1.10 Definition: Inklusion, echte Inklusion, Gleichheit

Es seien  $M$  und  $N$  zwei Mengen. Dann gilt

- (1)  $M \subseteq N$  genau dann, wenn für alle Objekte  $a$  aus  $a \in M$  folgt  $a \in N$  ( $M$  heißt dann eine **Teilmenge** von  $N$ ),
- (2)  $M = N$  genau dann, wenn  $M \subseteq N$  und  $N \subseteq M$  gelten, also für alle Objekte  $a$  die Aussage  $a \in M$  genau dann gilt, wenn  $a \in N$  gilt ( $M$  und  $N$  heißen dann **gleich**),
- (3)  $M \neq N$  genau dann, wenn  $M = N$  nicht gilt ( $M$  und  $N$  heißen dann **ungleich**),
- (4)  $M \subset N$  genau dann, wenn  $M \subseteq N$  und  $M \neq N$  gelten ( $M$  heißt dann eine **echte Teilmenge** von  $N$ ).

Ist die Menge  $M$  eine (echte) Teilmenge der Menge  $N$ , so sagt man auch, dass  $M$  in  $N$  (echt) enthalten ist.  $\square$

Das Symbol „ $\subseteq$ “ heißt auch **Mengeninklusion**. Es ist, wie das Gleichheitssymbol „ $=$ “, das Ungleichsymbol „ $\neq$ “ und die **echte Mengeninklusion** „ $\subset$ “ eine Testoperation auf Mengen, da die Konstruktionen  $M \subseteq N$ ,  $M = N$ ,  $M \neq N$  und  $M \subset N$  alle Aussagen im früher eingeführten Sinn darstellen, also entweder wahr oder falsch sind. Statt  $M \subseteq N$  schreibt man auch  $N \supseteq M$ , wenn etwa bei einer Rechnung die Mengen in der „falschen“ Reihenfolge auftauchen. Analog schreibt man statt  $M \subset N$  auch  $N \supset M$ .

### 1.1.11 Satz: Reflexivität, Antisymmetrie, Transitivität

Für alle Mengen  $M, N$  und  $P$  gelten die folgenden Aussagen:

- (1)  $M \subseteq M$  (Reflexivität)
- (2) Aus  $M \subseteq N$  und  $N \subseteq M$  folgt  $M = N$  (Antisymmetrie)
- (3) Aus  $M \subseteq N$  und  $N \subseteq P$  folgt  $M \subseteq P$  (Transitivität)

**Beweis:** (1) Die Aussage  $M \subseteq M$  gilt genau dann, wenn für alle Objekte  $a$  aus  $a \in M$  folgt  $a \in M$ . Letzteres ist wahr, also ist auch  $M \subseteq M$  wahr.

(2) Hier verwenden wir, dass die Gültigkeit der zwei Aussagen  $M \subseteq N$  und  $N \subseteq M$  per Definition sogar zur Gültigkeit der Aussage  $M = N$  äquivalent (d.h. logisch gleichwertig) ist. Also folgt insbesondere  $M = N$  aus  $M \subseteq N$  und  $N \subseteq M$ .

(3) Es gelte  $M \subseteq N$  und auch  $N \subseteq P$ . Dann trifft für alle Objekte  $a$  das Folgende zu: Aus  $a \in M$  folgt  $a \in N$ , weil  $M \subseteq N$  wahr ist, also auch  $a \in P$ , weil  $N \subseteq P$  wahr ist. Dies zeigt  $M \subseteq P$ .  $\square$

Dieses ist der erste Beweis des vorliegenden Texts. Es werden noch viele weitere folgen. Durch die Markierungen (1) bis (3) im Beweis von Satz 1.1.11 ist angezeigt, welche der Behauptungen gerade bewiesen wird. Solche selbsterklärenden Markierungen werden wir später ohne weitere Kommentare immer wieder verwenden.

Per Definition gibt es genau eine Menge, die keine Elemente enthält. Diese wird nun eingeführt und mit einem speziellen Symbol bezeichnet.

### 1.1.12 Definition: leere Menge

Mit  $\emptyset$  wird die **leere Menge** bezeichnet. Sie ist diejenige Menge, die keine Elemente enthält. Also gilt  $a \notin \emptyset$  für alle Objekte  $a$ .  $\square$

Bei der expliziten Darstellung von Mengen haben wir die Elemente aufgezählt und mit den Mengenklammern geklammert. Wenn man diese Darstellung auf die leere Menge überträgt, dann stehen zwischen den Mengenklammern gar keine Elemente. Deshalb wird in der Literatur auch oft „{}“ als Symbol für die leere Menge verwendet. Man beachte, dass  $\{\emptyset\}$  nicht die leere Menge ist, sondern diejenige Menge, welche die leere Menge als ihr einziges Element enthält.

Bei Aussagen ist es sehr nützlich, eine Aussage zur Verfügung zu haben, welche immer falsch ist. Im Folgenden sei diese mit **falsch** bezeichnet. Beispielsweise könnte man **falsch** als Abkürzung (oder andere Schreibweise) für  $1 \neq 1$  auffassen. Mit dieser Festlegung gilt  $\emptyset = \{x \mid \text{falsch}\}$ . Weiterhin gilt  $\emptyset \subseteq M$  für alle Mengen  $M$ , denn für alle Objekte  $a$  ist  $a \in \emptyset$  falsch und aus einer falschen Aussage kann man alle Aussagen folgern (wurde schon angemerkt und wird in Kapitel 2 bei der formalen Definition der Implikation explizit gezeigt), also auch  $a \in M$ . Weil wir sie später auch brauchen, definieren wir mit **wahr** die immer wahre Aussage. Sie ist die Negation der Aussage **falsch**. Wir beschließen

diesen Abschnitt mit einem Beispiel zu den Begriffen aus Definition 1.1.10 und einigen Folgerungen.

### 1.1.13 Beispiele: Inklusion, Gleichheit

Wir betrachten die beiden Mengen  $\{1, 2, 3\}$  und  $\{1, 2, 3, 4\}$  mit den drei Elementen 1, 2 und 3 bzw. den vier Elementen 1, 2, 3 und 4. Es gelten dann sowohl die Inklusion

$$\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$$

als auch die echte Inklusion

$$\{1, 2, 3\} \subset \{1, 2, 3, 4\}$$

als auch die Ungleichung (oder Ungleichheit)

$$\{1, 2, 3\} \neq \{1, 2, 3, 4\}.$$

Die Gleichung (oder Gleichheit) dieser Mengen gilt hingegen nicht. Weiterhin gilt etwa die Inklusions-Eigenschaft

$$\{x \in \mathbb{N} \mid x \neq 2 \text{ und } x \text{ Primzahl}\} \subseteq \{x \in \mathbb{N} \mid x \text{ ungerade}\},$$

weil alle Primzahlen ungleich 2 ungerade natürliche Zahlen sind. Auch hier liegt eine echte Inklusion vor.  $\square$

Allgemein gelten die folgenden zwei wichtigen Eigenschaften, die wir immer wieder verwenden werden: Folgt für alle Objekte  $a$  die Aussage  $A_2(a)$  aus der Aussage  $A_1(a)$ , so gilt  $\{x \mid A_1(x)\} \subseteq \{x \mid A_2(x)\}$ , und gilt für alle Objekte  $a$  die Aussage  $A_1(a)$  genau dann, wenn die Aussage  $A_2(a)$  gilt, so gilt  $\{x \mid A_1(x)\} = \{x \mid A_2(x)\}$ . Die Leserin oder der Leser überlege sich, wie man in analoger Weise zeigen kann, dass die Ungleichheit  $\{x \mid A_1(x)\} \neq \{x \mid A_2(x)\}$  von Mengen gilt.

## 1.2 Einige Konstruktionen auf Mengen

Bisher können wir nur Mengen definieren – explizit oder deskriptiv – und sie dann vergleichen oder, allgemeiner, logische Aussagen über Mengen formulieren. Nun führen wir gewisse Konstruktionen (auch Operationen genannt) auf Mengen ein, die es erlauben, aus gegebenen Mengen neue zu erzeugen. Dies führt zu einer weiteren Darstellung von Mengen, nämlich durch sogenannte Mengenausdrücke, in denen diese Konstruktionen auf vorgegebene Mengen angewendet werden.

### 1.2.1 Definition: binäre Vereinigung, binärer Durchschnitt, Differenz

Es seien  $M$  und  $N$  Mengen. Dann definieren wir die folgenden Mengen:

- (1)  $M \cup N := \{x \mid x \in M \text{ oder } x \in N\}$
- (2)  $M \cap N := \{x \mid x \in M \text{ und } x \in N\}$
- (3)  $M \setminus N := \{x \mid x \in M \text{ und } x \notin N\}$

Die Konstruktion  $M \cup N$  heißt **Vereinigung** von  $M$  und  $N$ , bei  $M \cap N$  spricht man vom **Durchschnitt** von  $M$  und  $N$  und  $M \setminus N$  ist die **Differenz** von  $M$  und  $N$ .  $\square$

In der obigen Definition bezeichnet das spezielle Symbol „:=“ die **definierende Gleichheit**. Durch deren Verwendung wird ausgedrückt, dass – per Definition – die linke Seite der entsprechenden Gleichung gleich der rechten Seite ist. Definierende Gleichheiten werden in der Mathematik insbesondere dazu benutzt, neue Konstruktionen, neue Symbole, Abkürzungen oder Namen für gewisse Dinge einzuführen.

Setzt man die in der obigen Definition eingeführten Konstruktionen auf Mengen (bzw. die sie realisierenden Operationen „ $\cup$ “, „ $\cap$ “ und „ $\setminus$ “ auf Mengen) mit dem Enthalteinsymbol „ $\in$ “ in Beziehung, so gilt offensichtlich  $x \in M \cup N$  genau dann, wenn  $x \in M$  gilt oder  $x \in N$  gilt, es gilt  $x \in M \cap N$  genau dann, wenn  $x \in M$  und  $x \in N$  gelten, und es gilt  $x \in M \setminus N$  genau dann, wenn  $x \in M$  gilt und  $x \in N$  nicht gilt. Für die deskriptiven Darstellungen von Mengen mittels Aussagen  $A_1(x)$  und  $A_2(x)$  hat man die Gleichung

$$\{x \mid A_1(x)\} \cup \{x \mid A_2(x)\} = \{x \mid A_1(x) \text{ oder } A_2(x)\}$$

für die Vereinigung solcher Mengen,

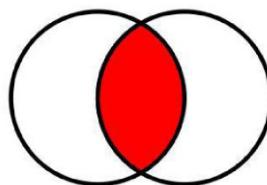
$$\{x \mid A_1(x)\} \cap \{x \mid A_2(x)\} = \{x \mid A_1(x) \text{ und } A_2(x)\}$$

für den Durchschnitt solcher Mengen und

$$\{x \mid A_1(x)\} \setminus \{x \mid A_2(x)\} = \{x \mid A_1(x) \text{ und nicht } A_2(x)\}$$

für die Differenz solcher Mengen. In der letzten Darstellung besagt die Notation der rechten Seite, dass die Aussage  $A_1(x)$  gilt und die Aussage  $A_2(x)$  nicht gilt.

Die eben eingeführten drei Konstruktionen auf Mengen kann man anschaulich sehr gut mit eingefärbten oder schraffierten Bereichen in der Zeichenebene darstellen. Diese Zeichnungen nennt man auch **Venn-Diagramme**. Der Name geht auf den englischen Mathematiker John Venn (1834-1923) zurück. In solchen Venn-Diagrammen sind die Mengen durch umrandete Flächen dargestellt, in der Regel sind die Umrandungen dabei Kreise oder Ellipsen. Bei vielen Mengen sind aber auch beliebige geschlossene Kurven als Umrandungen vorteilhaft. Das folgende Bild zeigt das Venn-Diagramm des Durchschnitts  $M \cap N$  zweier Mengen  $M$  und  $N$ . Hier werden  $M$  und  $N$  durch Kreisflächen dargestellt und ihr Durchschnitt durch die eingefärbte Fläche.



Analog kann man auch  $M \cup N$  mittels Kreisflächen darstellen, wo die gesamte Fläche eingefärbt ist, und auch  $M \setminus N$ , wo der Teil der  $M$  darstellenden Kreisfläche eingefärbt

ist, der nicht zu der  $N$  darstellenden Kreisfläche gehört. Solche anschaulichen Bilder sind natürlich nicht als Beweise erlaubt. Sie sind jedoch sehr hilfreich, wenn es darum geht, Sachverhalte zu visualisieren und neue Eigenschaften zu entdecken. Diese Bemerkung gilt im Allgemeinen für die Verwendung von Bildern in der Mathematik.

Statt  $M \setminus N$  wird manchmal auch  $\mathbf{C}_M N$  geschrieben und man sagt dann auch „Komplement von  $N$  bezüglich  $M$ “. Es gibt viele Situationen, wo die Menge  $M$  fixiert ist, sich alle Überlegungen also in ihr abspielen. Man nennt  $M$  dann auch das (derzeitig verwendete) **Universum**. Ist  $N$  dann eine Teilmenge des Universums  $M$ , so spricht man bei  $M \setminus N$  auch vom (absoluten) **Komplement** von  $N$  und schreibt dafür in der Regel  $\overline{N}$  (oder manchmal auch  $N^c$ ).

### 1.2.2 Beispiele: Vereinigung, Durchschnitt, Differenz

Wir betrachten die folgenden Mengen

$$M := \{0, 2, 4\} \quad N := \{x \in \mathbb{N} \mid x \leq 10\}$$

Dann gelten offensichtlich die folgenden Gleichungen.

- (1)  $M \cup N = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = N$
- (2)  $M \cap N = \{0, 2, 4\} = M$
- (3)  $N \setminus M = \{1, 3, 5, 6, 7, 8, 9, 10\}$
- (4)  $M \setminus N = \emptyset$

Um  $M \cup N$  „auszurechnen“, schreibt man erst die Elemente von  $M$  als Liste hin. Dann geht man  $N$  Element für Element durch und fügt jene Elemente an die Liste an, die nicht in  $M$  vorkommen. Analoge Verfahrensweisen überlege sich die Leserin oder der Leser auch für den Durchschnitt und die Differenz.  $\square$

Zwischen Inklusion, Vereinigung und Durchschnitt von Mengen besteht ein enger Zusammenhang. Er war schon im letzten Beispiel ersichtlich und wird im folgenden Satz explizit angegeben.

### 1.2.3 Satz: Inklusion, Vereinigung, Durchschnitt

Für alle Mengen  $M$  und  $N$  sind die folgenden drei Aussagen äquivalent:

- (1)  $M \subseteq N$
- (2)  $M \cap N = M$
- (3)  $M \cup N = N$

**Beweis:** Wir beweisen zuerst, dass aus der Aussage (1) die Aussage (2) folgt. Dazu haben wir die beiden Inklusionen  $M \cap N \subseteq M$  und  $M \subseteq M \cap N$  zu zeigen.

Beweis von  $M \cap N \subseteq M$ : Es sei  $a$  ein beliebiges Objekt. Gilt  $a \in M \cap N$ , so gilt dies

genau dann, wenn  $a \in M$  und  $a \in N$  gelten. Also gilt insbesondere  $a \in M$ .

Beweis von  $M \subseteq M \cap N$ : Es sei wiederum  $a$  ein beliebiges Objekt. Gilt  $a \in M$ , so gilt auch  $a \in N$  wegen der Voraussetzung  $M \subseteq N$ . Also gelten die beiden Aussagen  $a \in M$  und  $a \in N$  und dies ist gleichwertig zur Gültigkeit von  $a \in M \cap N$ .

Nun zeigen wir die Umkehrung, also wie (1) aus (2) folgt. Es sei  $a$  ein beliebiges Objekt. Gilt  $a \in M$ , so ist dies äquivalent zu  $a \in M \cap N$ , da wir  $M = M \cap N$  voraussetzen. Aus  $a \in M \cap N$  folgt insbesondere  $a \in N$ .

Die Aussagen „aus (1) folgt (3)“ und „aus (3) folgt (1)“ zeigt man vollkommen analog. Damit sind auch (1) und (3) äquivalent und die Äquivalenz von (1) und (2) und von (1) und (3) zeigt die Äquivalenz von (2) und (3).  $\square$

Bei diesem Beweis haben wir schon etwas an logischen Schlüssen verwendet, nämlich, dass für beliebige Aussagen  $A_1, A_2, A_3$  die folgenden Eigenschaften gelten:

- (1) Folgt  $A_2$  aus  $A_1$  und  $A_1$  aus  $A_2$ , so sind  $A_1$  und  $A_2$  äquivalent.
- (2) Sind  $A_1$  und  $A_2$  äquivalent und  $A_2$  und  $A_3$  äquivalent, so sind auch  $A_1$  und  $A_3$  äquivalent.
- (3) Aus  $A_1$  und  $A_2$  folgt  $A_1$ .

Dass diese logischen Schlüsse korrekt sind, werden wir im nächsten Kapitel zeigen. Der Beweis von Satz 1.2.3 wurde, wie auch der von Satz 1.1.11, im Hinblick auf die logischen Zusammenhänge und Folgerungen noch in normaler Umgangssprache abgefasst. Wenn wir im zweiten Kapitel die formale Sprache der mathematischen Logik eingeführt haben, dann werden die Beweise diese mathematische „Kunstsprache“ mit verwenden, um Teile der Umgangssprache zu ersetzen. Solche Beweise werden dann in der Regel wesentlich knapper und prägnanter und verwenden die logischen Regeln auch besser erkennbar. Im folgenden Satz stellen wir einige weitere wichtige Regeln für die Vereinigung und den Durchschnitt von Mengen vor. Die Eigenschaften in (1) nennt man Kommutativität, die in (2) Assoziativität, die in (3) Distributivität und die in (5) Monotonie. Weil in (4) eine Menge im Sinne des Enthalteins zwischen zwei Mengen liegt, nennt man dies auch oft eine Einschließungseigenschaft.

#### 1.2.4 Satz: Kommutativität, Assoziativität, Distributivität

Für alle Mengen  $M, N$  und  $P$  gelten die folgenden Aussagen:

- (1)  $M \cup N = N \cup M$  und  $M \cap N = N \cap M$
- (2)  $M \cup (N \cup P) = (M \cup N) \cup P$  und  $M \cap (N \cap P) = (M \cap N) \cap P$
- (3)  $M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$  und  $M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$
- (4)  $M \cap N \subseteq M \subseteq M \cup N$
- (5)  $M \subseteq N$  impliziert  $M \cup P \subseteq N \cup P$  und  $M \cap P \subseteq N \cap P$

**Beweis:** (1) Es gilt

$$\begin{aligned}
 M \cup N &= \{x \mid x \in M \text{ oder } x \in N\} && \text{Definition } \cup \\
 &= \{x \mid x \in N \text{ oder } x \in M\} && \text{Eigenschaft „oder“} \\
 &= N \cup M && \text{Definition } \cup
 \end{aligned}$$

und analog zeigt man auch die Aussage  $M \cap N = N \cap M$ .

(2) Hier bekommen wir die erste Gleichung durch die Rechnung

$$\begin{aligned}
 M \cup (N \cup P) &= \{x \mid x \in M \text{ oder } x \in N \cup P\} && \text{Definition } \cup \\
 &= \{x \mid x \in M \text{ oder } x \in N \text{ oder } x \in P\} && \text{Definition } \cup \\
 &= \{x \mid x \in M \cup N \text{ oder } x \in P\} && \text{Definition } \cup \\
 &= (M \cup N) \cup P && \text{Definition } \cup
 \end{aligned}$$

und die zweite Gleichung beweist sich ebenfalls analog.

Die verbleibenden Aussagen (3) bis (5) beweist man ebenfalls, indem man einige sehr einfache logische Eigenschaften von „und“ und „oder“ verwendet.  $\square$

Beim Beweis von (1) haben wir benutzt, dass „oder“ kommutativ ist, und beim Beweis von (2) haben wir verwendet, dass „oder“ assoziativ ist. Die Kommutativität bedeutet, dass „ $A_1$  oder  $A_2$ “ und „ $A_2$  oder  $A_1$ “ äquivalent sind. Die Assoziativität bedeutet, dass es im Fall einer Aussage „ $A_1$  oder  $A_2$  oder  $A_3$ “ egal ist, ob man zuerst „ $A_1$  oder  $A_2$ “ zu einer Aussage  $B$  zusammenfasst und dann „ $B$  oder  $A_3$ “ betrachtet, oder zuerst „ $A_2$  oder  $A_3$ “ zu einer Aussage  $B$  zusammenfasst und dann „ $A_1$  oder  $B$ “ betrachtet. Beides führt zum selben Resultat. Auch „und“ ist kommutativ und assoziativ. Dies folgt alles sofort aus unserem naiven Verständnis dieser logischen Verknüpfungen.

Wegen der Gleichungen aus Teil (2) dieses Satzes kommt es bei der Vereinigung und dem Durchschnitt von mehr als zwei Mengen nicht darauf an, in welcher Art man diese „aufbaut“. Etwa kann man  $M_1, M_2, M_3, M_4$  durch  $M_1 \cup (M_2 \cup (M_3 \cup M_4))$  als auch durch  $(M_1 \cup M_2) \cup (M_3 \cup M_4)$  vereinigen. Beides liefert die gleiche Menge. Deshalb lässt man die Klammerung weg, schreibt also  $M_1 \cup M_2 \cup M_3 \cup M_4$ . Dies ist die gleiche Menge wie etwa  $M_4 \cup M_2 \cup M_3 \cup M_1$ , denn Teil (1) des obigen Satzes sagt aus, dass die Reihenfolge keine Rolle spielt.

Bisher können wir nur endlich viele Mengen vereinigen und deren Durchschnitte bilden (man sagt hier auch kurz „schneiden“), indem wir alles auf die Vereinigung und den Durchschnitt von zwei Mengen zurückführen. Nun erweitern wir dieses auf beliebig viele Mengen, d.h. auf Mengen von Mengen.

### 1.2.5 Definition: beliebige Vereinigung und beliebiger Durchschnitt

Es sei  $\mathcal{M}$  eine Menge von Mengen. Wir definieren zwei Mengen  $\bigcup \mathcal{M}$  und  $\bigcap \mathcal{M}$  durch die Festlegungen

$$(1) \quad \bigcup \mathcal{M} := \{x \mid \text{Es gibt } X \in \mathcal{M} \text{ mit } x \in X\}$$

$$(2) \cap \mathcal{M} := \{x \mid \text{Für alle } X \in \mathcal{M} \text{ gilt } x \in X\}$$

und nennen die Konstruktionen  $\cup \mathcal{M}$  und  $\cap \mathcal{M}$  die **Vereinigung** bzw. den **Durchschnitt** aller Mengen von  $\mathcal{M}$  (oder kürzer: beliebige Vereinigung und beliebigen Durchschnitt).  $\square$

Manchmal schreibt man auch  $\bigcup_{X \in \mathcal{M}} X$  und  $\bigcap_{X \in \mathcal{M}} X$  für  $\cup \mathcal{M}$  bzw.  $\cap \mathcal{M}$ . Wir bleiben aber bei den kürzeren Schreibweisen der obigen Definition. Offensichtlich gelten die Gleichungen  $\cup\{M, N\} = M \cup N$  und  $\cap\{M, N\} = M \cap N$  im Fall von  $\mathcal{M} = \{M, N\}$ , und damit ist die neue Definition der beliebigen Vereinigungen und Durchschnitte eine Erweiterung der ursprünglichen nur binären (bzw. endlichen) Vereinigungen und Durchschnitte.

Für diese neuen beliebigen Vereinigungen und Durchschnitte übertragen sich alle Eigenschaften von Satz 1.2.4 (3) bis (5), wenn man die Notation entsprechend anpasst. Wir zeigen dies am Beispiel von Punkt (4).

### 1.2.6 Satz: Einschließungseigenschaft

Es sei  $\mathcal{M}$  eine Menge von Mengen mit  $\mathcal{M} \neq \emptyset$ . Dann gilt für alle  $M \in \mathcal{M}$  die Einschließungseigenschaft  $\cap \mathcal{M} \subseteq M \subseteq \cup \mathcal{M}$ .

**Beweis:** Erste Inklusion: Es sei  $a$  ein beliebiges Objekt. Gilt  $a \in \cap \mathcal{M}$ , so gilt  $a \in X$  für alle  $X \in \mathcal{M}$ . Folglich gilt auch  $a \in M$ , da  $M \in \mathcal{M}$  vorausgesetzt ist.

Zweite Inklusion: Wiederum sei  $a$  beliebig vorgegeben. Gilt  $a \in M$ , so gibt es ein  $X \in \mathcal{M}$ , nämlich  $X := M$ , mit  $a \in X$ . Also gilt per Definition  $a \in \cup \mathcal{M}$ .

Später werden wir noch lernen, dass eine Aussage der Form „für alle  $a \in \emptyset$  gilt ...“ immer wahr ist. Damit gilt die Einschließungseigenschaft auch für  $\mathcal{M}$  als die leere Menge (von Mengen). Man kann beliebige Vereinigungen und Durchschnitte in einer speziellen Weise beschreiben. Dies wird nun gezeigt.

### 1.2.7 Satz: rekursives Vereinigen und Schneiden

Es sei  $\mathcal{M}$  eine Menge von Mengen. Dann gelten, falls  $\mathcal{M} \neq \emptyset$  zutrifft, für alle Mengen  $M \in \mathcal{M}$  die folgenden Gleichungen:

$$(1) \cup \mathcal{M} = M \cup \cup(\mathcal{M} \setminus \{M\})$$

$$(2) \cap \mathcal{M} = M \cap \cap(\mathcal{M} \setminus \{M\})$$

Weiterhin gilt im Fall der leeren Menge von Mengen die Eigenschaft  $\cup \emptyset = \emptyset$ .

**Beweis:** Wir beginnen mit Aussage (1) und zeigen hier zuerst die Inklusion „ $\subseteq$ “: Es sei  $a$  ein beliebiges Objekt mit  $a \in \cup \mathcal{M}$ . Dann gibt es  $X_0 \in \mathcal{M}$  mit  $a \in X_0$ . Nun unterscheiden wir zwei Fälle:

- (a) Es gelte  $X_0 = M$ . Dann gilt auch  $a \in M$  und daraus folgt  $a \in M \cup \cup(\mathcal{M} \setminus \{M\})$ .
- (b) Es gelte  $X_0 \neq M$ . Dann gilt  $X_0 \in \mathcal{M} \setminus \{M\}$ . Folglich gibt es eine Menge  $X$  mit  $X \in \mathcal{M} \setminus \{M\}$ , nämlich  $X := X_0$ , mit  $a \in X$ . Dies zeigt, dass  $a \in \cup(\mathcal{M} \setminus \{M\})$  gilt und somit gilt auch die Aussage  $a \in M \cup \cup(\mathcal{M} \setminus \{M\})$ .

Wir kommen zum Beweis der verbleibenden Inklusion „ $\supseteq$ “: Es sei ein beliebiges Objekt  $a$  mit  $a \in M \cup \bigcup(\mathcal{M} \setminus \{M\})$  vorgegeben. Dann gilt  $a \in M$  oder es gilt  $a \in \bigcup(\mathcal{M} \setminus \{M\})$ . Wir unterscheiden wiederum zwei Fälle:

- (a) Es gelte  $a \in M$ . Da  $M \in \mathcal{M}$  gilt, gibt es also ein  $X \in \mathcal{M}$ , nämlich  $X := M$ , mit  $a \in X$ . Dies zeigt  $a \in \bigcup \mathcal{M}$ .
- (b) Es gelte  $a \in \bigcup(\mathcal{M} \setminus \{M\})$ . Dann gibt es ein  $X \in \mathcal{M} \setminus \{M\}$  mit  $a \in X$ . Für dieses  $X$  gilt natürlich auch  $X \in \mathcal{M}$ . Folglich haben wir wiederum  $a \in \bigcup \mathcal{M}$ .

Die Gleichung (2) zeigt man analog zum Beweis von (1).

Die verbleibende Gleichung folgt aus der Tatsache, dass es kein  $X \in \emptyset$  gibt, also auch kein  $X \in \emptyset$  mit  $x \in X$ . Daraus folgt nämlich

$$\bigcup \emptyset = \{x \mid \text{Es gibt } X \in \emptyset \text{ mit } x \in X\} = \{x \mid \text{falsch}\} = \emptyset.$$

□

Um auch  $\bigcap \emptyset$  bestimmen zu können, muss man annehmen, dass alle betrachteten Objekte aus einer festgelegten Menge  $M$  sind, also  $M$  ein Universum ist. Dann bekommt man die Eigenschaft  $\bigcap \emptyset = M$ . Genauer können wir auf dies aber hier noch nicht eingehen.

Es wurde schon bemerkt, dass man endliche Vereinigungen und Durchschnitte schrittweise auf die binären Vereinigungen und Durchschnitte zurückführen kann. Wir führen nun formal entsprechende Notationen ein, fassen dabei aber die endlichen Vereinigungen und Durchschnitte als Spezialfälle von beliebigen Vereinigungen und Durchschnitten auf.

### 1.2.8 Definition: indizierte Vereinigung und indizierter Durchschnitt

Für eine endliche und nichtleere Menge  $\mathcal{M}$  von  $n$  Mengen mit der expliziten Darstellung  $\mathcal{M} = \{M_1, \dots, M_n\}$  definieren wir:

$$(1) \quad \bigcup_{i=1}^n M_i := \bigcup \{M_1, \dots, M_n\}$$

$$(2) \quad \bigcap_{i=1}^n M_i := \bigcap \{M_1, \dots, M_n\}$$

□

Aus der Definition 1.2.8 und Satz 1.2.7 folgen dann sofort die folgenden Eigenschaften:

$$(1) \quad \bigcup_{i=1}^1 M_i = \bigcap_{i=1}^1 M_i = M_1$$

$$(2) \quad \bigcup_{i=1}^n M_i = M_n \cup \bigcup_{i=1}^{n-1} M_i, \text{ falls } n > 1.$$

$$(3) \quad \bigcap_{i=1}^n M_i = M_n \cap \bigcap_{i=1}^{n-1} M_i, \text{ falls } n > 1.$$

Mit diesen Gleichungen kann man, etwa durch ein entsprechendes Programm, sofort endliche Vereinigungen und Durchschnitte von Mengen berechnen.

Zum Schluss dieses Abschnitts betrachten wir nun noch Eigenschaften der Differenz von Mengen. Hier sind die drei wichtigsten Eigenschaften. Man verdeutlicht sich diese auch anhand von Venn-Diagrammen.

### 1.2.9 Satz: Eigenschaften der Mengendifferenz

Für alle Mengen  $M, N$  und  $P$  gelten die folgenden Aussagen:

- (1)  $M \setminus (N \cup P) = (M \setminus N) \cap (M \setminus P)$
- (2)  $M \setminus (N \cap P) = (M \setminus N) \cup (M \setminus P)$
- (3)  $M \setminus (M \setminus N) = M \cap N$

**Beweis:** Die Gleichung (1) zeigt man wie folgt, wobei wir im zweiten Schritt als logische Eigenschaft verwenden, dass ein Objekt genau dann nicht ein Element einer Vereinigung ist, wenn es in keiner der beiden Mengen enthalten ist:

$$\begin{aligned} M \setminus (N \cup P) &= \{x \mid x \in M \text{ und } x \notin N \cup P\} \\ &= \{x \mid x \in M \text{ und } x \notin N \text{ und } x \notin P\} \\ &= \{x \mid x \in M \text{ und } x \notin N \text{ und } x \in M \text{ und } x \notin P\} \\ &= \{x \mid x \in M \text{ und } x \notin N\} \cap \{x \mid x \in M \text{ und } x \notin P\} \\ &= (M \setminus N) \cap (M \setminus P) \end{aligned}$$

Hier ist der Beweis von Gleichung (2), bei dem für das dritte Gleichheitszeichen eine weitere einfache logische Eigenschaft verwendet wird, die wir später in Kapitel 2 mittels Formeln genau beschreiben werden.

$$\begin{aligned} M \setminus (N \cap P) &= \{x \mid x \in M \text{ und } x \notin N \cap P\} \\ &= \{x \mid x \in M \text{ und } (x \notin N \text{ oder } x \notin P)\} \\ &= \{x \mid (x \in M \text{ und } x \notin N) \text{ oder } (x \in M \text{ und } x \notin P)\} \\ &= \{x \mid x \in M \text{ und } x \notin N\} \cup \{x \mid x \in M \text{ und } x \notin P\} \\ &= (M \setminus N) \cup (M \setminus P) \end{aligned}$$

Der verbleibende Beweis von Gleichung (3) ist von ähnlicher Schwierigkeit wie die bisher gezeigten zwei Beweise. Er sei deshalb der Leserin oder dem Leser als Übungsaufgabe gestellt.  $\square$

Wir erinnern nun an das (absolute) Komplement  $\overline{N}$  von  $N$ , wenn  $N \subseteq M$  vorausgesetzt und  $M$  als Universum fixiert ist. Da in einer solchen Situation  $\overline{N}$  als gleichwertig zu  $M \setminus N$  erklärt ist, ergibt sich aus Satz 1.2.9 sofort der folgende Satz durch Umschreiben in die andere Notation. Bei Punkt (3) verwenden wir zusätzlich noch die Eigenschaft  $M \cap N = N$ .

### 1.2.10 Satz: Eigenschaften des Komplements

Es sei  $M$  eine fest gewählte Menge, d.h. also ein Universum. Dann gelten die drei Gleichungen:

- (1)  $\overline{N \cup P} = \overline{N} \cap \overline{P}$  (de Morgan)
- (2)  $\overline{N \cap P} = \overline{N} \cup \overline{P}$  (de Morgan)
- (3)  $\overline{\overline{N}} = N$

für alle Mengen  $N$  und  $P$  mit  $N \subseteq M$  und  $P \subseteq M$ . □

Die Bezeichnung „Regeln von de Morgan“ für die beiden Gleichungen (1) und (2) dieses Satzes nimmt Bezug auf den englischen Mathematiker Augustus de Morgan (1806-1871). Dieser kann als einer der Begründer der modernen mathematischen Logik angesehen werden. Neben den Eigenschaften der letzten zwei Sätze gelten noch viele weitere Eigenschaften für die Mengenoperationen, auch in Verbindung mit der leeren Menge und einem eventuellen Universum. Beispielsweise gelten  $M \cup \emptyset = M$  und  $M \cap \emptyset = \emptyset$  und es ist, bei  $M$  als dem angenommenen Universum,  $X \subseteq Y$  äquivalent zu  $X \cap \bar{Y} = \emptyset$  und auch zu  $\bar{X} \cup Y = M$ . Der abstrakte Hintergrund vieler dieser Gesetze ist die Boolesche Algebra, benannt nach dem englischen Mathematiker George Boole (1815-1864), ebenfalls einem der Begründer der modernen mathematischen Logik.

### 1.3 Potenzmengen und Kardinalitäten

Mengen dürfen, wie wir schon zeigten, auch Mengen als Elemente haben, was zu einer gewissen „Schachtelungstiefe“ von Mengen führt. Man sieht dies etwa an den Mengen  $\{1\}$  (mit 1 als Tiefe),  $\{1, \{1\}\}$  (mit 2 als Tiefe) und  $\{1, \{1\}, \{1, \{1\}\}\}$  (mit 3 als Tiefe), was man beliebig fortführen kann. Man kann die Schachtelungstiefe bei den expliziten Darstellungen aus der Klammerung bekommen. Die bisherigen Konstruktionen auf Mengen veränderten die Schachtelungstiefe nicht, die folgende neue Konstruktion tut es hingegen, weil sie gegebene Mengen zu einer neuen Menge zusammenfasst. Wir betrachten sie auch in Verbindung mit einer Konstruktion, die Mengen die Anzahl der in ihnen vorkommenden Elemente zuordnet.

#### 1.3.1 Definition: Potenzmenge

Zu einer Menge  $M$  definieren wir  $\mathcal{P}(M) := \{X \mid X \subseteq M\}$  als Menge der Teilmengen von  $M$  und bezeichnen  $\mathcal{P}(M)$  als die **Potenzmenge** der Menge  $M$ . □

Es sind also  $X \in \mathcal{P}(M)$  und  $X \subseteq M$  äquivalente Aussagen. Manchmal wird die Potenzmenge von  $M$  auch mit  $2^M$  bezeichnet. Den Grund dafür lernen wir später kennen. Wir bleiben aber in diesem Text bei der Bezeichnung von Definition 1.3.1. Nachfolgend geben wir einige Beispiele für Potenzmengen an.

#### 1.3.2 Beispiele: Potenzmenge

Hier sind vier einfache Beispiele für die Potenzmengenkonstruktion:

- (1)  $\mathcal{P}(\emptyset) = \{\emptyset\}$
- (2)  $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$
- (3)  $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- (4)  $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Insbesondere gilt für jede Menge  $M$ , dass  $\emptyset \in \mathcal{P}(M)$  und auch  $M \in \mathcal{P}(M)$ . Man beachte noch einmal den Unterschied zwischen den beiden Mengen  $\emptyset$  und  $\{\emptyset\}$ . □

Im Hinblick auf die Vereinigung und den Durchschnitt beliebiger Mengen gelten die beiden folgenden Gleichungen:

$$\bigcup \mathcal{P}(M) = M \quad \bigcap \mathcal{P}(M) = \emptyset$$

Die Potenzmenge wird bei mengentheoretischen Untersuchungen gerne als Bezugsmenge genommen. Es gelten nämlich, falls  $X, Y \in \mathcal{P}(M)$ , die folgenden Eigenschaften:

$$X \cup Y \in \mathcal{P}(M) \quad X \cap Y \in \mathcal{P}(M) \quad X \setminus Y \in \mathcal{P}(M)$$

Spielen sich alle Untersuchungen in der Potenzmenge von  $M$  ab, dann ist  $M$  das Universum. Dies impliziert

$$\bigcap \emptyset = \{x \in M \mid \text{für alle } X \in \emptyset \text{ gilt } x \in X\} = \{x \in M \mid \text{wahr}\} = M.$$

Potenzmengen werden sehr schnell sehr groß. Es ist sogar für kleine Mengen nicht einfach, die Potenzmenge explizit anzugeben. Oft werden Elemente beim Hinschreiben vergessen. Der folgende Satz zeigt, wie man die Potenzmenge schrittweise auf eine systematische Weise konstruieren kann. Er beschreibt quasi ein Berechnungsverfahren (einen Algorithmus) dafür.

### 1.3.3 Satz: Konstruktion der Potenzmenge

Es sei  $M$  eine Menge und  $a$  ein Objekt mit  $a \notin M$ . Dann sind für alle Mengen  $X$  die folgenden Aussagen äquivalent:

$$(1) \quad X \in \mathcal{P}(M \cup \{a\})$$

$$(2) \quad X \in \mathcal{P}(M) \text{ oder es gibt eine Menge } Y \text{ mit } Y \in \mathcal{P}(M) \text{ und } X = Y \cup \{a\}$$

Insbesondere gilt  $\mathcal{P}(M \cup \{a\}) = \mathcal{P}(M) \cup \{X \mid \text{Es gibt } Y \in \mathcal{P}(M) \text{ mit } X = Y \cup \{a\}\}$ .

**Beweis:** Wir beginnen mit dem Beweis von (2) aus (1). Dazu sei  $X \in \mathcal{P}(M \cup \{a\})$  beliebig vorgegeben. Wir unterscheiden zwei Fälle.

(a) Es gelte  $a \notin X$ . Dann gilt sogar  $X \subseteq M$ , also auch  $X \in \mathcal{P}(M)$ .

(b) Es gelte  $a \in X$ . Wir definieren die Menge  $Y$  durch  $Y := X \setminus \{a\}$ . Dann gilt  $Y \subseteq M$ , also genau  $Y \in \mathcal{P}(M)$ , und es gilt auch noch  $X = (X \setminus \{a\}) \cup \{a\} = Y \cup \{a\}$ .

Nun zeigen wir, dass (1) aus (2) folgt. Auch hier gibt es zwei Fälle:

(a) Es gelte  $X \in \mathcal{P}(M)$ . Dann haben wir  $X \subseteq M$  und dies impliziert  $X \subseteq M \cup \{a\}$ , was genau der Aussage  $X \in \mathcal{P}(M \cup \{a\})$  entspricht.

(b) Es gelte  $X = Y \cup \{a\}$  mit einer Menge  $Y$ , für die  $Y \subseteq M$  wahr ist. Dann bringt Satz 1.2.4, dass  $X = Y \cup \{a\} \subseteq M \cup \{a\}$  gilt, und dies zeigt  $X \in \mathcal{P}(M \cup \{a\})$ .  $\square$

Im nachfolgenden Beispiel zeigen wir, wie man mit Hilfe dieses Satzes Potenzmengen berechnen kann, indem man mit der leeren Menge startet und solange Elemente einfügt, bis die vorgegebene Menge erreicht ist. Parallel zu dieser Berechnung erzeugt man auch alle Potenzmengen.

### 1.3.4 Beispiel: Konstruktion der Potenzmenge

Wir bestimmen die Potenzmenge  $\mathcal{P}(\{1, 2, 3\})$ , indem wir die Menge  $\{1, 2, 3\}$  schreiben als Vereinigung  $\emptyset \cup \{1\} \cup \{2\} \cup \{3\}$  und, startend mit der leeren Menge, immer wieder Satz 1.3.3 verwenden. In Form einer Tabelle sieht dies wie folgt aus:

| Menge $M$     | Potenzmenge $\mathcal{P}(M)$  |
|---------------|---|
| $\emptyset$   | $\{\emptyset\}$   |
| $\{1\}$       | $\{\emptyset, \{1\}\}$  |
| $\{1, 2\}$    | $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$   |
| $\{1, 2, 3\}$ | $\{\emptyset, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ |

Es fällt auf, dass sich bei jedem Schritt die Anzahl der Elemente in der Potenzmenge genau verdoppelt. Wir kommen auf diese fundamentale Eigenschaft später noch zurück und werden sie auch formal beweisen.  $\square$

Um über Anzahlen von Elementen in Mengen auch formal reden und mit mathematischen Mitteln argumentieren zu können, brauchen wir neue Begriffe. Diese werden nun eingeführt. Wir können dies leider nicht in voller Strenge tun, da dies zum jetzigen Stand des Texts viel zu kompliziert wäre. Für das praktische mathematische Arbeiten genügen unsere Formalisierungen aber.

### 1.3.5 Definition: Endlichkeit einer Menge

Eine Menge  $M$  heißt **endlich**, falls  $M = \emptyset$  gilt oder es ein  $n \in \mathbb{N}$  mit  $n \geq 1$  gibt und Objekte  $a_1, \dots, a_n$  so existieren, dass  $M = \{a_1, \dots, a_n\}$  zutrifft.  $\square$

Man kann die Endlichkeit einer Menge auch ohne Rückgriff auf natürliche Zahlen und die explizite Darstellung mittels der drei Punkte festlegen. Es ist nämlich  $M$  genau dann endlich, wenn für alle nichtleeren Teilmengen  $\mathcal{M}$  der Potenzmenge  $\mathcal{P}(M)$  die folgende Eigenschaft gilt: Es gibt eine Menge  $X \in \mathcal{M}$  so, dass kein  $Y \in \mathcal{M}$  mit  $Y \subset X$  existiert. Aufgrund dieser Beschreibung ist beispielsweise die Menge  $\mathbb{N}$  der natürlichen Zahlen nicht endlich; man nehme etwa die nichtleere Menge

$$\{\mathbb{N}, \mathbb{N} \setminus \{0\}, \mathbb{N} \setminus \{0, 1\}, \dots\} = \{\{x \in \mathbb{N} \mid x \geq n\} \mid n \in \mathbb{N}\}$$

als  $\mathcal{M}$ . In diesem Fall gibt es keine Menge  $X$  aus  $\mathcal{M}$ , in der keine echte Teilmenge mehr enthalten ist. Auch mit speziellen Funktionen kann man die Endlichkeit von Mengen ohne Benutzung von natürlichen Zahlen und expliziten Darstellungen spezifizieren. Wir kommen darauf in Kapitel 5 zurück. Für die folgenden Überlegungen nehmen wir aber die einfache Festlegung aus Definition 1.3.5 als Arbeitsgrundlage.

### 1.3.6 Definition: Kardinalität

Für eine endliche Menge  $M$  bezeichnet  $|M|$  ihre **Kardinalität**. Sie ist definiert mittels

- (1)  $|M| = 0$ , falls  $M = \emptyset$ , und
- (2)  $|M| = n$ , falls  $M$  die explizite Darstellung  $M = \{a_1, \dots, a_n\}$  mit  $n \geq 1$  Objekten  $a_1$  bis  $a_n$  besitzt.  $\square$

Für den Punkt (2) dieser Festlegung ist wesentlich, dass, per Definition, in expliziten Darstellungen von Mengen Mehrfachauflistungen von Elementen verboten sind, also beispielsweise  $\{1, 2, 2, 3, 3\}$  keine explizite Darstellung einer Menge ist. Die Kardinalität  $|M|$  gibt also die Anzahl der Elemente an, die in der Menge  $M$  enthalten sind. Man beachte, dass die Notation  $|M|$  nur für endliche Mengen erklärt ist. Somit sind etwa  $|\mathbb{N}|$  und  $|\mathbb{Z}|$  nicht zulässige Ausdrücke. Statt Kardinalität benutzt man manchmal auch die Bezeichnungen „Größe“ oder „Betrag“ oder „Mächtigkeit“. Für die Kardinalität von Mengen gilt die folgende wichtige Aussage.

### 1.3.7 Satz: Kardinalitätsformel

Für alle endlichen Mengen  $M$  und  $N$  gilt die folgende Kardinalitätsformel:

$$|M \cup N| = |M| + |N| - |M \cap N|$$

Im Fall von  $M \cap N = \emptyset$  (man sagt hier:  $M$  und  $N$  sind **disjunkt** oder haben leeren Schnitt) gilt also insbesondere die Gleichheit

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

**Beweis:** Wir unterscheiden einige Fälle. Es sei im ersten Fall eine der beiden Mengen leer, etwa  $N$ . Dann gilt die Gleichung aufgrund der Rechnung

$$|M \cup N| = |M| = |M| + 0 - 0 = |M| + |N| - |M \cap N|.$$

Nun gelte im zweiten Fall  $M \neq \emptyset$  und  $N \neq \emptyset$  mit  $M = \{a_1, \dots, a_m\}$  und  $N = \{b_1, \dots, b_n\}$ , wobei  $m$  und  $n$  natürliche Zahlen ungleich Null seien. Gilt  $M \cap N = \emptyset$ , so bekommen wir das gewünschte Ergebnis durch

$$\begin{aligned} |M \cup N| &= |\{a_1, \dots, a_m, b_1, \dots, b_n\}| \\ &= m + n \\ &= |\{a_1, \dots, a_m\}| + |\{b_1, \dots, b_n\}| - 0 \\ &= |M| + |N| - |M \cap N|. \end{aligned}$$

Schließlich gelte im dritten Fall  $M \cap N \neq \emptyset$  und es sei  $M \cap N = \{a_1, \dots, a_r\} = \{b_1, \dots, b_r\}$ , mit einer natürlichen Zahl  $r$ , die  $r \leq m$  und  $r \leq n$  erfüllt. Dass die ersten  $r$  Elemente von  $M$  und  $N$  übereinstimmen, kann man bei der expliziten Darstellung dieser Mengen jeweils durch eine entsprechende Aufschreibung erreichen. Nun gilt

$$\begin{aligned} |M \cup N| &= |\{a_1, \dots, a_m, b_{r+1}, \dots, b_n\}| \\ &= m + (n - r) \\ &= |\{a_1, \dots, a_m\}| + |\{b_1, \dots, b_n\}| - |\{a_1, \dots, a_r\}| \\ &= |M| + |N| - |M \cap N| \end{aligned}$$

und durch diese Rechnung ist der Beweis beendet.  $\square$

Das nachfolgende kleine Beispiel demonstriert den eben gezeigten Sachverhalt der Kardinalitätsformel noch einmal.

### 1.3.8 Beispiel: Kardinalität

Wir betrachten die folgenden zwei Mengen:

$$M := \{1, 3, 5\} \quad N := \{0, 3, 5, 6\}$$

Dann gelten  $|M| = 3$  und  $|N| = 4$  und  $M \cap N = \{3, 5\}$ , folglich  $|M \cap N| = 2$ . Weiterhin rechnet man schnell aus, dass  $M \cup N = \{0, 1, 3, 5, 6\}$  gilt, also auch  $|M \cup N| = 5$ . Fassen wir alles zusammen, so erhalten wir

$$5 = |M \cup N| = |M| + |N| - |M \cap N| = 3 + 4 - 2.$$

□

Nach Satz 1.3.3 bekommt man die Potenzmenge  $\mathcal{P}(M)$  von  $M$  aus der Potenzmenge von  $\mathcal{P}(M \setminus \{a\})$ , indem man die Potenzmenge  $\mathcal{P}(M \setminus \{a\})$  nimmt und in diese alle Mengen der Form  $X \cup \{a\}$  mit der Menge  $X$  aus  $\mathcal{P}(M \setminus \{a\})$  einfügt. Also hat die Potenzmenge  $\mathcal{P}(M)$  genau doppelt so viele Elemente wie die Potenzmenge  $\mathcal{P}(M \setminus \{a\})$ . Macht man nun mit  $\mathcal{P}(M \setminus \{a\})$  weiter, so hat diese doppelt so viele Elemente wie  $\mathcal{P}(M \setminus \{a, b\})$ . Dies bringt schließlich das folgende Resultat:

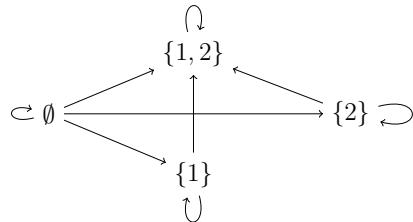
### 1.3.9 Satz: Kardinalität der Potenzmenge

Für alle endlichen Mengen  $M$  gilt die Gleichung  $|\mathcal{P}(M)| = 2^{|M|}$ .

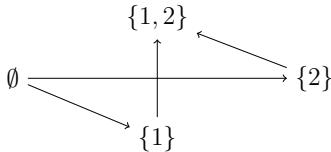
□

Mit den uns derzeit zur Verfügung stehenden logischen Mitteln können wir Satz 1.3.9 noch nicht streng formal beweisen. Wir verschieben deshalb den Beweis auf später. Seine Aussage ist der Grund dafür, dass auch  $2^M$  als Bezeichnung für die Potenzmenge von  $M$  verwendet wird. Dann gilt nämlich die Gleichung  $|2^M| = 2^{|M|}$ .

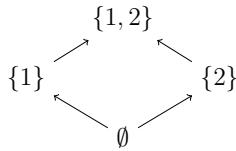
Oft ist es sehr hilfreich, kleine Potenzmengen graphisch durch Diagramme darzustellen. Dazu zeichnet man die Elemente der Menge  $\mathcal{P}(M)$  wohl separiert in der Zeichenebene und zeichnet dann einen Pfeil von einer Menge  $X$  nach einer Menge  $Y$  genau dann, wenn  $X \subseteq Y$  gilt. Hier ein kleines Beispiel mit  $\{1, 2\}$  als Menge  $M$ :



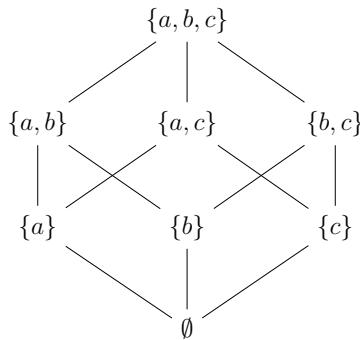
Solche bildliche Darstellungen von Potenzmengen und deren Inklusionsbeziehungen haben in der Regel schon bei kleinen Mengen sehr viele Pfeile und sind also sehr schnell unübersichtlich. Sie werden sehr viel übersichtlicher, wenn man nur die unbedingt notwendigen Pfeile zeichnet, also einen von der Menge  $X$  nach der Menge  $Y$  genau dann, wenn die echte Inklusion  $X \subset Y$  gilt (damit fallen schon alle Schlingen weg) und es keine Menge  $Z$  gibt mit  $X \subset Z$  und  $Z \subset Y$ , oder, in der gängigen kürzeren Schreibweise, mit  $X \subset Z \subset Y$ . Aus dem obigen Bild erhalten wir dann das folgende Bild, in dem alle überflüssigen Pfeile entfernt sind.



Nun ordnet man die Mengen in der Zeichenebene so an, dass alle Pfeile immer echt nach oben führen. Mit dieser Technik erhalten wir dann folgendes Bild.



Nun kann man sogar noch die Pfeilspitzen weglassen, da man weiß, dass sie immer bei den oberen Mengen sind. Zur Demonstration, wie einfach und übersichtlich dann die Bilder werden, wenn man sie schön zeichnet, ist hier noch einmal die Darstellung für eine etwas größere Potenzmenge angegeben, nämlich die von  $\{a, b, c\}$ , welche acht Elemente besitzt.



An diesem Bild sieht man sehr schön, wie die Mengen bezüglich der Mengeninklusion angeordnet sind. Auch Vereinigungen und Durchschnitte kann man bestimmen, indem man bestimmten Pfeilwegen folgt. Wir kommen darauf im Kapitel über Relationen zurück. Man bezeichnet solche Graphiken als **Ordnungs- oder Hasse-Diagramme**. Die zweite Bezeichnung erinnert an den deutschen Mathematiker Helmut Hasse (1898-1979). Das „schöne“ Zeichnen solcher graphischen Darstellungen mittels geeigneter Algorithmen ist seit Jahren ein intensives Forschungsgebiet der theoretischen Informatik.

## 1.4 Relationen und Funktionen

Mengen sind das erste fundamentale Prinzip, Objekte zu einer neuen mathematischen Struktur zusammenzufassen. Nachfolgend führen wir nun ein zweites solches Prinzip ein. Wir werden später angeben, wie man es auf das erste Prinzip zurückführen kann. Es ist ein allgemeines Bestreben der an den Grundlagen orientierten Teile der Mathematik,

alles, was man konstruiert, auf Mengen zurückzuführen, also, wie man sagt, in der Sprache der Mengenlehre auszudrücken. In der Praxis geht man aber viel pragmatischer vor und verzichtet in der Regel auf eine mengentheoretische Modellierung der Konzepte, die man neu einführt.

### 1.4.1 Definition: Paar, binäres direktes Produkt

Es seien  $M$  und  $N$  beliebige Mengen.

- (1) Zu Objekten  $a$  und  $b$  heißt die Konstruktion  $(a, b)$  ein (geordnetes) **Paar** mit **erster Komponente**  $a$  und **zweiter Komponente**  $b$ .
- (2) Die Menge aller Paare  $(a, b)$  mit  $a \in M$  und  $b \in N$  heißt das (binäre) **direkte Produkt** oder **kartesische Produkt** (benannt nach dem französischen Mathematiker Réne Descartes (1596-1650)) der Mengen  $M$  und  $N$  und wird mit  $M \times N$  bezeichnet. Es gilt also die definierende Gleichheit  $M \times N := \{(a, b) \mid a \in M \text{ und } b \in N\}$ .

Manchmal verwendet man auch  $\langle a, b \rangle$  als Notation für Paare. □

Wie schon bemerkt, ist Mengenlehre ein Fundament der Mathematik und bei einem strengen Vorgehen wird versucht, wie oben bemerkt, alles auf sie zurückzuführen. Das gelingt bei Paaren einfach, wenn man  $(a, b)$  als Abkürzung für die Menge  $\{a, \{a, b\}\}$  auffasst, wie vom polnischen Mathematiker Kazimierz Kuratowski (1896-1980) vorgeschlagen. Noch eleganter ist die Modellierung mittels  $\{\{a\}, \{a, b\}\}$ . Hier bekommt man nämlich bei  $a \neq b$  die erste Komponente als das einzige Element des Durchschnitts  $\{a\} \cap \{a, b\}$  der beiden Mengen  $\{a\}$  und  $\{a, b\}$  und die zweite Komponente als das einzige Element der sogenannten symmetrischen Differenz  $(\{a\} \setminus \{a, b\}) \cup (\{a, b\} \setminus \{a\})$  der beiden Mengen  $\{a\}$  und  $\{a, b\}$ . Wir wollen dies aber nicht vertiefen. Hingegen ist die folgende Bemerkung wichtig, denn sicher hat sich manche Leserin oder mancher Leser an der Notation in Punkt (2) der obigen Definition gestört.

### 1.4.2 Bemerkung: Zermelo-Mengenkomprehension

In der obigen Definition 1.4.1 haben wir das Prinzip der deskriptiven Mengendarstellung streng genommen verletzt. Da diese die Form  $\{x \mid A(x)\}$  hat, wobei  $x$  eine Variable ist und  $A(x)$  eine Aussage sein muss, hätten wir eigentlich genau genommen

$$M \times N := \{x \mid \text{Es gibt } a \in M \text{ und } b \in N \text{ mit } x = (a, b)\}$$

(mit einer ziemlich komplizierten Aussage  $A(x)$ ) schreiben müssen. Dies sieht wesentlich unnatürlicher aus und ist auch schwerer zu verstehen als die originale Schreibweise. Es ist deshalb ein allgemeiner Gebrauch der Mathematik, aus Gründen der Lesbarkeit die deskriptive Beschreibung einer Menge in der Gestalt

$$\{x \mid \text{Es gibt } y_1, \dots, y_n \text{ mit } x = E(y_1, \dots, y_n) \text{ und } A(y_1, \dots, y_n)\},$$

wobei  $E(y_1, \dots, y_n)$  ein Ausdruck in den Variablen  $y_1, \dots, y_n$  ist, durch die Notation

$$\{E(y_1, \dots, y_n) \mid A(y_1, \dots, y_n)\}$$

abzukürzen. Letztere Form der deskriptiven Darstellung von Mengen nennt man die **Zermelo-Mengenkomprehension**, sie ist nach dem deutschen Mathematiker Ernst Zermelo (1871-1953) benannt, dem Begründer der axiomatischen Mengenlehre. Damit vereinfacht sich etwa die Gleichung von Satz 1.3.3 zu  $\mathcal{P}(M \cup \{a\}) = \mathcal{P}(M) \cup \{Y \cup \{a\} \mid Y \in \mathcal{P}(M)\}$ .  $\square$

Nach dieser Klärung der vereinfachenden Schreibweise bei direkten Produkten befassen wir uns nun mit der Kardinalität von direkten Produkten von endlichen Mengen. Wir erhalten durch relativ einfache Rechnungen das folgende Resultat (in dem wir explizit ein Multiplikationssymbol verwenden; normalerweise wird die Multiplikation durch Hintereinanderschreiben ihrer Argumente ausgedrückt).

### 1.4.3 Satz: Kardinalität von direkten Produkten

Für alle endlichen Mengen  $M$  und  $N$  gilt die Gleichung  $|M \times N| = |M| \cdot |N|$ .

**Beweis:** Wir unterscheiden zwei Fälle. Zuerst sei für die Menge  $M$  die explizite Darstellung  $M := \{a_1, \dots, a_n\}$  mit  $n \geq 1$  Objekten angenommen. Dann rechnen wir die Behauptung unter Verwendung der Kardinalitätsformel wie folgt nach:

$$\begin{aligned} |M \times N| &= \left| \bigcup_{i=1}^n \{(a_i, b) \mid b \in N\} \right| \\ &= |\{(a_1, b) \mid b \in N\}| + \dots + |\{(a_n, b) \mid b \in N\}| \\ &= |N| + \dots + |N| \quad (n\text{-mal}) \\ &= |M| \cdot |N| \end{aligned}$$

Ist hingegen im zweiten Fall  $M = \emptyset$ , so folgt  $M \times N = \emptyset$  (darauf werden wir später noch genau eingehen, wenn die entsprechenden logischen Grundlagen zur Verfügung stehen) und dies zeigt diesen Fall, da

$$|M \times N| = |\emptyset| = 0 = 0 \cdot |N| = |M| \cdot |N|. \quad \square$$

Man beachte, dass  $M \times (N \times P) \neq (M \times N) \times P$  gilt. Beispielweise bekommen wir für die drei Mengen  $M := \{1\}$ ,  $N := \{a, b\}$  und  $P := \{\heartsuit, \diamondsuit\}$  die Menge

$$M \times (N \times P) = \{(1, (a, \diamondsuit)), (1, (a, \heartsuit)), (1, (b, \diamondsuit)), (1, (b, \heartsuit))\},$$

also eine Menge von Paaren, deren zweite Komponenten wiederum Paare sind, während

$$(M \times N) \times P = \{((1, a), \diamondsuit), ((1, b), \diamondsuit), ((1, a), \heartsuit), ((1, b), \heartsuit)\}$$

bei der anderen Klammerung gilt. Hier sind die ersten Komponenten der Paare wieder Paare. Allerdings gilt die Gleichheit  $|M \times (N \times P)| = |M| \cdot |N| \cdot |P| = |(M \times N) \times P|$  nach dem obigen Satz im Fall von endlichen Mengen.

Wir kommen nun zu den Relationen, einen der fundamentalsten Begriffe der Mathematik. Auf diesen Begriff stützt sich z.B., wie wir bald sehen werden, der Funktionsbegriff, also ein weiterer der fundamentalsten Begriffe der Mathematik. Das Wort „Relation“ beschreibt in der Umgangssprache Beziehungen zwischen Objekten, wie etwa in der Aussage

die Zugspitze **ist höher** als der Watzmann,

wo eine Beziehung zwischen zwei Objekten gleicher Art (hier Berge) beschrieben wird, oder in der Aussage

Kiel **liegt an** der Ostsee,

wo eine Beziehung zwischen zwei Objekten verschiedener Arten (hier Städte und Gewässer) beschrieben wird, oder in der Aussage

die Nordsee **ist tiefer als** die Ostsee,

wo wiederum eine Beziehung zwischen zwei Objekten gleicher Art (hier Gewässer) beschrieben wird. In der Mathematik führt man Relationen wie folgt ein.

#### 1.4.4 Definition: Relation

Sind  $M$  und  $N$  Mengen, so heißt eine Teilmenge  $R$  von  $M \times N$  eine **Relation** von  $M$  nach  $N$ . Es ist  $M$  die **Quelle** oder der **Vorbereich** von  $R$  und  $N$  das **Ziel** oder der **Nachbereich** von  $R$ . Im Fall  $M = N$  nennt man  $R$  auch eine Relation auf  $M$ . Gilt  $(a, b) \in R$ , so sagt man, dass  $a$  und  $b$  **in Relation  $R$  stehen**.  $\square$

Man beachte, dass Relationen Mengen sind. Folglich kann man sie vereinigen, schneiden, Differenzen und Komplemente bilden usw. Wegen der speziellen Struktur der Elemente von Relationen gibt es aber noch Operationen, die verwenden, dass die Elemente Paare sind. Darauf kommen wir in späteren Kapiteln noch zurück. Nachfolgend geben wir nun zuerst einige einfache Beispiele für Relationen an, die wohl schon bekannt sind.

#### 1.4.5 Beispiele: Relationen

Die **übliche Ordnung**  $\leq$  auf der Menge  $\mathbb{N}$  der natürlichen Zahlen ist formal eine Relation von  $\mathbb{N}$  nach  $\mathbb{N}$ , also auf der Menge  $\mathbb{N}$ , und z.B. mit Hilfe der Addition definierbar durch

$$\leq := \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid \text{Es gibt } z \in \mathbb{N} \text{ mit } x + z = y\}.$$

Daraus bekommt man die **strikte Ordnung**  $<$  auf der Menge  $\mathbb{N}$  als Relation durch die folgende Konstruktion:

$$< := \leq \cap \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \neq y\}$$

Auch die **Teilbarkeitsrelation**  $|$  ist eine Relation auf  $\mathbb{N}$  und ist festgelegt durch

$$| := \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid \text{Es gibt } z \in \mathbb{N} \text{ mit } xz = y\}.$$

Bei solchen bekannten Relationen verwendet man oft eine Infix-Notation und schreibt  $x \leq y$  statt  $(x, y) \in \leq$  und  $x < y$  statt  $(x, y) \in <$  und  $x | y$  statt  $(x, y) \in |$ . Auch schreibt man beispielsweise  $x \geq y$  statt  $y \leq x$  wenn es in Berechnungen zweckmäßig ist.  $\square$

Infix-Schreibweisen für Relationen sind viel gebräuchlicher als die mengentheoretische Schreibweise mit dem Symbol „ $\in$ “. Sie sind auch viel besser lesbar und erleichtern auch das Spezifizieren von Relationen. Deshalb legen wir fest.

### 1.4.6 Festlegung: Spezifikation von Relationen

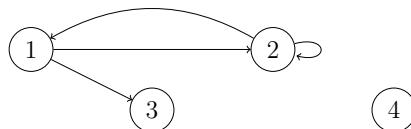
Ist  $R \subseteq M \times N$  eine Relation, so schreiben wir  $a R b$  statt  $(a, b) \in R$ . Auch die Spezifikation verändern wir. Statt der definierenden Gleichung  $R := \{(x, y) \in M \times N \mid A(x, y)\}$  führen wir  $R$  in der Regel wie folgt ein: Die Relation  $R \subseteq M \times N$  ist für alle  $x \in M$  und  $y \in N$  erklärt durch  $x R y$  genau dann, wenn  $A(x, y)$  gilt.  $\square$

Eine Einführung der Ordnung auf der Menge  $\mathbb{N}$  lautet nun etwa so: Die Relation  $\leq$  von  $\mathbb{N}$  nach  $\mathbb{N}$  ist für alle  $x, y \in \mathbb{N}$  definiert durch  $x \leq y$  genau dann, wenn es ein  $z \in \mathbb{N}$  gibt mit  $x + z = y$ . Wenn wir ab dem zweiten Kapitel die Sprache der Logik zur Verfügung haben werden, dann wird die obige Phrase „ $x R y$  genau dann, wenn  $A(x, y)$  gilt“ zu einer **definierenden Äquivalenz** „ $x R y : \iff A(x, y)$ “ mit dem speziellen Zeichen „ $: \iff$ “ werden, was die Lesbarkeit nochmals verbessern wird.

Zwei sehr gebräuchliche Darstellungen von kleinen Relationen sind Pfeildiagramme und Kreuzchentabellen. Wir geben nachfolgend ein kleines Beispiel an, das selbsterklärend ist. Dazu sei  $M := \{1, 2, 3, 4\}$  unterstellt.

Relation  $\{(1, 2), (1, 3), (2, 1), (2, 2)\}$

Pfeildiagramm



Kreuzchentabelle

|   | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 |   | X | X |   |
| 2 | X | X |   |   |
| 3 |   |   |   |   |
| 4 |   |   |   |   |

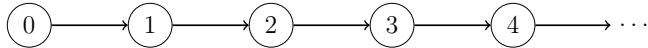
Die letzte Darstellung wird in der Informatik insbesondere im Rahmen von Booleschen Feldern verwendet, um Relationen in Programmiersprachen zu implementieren. Die Kreuzchentabelle wird dann zu einem zweidimensionalen Feld der entsprechenden Programmiersprache, jedes Kreuzchen zum Wert **true** (wahr) und jeder freie Platz zum Wert **false** (falsch). Pfeildiagramme und Kreuzchentabellen dienen oft dazu, sich Eigenschaften zu verdeutlichen. Bei solchen Vorgehensweisen sind sie sogar bei unendlichen Relationen anwendbar, wenn klar ist, wie sich die endliche Zeichnung auf das Unendliche fortsetzt. Wir kommen nun zu speziellen Relationen.

### 1.4.7 Definition: eindeutige und totale Relation

Es sei  $R \subseteq M \times N$  eine Relation.

- (1)  $R$  heißt **eindeutig**, falls für alle  $x \in M$  und  $y, z \in N$  gilt: Aus  $x R y$  und  $x R z$  folgt  $y = z$ .
- (2)  $R$  heißt **total**, falls für alle  $x \in M$  ein  $y \in N$  mit  $x R y$  existiert.  $\square$

Beispielweise ist die Nachfolger-Relation  $nachf$  auf der Menge  $\mathbb{N}$ , welche für alle  $x, y \in \mathbb{N}$  festgelegt ist durch  $x nachf y$  genau dann, wenn  $x + 1 = y$  gilt, eindeutig. Aus  $x nachf y$  und  $x nachf z$  bekommen wir nämlich  $z = x + 1 = y$ . Hier ist das Pfeildiagramm dieser Relation, wobei klar ist, wie es ins Unendliche fortzusetzen ist.



Im Pfeildiagramm bedeutet der Begriff „eindeutig“: Jedes Objekt verlässt **höchstens** ein Pfeil. Die oben aufgeführten zwei Relationen  $\leq$  und  $|$  sind nicht eindeutig. Weiterhin heißt im Pfeildiagramm „total“: Jedes Objekt verlässt **mindestens** ein Pfeil. Also ist  $nachf$  auch total. Auch die Relationen  $\leq$  und  $|$  sind total. Hingegen ist die Vorgänger-Relation  $vorg$  auf der Menge  $\mathbb{N}$  nicht total, wenn man  $x vorg y$  mittels  $y + 1 = x$  für alle  $x, y \in \mathbb{N}$  festgelegt. Hier ist das Pfeildiagramm der Vorgänger-Relation:



Die Null verlässt kein Pfeil, denn sie hat ja keinen Vorgänger in der Menge der natürlichen Zahlen. Hingegen ist die Vorgänger-Relation  $vorg$  eindeutig. Bei den Kreuzchentabellen erkennt man die Eindeutigkeit einer Relation daran, dass in jeder Zeile sich höchstens ein Kreuzchen befindet, und die Totalität einer Relation daran, dass in jeder Zeile sich mindestens ein Kreuzchen befindet. Eindeutige und totale Relationen bekommen einen eigenen Namen, denn sie bilden, neben den Mengen, wahrscheinlich die fundamentalsten Objekte der Mathematik. Den folgenden Begriff und einige der nachfolgenden Notationen kennt man schon man von der weiterbildenden Schule her; ihre Einführung geschieht dort aber nicht in der formalen Weise über Relationen wie in diesem Text, sondern in der Regel intuitiv durch Ausdrücke oder Gleichungen mit „unabhängigen und abhängigen Variablen“.

#### 1.4.8 Definition: Funktion

Eine eindeutige und totale Relation  $R \subseteq M \times N$  heißt eine **Funktion** (oder **Abbildung**) von  $M$  und  $N$ . Das zu  $x \in M$  eindeutig existierende Objekt  $y \in N$  mit  $x R y$  wird als  $R(x)$  bezeichnet und heißt das **Bild** (oder **Bildelement**) von  $x$  unter  $R$ .  $\square$

Wesentlich bei Funktionen ist also die Gleichwertigkeit von  $x R y$  und  $y = R(x)$ , welche wir später noch öfter verwenden werden. Der Ausdruck  $R(x)$  heißt auch **Funktionsanwendung** (oder Funktionsapplikation) und  $x$  das Argument. Gilt  $y = R(x)$ , so heißt  $y$  das Resultat der Anwendung von  $R$  auf  $x$ . Bei Funktionen verwendet man normalerweise kleine Buchstaben zur Bezeichnung, etwa  $f$  oder  $g$ . Auch schreibt man dann nicht  $f \subseteq M \times N$ , sondern  $f : M \rightarrow N$ , und nennt  $M \rightarrow N$  die **Funktionalität**,  $M$  die **Quelle** (oder **Argumentmenge**) und  $N$  das **Ziel** (oder **Resultatmenge**) von  $f$ . Ist die Quelle ein direktes Produkt, also  $f : M \times N \rightarrow P$ , so müsste man zu  $(a, b) \in M \times N$  das Bild eigentlich mit  $f((a, b))$  bezeichnen. Hier schreibt man vereinfachend nur  $f(a, b)$ . Funktionsanwendungen werden oftmals auch noch anders notiert. Bei zwei Argumenten ist eine Infix-Schreibweise vorherrschend, wie etwa bei der Addition, wo man  $x + y$  statt  $+(x, y)$  schreibt. Liegt nur ein Argument vor, so gibt es etwa Präfix-Schreibweisen  $f x$  als auch Postfix-Schreibweisen  $x f$ . Bei manchen Funktionen wird sogar auf ein Symbol verzichtet, wie etwa bei der Multiplikation  $xy$  und der Potenzierung  $x^n$  von Zahlen. Solche speziellen Funktionen werden oft auch **Operationen** genannt.

### 1.4.9 Beispiele: Funktionen

Nachfolgend sind vier Definitionen von Funktionen angegeben. Man lässt bei solchen Spezifikationen normalerweise die Phrase „... ist für alle ... definiert durch ...“ weg und verwendet auch das normale Gleichheitssymbol „=“ statt des Symbols „:=“ der definierenden Gleichheit. In (2) bestimmt die Wurzeloperation den positiven Wurzelwert des Arguments.

- (1)  $f_1 : \mathbb{N} \rightarrow \mathbb{N}$ , wobei  $f_1(x) = 3x^2 + 1$ .
- (2)  $f_2 : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , wobei  $f_2(x, y) = \sqrt{x^2 + y^2}$ .
- (3)  $f_3 : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ , wobei  $f_3(x) = \{x\}$ .
- (4)  $f_4 : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ , wobei  $f_4(x) = (x, x^2)$ .

Mit diesen Festlegungen gelten etwa  $f_1(3) = 3 \cdot 3^2 + 1 = 28$ ,  $f_2(3, 4) = \sqrt{3^2 + 4^2} = 5$ ,  $f_3(1) = \{1\}$  und  $f_4(5) = (5, 25)$ . Das Anwenden einer Funktion auf Elemente heißt also das Ersetzen der Variablen im Ausdruck, der die Funktion definiert, durch das jeweilige Element und dann das Ausrechnen des neuen Ausdrucks.  $\square$

Dies war eine knappe Einführung in Relationen und Funktionen. Wir werden das Thema später noch wesentlich vertiefen. Eines haben wir aber noch zu klären: Da Mengen Zusammenfassungen von wohlunterschiedenen Objekten sind, ist noch zu sagen, was die Gleichheit von Paaren ist. Wenn man  $(a, b)$  als Abkürzung für die Menge  $\{a, \{a, b\}\}$  oder die Menge  $\{\{a\}, \{a, b\}\}$  auffasst, ist klar, wann zwei Paare gleich sind.

### 1.4.10 Definition: Gleichheit von Paaren

Für alle Paare  $(a, b)$  und  $(c, d)$  definieren wir die **Gleichheit**  $(a, b) = (c, d)$  genau dann als gültig, wenn  $a = c$  und  $b = d$  gelten.  $\square$

Zwei Relationen  $R$  und  $S$  sind (mengentheoretisch) gleich, wenn sie als Mengen gleich sind, sie also dieselben Paare enthalten. Wir haben Relationen nur in Verbindung mit den Mengen betrachtet, zwischen denen sie definiert sind. Deshalb setzen wir bei einem Gleichheitstest  $R = S$  in Zukunft immer implizit voraus, dass  $R$  und  $S$  die gleiche Quelle und das gleiche Ziel besitzen. Genaugenommen definieren wir die Gleichheit also nur für solche Relationen. Man kann die Gleichheit auch für alle Relationen definieren, indem man zum Gleichsein von  $R$  und  $S$  fordert, dass  $R$  und  $S$  die gleiche Quelle und das gleiche Ziel besitzen und als Mengen gleich sind.

Funktionen sind spezielle Relationen. Da  $(x, y) \in f$  mit  $f(x) = y$  per Definition gleichwertig ist, bekommen wir das folgende Resultat. Man beachte, dass wir den Test auf Gleichheit wiederum nur für Funktionen der gleichen Funktionalität betrachten.

### 1.4.11 Satz: Gleichheit von Funktionen

Für alle Funktionen  $f, g : M \rightarrow N$  gilt  $f = g$  genau dann, wenn  $f(x) = g(x)$  für alle  $x \in M$  gilt.

**Beweis:** Es gilt  $f = g$  genau dann, wenn gilt

(a) für alle  $(x, y) \in M \times N$  gilt  $(x, y) \in f$  genau dann, wenn  $(x, y) \in g$ .

In der obigen Schreibweise wird die Aussage (a) zur Aussage

(b) für alle  $x \in M, y \in N$  gilt  $f(x) = y$  genau dann, wenn  $g(x) = y$ .

Die Aussage (b) ist nun äquivalent zu

(c) für alle  $x \in M$  gilt  $f(x) = g(x)$ .

Wenn man in (b) nämlich  $y$  als das Bildelement  $f(x)$  wählt, so bekommt man  $f(x) = f(x)$ .

Diese Aussage ist wahr. Aus der vorausgesetzten logischen Gleichwertigkeit folgt nun auch, dass die Aussage  $g(x) = f(x)$  wahr ist. Gilt umgekehrt  $f(x) = g(x)$ , also (c), so ist offensichtlich für alle  $y \in N$  die Aussage  $f(x) = y$  genau dann wahr, wenn die Aussage  $g(x) = y$  wahr ist.  $\square$

Man beachte, dass durch diesen Satz die Gleichheit von Funktionen nur dann durch die Gleichheit von allen Funktionsanwendungen auf die Elemente der gemeinsamen Quelle beschrieben werden kann, wenn die zu vergleichenden Funktionen die gleiche Funktionalität besitzen. Wenn man ganz korrekt ist, dann braucht dieser Satz eigentlich noch  $M \neq \emptyset$  als weitere Voraussetzung, wobei dies aus logischen Gründen dann  $N \neq \emptyset$  impliziert. Für  $M = \emptyset$  ist der Ausdruck  $f(x)$  nämlich für kein  $x \in M$  definiert, weil es eben so ein  $x$  nicht gibt. Später werden wir zeigen, dass die leere Menge von Paaren mit der leeren Menge als Quelle eine Funktion ist. Bei Anwendungen von Funktionen in der Praxis sind Quelle und Ziel immer nicht leer und somit Satz 1.4.11 in seiner obigen Formulierung anwendbar.

Nach dem obigen Satz 1.4.11 gilt somit für die drei Funktionen  $f_1, f_2, f_3 : \mathbb{N} \rightarrow \mathbb{N}$  mit den Festlegungen

$$f_1(x) = x^2 - 1 \quad f_2(x) = (x+1)(x-1) \quad f_3(x) = x + 1$$

die Gleichheit  $f_1 = f_2$ , da  $f_2(x) = (x+1)(x-1) = x^2 - x + x - 1 = x^2 - 1 = f_1(x)$  für alle  $x \in \mathbb{N}$  gilt, aber auch die Ungleichheit  $f_1 \neq f_3$ , da beispielsweise  $f_1(1) = 1^2 - 1 = 0 \neq 2 = 1 + 1 = f_3(1)$  zutrifft.

## 1.5 Einige Ergänzungen zum Funktionsbegriff

Wir wollen diese Einführung in die Mengen, Relationen und Funktionen mit einigen Bemerkungen zu den Funktionen abschließen. Diese betreffen insbesondere die Unterscheidung von verschiedenen Fällen bei der Festlegung von Funktionen, das Prinzip der Rekursion und die sogenannte implizite Definition von Funktionen. Fallunterscheidungen stellen nur spezielle Schreibweisen dar. Die beiden anderen Konzepte sind hingegen inhaltlicher Natur und tauchen insbesondere in der Informatik beim Arbeiten mit Funktionen oft auf.

Wir hatten im letzten Abschnitt angegeben, wie man Funktionen normalerweise in der Mathematik festlegt, nämlich in der Form

$$f : M \rightarrow N \quad f(x) = E(x),$$

wobei  $E(x)$  ein Ausdruck in der Variablen  $x$  ist, der festlegt, was zu  $x$  der Wert von  $f$  ist. Diese Art der Definition (Spezifikation, Angabe) von Funktionen wird auch **explizit**

genannt. Nun kommt es vor, dass bei solchen Angaben auch verschiedene Fälle auftreten können. Ein Beispiel ist etwa der **Absolutbetrag**  $|x|$  einer reellen Zahl  $x$ , welcher definiert ist durch  $|x| = x$ , falls  $x \geq 0$ , und durch  $|x| = -x$ , falls  $x < 0$ . Wenn man dies als Funktionsdefinition angibt, so verwendet man in der Regel eine geschweifte Klammer, um die verschiedenen Fälle auseinanderzuhalten, schreibt also

$$|\cdot| : \mathbb{R} \rightarrow \mathbb{R} \quad |x| = \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{falls } x < 0, \end{cases}$$

wobei der Punkt in der Angabe der Bezeichnung der Funktion zeigt, wo bei Anwendungen die Argumente stehen, oder auch

$$|\cdot| : \mathbb{R} \rightarrow \mathbb{R} \quad |x| = \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{sonst,} \end{cases}$$

wobei nun zusätzlich das Wort „sonst“ den nicht durch „falls“ abgedeckten Fall meint. Eine Verallgemeinerung dieser Schreibweisen auf mehr als zwei Fälle ist offensichtlich.

Fallunterscheidungen treten insbesondere in Definitionen von Funktionen auf, wenn das Prinzip der **Rekursion** verwendet wird. Rekursion heißt, dass bei einer Definition des Wertes  $f(x)$  andere Werte von  $f$  verwendet werden dürfen. Häufig sind die folgenden beiden Situationen:

- (1) Eine Funktion, die explizit gegeben ist, wird in Form einer rekursiven Beschreibung angegeben; es wird also eine sogenannte rekursive Darstellung bewiesen.
- (2) Es wird das Prinzip der Rekursion verwendet, um die Funktion explizit zu spezifizieren.

Ein sehr bekanntes Beispiel für eine Rekursion ist die Berechnung des **größten gemeinsamen Teilers** von zwei natürlichen Zahlen  $x$  und  $y$ . Wird dieser mit  $\text{ggT}(x, y)$  bezeichnet, so kann man für die entsprechend explizit definierte Funktion

$$\text{ggT} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

mit der Festlegung

$$\text{ggT}(x, y) = \begin{cases} \max \{z \in \mathbb{N} \mid z|x \text{ und } z|y\} & \text{falls } x \neq 0 \text{ und } y \neq 0 \\ 0 & \text{sonst,} \end{cases}$$

in der die Operation *max* zu einer endlichen und nichtleeren Teilmenge von  $\mathbb{N}$  deren größtes Element bestimmt<sup>1</sup>, nach einigen Rechnungen die Gleichung

$$\text{ggT}(x, y) = \begin{cases} x & \text{falls } y = 0 \\ \text{ggT}(y, \text{mod}(x, y)) & \text{sonst} \end{cases}$$

beweisen, wobei  $\text{mod}(x, y)$  den Rest der ganzzahligen Division von  $x$  durch  $y$  bezeichnet (genauer werden wir diese Operation in Kapitel 6 behandeln). Dadurch kann man größte gemeinsame Teiler einfach bestimmen, etwa durch die Rechnung

$$\text{ggT}(6, 18) = \text{ggT}(18, 6) = \text{ggT}(6, 0) = 6$$

---

<sup>1</sup>Die Fallunterscheidung in der Festlegung von  $\text{ggT}(x, y)$  ist notwendig, da  $\{z \in \mathbb{N} \mid z|0 \text{ und } z|0\} = \mathbb{N}$  gilt und die Menge  $\mathbb{N}$  kein größtes Element besitzt.

den von 6 und 18 oder durch die Rechnung

$$\text{ggT}(24, 4) = \text{ggT}(4, 0) = 4$$

den von 24 und 4. Das erste Vorgehen „Herleitung einer Rekursion“ ist insbesondere in der Informatik von Bedeutung, wenn funktional programmiert wird. Letzteres heißt, dass im Prinzip mit Funktionen Berechnungsverfahren formuliert werden und diese in der verwendeten Programmiersprache nur in einer speziellen Schreibweise notiert sind. Man vergleiche etwa mit den Bemerkungen zu Satz 1.2.7.

Das zweite Vorgehen „Definition durch eine Rekursion“ wird normalerweise verwendet, wenn Funktionen auf Mengen arbeiten, die durch irgendwelche Operationen aus gewissen Konstanten aufgebaut werden. Wir werden es im Laufe des Texts noch oft kennenlernen, neben den natürlichen Zahlen (fortwährend im Text) beispielsweise bei den linearen Listen und den Binäräbäumen in Kapitel 3. Im letzten Abschnitt dieses Kapitels werden wir auch den theoretischen Hintergrund knapp skizzieren.

Wir wollen nun noch eine weitere Verwendung von Fallunterscheidungen erwähnen. Von der weiterbildenden Schule her bekannt sind sicher die sogenannten **rationalen Funktionen** als Brüche von sogenannten **ganzrationalen Funktionen** oder Polynomfunktionen. Hier ist ein Beispiel für eine rationale Funktion:

$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \frac{3x^2 + 2x + 1}{x^2 - 1}$$

Im Sinne der ursprünglichen Definition handelt es sich bei  $f$  eigentlich um keine Funktion. Es ist nämlich die Totalitätsbedingung verletzt, denn zum Argument  $x := 1$  ist der  $f(x)$  spezifizierende Ausdruck wegen einer Division durch Null nicht definiert. Man spricht in diesem Zusammenhang, wenn man es genau nimmt, dann von **partiellen Funktionen** und verwendet zu deren Festlegung Fallunterscheidungen. Die obige partielle Funktion wird bei so einer Vorgehensweise dann oft wie folgt angeben:

$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \begin{cases} \frac{3x^2 + 2x + 1}{x^2 - 1} & \text{falls } x \neq 1 \\ \text{undefiniert} & \text{sonst} \end{cases}$$

Partielle Funktionen sind insbesondere in der Informatik häufig, etwa bei der mathematischen Beschreibung von Datenstrukturen (wie Listen und Bäumen, zu denen wir im dritten Kapitel kommen), wenn gewisse Operationen (Zugriffe auf Teilstrukturen usw.) nicht auf allen Objekten ausgeführt werden können.

Neben der expliziten Definition von Funktionen gibt es noch die **implizite Definition**. Hier wird zu einer Funktion  $f : M \rightarrow N$  und für alle  $x \in M$  und  $y \in N$  durch eine Eigenschaft festgelegt, wann genau  $f(x) = y$  gilt. Beispielsweise kann man den ganzzahligen Anteil des dualen Logarithmus als eine Funktion  $\text{glog}_2 : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$  dadurch spezifizieren, dass man für alle  $x \in \mathbb{N} \setminus \{0\}$  und  $y \in \mathbb{N}$  fordert

$$\text{glog}_2(x) = y \text{ gilt genau dann, wenn } 2^y \leq x \text{ und } x < 2^{y+1}.$$

Es handelt sich hier also um die Übertragung der Festlegung 1.4.6 von den Relationen auf die Funktionen. Natürlich ist vorher explizit nachzuweisen, dass tatsächlich eine Funktion

vorliegt, also im gegebenen Beispiel die Schreibweise  $\text{glog}_2(x) = y$  sinnvoll ist. Denn zunächst könnte es mehrere  $y$  geben, welche die Bedingung erfüllen, und man wüsste nicht, welches davon mit  $\text{glog}_2(x)$  bezeichnet wird.

Es gibt Situationen, wo eine implizite Angabe einer Funktion vorteilhaft ist. Dies ist auch im Fall des ganzzahligen Anteils des dualen Logarithmus so. Man kann nämlich aus der obigen impliziten Darstellung relativ leicht die Rekursion

$$\text{glog}_2(x) = \begin{cases} 0 & \text{falls } x = 1 \\ \text{glog}_2\left(\frac{x}{2}\right) + 1 & \text{falls } x \neq 1 \text{ und } x \text{ gerade} \\ \text{glog}_2\left(\frac{x-1}{2}\right) + 1 & \text{falls } x \neq 1 \text{ und } x \text{ ungerade} \end{cases}$$

zeigen, welche sofort zu einem funktionalen Programm führt. Aus der expliziten Definition

$$\text{glog}_2(x) = \max \{y \in \mathbb{N} \mid 2^y \leq x\}$$

der Funktion  $\text{glog}_2$ , mit der Operation  $\max$  wie oben eingeführt, bekommt man diese Rekursion nicht so leicht.

## 1.6 Übungsaufgaben

### Aufgabe

Wir betrachten die folgenden zwei Mengen:

$$M := \{x \in \mathbb{N} \mid 2^x \leq 10\} \quad N := \{y \in \mathbb{N} \mid \text{Es gibt } z \in \mathbb{N} \text{ mit } y = z^2 \text{ und } z \leq 5\}$$

Geben Sie die beiden Mengen  $M$  und  $N$  sowie  $M \cup N$ ,  $M \cap N$  und  $M \setminus N$  explizit an, d.h. durch die in Mengenklammern eingeschlossene Aufzählung ihrer Elemente.

### Aufgabe

Es seien  $X$  und  $Y$  zwei in der Menge  $M$  enthaltene Mengen. Formulieren Sie einen Ausdruck zur Beschreibung der Menge

$$\{x \in M \mid \text{Aus } x \in X \text{ folgt } x \in Y\},$$

in dem nur die Mengen  $X$ ,  $Y$ ,  $M$  und die Mengenoperationen von Kapitel 1 Verwendung finden.

### Aufgabe

Eine Menge von Mengen  $\mathcal{M}$  werde durch die nachfolgenden zwei Regeln (a) und (b) definiert:

$$(a) \text{ Es gilt } \emptyset \in \mathcal{M}. \quad (b) \text{ Für alle } X \in \mathcal{M} \text{ gilt auch } X \cup \{X\} \in \mathcal{M}.$$

- (1) Geben Sie die Liste der ersten fünf Mengen an, welche durch die Regeln (a) und (b) als in  $\mathcal{M}$  enthalten definiert werden.
- (2) In welchen Beziehungen stehen die fünf Mengen aus (1) untereinander hinsichtlich der Inklusion  $\subseteq$  und des Enthaltsenseins  $\in$ ?

## Aufgabe

Es seien  $\mathcal{M}$  und  $\mathcal{N}$  Mengen von Mengen mit der Eigenschaft  $\mathcal{M} \subseteq \mathcal{N}$ . Beweisen Sie die folgenden Aussagen:

$$\bigcup \mathcal{M} \subseteq \bigcup \mathcal{N} \quad \bigcap \mathcal{N} \subseteq \bigcap \mathcal{M}$$

## Aufgabe

Es sei  $n$  eine natürliche Zahl.

- (1) Spezifizieren Sie deskriptiv eine Menge  $T_n$ , die genau die positiven ganzzahligen Teiler von  $n$  enthält, d.h. jede Zahl  $x \in \mathbb{N} \setminus \{0\}$ , für die  $\frac{n}{x} \in \mathbb{N}$  gilt.
- (2) Geben Sie die Menge  $T_{15}$  explizit an.
- (3) Definieren Sie, aufbauend auf (1), deskriptiv die Menge aller Primzahlen.

## Aufgabe

Eine Menge  $M$  sei durch  $M := \{a, b, c\}$  festgelegt.

- (1) Zeichnen Sie das Hasse-Diagramm der Potenzmenge  $\mathcal{P}(M)$ .
- (2) Wir betrachten die folgende Teilmenge  $\mathcal{N}$  von  $\mathcal{P}(M)$ :

$$\mathcal{N} := \{\{a, b, c\}, \{a, b\}, \{a, c\}\}$$

Formulieren Sie, ohne die Elemente von  $\mathcal{N}$  explizit zu verwenden, eine Eigenschaft  $E(X)$  über den Elementen von  $\mathcal{P}(M)$ , so dass  $E(X)$  und  $X \in \mathcal{N}$  äquivalente Aussagen sind.

- (3) Für welche Elemente (Mengen)  $X$  der Menge  $\mathcal{N}$  gibt es ein Element (Menge)  $Y$  in  $\mathcal{N}$  mit  $Y \subseteq X$  und  $c \notin Y$ ?

## Aufgabe

Es sei  $M$  eine Menge. Zeigen Sie für alle  $X, Y, Z \in \mathcal{P}(M)$ :

- (1) Aus  $X \subseteq Y$  folgen  $X \cup Z \subseteq Y \cup Z$  und  $X \cap Z \subseteq Y \cap Z$ .
- (2) Die folgenden drei Aussagen sind äquivalent:

$$X \subseteq Y \quad \overline{X} \cup Y = M \quad X \cap \overline{Y} = \emptyset$$

Dabei wird in (2) das Komplement bezüglich  $M$  gebildet.

## Aufgabe

Wie viele Elemente besitzt  $\mathcal{P}(\{\emptyset, \{\emptyset, 1\}\})$ ? Geben Sie die Potenzmenge  $\mathcal{P}(\{\emptyset, \{\emptyset, 1\}\})$  explizit an.

## Aufgabe

Es seien definiert  $X := \{1\}$ ,  $Y := \{a, b\}$  und  $Z := \{\emptyset, \{\emptyset\}\}$ .

- (1) Wie viele Elemente besitzt die Menge  $X \times (Y \times \mathcal{P}(Z))$ ?
- (2) Geben Sie die Menge  $X \times (Y \times \mathcal{P}(Z))$  explizit an.
- (3) Wie viele Teilmengen von  $X \times (Y \times \mathcal{P}(Z))$  (d.h. Relationen von  $X$  nach  $Y \times \mathcal{P}(Z)$ ) gibt es und wie viele davon sind eindeutig bzw. Funktionen (mit Begründungen)?

## Aufgabe

Beweisen Sie für die durch

$$f(x) = x^2 + 3 \quad g(x) = (x+1)(x-1) + 4$$

definierten Funktionen  $f : \mathbb{N} \rightarrow \mathbb{N}$  und  $g : \mathbb{N} \rightarrow \mathbb{N}$  die Eigenschaft  $f = g$ .

## Aufgabe

Wir betrachten eine Menge  $M$  und eine Relation  $R$  auf  $M$ , welche definiert sind durch  $M := \{-2, -1, 0, 1, 2\}$  und  $R := \{(x, y) \in M \times M \mid x^2 + y^2 \leq 2\}$ .

- (1) Geben Sie die Relation  $R \subseteq M \times M$  in den folgenden Darstellungen an:
  - (a) Explizite Darstellung als Menge.
  - (b) Pfeildiagramm.
  - (c) Kreuzentabelle.
- (2) Ist die Relation  $R$  eindeutig bzw. total?

## Aufgabe

Zu einer Relation  $R \subseteq M \times N$  ist die transponierte Relation  $R^T \subseteq N \times M$  durch

$$R^T := \{(y, x) \mid x R y\}$$

definiert. Beweisen Sie für alle Relationen  $R, S \subseteq M \times N$  die Gleichungen  $(R^T)^T = R$ ,  $R^T \cup S^T = (R \cup S)^T$  und  $R^T \cap S^T = (R \cap S)^T$ .

## Aufgabe

Es sei  $P$  eine Menge von Personen und die Relationen  $V$  und  $M$  auf  $P$  seien wie folgt für alle Personen  $x$  und  $y$  aus  $M$  festgelegt:  $x V y$  gilt, falls  $x$  der Vater von  $y$  ist, und  $x M y$  gilt, falls  $x$  die Mutter von  $y$  ist. Definieren Sie mit Hilfe von  $V$  und  $M$  und ohne auf einzelne Personen Bezug zu nehmen eine Relation  $K$  auf  $P$  so, dass für alle Personen  $x$  und  $y$  die Beziehung  $x K y$  genau dann gilt, wenn  $x$  ein Kind von  $y$  ist.

## 2 Logische Grundlagen

Neben der Mengenlehre ist die Logik das zweite Fundament der Mathematik. Die Mengenlehre wird gebraucht, um die Objekte, für die man sich in der Mathematik interessiert, zu konstruieren, zu modellieren und zu manipulieren. Bisher kennen wir Paare, Relationen und Funktionen. Später werden noch lineare Listen, Bäume und Graphen dazukommen. Die Logik wird gebraucht, wenn in der Mathematik Beweise geführt werden, also in einer gewissen (logischen) Art und Weise argumentiert wird, um zu zeigen, dass eine Aussage wahr ist. Im Folgenden gehen wir auf die logischen Grundlagen der Mathematik ein. Auch hier wählen wir wieder einen **naiven** Zugang. Für die formale mathematische Logik gibt es im Laufe des Informatik-Studiums eigene Vorlesungen.

### 2.1 Sprache und Ausdrucksweise der Mathematik

Das Hauptgeschäft der Mathematikerinnen und Mathematiker ist das Beweisen. Dies heißt, zu einer aufgestellten Behauptung – einer Aussage im Sinne von Definition 1.1.4, normalerweise Satz genannt (oder Lemma, Hauptsatz, Proposition, Theorem etc.) – eine Rechtfertigung zu liefern, bei der, neben den schon bewiesenen Aussagen und einigen Grundannahmen (den sogenannten **Axiomen**), nur Regeln des logischen Schließens verwendet werden.

Wir haben Beweise im ersten Kapitel des Texts bisher mit den Mitteln der Umgangssprache geführt. Dabei ist vielleicht vielen Leserinnen und Lesern aufgefallen, dass bei der Formulierung der zu beweisenden Aussagen (welche wir dort immer als Sätze bezeichneten) gewisse Konstruktionen (Redewendungen, Formulierungen) immer wieder verwendet wurden und bei den Beweisen der Sätze, d.h. den logischen Rechtfertigungen der entsprechenden Aussagen, ebenfalls gewisse Konstruktionen (logische Schlussweisen und Argumentationen) immer wieder verwendet wurden. Die immer wieder verwendeten Konstruktionen beim Aufbau von Aussagen sind die nachfolgend angegebenen, in denen  $A$ ,  $A_1$  und  $A_2$  für Aussagen stehen,  $x$  für ein Objekt steht und  $A(x)$  wiederum für eine Aussage, nun über das Objekt  $x$ , steht.

- (1)  $A$  gilt nicht, bzw.  $A$  ist falsch (**Negation** von  $A$ ).
- (2)  $A_1$  gilt und  $A_2$  gilt, bzw.  $A_1$  und  $A_2$  gelten (**Konjunktion** von  $A_1$  und  $A_2$ ).
- (3)  $A_1$  gilt oder  $A_2$  gilt, bzw.  $A_1$  oder  $A_2$  gilt (**Disjunktion** von  $A_1$  und  $A_2$ ).
- (4) Aus  $A_1$  folgt  $A_2$ , bzw.  $A_1$  impliziert  $A_2$ , bzw. wenn  $A_1$  gilt, dann gilt auch  $A_2$  (**Implikation** von  $A_2$  aus  $A_1$ ).
- (5)  $A_1$  und  $A_2$  sind äquivalent, bzw.  $A_1$  und  $A_2$  sind gleichwertig, bzw. es gilt  $A_1$  genau dann, wenn  $A_2$  gilt (**Äquivalenz** von  $A_1$  und  $A_2$ ).
- (6) Für alle  $x$  gilt  $A(x)$  (**Allquantifizierung** mittels  $x$ ).
- (7) Es gibt ein  $x$  mit  $A(x)$ , bzw. es existiert ein  $x$ , so dass  $A(x)$  gilt (**Existenzquantifizierung** mittels  $x$ ).

Einige der bei den Beweisen von Kapitel 1 verwendeten umgangssprachlichen Schlussweisen sind etwa die nachfolgend aufgeführten, wobei wir auch jeweils eine Verwendungsstelle angeben.

- (1) „ $A$  impliziert  $A$ “ (Beweis von Satz 1.1.11, Teil (1)).
- (2) Gelten „ $A_1$  impliziert  $A_2$ “ und „ $A_2$  impliziert  $A_3$ “, dann gilt auch „ $A_1$  impliziert  $A_3$ “ (Beweis von Satz 1.1.11, Teil (3)).
- (3) „ $A_1$  und  $A_2$ “ ist äquivalent zu „ $A_2$  und  $A_1$ “ (Beweis von Satz 1.2.4, Teil (1)).
- (4) Gilt  $A(a)$ , so gilt auch „es gibt ein  $x$  mit  $A(x)$ “ (Beweis von Satz 1.2.6).
- (5) Gilt „es gilt  $A(x)$  für alle  $x$ “, so gilt  $A(a)$  (Beweis von Satz 1.4.11).

Dies alles wird, gegebenenfalls nach einer gewissen Eingewöhnung, wesentlich prägnanter, besser lesbar und auch besser manipulierbar, wenn man statt der Umgangssprache die Formelsprache der Mathematik verwendet. Ihre wichtigsten Symbole werden nachfolgend eingeführt. Sie entsprechen genau den obigen Konstruktionen (1) bis (7).

### 2.1.1 Definition: Konstruktionen der mathematischen Formelsprache

Die oben unter (1) bis (7) umgangssprachlich formulierten Aussagen werden in der Formelsprache der Mathematik wie folgt formuliert:

- (1)  $\neg A$
- (2)  $A_1 \wedge A_2$
- (3)  $A_1 \vee A_2$
- (4)  $A_1 \Rightarrow A_2$
- (5)  $A_1 \Leftrightarrow A_2$
- (6)  $\forall x : A(x)$  (Hier ist  $x$  durch das Symbol „ $\forall$ “ gebunden.)
- (7)  $\exists x : A(x)$  (Hier ist  $x$  durch das Symbol „ $\exists$ “ gebunden.)

Damit man beim Hinschreiben von Aussagen unter Verwendung der eben eingeführten Symbole Klammern sparen kann, wird angenommen, dass die Bindung der Symbole von oben nach unten in Gruppen abnimmt. Es bindet das Symbol „ $\neg$ “ am stärksten, dann kommen die Symbole „ $\wedge$ “ und „ $\vee$ “, die gleich stark binden, dann kommen die Symbole „ $\Rightarrow$ “ und „ $\Leftrightarrow$ “, die ebenfalls gleich stark binden, und am schwächsten binden der **Allquantor** „ $\forall$ “ und der **Existenzquantor** „ $\exists$ “.  $\square$

Statt  $\forall x : ((\neg A_1 \wedge A_2) \Rightarrow A_3)$  kann man also  $\forall x : \neg A_1 \wedge A_2 \Rightarrow A_3$  schreiben. Die obigen fünf umgangssprachlichen logischen Schlussweisen schreiben sich mit Hilfe der eben eingeführten Symbole wie folgt:

- (1)  $A \Rightarrow A$  (Reflexivität)
- (2)  $(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_3) \Rightarrow (A_1 \Rightarrow A_3)$  (Transitivität)
- (3)  $(A_1 \wedge A_2) \Leftrightarrow (A_2 \wedge A_1)$  (Kommutativität)
- (4)  $A(a) \Rightarrow (\exists x : A(x))$  (Zeuge zeigt Existenzquantifizierung)

$$(5) (\forall x : A(x)) \Rightarrow A(a) \quad (\text{Spezialisierung einer Allquantifizierung})$$

Solche in der Formelsprache hingeschriebenen Aussagen bezeichnen wir in Zukunft als **Formeln**. Allquantifizierungen und Existenzquantifizierungen kommen normalerweise nur in Verbindung mit Mengen vor, für deren Objekte die Variablen als Platzhalter stehen. Man kann dies auch als Typisierung von Variablen in Quantifizierungen oder als typisierte Quantifizierungen auffassen, wie wir es in Kapitel 1 schon einmal erwähnt haben. Für diese speziellen Konstruktionen werden Abkürzungen verwendet. Diese führen wir nun ein.

### 2.1.2 Festlegung: Quantoren mit typisierten Variablen

Es wird die Formel  $\forall x : x \in M \Rightarrow A(x)$  abgekürzt zu  $\forall x \in M : A(x)$ , und es wird die Formel  $\exists x : x \in M \wedge A(x)$  abgekürzt zu  $\exists x \in M : A(x)$   $\square$

Bis jetzt wissen wir nur, wie man Aussagen durch die Symbole von Definition 2.1.1 formal als Formeln hinschreibt. Was solche Formeln dann bedeuten, ist zumindest für die mittels der Konstruktionen (1), (2), (6) und (7) von Definition 2.1.1 aufgebauten intuitiv klar. Bei Formeln der Gestalt (3) kann man diskutieren, ob  $A_1 \vee A_2$  ausschließend (genau eine der Formeln muss wahr sein) oder nicht ausschließend (mindestens eine der Formeln muss wahr sein) gemeint ist. Und bei (4) ist nicht sofort klar, was passiert, wenn  $A_1$  nicht gilt. Wir werden uns bei den formalen Festlegungen von (3) und (4) später genau an das halten, was wir in Abschnitt 1.1 informell beschrieben haben. Die spezielle Interpretation von (4) hat natürlich auch Auswirkungen auf die Interpretation von (5), wenn man für die Implikation und die Äquivalenz die folgende „natürliche“ Eigenschaft fordert, die wir in Kapitel 1 beim Beweis von Satz 1.3.3 auch schon umgangssprachlich verwendet haben.

$$(A_1 \Leftrightarrow A_2) \Leftrightarrow (A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1)$$

In der „klassischen“ mathematischen Logik werden die obigen Konstruktionen normalerweise in zwei Gruppen aufgeteilt. Betrachtet man nur Formeln, die ohne Quantoren aufgebaut sind, so nennt man die entsprechende Logik Aussagenlogik. Diese wird im nächsten Abschnitt betrachtet. Kommen noch die beiden Quantoren hinzu, so spricht man von der Prädikatenlogik. Mit dieser Logik befassen wir uns im dritten Abschnitt dieses Kapitels.

## 2.2 Grundlagen der Aussagenlogik

Bei der Aussagenlogik beschäftigt man sich mit Formeln der Mathematik, in denen nur die Konstruktionen (1) bis (5) von Definition 2.1.1 vorkommen. Da man den Konstruktionsprozess ja mit irgendetwas beginnen muss, legt man eine Menge von sogenannten **atomaren Aussagen** oder **Aussagenvariablen** zugrunde, die für nicht weiter spezifizierte elementare und unzerteilbare Aussagen stehen. Man nimmt dazu einfach gewisse Symbole, wie  $a, b, a_1, a_2, \dots$ , und fügt diese zu einer Menge zusammen.

### 2.2.1 Definition: Formeln der Aussagenlogik

Es sei  $X := \{a_1, a_2, \dots, a_n\}$  eine nichtleere Menge atomarer Aussagen. Dann ist die Menge  $\mathcal{A}$  der **aussagenlogischen Formeln** über  $X$  durch die folgenden Regeln definiert:

- (1) Für alle  $a \in X$  gilt  $a \in \mathcal{A}$ .

- (2) Für alle  $A \in \mathcal{A}$  gilt  $\neg A \in \mathcal{A}$ .
- (3) Für alle  $A_1, A_2 \in \mathcal{A}$  gelten auch  $A_1 \wedge A_2 \in \mathcal{A}$ ,  $A_1 \vee A_2 \in \mathcal{A}$ ,  $A_1 \Rightarrow A_2 \in \mathcal{A}$  und  $A_1 \Leftrightarrow A_2 \in \mathcal{A}$ .

Damit man nicht noch zusätzliche Elemente in die Menge  $\mathcal{A}$  bekommt, die man nicht als Formeln haben will, legt man noch fest:

- (4) Es gibt keine Elemente in  $\mathcal{A}$  außer denen, die durch die Regeln (1) bis (3) zugelassen werden.

Zu Strukturierungszwecken sind bei den Anwendungen von (2) und (3) noch die Klammern „(“ und „)“ erlaubt. Die Vorrangregeln der Formeln von  $\mathcal{A}$  sind genau die, welche in Definition 2.1.1 festgelegt wurden.  $\square$

Nachfolgend geben wir einige Beispiele an.

### 2.2.2 Beispiele: aussagenlogische Formeln

Es seien  $a, b, c$  atomare Aussagen, d.h.  $X := \{a, b, c\}$ . Dann sind

$$a \wedge b \Rightarrow a \vee b \quad \neg a \Rightarrow (b \Rightarrow a) \quad a \wedge b \Rightarrow (a \wedge b) \vee c$$

drei aussagenlogische Formeln. Verwendet man überflüssige Klammern, so schreiben sich diese Formeln auch wie folgt:

$$(a \wedge b) \Rightarrow (a \vee b) \quad (\neg a) \Rightarrow (b \Rightarrow a) \quad (a \wedge b) \Rightarrow ((a \wedge b) \vee c)$$

Zusätzliche Klammern machen manchmal Zusammenhänge klarer. Zu viele Klammern können hingegen auch verwirren. Es ist deshalb sinnvoll, ein vernünftiges Mittelmaß zu finden. Hingegen sind die Gebilde

$$a \Rightarrow \Rightarrow \quad \Rightarrow (a \wedge b) \quad (a \Rightarrow b) \Rightarrow a \vee b$$

offensichtlich keine aussagenlogischen Formeln.  $\square$

Erinnern wir uns: Aussagen sind nach Aristoteles sprachliche Gebilde, von denen es Sinn macht, zu sagen, ob sie wahr oder falsch sind. Man ordnet ihnen also einen Wahrheitswert zu. Damit wir mit Wahrheitswerten formal argumentieren können, modellieren wir sie durch spezielle Objekte.

### 2.2.3 Definition: Wahrheitswerte

Die Menge  $\mathbb{B} := \{W, F\}$  heißt Menge der **Wahrheitswerte**. Dabei steht  $W$  für „wahr“ (oder gültig, richtig) und  $F$  für „falsch“ (oder nicht gültig, nicht richtig).  $\square$

Manchmal werden auch andere Bezeichnungen für Wahrheitswerte verwendet, etwa  $L$  oder  $1$  statt  $W$  und  $O$  oder  $0$  statt  $F$ . Um den Wahrheitswert (kurz: den Wert) einer aussagenlogischen Formel bestimmen zu können, muss man nur wissen, welchen Wert die jeweils darin vorkommenden atomaren Aussagen haben und wie diese Werte sich durch die sogenannten **Junkturen** „ $\neg$ “, „ $\wedge$ “, „ $\vee$ “, „ $\Rightarrow$ “ und „ $\Leftrightarrow$ “ fortsetzen. Letzteres wird nachfolgend

definiert. Die Werte der atomaren Aussagen werden normalerweise nicht spezifiziert. Sie ergeben sich jeweils aus dem vorliegenden Kontext. So hat z.B. die atomare Aussage  $1 < 2$  den Wert **W** und die atomare Aussage  $1 \in \{2, 3\}$  den Wert **F**. Wenn wir jedoch die speziellen Aussagen **wahr** und **falsch** aus Kapitel 1 nun als atomare Aussagen auffassen, dann wird natürlich **W** für **wahr** als Wert festgelegt und **F** als Wert für **falsch**.

#### 2.2.4 Definition: Bedeutung der Junktoren

Die Werte der aussagenlogischen Formeln, welche in Definition 2.1.1 nach den Regeln (2) und (3) gebildet werden, sind durch die nachfolgenden Tafeln festgelegt:

(1) Negation

| $A$      | $\neg A$ |
|----------|----------|
| <b>W</b> | <b>F</b> |
| <b>F</b> | <b>W</b> |

(2) Konjunktion

| $A_1$    | $A_2$    | $A_1 \wedge A_2$ |
|----------|----------|------------------|
| <b>W</b> | <b>W</b> | <b>W</b>         |
| <b>W</b> | <b>F</b> | <b>F</b>         |
| <b>F</b> | <b>W</b> | <b>F</b>         |
| <b>F</b> | <b>F</b> | <b>F</b>         |

(3) Disjunktion

| $A_1$    | $A_2$    | $A_1 \vee A_2$ |
|----------|----------|----------------|
| <b>W</b> | <b>W</b> | <b>W</b>       |
| <b>W</b> | <b>F</b> | <b>W</b>       |
| <b>F</b> | <b>W</b> | <b>W</b>       |
| <b>F</b> | <b>F</b> | <b>F</b>       |

(4) Implikation

| $A_1$    | $A_2$    | $A_1 \Rightarrow A_2$ |
|----------|----------|-----------------------|
| <b>W</b> | <b>W</b> | <b>W</b>              |
| <b>W</b> | <b>F</b> | <b>F</b>              |
| <b>F</b> | <b>W</b> | <b>W</b>              |
| <b>F</b> | <b>F</b> | <b>W</b>              |

(5) Äquivalenz

| $A_1$    | $A_2$    | $A_1 \Leftrightarrow A_2$ |
|----------|----------|---------------------------|
| <b>W</b> | <b>W</b> | <b>W</b>                  |
| <b>W</b> | <b>F</b> | <b>F</b>                  |
| <b>F</b> | <b>W</b> | <b>F</b>                  |
| <b>F</b> | <b>F</b> | <b>W</b>                  |

Durch (3) wird die Disjunktion „nicht ausschließend“ (vergl. mit Abschnitt 1.1).  $\square$

Man beachte, dass die Implikation durch die entsprechende Tafel von (4) so spezifiziert ist, dass im Sinne der Logik aus einer falschen Aussage alles gefolgert werden kann (vergl. nochmals mit Abschnitt 1.1). Die Zuordnung von Wahrheitswerten zu den atomaren Aussagen nennt man eine **Belegung**. Auch den zugeordneten Wahrheitswert nennt man dann so. Kennt man also die Belegung ihrer atomaren Aussagen, so kann man den Wert einer jeden aussagenlogischen Formel gemäß den Tafeln von Definition 2.2.4 ausrechnen. Formal kann man den Wert einer Formel zu einer Belegung definieren, indem man Belegungen

als Funktionen spezifiziert und bei der Wertdefinition dem Aufbau der Formeln folgt. Wir bleiben hier aber informeller, da dies für alles Weitere genügt. Belegungen geben wir nachfolgend durch das Zeichen  $\hat{=}$  an.

### 2.2.5 Beispiel: Berechnung des Wertes einer Formel

Es sei die Menge  $X := \{a, b, c\}$  von drei atomaren Aussagen (Aussagenvariablen) gegeben. Wir berechnen den Wert der aussagenlogischen Formel

$$\neg((a \Rightarrow (b \Rightarrow c)) \wedge (a \vee b))$$

zur Belegung der atomaren Aussagen mittels  $a \hat{=} W$ ,  $b \hat{=} W$  und  $c \hat{=} F$  und stellen die Berechnung als Folge von Schritten dar. Im ersten Schritt ersetzen wir jede atomare Aussage durch ihre Belegung. Dies bringt:

$$\neg((W \Rightarrow (W \Rightarrow F)) \wedge (W \vee W))$$

Dann werten wir dies, wie von der weiterbildenden Schule her bei arithmetischen Ausdrücken bekannt, von innen nach außen aus. Dies bringt zuerst

$$\neg((W \Rightarrow F) \wedge W),$$

indem die Tafeln für „ $\Rightarrow$ “ und „ $\vee$ “ angewendet werden, und dann

$$\neg(F \wedge W)$$

indem die Tafel für „ $\Rightarrow$ “ angewendet wird, und dann

$$\neg F,$$

indem die Tafel für „ $\wedge$ “ angewendet wird, und schließlich

$$W,$$

indem die Tafel für „ $\neg$ “ angewendet wird. Also ist die Ausgangsformel zur Belegung  $a \hat{=} W$ ,  $b \hat{=} W$  und  $c \hat{=} F$  wahr.  $\square$

Eine oft vorkommende Aufgabe ist, zu zeigen, dass zwei Formeln  $A_1$  und  $A_2$  den gleichen Wert haben, unabhängig davon, ob dieser  $W$  oder  $F$  ist. Wenn man dies als Beziehung zwischen Formeln definiert, dann erhält man die folgende Festlegung.

### 2.2.6 Definition: logische Äquivalenz

Zwei aussagenlogische Formeln heißen **logisch äquivalent**, wenn jede Belegung ihrer atomaren Aussagen durch jeweils gleiche Wahrheitswerte dazu führt, dass die beiden Formeln den gleichen Wert besitzen.  $\square$

Die logische Äquivalenz von aussagenlogischen Formeln bestimmt man oft dadurch, dass man zu einer angenommenen festen Belegung in Form einer Tabelle alle möglichen Werte gemäß dem Aufbau durchprobiert und die entstehenden Werte jeweils vergleicht. Wir demonstrieren dieses Vorgehen mittels Wahrheitstabellen, welches in seiner nun gebräuchlichen Form dem österreichischen Philosophen Ludwig Wittgenstein (1889-1951) und dem polnischen Logiker und Mathematiker Emil Post (1897-1954) zugeschrieben wird, im nächsten Satz anhand einiger bekannter Formeln.

### 2.2.7 Satz: grundlegende logische Äquivalenzen

Die nachfolgend angegebenen sieben Paare von aussagenlogischen Formeln sind jeweils logisch äquivalent.

- |     |                             |  |
|-----|-----------------------------|--|
| (1) | $A$                         | $\neg\neg A$   |
| (2) | $A_1 \Leftrightarrow A_2$   | $(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1)$ |
| (3) | $A_1 \Rightarrow A_2$       | $\neg A_1 \vee A_2$                                  |
| (4) | $\neg(A_1 \wedge A_2)$      | $\neg A_1 \vee \neg A_2$                             |
| (5) | $\neg(A_1 \vee A_2)$        | $\neg A_1 \wedge \neg A_2$                           |
| (6) | $A_1 \wedge (A_2 \vee A_3)$ | $(A_1 \wedge A_2) \vee (A_1 \wedge A_3)$             |
| (7) | $A_1 \vee (A_2 \wedge A_3)$ | $(A_1 \vee A_2) \wedge (A_1 \vee A_3)$               |

**Beweis:** (1) Wir betrachten die folgende Tabelle aller möglicher Werte von  $A$ ,  $\neg A$  und  $\neg\neg A$  zu einer beliebig vergebenen Belegung (die im Beweis nicht explizit gebraucht wird):

| $A$ | $\neg A$ | $\neg\neg A$ |
|-----|----------|--------------|
| W   | F        | W            |
| F   | W        | F            |

Da die erste und die dritte Spalte identisch sind, ist die logische Äquivalenz gezeigt.

(2) In diesem Fall ist die Tabelle aller möglichen Werte von  $A_1$  und  $A_2$  und die sich daraus ergebenden Werte von  $A_1 \Leftrightarrow A_2$  und von  $(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1)$  analog zum Beweis von (1) wie folgt gegeben. Ihre dritte und vierte Spalte sind wiederum identisch. Dadurch ist die Behauptung gezeigt.

| $A_1$ | $A_2$ | $A_1 \Leftrightarrow A_2$ | $(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1)$ |
|-------|-------|---------------------------|--|
| W     | W     | W                         | W  |
| W     | F     | F                         | F  |
| F     | W     | F                         | F  |
| F     | F     | W                         | W  |

(3) Und hier ist noch die Tabelle aller möglichen Werte von  $A_1$  und  $A_2$  und den sich daraus ergebenden Werten für  $A_1 \Rightarrow A_2$ ,  $\neg A_1$  und  $\neg A_1 \vee A_2$  analog zum Beweis von (2), wobei die dritte und fünfte Spalte die behauptete logische Äquivalenz zeigen.

| $A_1$ | $A_2$ | $A_1 \Rightarrow A_2$ | $\neg A_1$ | $\neg A_1 \vee A_2$ |
|-------|-------|-----------------------|------------|---------------------|
| W     | W     | W                     | F          | W                   |
| W     | F     | F                     | F          | F                   |
| F     | W     | W                     | W          | W                   |
| F     | F     | W                     | W          | W                   |

Die Behauptungen (4) bis (7) beweist man vollkommen analog.  $\square$

Man nennt die logischen Äquivalenzen (4) und (5) von Satz 2.2.7 wiederum **Regel von de Morgan** und die logischen Äquivalenzen (6) und (7) **Distributivgesetze**. Der folgende Satz setzt nun die logische Äquivalenz von Formeln, die ja eine Beziehung zwischen Formeln herstellt, also eine Relation auf der Menge  $\mathcal{A}$  im Sinne von Kapitel 1 ist, mit dem Wert (also der Gültigkeit) einer Formel in Beziehung. Das Resultat wird niemanden

überraschen. Es zeigt aber sehr schön, dass man in der Mathematik oft auf verschiedenen Sprachebenen argumentiert. Es wird in ihm nämlich die Äquivalenz auf drei verschiedenen Ebenen angegeben, in (2) in Gestalt einer Formel, in (1) in Gestalt einer speziellen Beziehung zwischen Formeln und schließlich noch auf der umgangssprachlichen Metaebene.

### 2.2.8 Satz: logische Äquivalenz und Gültigkeit

Für alle aussagenlogischen Formeln  $A_1$  und  $A_2$  sind die folgenden zwei Eigenschaften äquivalent.

- (1) Die Formeln  $A_1$  und  $A_2$  sind logisch äquivalent.
- (2) Die Formel  $A_1 \Leftrightarrow A_2$  hat den Wert  $W$  für alle Belegungen ihrer atomaren Aussagen.

**Beweis:** Wir zeigen zuerst, dass (2) aus (1) folgt. Es seien also  $A_1$  und  $A_2$  logisch äquivalent. Weiterhin sei eine beliebige Belegung der atomaren Aussagen gegeben. Wir unterscheiden zwei Fälle.

- (a) Beide Formeln haben zu der gegebenen Belegung  $W$  als Wert. Dann hat aufgrund von Definition 2.2.4, Punkt (5), auch die Formel  $A_1 \Leftrightarrow A_2$  den Wert  $W$ .
- (b) Beide Formeln haben zu der Belegung  $F$  als Wert. Dann hat aufgrund von Definition 2.2.4, Punkt (5), die Formel  $A_1 \Leftrightarrow A_2$  ebenfalls den Wert  $W$ .

Nun beweisen wir, dass (1) aus (2) folgt. Dazu sei eine beliebige Belegung der atomaren Aussagen vorgegeben. Hat die Formel  $A_1 \Leftrightarrow A_2$  bezüglich ihr den Wert  $W$ , dann müssen  $A_1$  und  $A_2$  bezüglich ihr beide den Wert  $W$  oder beide den Wert  $F$  haben. Dies sehen wir, indem wir in Definition 2.2.4 (5) alle Zeilen der Tabelle durchgehen. Die Formeln sind also per Definition logisch äquivalent.  $\square$

Satz 2.2.7 besagt insbesondere, dass die folgenden aussagenlogischen Formeln für alle Belegungen der atomaren Aussagen den Wert  $W$  haben, also immer wahr sind:

$$\begin{aligned}
A &\Leftrightarrow \neg\neg A \\
(A_1 \Leftrightarrow A_2) &\Leftrightarrow (A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1) \\
(A_1 \Rightarrow A_2) &\Leftrightarrow \neg A_1 \vee A_2 \\
\neg(A_1 \wedge A_2) &\Leftrightarrow \neg A_1 \vee \neg A_2 \\
\neg(A_1 \vee A_2) &\Leftrightarrow \neg A_1 \wedge \neg A_2 \\
A_1 \wedge (A_2 \vee A_3) &\Leftrightarrow (A_1 \wedge A_2) \vee (A_1 \wedge A_3) \\
A_1 \vee (A_2 \wedge A_3) &\Leftrightarrow (A_1 \vee A_2) \wedge (A_1 \vee A_3)
\end{aligned}$$

Neben diesen Formeln gibt es noch weitere wichtige Formeln der Aussagenlogik, beispielsweise die offensichtliche Kommutativität und die auch offensichtliche Assoziativität der Konjunktion und der Disjunktion, welche erlauben, Klammern zu sparen. Auch ist klar, dass  $A \vee \neg A$  und **wahr** logisch äquivalent sind und dieses auch für  $A \wedge \neg A$  und **falsch** zutrifft. Wir wollen aber nicht näher auf weitere wichtige wahre Formeln der Aussagenlogik eingehen, sondern uns nun einem anderen Thema aus diesem Gebiet zuwenden.

Bisher stellt die tabellarische Methode die einzige Möglichkeit dar, zu zeigen, dass zwei

Formeln logisch äquivalent sind. Bei großen Formeln stößt diese Methode bald an ihre Grenzen, da die Anzahl der Belegungen ihrer atomaren Formeln sehr groß wird. Hier ist es viel vorteilhafter, zu rechnen, wie man es von der weiterbildenden Schule her von den Zahlen und den arithmetischen Ausdrücken kennt. Diese zweite Möglichkeit, die logischen Äquivalenzen von aussagenlogischen Formeln zu beweisen, besteht in **logischen Umformungen** gemäß schon als richtig bewiesenen logischen Äquivalenzen (in diesem Zusammenhang auch **Regeln** genannt). Dem liegt zugrunde, dass

- (1) die Formeln  $A_1$  und  $A_3$  logisch äquivalent sind, wenn es eine Formel  $A_2$  so gibt, dass  $A_1$  und  $A_2$  logisch äquivalent sind und  $A_2$  und  $A_3$  logisch äquivalent sind und
- (2) die Formeln  $A_1$  und  $A_2$  logisch äquivalent sind, wenn es in  $A_1$  eine Teilformel gibt, deren Ersetzung durch eine logisch äquivalente Formel  $A_2$  liefert.

So sind etwa  $A_1 \wedge A_2$  und  $A_1 \wedge A_3$  logisch äquivalent, wenn  $A_2$  und  $A_3$  logisch äquivalent sind, und  $\neg(A_1 \Rightarrow A_2)$  und  $\neg(A_1 \Rightarrow A_3)$  sind logisch äquivalent, wenn  $A_2$  und  $A_3$  logisch äquivalent sind. Normalerweise schreibt man solche Beweise durch logische Umformungen in Form von sogenannten **Äquivalenzketten** auf, wie etwa beim Beweis

$$\begin{aligned} A_1 &\iff A_2 && \text{Begründung des Schritts} \\ &\iff A_3 && \text{Begründung des Schritts} \\ &\iff A_4 && \\ &\iff A_5 && \text{Begründung des Schritts} \end{aligned}$$

der logischen Äquivalenz von  $A_1$  und  $A_5$  mittels der Zwischenformeln  $A_2$ ,  $A_3$  und  $A_4$ . In so einer **Rechnung** steht das Symbol „ $\iff$ “ (man beachte den Unterschied zum Junktor „ $\Leftrightarrow$ “) für die Relation der logischen Äquivalenz auf der Menge  $\mathcal{A}$ . Begründungen können in solchen Rechnungen weggelassen werden, wenn sie offensichtlich sind. Auch Angaben im umgebenden Text sind oft sinnvoll. Nachfolgend geben wir drei Beispiele an.

## 2.2.9 Satz: weitere logische Äquivalenzen

Für aussagenlogische Formeln gelten die folgenden logischen Äquivalenzen:

- (1)  $A_1 \Rightarrow (A_2 \Rightarrow A_3) \iff A_1 \wedge A_2 \Rightarrow A_3$
- (2)  $A_1 \Rightarrow A_2 \iff \neg A_2 \Rightarrow \neg A_1$
- (3)  $A_1 \Rightarrow A_2 \iff A_1 \Rightarrow A_1 \wedge A_2$  und  $A_1 \Rightarrow A_2 \iff A_1 \vee A_2 \Rightarrow A_2$

**Beweis:** (1) Hier kommen wir mit der folgenden Äquivalenzkette zum Ziel.

$$\begin{aligned} A_1 \Rightarrow (A_2 \Rightarrow A_3) &\iff \neg A_1 \vee (A_2 \Rightarrow A_3) && \text{Satz 2.2.7, (3)} \\ &\iff \neg A_1 \vee (\neg A_2 \vee A_3) && \text{Satz 2.2.7, (3)} \\ &\iff (\neg A_1 \vee \neg A_2) \vee A_3 && \text{Assoziativität} \\ &\iff \neg(A_1 \wedge A_2) \vee A_3 && \text{de Morgan} \\ &\iff A_1 \wedge A_2 \Rightarrow A_3 && \text{Satz 2.2.7, (3)} \end{aligned}$$

(2) Die Behauptung folgt aus der folgenden Rechnung.

$$\begin{aligned} A_1 \Rightarrow A_2 &\iff \neg A_1 \vee A_2 && \text{Satz 2.2.7, (3)} \\ &\iff A_2 \vee \neg A_1 && \text{Kommutativität} \\ &\iff \neg \neg A_2 \vee \neg A_1 && \text{Satz 2.2.7, (1)} \\ &\iff \neg A_2 \Rightarrow \neg A_1 && \text{Satz 2.2.7, (3)} \end{aligned}$$

(3) Die linke logische Äquivalenz folgt aus der Rechnung

$$\begin{aligned}
 A_1 \Rightarrow A_1 \wedge A_2 &\iff \neg A_1 \vee (A_1 \wedge A_2) && \text{Satz 2.2.7, (3)} \\
 &\iff (\neg A_1 \vee A_1) \wedge (\neg A_1 \vee A_2) && \text{Distributivit\"at} \\
 &\iff \mathbf{wahr} \wedge (\neg A_1 \vee A_2) \\
 &\iff \neg A_1 \vee A_2 \\
 &\iff A_1 \Rightarrow A_2 && \text{Satz 2.2.7, (3)}
 \end{aligned}$$

(wobei die Schritte ohne Begründungen klar sind) und  $A_1 \Rightarrow A_2 \iff A_1 \vee A_2 \Rightarrow A_2$  zeigt man in einer ähnlichen Weise.  $\square$

Mittels der bisherigen Formeln und Regeln (und noch vieler Regeln, die wir aus Platzgründen nicht betrachten) kann man nun die Beweise von Kapitel 1, in denen keine Quantoren auftauchen, wesentlich knapper und präziser formulieren. Wir wollen dies nun demonstrieren. Dabei greifen wir zwei Mengengleichheiten auf, von denen wir eine schon umgangssprachlich in Kapitel 1 bewiesen haben. Die folgenden Rechnungen sind sehr detailliert und deshalb etwas l\"anglich; wer erfahrener in der Mathematik ist, wendet in einem Umformungsschritt oft mehrere Regeln gleichzeitig an. Dies macht die Ketten k\"urzer.

### 2.2.10 Beispiele: Beweis von Mengengleichheiten

Für alle Mengen  $M$ ,  $N$  und  $P$  und alle Objekte  $x$  können wir wie folgt logisch umformen.

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

Diese Rechnung zeigt die Mengengleichheit  $M \setminus (N \cap P) = (M \setminus N) \cup (M \setminus P)$ . Analog bekommen wir, indem wir wiederum das Symbol „ $\notin$ “ durch das logische Negationssymbol „ $\neg$ “ und das Enthalteinssymbol „ $\in$ “ ausdrücken, die Rechnung

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

und diese zeigt  $M \setminus (M \setminus N) = M \cap N$ . Wir haben in diesen Rechnungen keine Begründungen angegeben und empfehlen der Leserin oder dem Leser zu Übungszwecken, diese zu ergänzen.  $\square$

Neben der Relation der logischen Äquivalenz auf  $\mathcal{A}$  gibt es noch die Relation der logischen Implikation auf  $\mathcal{A}$ . Eine aussagenlogische Formel  $A_1$  **impliziert logisch** eine aussagenlogische Formel  $A_2$ , wenn für alle Belegungen ihrer atomaren Aussagen durch jeweils gleiche Wahrheitswerte gilt: Liefert  $A_1$  den Wert  $W$ , so liefert auch  $A_2$  den Wert  $W$ . Man kann zeigen, dass dies gleichwertig dazu ist, dass der Wert der Formel  $A_1 \Rightarrow A_2$  für alle Belegungen immer gleich zu  $W$  ist.

Logische Implikationen kann man ebenfalls tabellarisch oder durch Umformungen zeigen. Wir wollen hier nicht auf alle Einzelheiten eingehen, da vieles analog zum Vorgehen bei logischen Äquivalenzen funktioniert, sondern nur ein schematisches Beispiel für die zweite Methode skizzieren. Eine Rechnung zum Beweis der logischen Implikation von  $A_6$  aus  $A_1$  mit Zwischenformeln  $A_2, A_3, A_4$  und  $A_5$  wäre etwa

$$\begin{array}{ll} A_1 \iff A_2 & \text{Begründung des Schritts} \\ \implies A_3 & \text{Begründung des Schritts} \\ \implies A_4 & \\ \iff A_5 & \text{Begründung des Schritts} \\ \iff A_6. & \end{array}$$

Hier stellt „ $\implies$ “ die Relation der logischen Implikation auf  $\mathcal{A}$  dar, der erste Schritt ist eine Äquivalenzumformung, dann kommen zwei Implikationsumformungen und am Schluss kommen noch einmal zwei Äquivalenzumformungen. Zwei der Schritte besitzen keine Begründung. Für solche Beweise wichtig ist, neben den obigen Eigenschaften (1) und (2) der logischen Äquivalenz, dass für alle Formeln  $A_1, A_2$  und  $A_3$

- (1) aus  $A_1 \implies A_2$  und  $A_2 \implies A_3$  folgt  $A_1 \implies A_3$ ,
- (2) aus  $A_1 \implies A_2$  und  $A_2 \iff A_3$  folgt  $A_1 \implies A_3$
- (3) und aus  $A_1 \iff A_2$  und  $A_2 \implies A_3$  folgt  $A_1 \implies A_3$ .

Man beachte, dass  $A_1 \implies A_2$  nicht immer gilt, wenn  $A_2$  aus  $A_1$  dadurch entsteht, dass eine Teilformel durch eine Formel ersetzt wird, die von der Teilformel logisch impliziert wird. Das Vorkommen von Negationen und Implikationen macht hier Schwierigkeiten. Die wichtigste Verbindung zwischen der logischen Äquivalenz und der logischen Implikation ist im nachfolgenden Satz angegeben. Sie ist die Entsprechung der schon erwähnten und für jede Belegung  $W$  als Wert liefernden Formel  $(A_1 \iff A_2) \Leftrightarrow (A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_1)$  in der mathematischen Umgangssprache, indem die Junktoren „ $\iff$ “, „ $\Rightarrow$ “ und „ $\wedge$ “ durch die zwei Relationen „ $\iff$ “ und „ $\implies$ “ und das umgangssprachliche „und“ ersetzt werden. Der Satz wird oft beim Beweisen von logischen Äquivalenzen verwendet, indem man den Beweis von  $A_1 \iff A_2$  in zwei Beweise von logischen Implikationen aufspaltet.

### 2.2.11 Satz: logische Äquivalenz und logische Implikation

Für alle aussagenlogischen Formeln  $A_1$  und  $A_2$  gilt die logische Äquivalenz  $A_1 \iff A_2$  genau dann, wenn die logischen Implikationen  $A_1 \implies A_2$  und  $A_2 \implies A_1$  gelten.  $\square$

An dieser Stelle ist noch eine Warnung angebracht. Die Erfahrung zeigt, dass bei Ketten logischer Umformungen besonders Anfänger den Fehler machen, eine logische Äquivalenz zu behaupten, auch wenn sie nur eine logische Implikation überprüft haben (und möglicherweise auch nur eine solche gilt). Dies liegt oft daran, dass man für die andere logische Implikation von rechts nach links oder von unten nach oben denken muss, was nicht dem gewohnten Fluss entspricht. Es wird daher eindringlich empfohlen, bei einer behaupteten logischen Äquivalenz  $A_1 \iff A_2$  wirklich beide logischen Implikationen  $A_1 \implies A_2$  und  $A_2 \implies A_1$  zu prüfen.

Weitere wichtige Regeln beim Rechnen mit logischen Implikationen bzw. dem Beweisen sind  $A_1 \wedge A_2 \implies A_1$  und  $A_1 \implies A_1 \vee A_2$ , diese entsprechen der Einschließungseigenschaft bei Mengen, der sogenannte **Modus ponens**  $A_1 \wedge (A_1 \implies A_2) \implies A_2$ , sowie **falsch  $\implies A$**  und  **$A \implies wahr$** . Alle diese Eigenschaften sind wiederum Entsprechungen von aussagenlogischen Formeln, die immer der Wert  $W$  liefern. Beispielsweise ist  $A_1 \wedge (A_1 \implies A_2) \Rightarrow A_2$  die Entsprechung des Modus ponens.

## 2.3 Grundlagen der Prädikatenlogik

Die im letzten Abschnitt vorgestellte Aussagenlogik und deren Regeln zur logischen Äquivalenz und zur logischen Implikation auf ihren Formeln stellen einen Rahmen dar, in dem die meisten der einem mathematischen Beweis zugrundeliegenden logischen Schritte formalisiert werden können. Für die gesamte Mathematik ist ihre Ausdrucksstärke aber viel zu schwach. Mathematik will ja oft Aussagen über alle Objekte einer vorgegebenen Menge machen oder auch darüber, ob ein Objekt mit einer bestimmten Eigenschaft existiert. Dies ist in der Aussagenlogik nicht möglich. Man braucht dazu noch die Allquantoren und die Existenzquantoren in Formeln, also alle in Abschnitt 2.1 eingeführten Möglichkeiten (1) bis (7) zur Konstruktion von Formeln. Um ein Gefühl für solche Formeln mit Quantoren zu bekommen, geben wir zuerst einige Beispiele an, die Aussagen (Eigenschaften von Objekten) als Formeln beschreiben, bevor wir dann später näher auf die Festlegung der entsprechenden Logik eingehen. Wie schon bei der Aussagenlogik, so werden wir auch im Folgenden nicht in der formalen Strenge vorgehen, wie es üblicherweise in einer Logikvorlesung der Fall ist.

### 2.3.1 Beispiele: Formeln der Prädikatenlogik

Es sei  $n$  eine natürliche Zahl. Die Formel  $A_1(n)$ , welche definiert ist als

$$\exists x : x \in \mathbb{N} \wedge n = 2x,$$

beschreibt dann, dass  $n$  eine **gerade** natürliche Zahl ist. Ihre Kurzform gemäß der Festlegung 2.1.2, bei der der Existenzquantor direkt mit dem Enthalteinssymbol „ $\in$ “ kombiniert wird, ist nachfolgend angegeben:

$$\exists x \in \mathbb{N} : n = 2x$$

Es muss also die Festlegung des Wertes von Formeln so erfolgen, dass die Formel  $A_1(n)$  den Wert  $W$  genau dann hat, wenn  $n$  eine gerade Zahl ist. Die Gültigkeit von  $n \in \mathbb{N}$  ist dabei explizit angenommen.

Es sei  $M$  eine Menge. Die Formel  $A_2(M)$ , nun definiert durch

$$\exists x : x \in M \wedge \forall y : y \in M \Rightarrow x = y,$$

beschreibt, dass die Menge  $M$  genau ein Element enthält. Sie muss also später  $W$  als Wert zugeordnet bekommen genau für alle Mengen  $M$  der speziellen Gestalt  $\{a\}$ , d.h. alle eelementigen Mengen  $M$ . Die Kurzform

$$\exists x \in M : \forall y \in M : x = y$$

von  $A_2(M)$  ergibt sich wieder aufgrund der Festlegung 2.1.2.

Will man mittels einer Formel festlegen, dass die Menge  $M$  genau zwei Elemente besitzt, so ist dies etwa möglich, indem man die obige Formel  $A_2(M)$  zur folgenden Formel  $A_3(M)$  abändert:

$$\exists x : x \in M \wedge \exists y : y \in M \wedge x \neq y \wedge \forall z : z \in M \Rightarrow z = x \vee z = y$$

Nach der Festlegung 2.1.2 ist  $A_3(M)$  gleichbedeutend zur folgenden Formel:

$$\exists x \in M : \exists y \in M : x \neq y \wedge \forall z \in M : z = x \vee z = y$$

Sogenannte Blöcke gleicher Quantoren zieht man oft zu einem Quantor zusammen, schreibt also statt der letzten Formel auch

$$\exists x \in M, y \in M : x \neq y \wedge \forall z \in M : z = x \vee z = y$$

oder sogar, noch kürzer, auch

$$\exists x, y \in M : x \neq y \wedge \forall z \in M : z = x \vee z = y.$$

Auch Abkürzungen wie  $a \leq x \leq b$  für  $a \leq x \wedge x \leq b$  und  $a \leq x < b$  für  $a \leq x \wedge x < b$  sind in der Praxis üblich. Man sollte aber solche Vereinfachungen der Schreibweisen nicht übertreiben, insbesondere im Hinblick auf die Quantifizierungen. Beim formalen Arbeiten mit Formeln sind sie nämlich manchmal hinderlich und müssen in gewissen Situationen erst wieder rückgängig gemacht werden, damit man die gewünschten Rechnungen durchführen kann.  $\square$

Man beachte, dass man nicht durch  $|M| = 1$  spezifizieren kann, dass  $M$  eine eelementige Menge ist, und auch nicht durch  $|M| = 2$ , dass  $M$  zweielementig ist. Der Ausdruck  $|M|$  ist nämlich nur für endliche Mengen definiert und liefert nur für solche Mengen eine natürliche Zahl als Wert. Damit ist nicht klar, was die Werte der Formeln  $|M| = 1$  und  $|M| = 2$  für unendliche Mengen sind.

In den obigen Beispielen haben wir zu den Formeln auch jeweils in der (mathematischen) Umgangssprache angegeben, was sie besagen. Formeln sind ein wichtiges Hilfsmittel, wenn man Eigenschaften eindeutig beschreiben will. Eine Spezifikation in der Umgangssprache führt oft zu Mehrdeutigkeiten. Formeln und ihre mathematische Manipulation sind auch wichtig, wenn Beweise geführt werden.

### 2.3.2 Beispiel: Mehrdeutigkeit bei Umgangssprache

Es sei die Aufgabe gestellt, die Menge  $M$  der Quadrate der Vielfachen von 4 anzugeben, die kleiner als 18 sind. Was hat nun kleiner als 18 zu sein? Die obige umgangssprachliche Formulierung erlaubt zwei Interpretationen. Ist „kleiner als 18“ eine Forderung an die Quadrate der Vielfachen von 4, so sind nur 0 und 16 die möglichen Objekte von  $M$ , also

$$M := \{x \in \mathbb{N} \mid \exists n \in \mathbb{N} : x = (4n)^2 \wedge x \leq 18\} = \{0, 16\},$$

da schon  $8^2 > 18$  gilt. Haben jedoch die Vielfachen von 4 kleiner als 18 zu sein, so gilt

$$M := \{x \in \mathbb{N} \mid \exists n \in \mathbb{N} : x = (4n)^2 \wedge 4n \leq 18\} = \{0, 16, 64, 144, 256\}.$$

Durch die deskriptiven Mengenbeschreibungen mittels Formeln werden Mehrfachinterpretationen vermieden.  $\square$

Zu Mitteilungszwecken sind Formeln aber oft zu detailliert. Deshalb werden in der Mathematik entsprechende Begriffe für die Gültigkeiten von gewissen Formeln eingeführt, etwa „ $n$  ist eine Primzahl“ für die Gültigkeit der Formel

$$n \in \mathbb{N} \wedge n \geq 2 \wedge \forall x \in \mathbb{N} : 2 \leq x \wedge x \leq n - 1 \Rightarrow \neg(x \mid n)$$

oder „ $m$  und  $n$  sind teilerfremd“ für die Gültigkeit der Formel

$$m \in \mathbb{N} \wedge n \in \mathbb{N} \wedge \forall x \in \mathbb{N} : x \mid m \wedge x \mid n \Rightarrow x = 1.$$

Es ist wichtig für die Kommunikation, diese Begriffe und die sie spezifizierenden Formeln zu kennen. Für das formale mathematische Arbeiten ist ebenso wichtig, dass man in der Lage ist, umgangssprachliche Eigenschaften als Formeln zu spezifizieren, und man auch die wichtigsten logischen Regeln zur Manipulation von Formeln kennt.

### 2.3.3 Festlegung der Prädikatenlogik (Skizze)

Bei der genauen Definition der Formeln der Prädikatenlogik und ihrer Wahrheitswerte geht man grob wie folgt vor; wie man dies alles streng formal macht, lernt man in einer Vorlesung über mathematische Logik.

- (1) Zuerst legt man diejenigen Objekte fest, die den Betrachtungen zugrunde gelegt werden, etwa Zahlen, Funktionen, Mengen usw. Man fixiert also das **Universum**. Oft nimmt man  $\mathbb{U}$  als Bezeichnung für das Universum.
- (2) Dann führt man eine Menge von Variablen ein. Jede Variable ist ein Platzhalter für ein Objekt aus dem Universum  $\mathbb{U}$ . Oft wird  $X$  als Bezeichnung für die Menge der Variablen genommen. Beliebige Variablen heißen dann typischerweise  $x$  und  $y$ . Stehen Variablen für natürliche Zahlen, so nennt man sie oft  $m$  oder  $n$ .
- (3) Nun legt man die **atomaren Formeln**, auch **Primformeln** genannt, fest. Atomare Formeln sind normalerweise Relationsbeziehungen  $E_1 R E_2$  zwischen Ausdrücken  $E_1$  und  $E_2$ , wobei  $R$  ein Symbol für eine Relation ist und in den Ausdrücken  $E_1$  und  $E_2$  beim Aufbau, neben Symbolen für Objekte und Operationen (d.h. Funktionen), auch Variablen verwendet werden dürfen.

$$\begin{array}{lll} \text{Beispiele: } & 2 \leq x & x \leq n - 1 \\ & x \in M & y \in M \end{array} \quad \begin{array}{ll} x \mid (n+1)(n-1) & \\ & x = y \end{array}$$

Für alle Objekte aus dem Universum, die man für die Variablen einsetzen kann, muss der Wahrheitswert der atomaren Formeln festgelegt sein.

$$\begin{array}{lll} \text{Beispiele: } & 2 \leq 5 & (\text{hier ist } 5 \text{ für } x \text{ eingesetzt}) \\ & 2 \leq 0 & (\text{hier ist } 0 \text{ für } x \text{ eingesetzt}) \\ & 1 \in \emptyset & (\text{hier sind } 1 \text{ für } x \text{ und } \emptyset \text{ für } M \text{ eingesetzt}) \end{array} \quad \begin{array}{ll} \text{liefert W} & \\ \text{liefert F} & \\ \text{liefert F} & \end{array}$$

- (4) Wie in Definition 2.2.1 für die Aussagenlogik wird nun in analoger Weise die Menge  $\mathcal{F}$  aller **prädikatenlogischen Formeln** definiert:
- (a) Für alle atomaren Formeln  $P$  gilt  $P \in \mathcal{F}$ .
  - (b) Für alle  $A \in \mathcal{F}$  gilt  $\neg A \in \mathcal{F}$ .
  - (c) Für alle  $A_1, A_2 \in \mathcal{F}$  gelten  $A_1 \wedge A_2 \in \mathcal{F}$ ,  $A_1 \vee A_2 \in \mathcal{F}$ ,  $A_1 \Rightarrow A_2 \in \mathcal{F}$  und  $A_1 \Leftrightarrow A_2 \in \mathcal{F}$ .
  - (d) Für alle  $A(x) \in \mathcal{F}$  und  $x \in X$  gelten  $\forall x : A(x) \in \mathcal{F}$  und  $\exists x : A(x) \in \mathcal{F}$ .
  - (e) Es gibt keine Elemente in  $\mathcal{F}$  außer denen, die durch die Regeln (a) bis (d) zugelassen werden.

Die Vorrangregeln sind dabei wie früher schon eingeführt. In Regel (d) zeigt die Schreibweise  $A(x)$  an, dass die Variable  $x$  in der Formel  $A$  vorkommen kann. Mit  $A(a)$  bezeichnen wir dann die Formel, die aus  $A(x)$  entsteht, wenn  $x$  durch das Objekt  $a$  aus dem Universum  $\mathbb{U}$  ersetzt wird.

- (5) Bei der Definition der Werte von prädikatenlogischen Formeln **nimmt man an, dass alle Variablen durch einen Quantor gebunden** sind. Dann werden die fünf Junktoren „ $\neg$ “, „ $\wedge$ “, „ $\vee$ “, „ $\Rightarrow$ “ und „ $\Leftrightarrow$ “ wie in Abschnitt 2.2 behandelt. Also hat z.B.  $A_1 \wedge A_2$  den Wert W genau dann, wenn  $A_1$  und  $A_2$  beide den Wert W haben. Die Werte der Quantoren werden wie folgt definiert:
- (a) Die Formel  $\forall x : A(x)$  hat den Wert W genau dann, wenn die Formel  $A(a)$  den Wert W für alle Objekte  $a$  aus dem Universum  $\mathbb{U}$  hat.
  - (b) Die Formel  $\exists x : A(x)$  hat den Wert W genau dann, wenn es ein Objekt  $a$  in dem Universum  $\mathbb{U}$  gibt, so dass die Formel  $A(a)$  den Wert W hat.  $\square$

Somit hat, mit der oben getroffenen Annahme, dass keine Variablen frei vorkommen, also  $\forall x : A(x)$  den Wert W genau dann, wenn  $U = \{a \in U \mid A(a)\}$  gilt, und es hat  $\exists x : A(x)$  den Wert W genau dann, wenn  $\{a \in U \mid A(a)\} \neq \emptyset$  gilt. Wir wollen nun die eben skizzierte Vorgehensweise durch ein Beispiel erklären, in dem wir uns auf die drei bekannten Relationen „ $\geq$ “, „ $\leq$ “ und „ $|$ “ und die Subtraktion auf den natürlichen Zahlen stützen.

### 2.3.4 Beispiele: Werte von Formeln

Wir betrachten über dem Universum  $\mathbb{U}$ , welches als Menge  $\mathbb{N}$  definiert ist, die folgende prädikatenlogische Formel:

$$100 \geq 2 \wedge \forall x \in \mathbb{N} : 2 \leq x \wedge x \leq 100 - 1 \Rightarrow \neg(x \mid 100)$$

Nach der Definition des Wertes für Formeln der Gestalt  $A_1 \wedge A_2$  hat diese Formel genau dann den Wert  $W$ , wenn gelten:

(1) Die Formel  $100 \geq 2$  hat den Wert  $W$ .

(2) Die Formel  $\forall x \in \mathbb{N} : 2 \leq x \wedge x \leq 100 - 1 \Rightarrow \neg(x \mid 100)$  hat den Wert  $W$ .

Die atomare Formel  $100 \geq 2$  hat den Wert  $W$  nach der Festlegung der Relation „ $\geq$ “. Nach obigen Ausführungen und der Festlegung der Junktoren „ $\wedge$ “ und „ $\Rightarrow$ “ gilt (2) genau dann, wenn für alle  $a \in \mathbb{N}$  gilt:

(3) Haben die atomaren Formeln  $2 \leq a$  und  $a \leq 99$  den Wert  $W$ , so hat auch die atomare Formel  $\neg(a \mid 100)$  den Wert  $W$ .

Dies ist offensichtlich falsch, ein Gegenbeispiel ist  $a := 50$ . Also hat die Ausgangsformel den Wert  $F$ , sie ist also nicht gültig (oder falsch). Dies ist auch klar, da sie die Primzahleigenschaft von 100 spezifiziert und 100 keine Primzahl ist.

Nun verallgemeinern wir die obige Formel wie folgt, indem wir die Zahl 100 durch eine Variable  $n$  ersetzen.

$$n \geq 2 \wedge \forall x \in \mathbb{N} : 2 \leq x \wedge x \leq n - 1 \Rightarrow \neg(x \mid n)$$

Wenn wir diese Formel mit  $A(n)$  bezeichnen, so ist  $A(100)$  genau die obige Ausgangsformel. Wir wissen schon, dass deren Wert  $F$  ist. Für  $A(17)$ , also die Formel

$$17 \geq 2 \wedge \forall x \in \mathbb{N} : 2 \leq x \wedge x \leq 17 - 1 \Rightarrow \neg(x \mid 17),$$

in der die Variable  $n$  durch die Zahl 17 ersetzt ist, erhalten wir hingegen den Wert  $W$ , denn 17 ist eine Primzahl.  $\square$

Die Relation der logischen Äquivalenz, die wir schon von der Aussagenlogik her kennen, kann auch für prädikatenlogische Formeln definiert werden. Die Rolle der Belegungen der atomaren Aussagen übernehmen nun die Objekte, welche man für die sogenannten freien Variablen einsetzen kann. Dies führt zu der folgenden Festlegung:

### 2.3.5 Definition: logische Äquivalenz

Zwei prädikatenlogische Formeln heißen **logisch äquivalent**, wenn für alle Ersetzungen ihrer **freien Variablen** (also derjenigen Variablen, welche nicht durch einen Quantor gebunden sind) durch jeweils gleiche Objekte die entstehenden zwei Formeln den gleichen Wert besitzen.  $\square$

Gebundene Variablen sind für die logische Äquivalenz von prädikatenlogischen Formeln ohne Bedeutung, da man sie jederzeit umbenennen kann. So ist etwa  $\exists x \in \mathbb{N} : n = 2x$  logisch äquivalent zu  $\exists y \in \mathbb{N} : n = 2y$  und auch logisch äquivalent zu  $\exists z \in \mathbb{N} : n = 2z$ . Alle drei Formeln gelten genau dann, wenn  $n$  das Doppelte einer natürlichen Zahl ist, also eine gerade natürliche Zahl ist. Wesentlich sind nur die **freien** (also: ungebundenen) Variablen. In den eben gezeigten Formeln ist dies die Variable  $n$  (von der man nur weiß, dass sie für Zahlen steht). Es kann analog zur Aussagenlogik gezeigt werden, dass  $A_1$  und  $A_2$  logisch

äquivalente Formeln genau dann sind, wenn die Formel  $A_1 \Leftrightarrow A_2$  für alle Ersetzungen ihrer freien Variablen durch Objekte den Wert W hat.

Formeln stellen formalisierte Schreibweisen von mathematischen Aussagen dar. Wir haben im ersten Kapitel gezeigt, dass man Mathematik durchaus auch in der Umgangssprache betreiben kann. Wie weit man sie formalisiert oder formalisieren kann, hängt von einigen Faktoren ab, etwa vom zu behandelnden Stoff. An dieser Stelle ist deshalb noch eine Bemerkung angebracht.

### 2.3.6 Bemerkung: Sätze in der mathematischen Umgangssprache

Wenn man die in der mathematischen Umgangssprache formulierten Sätze (Lemmata, Theoreme usw.) formal als prädikatenlogische Formeln hinschreiben würde, so ist das Resultat immer eine Formel ohne freie Variablen. Deshalb bezeichnet man in der mathematischen Logik solche Formeln auch als Sätze. Ihr Wert ist W oder F, unabhängig von Nebenbedingungen, die bei freien Variablen gegeben sind. Die meisten sich aus der Umgangssprache ergebenden (Formel-)Sätze haben die folgende spezielle Gestalt:

$$(1) \forall x_1, \dots, x_n : A_1(x_1, \dots, x_n) \Rightarrow A_2(x_1, \dots, x_n)$$

In der mathematischen Umgangssprache schreibt man dann statt (1) beispielsweise:

$$(2) „Für alle  $x_1, \dots, x_n$  mit der Eigenschaft  $A_1(x_1, \dots, x_n)$  gilt  $A_2(x_1, \dots, x_n)$ .“$$

Aber auch Formulierungen der folgenden Art sind für (1) sehr häufig (und wurden auch in diesem Text schon benutzt):

$$(3) „Gegeben seien  $x_1, \dots, x_n$  so, dass  $A_1(x_1, \dots, x_n)$ . Dann gilt  $A_2(x_1, \dots, x_n)$ .“$$

Formulierungen der Gestalt (3) (oder von ähnlicher Gestalt) unterstellen durch die Phrase „Gegeben seien (beliebige)“ implizit eine Allquantifizierung. Sie werden gerne verwendet, wenn die Voraussetzungen  $A_1(x_1, \dots, x_n)$  eines Satzes umfangreich sind<sup>2</sup>. Das „Gegeben seien“ wird dabei quasi als eine Deklaration der Objekte  $x_1, \dots, x_n$  aufgefasst, so dass man diese sofort und ohne weitere Einführung im Beweis verwenden kann. Man vergleiche mit den bisherigen Beweisen. Im Fall von Formulierungen der Gestalt (2) beginnen manchmal Beweise in einführenden Lehrbüchern mit Sätzen wie „Es seien also  $x_1, \dots, x_n$  beliebig vorgegeben“, um nochmals zu betonen, dass man die (2) entsprechende Formel (1) dadurch beweist, dass die Implikation  $A_1(x_1, \dots, x_n) \Rightarrow A_2(x_1, \dots, x_n)$  für beliebige Objekte als wahr nachgewiesen wird. In der Regel wird in (2) das „Für alle“ aber auch implizit mit einer Deklaration der Objekte  $x_1, \dots, x_n$  verbunden und auf das „Es seien also  $x_1, \dots, x_n$  beliebig vorgegeben“ am Beginn des Beweises verzichtet. Die bisherigen Beweise zeigen, dass wir in diesem Text dieser zweiten Vorgehensweise folgen.

Für einen Anfänger birgt die Unterdrückung der Allquantifizierung in der umgangssprachlichen Formulierung von Sätzen die Gefahr, dass im Beweis gewisse logische Zusammenhänge verschleiert werden, die bei dem expliziten Gebrauch der Allquantifizierung klar

---

<sup>2</sup>Bei sehr umfangreichen Voraussetzungen, welche Konjunktionen von einzelnen Aussagen darstellen, werden die einzelnen Teilaussagen oft markiert. Damit kann man sich im Beweis einfacher auf sie beziehen, was oft das Verstehen erleichtert.

erkennbar sind. Wir werden darauf im weiteren Verlauf des Texts immer wieder zurückkommen, beispielsweise im vierten Kapitel bei der Vorstellung von Beweisprinzipien, die explizit darauf aufbauen, dass das zu beweisende Resultat umgangssprachlich in der Form (2) formuliert ist.  $\square$

Aufgrund von eventuell vorkommenden Quantifizierungen über unendliche Mengen kann man für prädikatenlogische Formeln die logische Äquivalenz zweier Formeln nicht mehr dadurch feststellen, dass man tabellarisch alle Objekte des Universums überprüft. Hier ist man auf logische Umformungen und weitere Beweistechniken (die wir in Kapitel 4 behandeln werden) angewiesen. Für die fünf Junktoren der Aussagenlogik gelten natürlich die logischen Äquivalenzen des letzten Abschnitts. Die wichtigsten logischen Äquivalenzen („Regeln“) für die beiden Quantoren sind nachfolgend ohne Beweise angegeben. In diesem Satz bezeichnet, wie auch schon bei der Aussagenlogik, das Symbol „ $\iff$ “ die Relation der logischen Äquivalenz auf der Menge  $\mathcal{F}$ .

### 2.3.7 Satz: Regeln für Quantoren

Für prädikatenlogische Formeln gelten die folgenden logischen Äquivalenzen:

- (1)  $\neg\forall x : A(x) \iff \exists x : \neg A(x)$  (de Morgan)
- (2)  $\neg\exists x : A(x) \iff \forall x : \neg A(x)$  (de Morgan)
- (3)  $\forall x : (A_1(x) \wedge A_2(x)) \iff (\forall x : A_1(x)) \wedge (\forall x : A_2(x))$
- (4)  $\exists x : (A_1(x) \vee A_2(x)) \iff (\exists x : A_1(x)) \vee (\exists x : A_2(x))$
- (5)  $\forall x : \text{wahr} \iff \text{wahr}$
- (6)  $\exists x : \text{falsch} \iff \text{falsch}$

Weiterhin gilt noch die folgende logische Äquivalenz, falls die Formel  $B$  nicht von der Variablen  $x$  abhängt (d.h.  $x$  in ihr nicht frei vorkommt).

$$(7) (\exists x : A(x)) \Rightarrow B \iff \forall x : (A(x) \Rightarrow B)$$

Diese sieben logischen Äquivalenzen bleiben wahr, wenn man die Quantifizierungen „ $\forall x$ “ und „ $\exists x$ “ durch die typisierten Quantifizierungen „ $\forall x \in M$ “ und „ $\exists x \in M$ “ ersetzt.  $\square$

Um das logische Umformen von Formeln nach diesen Regeln zu demonstrieren, zeigen wir durch die folgende Rechnung, wie man aus Regel (1) von Satz 2.3.7 zur Version von (1) kommt, in der nur über Elemente von  $M$  quantifiziert wird.

$$\begin{aligned} \neg\forall x \in M : A(x) &\iff \neg\forall x : x \in M \Rightarrow A(x) && \text{Festlegung 2.1.2} \\ &\iff \exists x : \neg(x \in M \Rightarrow A(x)) && \text{Satz 2.3.7 (1)} \\ &\iff \exists x : \neg(\neg(x \in M) \vee A(x)) && \text{Satz 2.2.7 (3)} \\ &\iff \exists x : \neg\neg(x \in M) \wedge \neg A(x) && \text{Satz 2.2.7 (5)} \\ &\iff \exists x : x \in M \wedge \neg A(x) && \text{Satz 2.2.7 (1)} \\ &\iff \exists x \in M : \neg A(x) && \text{Festlegung 2.1.2} \end{aligned}$$

Und hier ist noch die Rechnung, welche beweist, dass auch die Variante von Regel (5) von Satz 2.3.7 gilt, bei der man nur über die Elemente einer Menge  $M$  quantifiziert:

$$\begin{aligned}\forall x \in M : \text{wahr} &\iff \forall x : x \in M \Rightarrow \text{wahr} \\ &\iff \forall x : \text{wahr} \\ &\iff \text{wahr}\end{aligned}$$

Die Leserin oder der Leser überlege sich zu Übungszwecken, was die Begründungen der einzelnen Schritte sind.

Wir kommen nun zu einigen weiteren Beispielen für logische Umformungen von prädikatenlogischen Formeln.

### 2.3.8 Beispiele: Umformungen prädikatenlogischer Formeln

In Definition 1.1.10 haben wir die Mengengleichheit durch die Gleichwertigkeit von  $M = N$  und der Konjunktion von  $M \subseteq N$  und  $N \subseteq M$  festgelegt und dann bemerkt, dass

$$M = N \iff \forall x : x \in M \Leftrightarrow x \in N$$

gilt, wobei zur Vereinfachung hier die Umgangssprache schon durch logische Formeln ersetzt wurde. Die letzte logische Äquivalenz können wir nun durch die Rechnung

$$\begin{aligned}M = N &\iff M \subseteq N \wedge N \subseteq M && \text{Def. Gleichheit} \\ &\iff (\forall x : x \in M \Rightarrow x \in N) \wedge (\forall x : x \in N \Rightarrow x \in M) && \text{Def. Inklusion} \\ &\iff \forall x : (x \in M \Rightarrow x \in N) \wedge (x \in N \Rightarrow x \in M) && \text{Satz 2.3.7 (4)} \\ &\iff \forall x : x \in M \Leftrightarrow x \in N && \text{Satz 2.2.7 (2)}\end{aligned}$$

formal beweisen.

Hier ist ein Beispiel für eine weitere Umformung mittels logischer Äquivalenzen: Es seien  $\mathcal{M}$  und  $\mathcal{N}$  Mengen von Mengen. Dann gilt für alle Objekte  $x$  die folgende logische Äquivalenz, wobei in der Rechnung, neben der Festlegung 2.1.2 und einigen logischen Regeln (welche, das mache man sich zu Übungszwecken noch einmal klar), nur die Definition der beliebigen Mengenvereinigung und die Definition der binären Mengenvereinigung verwendet werden, nun aber mittels Formeln spezifiziert:

$$\begin{aligned}x \in \bigcup(\mathcal{M} \cup \mathcal{N}) &\iff \exists X \in \mathcal{M} \cup \mathcal{N} : x \in X \\ &\iff \exists X : X \in \mathcal{M} \cup \mathcal{N} \wedge x \in X \\ &\iff \exists X : (X \in \mathcal{M} \vee X \in \mathcal{N}) \wedge x \in X \\ &\iff \exists X : (X \in \mathcal{M} \wedge x \in X) \vee (X \in \mathcal{N} \wedge x \in X) \\ &\iff (\exists X : X \in \mathcal{M} \wedge x \in X) \vee (\exists X : X \in \mathcal{N} \wedge x \in X) \\ &\iff (\exists X \in \mathcal{M} : x \in X) \vee (\exists X \in \mathcal{N} : x \in X) \\ &\iff x \in \bigcup \mathcal{M} \vee x \in \bigcup \mathcal{N} \\ &\iff x \in (\bigcup \mathcal{M}) \cup (\bigcup \mathcal{N})\end{aligned}$$

Diese logische Äquivalenz zeigt, da sie für alle Objekte  $x$  gilt, die Mengengleichheit

$$\bigcup(\mathcal{M} \cup \mathcal{N}) = (\bigcup \mathcal{M}) \cup (\bigcup \mathcal{N}).$$

Auf die gleiche Art und Weise kann man durch die Rechnung

$$\begin{aligned} x \in \bigcap(\mathcal{M} \cup \mathcal{N}) &\iff \forall X \in \mathcal{M} \cup \mathcal{N} : x \in X \\ &\iff \forall X : X \in \mathcal{M} \cup \mathcal{N} \Rightarrow x \in X \\ &\iff \forall X : (X \in \mathcal{M} \vee X \in \mathcal{N}) \Rightarrow x \in X \\ &\iff \forall X : \neg(X \in \mathcal{M} \vee X \in \mathcal{N}) \vee x \in X \\ &\iff \forall X : (X \notin \mathcal{M} \wedge X \notin \mathcal{N}) \vee x \in X \\ &\iff \forall X : (X \notin \mathcal{M} \vee x \in X) \wedge (X \notin \mathcal{N} \vee x \in X) \\ &\iff \forall X : (X \in \mathcal{M} \Rightarrow x \in X) \wedge (X \in \mathcal{N} \Rightarrow x \in X) \\ &\iff (\forall X : X \in \mathcal{M} \Rightarrow x \in X) \wedge (\forall X : X \in \mathcal{N} \Rightarrow x \in X) \\ &\iff x \in \bigcap \mathcal{M} \wedge x \in \bigcap \mathcal{N} \\ &\iff x \in (\bigcap \mathcal{M}) \cap (\bigcap \mathcal{N}) \end{aligned}$$

für alle Objekte  $x$  auch die Mengengleichheit

$$\bigcap(\mathcal{M} \cup \mathcal{N}) = (\bigcap \mathcal{M}) \cap (\bigcap \mathcal{N})$$

verifizieren. Man beachte, dass es in den beiden Rechnungen entscheidend war, die durch die Festlegung 2.1.2 eingeführten abkürzenden Schreibweisen der Quantoren mit typisierten Variablen rückgängig zu machen. Weiterhin beachte man, dass die Gleichung  $\bigcap(\mathcal{M} \cap \mathcal{N}) = (\bigcap \mathcal{M}) \cap (\bigcap \mathcal{N})$  nicht gilt! Man mache sich dies an einem Beispiel klar.

Zwei Eigenschaften der Quantoren in Bezug auf die leere Menge, welche wir später immer wieder verwenden werden, sind die nachfolgend angegebenen:

$$\forall x \in \emptyset : A(x) \iff \mathbf{wahr} \quad \exists x \in \emptyset : A(x) \iff \mathbf{falsch}$$

Im folgenden Beweis der linken Eigenschaft verwenden wir im ersten Schritt die Festlegung 2.1.2 und im letzten Schritt Satz 2.3.7 (5).

$$\begin{aligned} \forall x \in \emptyset : A(x) &\iff \forall x : x \in \emptyset \Rightarrow A(x) \\ &\iff \forall x : \mathbf{falsch} \Rightarrow A(x) \\ &\iff \forall x : \mathbf{wahr} \\ &\iff \mathbf{wahr} \end{aligned}$$

Bei der rechten Eigenschaft kommt man wie folgt zum Ziel.

$$\begin{aligned} \exists x \in \emptyset : A(x) &\iff \exists x : x \in \emptyset \wedge A(x) \\ &\iff \exists x : \mathbf{falsch} \wedge A(x) \\ &\iff \exists x : \mathbf{falsch} \\ &\iff \mathbf{falsch} \end{aligned}$$

Hier verwenden wir im ersten Schritt ebenfalls die Festlegung 2.1.2. Am Ende verwenden wir Regel (6) von Satz 2.3.7.  $\square$

Analog zu den oben angegebenen logischen Äquivalenzketten kann man, wie auch bei der Aussagenlogik erwähnt, auch **logische Implikationen**  $A_1 \implies A_2$  durch Umformungsketten beweisen. Wir wollen auf den Begriff der logischen Implikation im Umfeld von prädikatenlogischen Formeln nicht weiter eingehen. Es ist aber für die interessierte Leserin oder den interessierten Leser sicher reizvoll, diesen Begriff durch einen Vergleich mit der Vorgehensweise bei der Aussagenlogik formal zu definieren. Als einzige wichtige Eigenschaft erwähnen wir nur, dass auch in der Prädikatenlogik die logische Äquivalenz  $A_1 \iff A_2$  genau dann wahr ist, wenn die zwei logischen Implikationen  $A_1 \implies A_2$  und  $A_2 \implies A_1$  wahr sind. Dies wird wiederum oft dazu verwendet, zu zeigen, dass zwei mathematische Aussagen, welche prädikatenlogischen Formeln entsprechen, logisch äquivalent sind. Man vergleiche nochmals mit den Bemerkungen am Ende von Abschnitt 2.1 und auch mit dem Ende von Abschnitt 2.2.

Neben den von uns bisher vorgestellten logischen Äquivalenzen gibt es noch eine Fülle weiterer wichtiger logischer Äquivalenzen (und logischer Implikationen) auf den prädikatenlogischen Formeln. Aus Platzgründen können wir nicht in voller Tiefe auf dieses Thema eingehen. Einige der wichtigsten Regeln sollen aber doch erwähnt werden. Das **konsistente Umbenennen von gebundenen Variablen** in Quantifizierungen gehört zu ihnen, da es in der Praxis sehr oft notwendig ist, um Kollisionen von Bezeichnungen zu vermeiden. Es besagt, dass die logische Äquivalenz

$$\forall x : A(x) \iff \forall y : A(y)$$

und auch die logische Äquivalenz

$$\exists x : A(x) \iff \exists y : A(y)$$

gelten, wobei die Formel  $A(y)$  aus der Formel  $A(x)$  dadurch entsteht, dass jedes ungebundene Vorkommen der Variablen  $x$  durch die Variable  $y$  ersetzt wird. Üblicherweise ist dabei  $y$  eine „neue“ oder „frische“ Variable, also eine, die in  $A(x)$  nicht vorkommt. Praktisch besagen diese zwei Regeln, dass bei Quantifizierungen die Bezeichnungen (Namen) der gebundenen Variablen nicht von Bedeutung sind. Sowohl die Formel  $\exists x : x \in \mathbb{N} \wedge n = 2x$  als auch die Formel  $\exists y : y \in \mathbb{N} \wedge n = 2y$  als auch die Formel  $\exists z : z \in \mathbb{N} \wedge n = 2z$  beschreiben beispielsweise, dass  $n$  gerade ist, was wir früher in der Form von typisierten Quantifizierungen auch schon erwähnt haben. Man vergleiche das konsistente Umbenennen von gebundenen Variablen in der Logik mit der Definition von Funktionen in der Mengenlehre. Auch dort sind die Parameterbezeichnungen frei wählbar und damit legen etwa  $f(x) = x^2$  und  $f(y) = y^2$  dieselbe Funktion  $f : \mathbb{R} \rightarrow \mathbb{R}$  fest.

Schließlich sollten noch die folgenden zwei Regeln erwähnt werden:

$$\forall x : A \iff A \quad \exists x : A \iff A$$

Sie besagen, dass beide Quantifizierungen  $\forall x : A$  und  $\exists x : A$  logisch äquivalent zu  $A$  sind, wenn die Variable  $x$  in der Formel  $A$  nicht frei vorkommt (also  $A$  nicht von  $x$  abhängt, was wir durch die Schreibweise  $A$  statt  $A(x)$  angezeigt haben). Unter der gleichen Voraussetzung gelten auch die folgenden zwei Regeln:

$$(\forall x : B(x)) \vee A \iff \forall x : (B(x) \vee A) \quad (\exists x : B(x)) \wedge A \iff \exists x : (B(x) \wedge A)$$

Sie verallgemeinern die beiden Distributivgesetze (6) und (7) von Satz 2.2.7 von der Aussagenlogik auf die Prädikatenlogik.

Wahrscheinlich ist allen Leserinnen und Lesern schon aufgefallen, dass die beiden Quantoren „ $\forall$ “ und „ $\exists$ “ die aussagenlogischen Verknüpfungen „ $\wedge$ “ und „ $\vee$ “ verallgemeinern. Für endliche Mengen kann man damit die Quantoren auf Junktoren zurückführen. Hat die endliche Menge  $M$  nämlich die explizite Darstellung  $M = \{a_1, a_2, \dots, a_n\}$ , so gilt für den Allquantor und die Konjunktion die logische Äquivalenz

$$\forall x \in M : A(x) \iff A(a_1) \wedge \dots \wedge A(a_n)$$

und für den Existenzquantor und die Disjunktion gilt die logische Äquivalenz

$$\exists x \in M : A(x) \iff A(a_1) \vee \dots \vee A(a_n).$$

Diese Eigenschaften sind sehr vorteilhaft, wenn beispielsweise im Rahmen einer Programmierung die Gültigkeit der linken Seiten algorithmisch getestet werden muss.

Wir wollen diesen Abschnitt nun mit einer Bemerkung zur definierenden logischen Äquivalenz beenden. Bei der Gleichheit kennen wir den Gleichheitstest  $E_1 = E_2$  und die definierende Gleichheit  $x := E$ . Erstere liefert einen Wahrheitswert, die zweite Art wird dazu verwendet, Symbole und Abkürzungen einzuführen. Analog dazu führt man, neben der üblichen logischen Äquivalenz zwischen (aussagenlogischen oder prädikatenlogischen) Formeln, noch die **definierende (logische) Äquivalenz** ein. Als Symbol verwendet man hier in der Regel „ $\iff$ “ und dessen Verwendung besagt, dass per Definition zwei Formeln als logisch gleichwertig zu betrachten sind.

Typischerweise werden definierende Äquivalenzen zur Spezifikation von Relationen gemäß der Festlegung 1.4.6 verwendet. Greifen wir die Beispiele von Abschnitt 1.4 noch einmal unter Benutzung des neuen Symbols auf, so ist durch

$$x \leq y : \iff \exists z \in \mathbb{N} : x + z = y$$

für alle  $x, y \in \mathbb{N}$  die übliche Ordnung auf den natürlichen Zahlen spezifiziert und durch

$$x | y : \iff \exists z \in \mathbb{N} : x \cdot z = y$$

für alle  $x, y \in \mathbb{N}$  die Teilbarkeitsrelation auf den natürlichen Zahlen. Das eben gezeigte Definitions muster mit einer Existenzquantifizierung wird auch bei vielen anderen Relationen angewendet.

## 2.4 Die Grenzen des naiven Mengenbegriffs

Durch das logische Rüstzeug der vergangenen Abschnitte sind wir nun in der Lage, viele der Umformungen und Argumentationen des ersten Kapitels formal nachzurechnen. Teilweise haben wir dies in diesem Kapitel auch demonstriert. Dieser ergänzende Abschnitt ist aber einem anderen Thema gewidmet. Wir wollen nachfolgend zeigen, wie man durch formales logisches Argumentieren relativ schnell an die Grenzen des naiven Mengenbegriffs von Kapitel 1 stößt, also Widersprüche erzeugt. Genau diese Widersprüche (auch Paradoxien der naiven Mengenlehre genannt) motivierten zu Beginn des 20. Jahrhunderts die

Entwicklung der sogenannten axiomatischen Mengenlehre, bei der man versucht, Widersprüche beim Umgang mit Mengen zu vermeiden.

Um einen Widerspruch beim naiven Mengenansatz aufzuzeigen, betrachten wir noch einmal den beliebigen Durchschnitt  $\bigcap \mathcal{M}$  von Mengen. Wenn wir die in Abschnitt 1.2 gegebene umgangssprachliche Definition mittels einer Formel ohne jede abkürzende Schreibweise angeben, so erhalten wir die folgende Festlegung:

$$\bigcap \mathcal{M} := \{x \mid \forall X : X \in \mathcal{M} \Rightarrow x \in X\}$$

Nun betrachten wir den Spezialfall von  $\mathcal{M}$  als die leere Menge (von Mengen), welcher, wie schon in Abschnitt 1.2 angemerkt wurde, nicht so einfach zu behandeln ist, wie die beliebige Vereinigung  $\bigcup \emptyset$ . Wir erhalten zuerst durch Einsetzung

$$\bigcap \emptyset = \{x \mid \forall X : X \in \emptyset \Rightarrow x \in X\}$$

und nach den Gesetzen der Logik folgt daraus nach einigen Umformungen die Gleichung

$$\bigcap \emptyset = \{x \mid \text{wahr}\}.$$

Da **wahr** per Definition immer gilt (also für alle Objekte wahr ist), ergibt sich als Menge  $\bigcap \emptyset$  nach der Definition der deskriptiven Mengenbeschreibung die Menge aller Objekte. An dieser Stelle stellt sich nun die Frage nach der Sinnhaftigkeit dieses Resultats.

Bei einer mengentheoretischen Grundlegung der Mathematik werden alle Objekte grundsätzlich als Mengen aufgefasst. So sind also beispielsweise alle natürlichen Zahlen spezielle Mengen. Die Null entspricht der leeren Menge  $\emptyset$ , die Eins entspricht der Menge  $\{\emptyset\}$ , die Zwei entspricht der Menge  $\{\emptyset, \{\emptyset\}\}$ , die Drei entspricht der Menge  $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$  und so weiter. Wie man Paare, Relationen und Funktionen durch Mengen beschreiben kann, haben wir im ersten Kapitel demonstriert. Weitere solche Beschreibungen, etwa von Tupeln, Folgen, Familien, linearen Listen und Binärbäumen, werden im Rest des Texts noch folgen.

Wenn jedes Objekt eine Menge ist, dann wird  $\bigcap \emptyset$  zur Menge aller Mengen. Dies führt jedoch zu einem Widerspruch. Gäbe es nämlich die Menge aller Mengen, so kann man auch die folgende spezielle Menge betrachten:

$$M := \{X \mid X \notin X\}$$

Es stellt sich nun die Frage, ob  $M$  ein Element von  $M$  ist. Ist dies der Fall, so folgt daraus  $M \notin M$  nach der Definition der deskriptiven Mengenbeschreibung und der Menge  $M$ , also gerade das Gegenteil der Annahme. Wenn  $M \in M$  als falsch angenommen wird, so folgt daraus in analoger Weise, dass  $M \notin M$  nicht gilt, also  $M \in M$  gilt. Die Aufdeckung dieser sogenannten Antinomie geht auf den englischen Mathematiker und Philosophen Bertrand Russell (1872-1970) zurück. Er teilte sie dem deutschen Logiker, Mathematiker und Philosophen Gottlob Frege (1848-1925) im Jahr 1902 brieflich mit. Das war schlagartig das Ende der naiven Mengenlehre im Cantorschen Sinne.

Wenn man also, wir bleiben trotzdem in der naiven Mengenlehre, ohne weitere Nebenbedingungen, einen beliebigen Durchschnitt  $\bigcap \mathcal{M}$  betrachtet, so muss man eigentlich immer

$\mathcal{M} \neq \emptyset$  voraussetzen. In der Regel unterdrückt man dies aber. Der Grund dafür ist, dass beim praktischen Arbeiten mit beliebigen Durchschnitten die Mengen aus der Menge  $\mathcal{M}$  von Mengen immer aus einem Universum stammen. Es gilt also  $\mathcal{M} \subseteq \mathcal{P}(U)$  für eine vorgegebene Menge  $U$ , beispielsweise festgelegt durch  $U := \bigcup \mathcal{M}$ . Bei einer solchen Auffassung wird auch die leere Menge (von Mengen)  $\emptyset$  als zu  $\mathcal{P}(U)$  gehörend betrachtet. Dies erlaubt dann die Festlegung  $\bigcap \emptyset = U$ . Unter Verwendung des Komplements und  $\mathcal{P}(U) = \bar{\emptyset}$  folgt dann  $\bigcap \emptyset = U = \bigcup \mathcal{P}(U) = \bigcup \bar{\emptyset}$ . Auch die dazu „duale“ Gleichung  $\bigcup \emptyset = \bigcap \bar{\emptyset}$  gilt.

In Abschnitt 2.1 haben wir auch erwähnt, dass die Einschließungseigenschaft sogar für die leere Menge gilt. Dies wollen wir nun beweisen. Wenn wir die Einschließungseigenschaft in der allgemeineren Form als Formel hinschreiben, wiederum ohne jede Abkürzung, so lautet sie wie folgt:

$$\forall \mathcal{M} : \forall M : M \in \mathcal{M} \Rightarrow (\bigcap \mathcal{M} \subseteq M \wedge M \subseteq \bigcup \mathcal{M})$$

Im Fall der leeren Menge für  $\mathcal{M}$  ergibt sich also die folgende Formel durch die Spezialisierung der obigen Allquantifizierung:

$$\forall M : M \in \emptyset \Rightarrow (\bigcap \emptyset \subseteq M \wedge M \subseteq \bigcup \emptyset)$$

Diese ist, nach den obigen Ausführungen, logisch äquivalent zur Formel

$$\forall M : \text{falsch} \Rightarrow (U \subseteq M \wedge M \subseteq \emptyset),$$

wenn wir die Menge  $U$  als Universum annehmen. Weil die immer falsche Aussage **falsch** die linke Seite der Implikation dieser Formel darstellt, gilt die Implikation und die Formel ist somit logisch äquivalent zur Formel

$$\forall M : \text{wahr}.$$

Diese Formel gilt. Also ist auch die Ausgangsformel  $\forall M : M \in \emptyset \Rightarrow (\bigcap \emptyset \subseteq M \wedge M \subseteq \bigcup \emptyset)$ , welche die Einschließungseigenschaft für die leere Menge beschreibt, gültig.

## 2.5 Übungsaufgaben

### Aufgabe

Es seien  $a$  und  $b$  atomare Aussagen. Zeigen Sie, dass die Formel

$$a \wedge (a \Rightarrow b) \Rightarrow b$$

für alle Werte von  $a$  und  $b$  wahr ist, indem Sie die Formel durch logische Umformungen in die immer wahre Formel **wahr** transformieren.

### Aufgabe

Zeigen Sie für beliebige atomare Aussagen  $a$  und  $b$  durch eine Überprüfung aller möglichen Werte die logische Äquivalenz der beiden Formeln  $(a \wedge b) \vee a$  und  $a$  und, darauf aufbauend, für beliebige Mengen  $A$  und  $B$  die Gleichheit  $(A \cap B) \cup A = A$ .

## Aufgabe

Es seien  $a$ ,  $b$  und  $c$  beliebige atomare Aussagen.

- (1) Beweisen Sie durch logische Umformungen, dass die drei Formeln

$$a \wedge b \Rightarrow c \quad a \Rightarrow \neg b \vee c \quad \neg(a \wedge b \wedge \neg c)$$

logisch äquivalent sind. Geben Sie dabei zu den einzelnen Rechenschritten die verwendeten Regeln entweder explizit oder in Form von Hinweisen (z.B. „de Morgan“ oder „Distributivgesetz“) an.

- (2) Geben Sie Werte für  $a$ ,  $b$  und  $c$  an, für die die Formeln von (1) wahr werden.  
(3) Geben Sie Werte für  $a$ ,  $b$  und  $c$  an, für die die Formeln von (1) falsch werden.

## Aufgabe

Neben der in Kapitel 2 vorgestellten Disjunktion  $\vee$  wird noch eine Variante  $\nabla$  verwendet, bei der  $a \nabla b$  genau dann wahr ist, wenn  $a$  wahr ist oder  $b$  wahr ist, aber nicht beide zugleich wahr sind. Definieren Sie die Verknüpfung  $\nabla$

- (1) durch die Angabe einer Wahrheitstabelle  
(2) mit Hilfe der Verknüpfungen  $\vee$ ,  $\wedge$  und  $\neg$ .

## Aufgabe

Es seien  $a$ ,  $b$  und  $c$  atomare Aussagen. Der Wert der Formel

$$c \Rightarrow \neg(\neg(a \wedge b) \Leftrightarrow (\neg b \vee \neg a))$$

hängt nur vom Wert genau einer der atomaren Aussagen ab. Welche atomare Aussage ist dies und wie bestimmt ihr Wert den Wert der Formel (mit Begründung)?

## Aufgabe

Es sei  $R \subseteq M \times M$  eine Relation auf  $M$ . Dann heißt  $M$   $R$ -dicht, falls die Formel

$$\forall x, y \in M : x R y \Rightarrow \exists z \in M : x R z \wedge z R y$$

gilt. Geben Sie ein Beispiel für eine  $R$ -dichte Menge an und auch ein Beispiel für eine Menge, die nicht  $R$ -dicht ist.

## Aufgabe

Geben Sie zu den Formeln

- (1)  $\forall x \in \mathbb{N} : (2 \leq x \leq 7 \wedge x \neq 5) \Rightarrow P(x)$   
(2)  $\exists x \in \mathbb{N} : (\frac{1}{2}x^2 - 2x = -\frac{6}{4}) \wedge P(x)$   
(3)  $\forall x \in \mathbb{N} : (\exists y \in \mathbb{N} : xy = 21) \Rightarrow P(x)$

jeweils logisch äquivalente Formeln an, in denen (ausgenommen gegebenenfalls in der Teilformel  $P(x)$ ) nicht mehr über die Variable  $x$  quantifiziert wird.

## Aufgabe

Es sei  $n$  eine natürliche Zahl. Spezifizieren Sie die folgenden Eigenschaften formal durch Formeln mit Quantoren.

- (1) Keine gerade natürliche Zahl teilt  $n$ .
- (2) Alle natürlichen Zahlen, die von  $n$  geteilt werden, sind echt kleiner als 100.
- (3) Multipliziert man die Zahl  $n$  mit  $n + 2$ , so ist das Resultat ein Vielfaches von 3.
- (4) Es ist  $n$  keine Zweierpotenz, aber eine Potenz von 3.

## Aufgabe

Was besagt die folgende Formel umgangssprachlich, wenn wir voraussetzen, dass durch die atomaren Formeln  $\text{primzahl}(x)$  die Primzahl-Eigenschaft von  $x$  spezifiziert wird?

$$\forall n \in \mathbb{N} : \exists p, q \in \mathbb{N} : \text{primzahl}(p) \wedge \text{primzahl}(q) \wedge p + 2 = q$$

## Aufgabe

Betrachten Sie die folgende Formel:

- (a)  $\forall x : \forall y : \exists M : x \in M \wedge y \in M \wedge (\forall z : z \in M \Rightarrow z = x \vee z = y)$
- (1) Was besagt die Formel (a) umgangssprachlich?
  - (2) Beweisen Sie durch logische Umformungen, dass die Formel (a) logisch äquivalent zur Formel

$$\forall x : \forall y : \exists M : x \in M \wedge y \in M \wedge \neg(\exists z : z \in M \wedge z \neq x \wedge z \neq y)$$

ist. Geben Sie dabei zu den einzelnen Schritten jeweils Begründungen an.

## Aufgabe

Geben Sie ein System von Regeln an, das formal festlegt, ob eine Variable in einer Formel der Prädikatenlogik vorkommt. Die Regeln sollen sich dabei am Aufbau der Formeln der Prädikatenlogik orientieren.

## Aufgabe

Zu Funktionen  $f, g : \mathbb{N} \rightarrow \mathbb{R}$  definiert man  $f \in o(g)$ , wenn für alle  $c \in \mathbb{R}$  mit  $c > 0$  ein  $n \in \mathbb{N}$  existiert, so dass  $|f(m)| < c |g(m)|$  für alle  $m \in \mathbb{N}$  mit  $m > n$  gilt.

- (1) Formalisieren Sie die  $f \in o(g)$  definierende Eigenschaft durch eine Formel mit Quantoren.
- (2) Weisen Sie nach, dass für die durch  $f(x) = 8x$  und  $g(x) = x^2$  definierten Funktionen  $f, g : \mathbb{N} \rightarrow \mathbb{R}$  die Eigenschaft  $f \in o(g)$  gilt.

### 3 Allgemeine direkte Produkte und Datenstrukturen

In Abschnitt 1.4 haben wir direkte Produkte  $M \times N$  als Mengen von Paaren  $(a, b)$  von Objekten eingeführt. Paare bestehen aus genau zwei Komponenten. In diesem Kapitel führen wir zuerst Tupel ein, die aus endlich vielen Komponenten bestehen, und, als deren Verallgemeinerungen, dann noch Folgen und Familien. Mengen von Tupeln nennt man allgemeine direkte Produkte. Schließlich zeigen wir noch, wie man mit Hilfe von direkten Produkten zwei in der Informatik sehr wichtige Datenstrukturen formal mathematisch erklären kann, nämlich lineare Listen und Binäräbäume.

#### 3.1 Tupel, Folgen und Familien

Eine offensichtliche Erweiterung der Definition von Paaren  $(a, b)$  und von (binären) direkten Produkten  $M \times N$  als Mengen von Paaren führt zur folgenden Festlegung von Tupeln und allgemeinen direkten Produkten.

##### 3.1.1 Definition: Tupel und allgemeines direktes Produkt

Es sei  $n \in \mathbb{N}$  mit  $1 \leq n$  vorgegeben. Weiterhin seien Mengen  $M_1, \dots, M_n$  gegeben.

- (1) Zu beliebigen Objekten  $a_i \in M_i$  für alle  $i$  mit  $1 \leq i \leq n$  heißt die Konstruktion  $(a_1, \dots, a_n)$  ein  **$n$ -Tupel** (kurz auch Tupel) und  $a_i$  die  **$i$ -te Komponente davon**.
- (2) Die Menge aller  $n$ -Tupel  $(a_1, \dots, a_n)$ , mit  $a_i \in M_i$  für alle  $i$  mit  $1 \leq i \leq n$ , heißt das  **$n$ -fache direkte oder  $n$ -fache kartesische Produkt** der Mengen  $M_i$ ,  $1 \leq i \leq n$ , und wird mit  $\prod_{i=1}^n M_i$  bezeichnet. Es gilt also:

$$\prod_{i=1}^n M_i := \{(x_1, \dots, x_n) \mid \forall i \in \mathbb{N} : 1 \leq i \leq n \Rightarrow x_i \in M_i\}$$

Falls  $M_1 = M_2 = \dots = M_n = M$  zutrifft, so schreibt man  $M^n$  statt  $\prod_{i=1}^n M_i$  und bezeichnet diese Menge als die  **$n$ -te Potenz** von  $M$ .  $\square$

In der Literatur ist auch die Schreibweise  $M_1 \times \dots \times M_n$  statt  $\prod_{i=1}^n M_i$  gebräuchlich. Dies ist insbesondere dann der Fall, wenn  $n$  eine konkrete kleine Zahl ist und so ein direktes Produkt von  $n$  konkreten Mengen bei der Definition von Funktionen Verwendung findet. Für  $n = 3$  und beispielsweise  $M_1 = M_2 = M_3 = \mathbb{R}$  sind also  $\prod_{i=1}^3 \mathbb{R}$ ,  $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$  und  $\mathbb{R}^3$  drei verschiedene Bezeichnungen für die Menge aller 3-Tupel mit reellen Komponenten. Eine Funktion, bei der diese Menge verwendet wird, ist etwa die nachfolgend definierte:

$$f : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \quad f(x, y, z) = \sqrt{x^2 + y^2 + z^2}$$

Wie bei den Paaren, so verwendet man auch bei Funktionsanwendungen mit Tupeln als Argumenten nur ein Klammerpaar. Man beachte den Unterschied zwischen dem 3-fachen direkten Produkt  $M_1 \times M_2 \times M_3$  und den geklammerten direkten Produkten (im bisherigen binären Sinn)  $M_1 \times (M_2 \times M_3)$  bzw.  $(M_1 \times M_2) \times M_3$ . Die erste Menge besteht aus 3-Tupeln (auch Tripel genannt)  $(a, b, c)$ , die zweite Menge aus Paaren  $(a, (b, c))$  mit Paaren als zweiten Komponenten und die dritte aus Paaren  $((a, b), c)$  mit Paaren als ersten Komponenten. Diese Bemerkung trifft in analoger Weise für allgemeine direkte Produkte von  $n > 2$  Mengen und geklammerte  $n - 1$  binäre direkte Produkte auf ihnen zu.

### 3.1.2 Bemerkung

Beim Arbeiten mit direkten Produkten kommen oftmals Quantifizierungen der speziellen Gestalt „ $\forall i \in \mathbb{N} : 1 \leq i \leq n \Rightarrow A(i)$ “ vor. Aus Gründen der besseren Lesbarkeit und des besseren Verstehens schreibt man dafür oft „ $\forall i \in \{1, \dots, n\} : A(i)$ “ und unterstellt für  $n = 0$ , dass  $\{1, \dots, n\}$  gleich der leeren Menge ist. Analog kürzt man „ $\exists i \in \mathbb{N} : 1 \leq i \leq n \wedge A(i)$ “ oft zu „ $\exists i \in \{1, \dots, n\} : A(i)$ “ ab.  $\square$

Man beachte, dass für  $n = 2$  bzw.  $n = 1$  die folgenden Gleichungen gelten:

- (1)  $\prod_{i=1}^2 M_i = \{(x_1, x_2) \mid x_1 \in M_1 \wedge x_2 \in M_2\} = M_1 \times M_2$
- (2)  $\prod_{i=1}^1 M_i = \{(x_1) \mid x_1 \in M_1\}$

Es ist also für  $n = 2$  das  $n$ -fache direkte Produkt gleich dem binären direkten Produkt, welches wir schon aus Kapitel 1 kennen. Für  $n = 1$  besteht das  $n$ -fache direkte Produkt aus einer Menge von geklammerten Elementen. Man identifiziert deshalb manchmal, etwa in der Theorie der formalen Sprachen,  $\prod_{i=1}^1 M_i$  und  $M_1$ , unterscheidet also nicht zwischen  $(x)$  und  $x$ . Als Verallgemeinerung von Satz 1.4.3 erhalten wir unmittelbar die folgende Eigenschaft.

### 3.1.3 Satz: Kardinalität direkter Produkte

Für alle natürlichen Zahlen  $n$  mit  $n \geq 1$  und alle endlichen Mengen  $M_1, \dots, M_n$  gilt die Gleichung  $|\prod_{i=1}^n M_i| = |M_1| \cdot \dots \cdot |M_n|$ .  $\square$

Üblicherweise wird das Produkt von  $n \geq 1$  Zahlen  $k_1, \dots, k_n$  mit  $\prod_{i=1}^n k_i$  bezeichnet. Eine rekursive Definition dieser Schreibweise ist durch die Gleichungen

$$\prod_{i=1}^1 k_i := k_1 \quad \prod_{i=1}^{n+1} k_i := k_{n+1} \cdot \prod_{i=1}^n k_i$$

gegeben. Man mache sich klar, dass auf diese Weise tatsächlich  $\prod_{i=1}^n k_i$  für alle  $n \in \mathbb{N} \setminus \{0\}$  und alle Zahlen  $k_1, \dots, k_n$  definiert wird und mit dem übereinstimmt, was man naiv und unter Verwendung von „ $\dots$ “ als  $k_1 \cdot \dots \cdot k_n$  schreiben würde. Wir werden auf Definitionen dieser Art später noch genauer eingehen. Mit der eben getroffenen Festlegung des allgemeinen Produkts von Zahlen bekommt man die Gleichung von Satz 3.1.3 in der Gestalt

$$|\prod_{i=1}^n M_i| = \prod_{i=1}^n |M_i|,$$

was die Verwendung des gleichen griechischen Buchstabens „ $\prod$ “ für beide Produktbildung rechtfertigt. Eine weitere Konsequenz von Satz 3.1.3 ist  $|M^n| = |M|^n$ . Die Kardinalität einer  $n$ -ten Potenz einer endlichen Menge  $M$  ist also genau die  $n$ -te Potenz (im Sinne von Zahlen) der Kardinalität von  $M$ .

In Abschnitt 1.4 haben wir festgelegt, das Bild eines Elements  $a$  unter einer Funktion  $f$  mit  $f(a)$  zu bezeichnen. Weiterhin haben wir bemerkt, dass, wenn  $a$  ein Paar  $(a_1, a_2)$  ist, man  $f(a_1, a_2)$  statt  $f((a_1, a_2))$  schreibt. Wir verallgemeinern dies nun, wie oben schon kurz bemerkt, auf Funktionen  $f : \prod_{i=1}^n M_i \rightarrow N$  und schreiben auch hier  $f(a_1, \dots, a_n)$

statt  $f((a_1, \dots, a_n))$  für das Bild von  $(a_1, \dots, a_n) \in \prod_{i=1}^n M_i$  unter  $f$ . Bei Funktionen in Verbindung mit Tupeln haben sich spezielle Sprechweisen gebildet, die wir nachfolgend angeben.

### 3.1.4 Sprechweisen: Stelligkeit und Wertigkeit

Hat eine Funktion  $n$ -Tupel als Argumente, so heißt sie  **$n$ -stellig**, und liefert sie  $n$ -Tupel als Werte, so heißt sie  **$n$ -wertig**.  $\square$

Bei diesen Sprechweisen wird nicht zwischen 1-Tupeln ( $a$ ) und den sie bildenden Objekten  $a$  unterschieden, womit etwa  $f : \mathbb{N} \rightarrow \mathbb{N}^2$  1-stellig und 2-wertig ist und  $g : \mathbb{N} \rightarrow \mathbb{N}$  1-stellig und 1-wertig ist. Nachfolgend geben wir drei weitere Beispiele für mehrstellige und mehrwertige Funktionen an.

### 3.1.5 Beispiele: Stelligkeit und Wertigkeit von Funktionen

Zuerst betrachten wir  $\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \mid x \geq 0\}$  und  $\mathbb{R}_{>0} := \{x \in \mathbb{R} \mid x > 0\}$ , also die Mengen der nichtnegativen bzw. positiven reellen Zahlen. Dann ist die Funktion

$$f : \mathbb{R}_{>0} \times \mathbb{R}_{\geq 0} \rightarrow \mathbb{R} \times \mathbb{R} \quad f(x, y) = (\sqrt{x^2 + y^2}, \arctan \frac{y}{x}),$$

welche kartesische Koordinaten im ersten Quadranten der Euklidischen Ebene (benannt nach dem griechischen Mathematiker Euklid (ca. 360-280 v. Chr.)) in ihre Polarkoordinaten, also das Paar („Länge“, „Winkel“), umrechnet, 2-stellig und 2-wertig. Der aus dem Paar  $(x, y)$  berechnete Winkel  $\varphi$  der Polarkoordinaten ist hier im Bogenmaß angegeben, mit  $0 \leq \varphi \leq \frac{\pi}{2}$ .

Ein Tripel  $(x, y, z)$  von natürlichen Zahlen heißt **pythagoräisch**, falls  $x^2 + y^2 = z^2$  gilt, also die Zahlen die Seitenlängen eines rechtwinkligen Dreiecks sind. Die Funktion

$$f : \mathbb{N}^3 \rightarrow \mathbb{B} \quad f(x, y, z) = \begin{cases} \text{W} & \text{falls } x^2 + y^2 = z^2 \\ \text{F} & \text{falls } x^2 + y^2 \neq z^2 \end{cases}$$

zum Testen von pythagoräischen Tripeln ist 3-stellig und 1-wertig. Die pythagoräischen Tripel sind nach dem griechischen Philosophen Pythagoras von Samos (ca. 570-510 v. Chr.) benannt, dessen Satz über die Seitenlängen eines rechtwinkligen Dreiecks in jeder höheren Schule behandelt wird.

Wir betrachten schließlich noch die nachfolgend gegebene Funktion, wobei  $n$  als positive natürliche Zahl angenommen ist und die Teilmenge  $\mathbb{N}_{\text{sort}}^n$  von  $\mathbb{N}^n$  genau aus den  $n$ -Tupeln  $(x_1, \dots, x_n)$  besteht, für die  $x_1 \leq x_2 \leq \dots \leq x_n$  gilt<sup>3</sup>.

$$f : \mathbb{N}_{\text{sort}}^n \rightarrow \mathbb{N} \quad f(x_1, \dots, x_n) = \begin{cases} \frac{x_n}{2} & \text{falls } n \text{ gerade} \\ \frac{x_{\frac{n+1}{2}}}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

Diese Funktion ordnet dem sortierten  $n$ -Tupel  $(x_1, \dots, x_n)$  den sogenannten **Median** (oder **Zentralwert**) zu, also den Wert in der Mitte bei ungeradem  $n$  oder den in der abgerundeten Mitte bei geradem  $n$ . Diese Funktion ist  $n$ -stellig und 1-wertig. Sie spielt in der

<sup>3</sup>Man sagt auch, dass die Zahlen aufsteigend sortiert sind. Die Leserin oder der Leser mache sich klar, wie man diese Eigenschaft ohne die Verwendung von „...“ durch eine Formel beschreiben kann.

mathematischen Statistik eine herausragende Rolle. □

Teilmengen von  $\mathbb{R}^2$  stellen geometrische Figuren in der Euklidischen Ebene dar, etwa

- (1)  $\mathbb{N}^2$  die Punkte eines Gitternetzes im ersten Quadranten,
- (2)  $\{(x, y) \in \mathbb{N}^2 \mid y = ax + b\}$  Geradenpunkte auf diesem Gitter, wobei die Gerade durch die Zahlen  $a$  und  $b$  gegeben ist,
- (3)  $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$  den Kreis (genauer: die Kreislinie) mit Radius  $r$  um den Punkt  $(0, 0)$ ,
- (4)  $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq r^2\}$  die Kreisfläche mit  $r$  als dem Radius des begrenzenden Kreises um den Punkt  $(0, 0)$ .

Teilmengen von  $\mathbb{R}^3$  stellen geometrische Formen im Euklidischen Raum dar. Auch hier geben wir einige Beispiele an. Es ist etwa

- (5)  $\{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz = q\}$  die durch die Zahlen  $a, b, c$  und  $q$  bestimmte Ebene,
- (6)  $\{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz \leq q\}$  einer der beiden durch die Ebene aus Teil (5) bestimmten Halbräume,
- (7)  $\{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq r^2\}$  die Vollkugel mit Radius  $r$  um den Punkt  $(0, 0, 0)$ .

Dabei haben wir implizit angenommen, dass entartete Fälle nicht auftreten, also in (3), (4) und (7) der Radius  $r$  nichtnegativ ist und in (5) und (6) aus  $a = b = c = 0$  folgt  $q = 0$ . Weiterhin haben wir, wie allgemein bei der deskriptiven Beschreibung von Teilmengen von direkten Produkten üblich, bei den Paaren und Tripeln gleich die Typisierung mit angegeben. So ist etwa  $\{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz = q\}$  eine abkürzende Schreibweise für  $\{(x, y, z) \mid x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge z \in \mathbb{R} \wedge ax + by + cz = q\}$ .

Wir haben alle unsere bisherigen mathematischen Konstruktionen immer auf Mengen zurückgeführt, also wollen wir dies auch für Tupel so halten. Es gibt hier unter anderem die folgende Möglichkeit: Man kann ein  $n$ -Tupel der Gestalt  $(x_1, \dots, x_n)$  auffassen als eine Funktion  $f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n M_i$  mit  $f(i) = x_i$  für alle  $i$  mit  $1 \leq i \leq n$ . Dann wird  $(x_1, \dots, x_n)$  nur eine spezielle Schreibweise zur Angabe dieser Funktion. Beispielsweise ist  $(a^0, a^1, a^2, a^3)$  (mit  $a \in \mathbb{R}$  unterstellt) die Tupelschreibweise für die Funktion  $f : \{1, 2, 3, 4\} \rightarrow \mathbb{R}$  mit der Definition  $f(i) = a^{i-1}$ . Da wir in Abschnitt 1.4 für Funktionen Relationen zur Definition herangezogen haben und jene Mengen von Paaren sind, also (wiederum nach Abschnitt 1.4) Mengen von Mengen der Form  $\{a, \{a, b\}\}$  oder der Form  $\{\{a\}, \{a, b\}\}$ , haben wir auch Tupel auf Mengen reduziert. Beispielsweise wird das 4-Tupel  $(a, b, c, d)$ , wenn wir die entsprechende Funktion als Relation auffassen, zur Menge

$$\{(1, a), (2, b), (3, c), (4, d)\}$$

und wenn wir die darin vorkommenden Paare gemäß der ersten Form als Mengen darstellen, so erhalten wir schließlich

$$\{\{1, \{1, a\}\}, \{2, \{2, b\}\}, \{3, \{3, c\}\}, \{4, \{4, d\}\}\}$$

als mengentheoretisches Modell von  $(a, b, c, d)$ . Die in Abschnitt 1.4 gegebene Festlegung der Gleichheit von Funktionen  $f$  und  $g$  durch die Gleichheit der Bilder  $f(x)$  und  $g(x)$  für alle Elemente  $x$  der Quelle zeigt, dass die folgende Definition der Gleichheit von Tupeln bei einer Auffassung von Tupeln als spezielle Funktionen mit der Gleichheit von Funktionen in Einklang steht.

### 3.1.6 Definition: komponentenweise Gleichheit

Für  $n$ -Tupel  $(x_1, \dots, x_n)$  und  $(y_1, \dots, y_n)$  gilt die **Gleichheit**  $(x_1, \dots, x_n) = (y_1, \dots, y_n)$  genau dann, wenn  $x_i = y_i$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq n$  gilt.  $\square$

Die Auffassung eines  $n$ -Tupels  $(x_1, \dots, x_n)$  als Funktion  $f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n M_i$  erlaubt auch sofort, durch eine Verallgemeinerung der Quelle auf die Menge  $\mathbb{N}$  aller natürlichen Zahlen unendliche Tupel einzuführen. Hier konzentriert man sich normalerweise auf Tupel mit Komponenten aus nur einer Menge. In der Analysis braucht man insbesondere solche mit Komponenten aus den reellen Zahlen  $\mathbb{R}$  und nennt diese dann (reelle) Folgen.

### 3.1.7 Definition: Folge

Eine (unendliche) **Folge** in einer Menge  $M$  (oder: von Objekten aus  $M$ ) ist eine Funktion  $f : \mathbb{N} \rightarrow M$ . Wir schreiben  $f_n$  statt  $f(n)$  und nennen  $f_n$  das  $n$ -te **Folgenglied**. Im Fall  $M = \mathbb{R}$  sprechen wir von reellen Folgen.  $\square$

Beispielsweise ist die Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}$  mit der Definition  $f(n) = \frac{1}{n+1}$  eine reelle Folge. In der Analysis gibt man Folgen auch in der Form  $(f_n)_{n \in \mathbb{N}}$  oder der Form  $(f_n)_{n \geq 0}$  an, also im vorliegenden Fall als  $(\frac{1}{n+1})_{n \in \mathbb{N}}$  oder als  $(\frac{1}{n+1})_{n \geq 0}$ . Wegen des speziellen Nenners schreibt man, nach einer Transformation, für unser spezielles Beispiel auch  $(\frac{1}{n})_{n \geq 1}$ . Schließlich verwendet man zur Verbesserung der Lesbarkeit oft auch eine Notation mit drei Punkten, wenn das Bildungsgesetz klar ist. So schreibt man beispielsweise  $(1, \frac{1}{2}, \frac{1}{3}, \dots)$  statt  $(\frac{1}{n+1})_{n \in \mathbb{N}}$  oder  $(\frac{1}{n})_{n \geq 1}$ , oder man gibt das Bildungsgesetz noch zusätzlich an, wie etwa in der Formulierung  $(1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots)$ . Lässt man in der Definition von Folgen in der Menge  $M$  statt  $\mathbb{N}$  eine beliebige nichtleere sogenannte Indexmenge  $I$  zu, so heißt die Funktion  $f : I \rightarrow M$  eine mit Elementen aus  $I$  indizierte **Familie** von Elementen in  $M$ . Man notiert Familien ebenfalls in der Regel in der Form  $(f_i)_{i \in I}$ .

Neben der oben gezeigten Darstellungsweise als Funktionen  $f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n M_i$  gibt es noch eine zweite gängige Möglichkeit, allgemeine direkte Produkte auf die bisher vorgestellten mengentheoretischen Konstruktionen zurückzuführen. Dabei geht man wie folgt rekursiv vor, indem man sich auf das binäre direkte Produkt von Definition 1.4.1 stützt. Hierbei sind  $n > 0$  und  $k < n$  vorausgesetzt.

$$\prod_{i=n}^n M_i := M_n \quad \prod_{i=k}^n M_i := M_k \times \left( \prod_{i=k+1}^n M_i \right)$$

Beispielsweise gilt also bei drei Mengen die Gleichung

$$\prod_{i=1}^3 M_i = M_1 \times \left( \prod_{i=2}^3 M_i \right) = M_1 \times \left( M_2 \times \left( \prod_{i=3}^3 M_i \right) \right) = M_1 \times (M_2 \times M_3).$$

Bei dieser mengentheoretischen Modellierung hat allgemein jedes Element aus  $\prod_{i=1}^n M_i$  die spezielle Form  $(a_1, (a_2, (\dots, (a_{n-1}, a_n) \dots)))$ . Man benutzt nun  $(a_1, a_2, \dots, a_{n-1}, a_n)$  als vereinfachende Schreibweise für diese rechtsgeklammerten Paare. Der Vorteil dieser Definitionsart von  $\prod_{i=1}^n M_i$  ist, dass, wenn man sie zu linearen Listen verallgemeinert, man genau die Listen-Datenstruktur bekommt, wie sie in allen modernen funktionalen Programmiersprachen (wie Scheme, ML oder Haskell) vorhanden ist. Ihr Nachteil ist, dass sie nicht auf Folgen verallgemeinert werden kann.

## 3.2 Lineare Listen

Tupel haben eine feste Anzahl von Komponenten. Hingegen sind lineare Listen von variabler Länge. Listen sind eine der fundamentalsten Strukturen der Informatik. Sie werden z.B. in der **Programmierung** und beim Entwurf **effizienter Datenstrukturen und Algorithmen** eingesetzt. Auch Untersuchungen von **formalen Sprachen** bauen auf Listen auf. In diesem Zusammenhang nennt man sie Wörter.

Ist  $M$  eine Menge und  $n \in \mathbb{N}$  mit  $n \geq 1$  vorgegeben, so bezeichnet  $M^n$  die Menge aller  $n$ -Tupel mit Elementen aus  $M$ . Im Fall, dass  $M$  endlich ist, haben wir  $|M^n| = |M|^n$ . Wir wollen nun  $M^n$  auch für  $n = 0$  so festlegen, dass  $|M^0| = |M|^0 = 1$  gilt. Also muss  $M^0$  aus genau einem Element bestehen. Im Hinblick auf die bisherigen Darstellung von Tupeln legen wir fest:

### 3.2.1 Definition: leeres Tupel

Für alle Mengen  $M$  definieren wir  $M^0 := \{()\}$  und nennen das spezielle Element  $()$  das **leere Tupel**.  $\square$

Man beachte, dass  $()$  als ein Symbol angesehen wird und nicht als aufgebaut mittels der zwei runden Klammern. In der Literatur werden beispielsweise auch der Buchstabe  $\varepsilon$  oder das Wort **nil** für das leere Tupel verwendet. Nun können wir die Menge aller beliebigen Tupel mit einer endlichen Zahl von Komponenten definieren. In der Informatik spricht man in diesem Zusammenhang oft von (endlichen) linearen Listen (oder Sequenzen oder Wörtern). Deswegen verwenden auch wir nachfolgend diese Terminologie.

### 3.2.2 Definition: lineare Liste, nichtleere und leere Liste

Zu einer Menge  $M$  definieren wir die Mengen  $M^+$  und  $M^*$  wie folgt:

- (1)  $M^+ := \bigcup\{M^n \mid n \in \mathbb{N} \setminus \{0\}\}$
- (2)  $M^* := \{()\} \cup M^+ = \bigcup\{M^n \mid n \in \mathbb{N}\}$

Ein Element  $s \in M^*$  heißt **lineare Liste** über  $M$ . Gilt  $s \in M^+$ , so heißt  $s$  **nichtleer**. Das Element  $() \in M^*$  heißt **leere Liste**.  $\square$

Es ist somit  $M^*$  die Menge aller linearen Listen über der Menge  $M$  und  $M^+$  die Menge aller nichtleeren linearen Listen über der Menge  $M$ . Wir haben in Definition 3.2.2 eine beliebige Menge  $M$  vorausgesetzt. Sinnvoll ist normalerweise nur  $M \neq \emptyset$ . Wir werden diese Zusatzeigenschaft im weiteren Verlauf des Texts aber nur fordern, wenn wir sie explizit

brauchen. Um mit linearen Listen umgehen zu können, etwa bei der Programmierung, benötigt man gewisse Operationen (Funktionen), wie etwa in analoger Weise bei den Zahlen beispielsweise die Addition und die Multiplikation zum Rechnen dienen. Es hat sich herausgestellt, dass man bei den linearen Listen mit genau einer Operation auskommt, bei der noch die Tupelstruktur der Listen wesentlich ist. Diese Operation fügt an lineare Listen von links (also von vorne) Elemente an. Wir notieren sie wie in der funktionalen Programmierung oft gebräuchlich.

### 3.2.3 Definition: Linksanfügen

Die Funktion „;“ der Funktionalität<sup>4</sup>  $M \times M^* \rightarrow M^*$  ist in Infix-Schreibweise für alle  $a \in M$  und  $s = (s_1, \dots, s_n) \in M^*$  definiert durch

$$a : s = (a, s_1, \dots, s_n).$$

Man nennt „;“ die Operation des **Linksanfügens** oder des Anfügens von vorne.  $\square$

In dieser Definition ist unterstellt, dass für  $n = 0$  die lineare Liste  $(s_1, \dots, s_n)$  gleich zur leeren Liste () ist. Wir werden diese Gleichheit auch im Rest des Texts verwenden, um unnötige Fallunterscheidungen zu vermeiden. Die Gleichsetzung von  $(s_1, \dots, s_n)$  und () im Fall  $n = 0$  entspricht genau der schon erwähnten Gleichsetzung der Mengen  $\{a_1, \dots, a_n\}$  und  $\emptyset$ . Jede lineare Liste  $s \in M^*$  ist also entweder leer oder von der Form  $a : t$ , mit  $a \in M$  und  $t \in M^*$ . Ist nämlich  $s$  nichtleer, so ist  $s$  ein  $n$ -Tupel  $(s_1, \dots, s_n)$  mit  $n \geq 1$ . Definiert man  $a := s_1$  und  $t := (s_2, \dots, s_n)$  (insbesondere  $t := ()$ , falls  $n = 1$ ), so gilt offensichtlich  $s = a : t$  nach der schon früher verwendeten Gleichheit von Tupeln, die natürlich auch bei Listen ihre Gültigkeit hat. Aufgrund der eben gezeigten Darstellung von linearen Listen kann man nun viele Operationen (Funktionen) auf linearen Listen definieren, indem man die Fälle „Liste ist leer“ und „Liste hat die Gestalt  $a : t$ “ unterscheidet. Vier wichtige Operationen sind nachfolgend angegeben.

### 3.2.4 Definition: Operationen auf linearen Listen

Es sei  $M \neq \emptyset$  eine Menge.

- (1) Die Funktion  $kopf : M^+ \rightarrow M$ , die jeder nichtleeren linearen Liste den **Listenkopf** (das erste Element) zuordnet, ist für alle  $a \in M$  und  $s \in M^*$  wie folgt definiert:

$$kopf(a : s) = a$$

- (2) Die Funktion  $rest : M^+ \rightarrow M^*$ , die von jeder nichtleeren linearen Liste den Listenkopf entfernt, also die Restliste bildet, ist für alle  $a \in M$  und  $s \in M^*$  wie folgt definiert:

$$rest(a : s) = s$$

- (3) Die Funktion  $|\cdot| : M^* \rightarrow \mathbb{N}$ , die jeder linearen Liste die **Länge** zuordnet und bei der der Punkt die Schreibweise der Funktionsanwendung angibt, ist für alle  $a \in M$  und  $s \in M^*$  wie folgt definiert:

$$|()| = 0 \quad |a : s| = 1 + |s|$$

---

<sup>4</sup>Wir wählen diese sprachliche Art, die Funktionalität anzugeben, weil die übliche Art mit dem trennenden Doppelpunkt hier zu der sonderbaren Schreibweise  $: : M \times M^* \rightarrow M^*$  führt.

- (4) Die Funktion  $\& : M^* \times M^* \rightarrow M^*$ , die zwei lineare Listen **konkateniert** (hintereinanderfügt), ist in Infix-Schreibweise für alle  $a \in M$  und  $s, t \in M^*$  wie folgt definiert:

$$() \& t = t \quad (a : s) \& t = a : (s \& t) \quad \square$$

Man beachte, dass in Definition 3.2.4 nirgends mehr verwendet wird, dass lineare Listen Tupel von Objekten sind. Man arbeitet nur mehr mit der Konstanten „()“ und der Operation „,:“ des Linksanfügens, mit denen man alle linearen Listen erzeugen kann. Mit Hilfe dieser beiden Konstruktionen kann man auch die **Gleichheit von linearen Listen** durch ihren Aufbau definieren. Es gibt hier die folgenden vier Fälle, wobei  $a, b \in M$  und  $s, t \in M^*$  beliebig vorausgesetzt ist:

- (1)  $() = () \iff \text{wahr}$
- (2)  $() = b : t \iff \text{falsch}$
- (3)  $a : s = () \iff \text{falsch}$
- (4)  $a : s = b : t \iff a = b \wedge s = t$

Die Leserin oder der Leser überlege sich, wie man auf diese Weise weitere wichtige Listenoperationen rekursiv festlegen kann, etwa das Anfügen von rechts (von hinten), das Entfernen des rechtesten (des letzten) Elements oder das Testen des Enthaltsenseins eines Objekts in einer linearen Liste.

### 3.2.5 Beispiele: Operationen auf linearen Listen

Wir setzen die Menge  $M := \{a, b, c, d\}$  voraus und betrachten die Listen  $s := (a, a, b, c, d)$  und  $t := (d, d, c, c)$ . Dann gelten offensichtlich für  $s$  und  $t$  die zwei Gleichungen

$$s = a : a : b : c : d : () \quad t = d : d : c : c : (),$$

die zeigen, wie man die Listen aus der leeren Liste durch Linksanfügen der Elemente nach und nach aufbaut. Nun demonstrieren wir, wie man anhand des jeweiligen Aufbaus die Operationen der Definition 3.2.4 anwenden kann und wie man die Resultate rekursiv termäßig berechnet. Wir beginnen mit der Berechnung des Listenkopfes von  $s$ :

$$\text{kopf}(s) = \text{kopf}(a : a : b : c : d : ()) = a$$

Als Nächstes zeigen wir, wie man den Listenkopf von  $s$  entfernt:

$$\text{rest}(s) = \text{rest}(a : a : b : c : d : ()) = a : b : c : d : () = (a, b, c, d)$$

Als drittes Beispiel berechnen wir die Länge von  $s$ :

$$\begin{aligned} |s| &= |a : a : b : c : d : ()| \\ &= 1 + |a : b : c : d : ()| \\ &= 1 + 1 + |b : c : d : ()| \\ &= 1 + 1 + 1 + |c : d : ()| \\ &= 1 + 1 + 1 + 1 + |d : ()| \\ &= 1 + 1 + 1 + 1 + 1 + |()| \\ &= 1 + 1 + 1 + 1 + 1 + 0 \\ &= 5 \end{aligned}$$

Schließlich zeigen wir durch die Rechnung

$$\begin{aligned}
s \& t &= (a : a : b : c : d : ()) \& t \\
&= a : ((a : b : c : d : ()) \& t) \\
&= a : a : ((b : c : d : ()) \& t) \\
&= a : a : b : ((c : d : ()) \& t) \\
&= a : a : b : c : ((d : ()) \& t) \\
&= a : a : b : c : d : ((()) \& t) \\
&= a : a : b : c : d : t \\
&= (a, a, b, c, d, d, d, c, c)
\end{aligned}$$

auch noch, wie man die beiden Listen  $s$  und  $t$  konkateniert.  $\square$

Für die bisher eingeführten Operationen auf den linearen Listen gelten viele wichtige Eigenschaften. Einige davon sind nachfolgend angegeben.

- (1)  $|s \& t| = |s| + |t|$  für alle  $s, t \in M^*$ .
- (2)  $(s \& t) \& u = s \& (t \& u)$  alle  $s, t, u \in M^*$ , d.h. die Konkatenationsoperation ist assoziativ.
- (3)  $() \& s = s$  und  $s \& () = s$  für alle  $s \in M^*$ , d.h. die Konkatenationsoperation besitzt die leere Liste als sogenanntes neutrales Element.
- (4)  $\text{kopf}(s \& t) = \text{kopf}(s)$  für alle  $s \in M^+$  und  $t \in M^*$ .
- (5)  $\text{rest}(s \& t) = \text{rest}(s) \& t$  für alle  $s \in M^+$  und  $t \in M^*$ .

Beim derzeitigen Stand des Texts sind wir noch nicht in der Lage, alle diese Eigenschaften formal aus den rekursiven Definitionen der Operationen auf den linearen Listen herzuleiten. Wir werden aber in Kapitel 4 eine spezielle Beweistechnik vorstellen und als korrekt beweisen, die es erlaubt, diese Beweise zu führen.

Für alle reellen Zahlen  $q \in \mathbb{R}$  mit  $q \neq 1$  und alle natürlichen Zahlen  $n \in \mathbb{N}$  gilt, wie man sich vielleicht (wenn man es beigebracht bekam) noch von der höheren Schule her erinnert, die Summenformel

$$1 + q + q^2 + \dots + q^n = \frac{q^{n+1} - 1}{q - 1}$$

der sogenannten **geometrischen Reihe**  $\sum_{i=0}^n q^i$ , also  $\sum_{i=0}^n q^i = \frac{q^{n+1} - 1}{q - 1}$ , wenn man durch die beiden Gleichungen

$$\sum_{i=0}^0 k_i := k_0 \quad \sum_{i=0}^{n+1} k_i := k_{n+1} + \sum_{i=0}^n k_i$$

die Summe  $\sum_{i=0}^n k_i$  von Zahlen  $k_0, \dots, k_n$  rekursiv analog zur Definition der allgemeinen Produktbildung  $\prod_{i=1}^n k_i$  in Abschnitt 3.1 festlegt<sup>5</sup>. Mit Hilfe der Summenformel der geometrischen Reihe kann man nun den folgenden Satz beweisen.

---

<sup>5</sup>Wegen der speziellen Anwendung beginnen wir hier mit dem Index 0. Die Leserin oder der Leser definiere zu Übungszwecken auch die Summe  $\sum_{i=1}^n k_i$  von  $n \geq 1$  Zahlen  $k_1, \dots, k_n$ .

### 3.2.6 Satz: Anzahl von Listen einer maximalen Länge

Für alle endlichen und nichtleeren Mengen  $M$  und alle natürlichen Zahlen  $n \in \mathbb{N}$  gilt die folgende Gleichung hinsichtlich der Anzahl der Listen mit Maximallänge  $n$ :

$$|\{s \in M^* \mid |s| \leq n\}| = \begin{cases} n+1 & \text{falls } |M|=1 \\ \frac{|M|^{n+1}-1}{|M|-1} & \text{falls } |M|>1 \end{cases}$$

**Beweis:** Die Mengen  $M^0, \dots, M^n$  sind paarweise disjunkt, da ihre Elemente verschiedene Längen haben. Dies bringt

$$|\{s \in M^* \mid |s| \leq n\}| = |\bigcup_{i=0}^n M^i| = \sum_{i=0}^n |M^i| = \sum_{i=0}^n |M|^i$$

aufgrund der Sätze 1.3.7 und 3.1.3. Ist nun  $|M| = 1$ , so folgt daraus die Gleichheit

$$|\{s \in M^* \mid |s| \leq n\}| = \sum_{i=0}^n |M|^i = \sum_{i=0}^n 1^i = n+1.$$

Im verbleibenden Fall bekommen wir die Behauptung durch die Rechnung

$$|\{s \in M^* \mid |s| \leq n\}| = \sum_{i=0}^n |M|^i = \frac{|M|^{n+1}-1}{|M|-1}$$

unter Verwendung der Summenformel der geometrischen Reihe.  $\square$

Im nächsten Beispiel geben wir eine kleine praktische Anwendung für den eben bewiesenen Satz an.

### 3.2.7 Beispiel: Auto-Kennzeichen

Wir betrachten die Menge der lateinischen Großbuchstaben, also  $M := \{A, B, C, \dots, Z\}$  mit der Kardinalität  $|M| = 26$ . Dann gilt

$$|\{s \in M^* \mid 1 \leq |s| \leq 2\}| = 26^0 + 26^1 + 26^2 - 1 = \frac{26^3 - 1}{25} - 1 = \frac{17575}{25} - 1 = 702.$$

Lässt man nun bei einem üblichen deutschen Auto-Kennzeichen nach dem Kürzel für die Stadt oder den Landkreis eine Buchstabenliste mit einem oder zwei Buchstaben zu und, daran folgend, (natürliche) Zahlen zwischen 10 und 999 (also 990 Zahlen), so bekommt man genau  $702 \cdot 990 = 694980$  verschiedene Möglichkeiten. Diese Anzahl von Buchstaben/Ziffern-Kombinationen reicht heutzutage nicht mehr für eine Stadt der Größe Berlins oder Hamburgs aus. Deshalb lässt man hier bei Auto-Kennzeichen Zahlen zwischen 10 und 9999 zu.  $\square$

Hat eine vorliegende lineare Liste  $s \in M^+$  als Tupel die Form  $(s_1, \dots, s_n)$ , wobei  $n \geq 1$ , so bezeichnet man das Element  $s_i$  als die *i-te Komponente* von  $s$ , für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq |s|$ . Auch die Operation des **Komponentenzugriffs** kann man ohne Bezug auf die Tupelstruktur durch den Aufbau der linearen Listen mittels der leeren Liste „()“

und der Operation „;“ spezifizieren. Dazu definiert man diese Operation, wir nennen sie  $\text{elem} : M^+ \times \mathbb{N} \rightarrow M$ , durch die rekursive Festlegung

$$\text{elem}(a : s, i) = \begin{cases} a & \text{falls } i = 1 \\ \text{elem}(s, i - 1) & \text{falls } i > 1 \end{cases}$$

für alle  $i \in \mathbb{N}$ ,  $a \in M$  und  $s \in M^*$ . Dann gilt  $\text{elem}(s, i) = s_i$  im Fall von  $1 \leq i \leq |s|$ . Allerdings ist  $\text{elem}$  keine Funktion im Sinne von Abschnitt 1.4 mehr, da  $\text{elem}(s, i)$  für alle  $i \in \mathbb{N}$  mit  $i = 0$  oder  $i > |s|$  nicht definiert ist. Man spricht im Fall von  $\text{elem}$ , wie schon im letzten Abschnitt des ersten Kapitels erwähnt wurde, von einer **partiellen Funktion**.

Eigentlich alle modernen funktionalen Programmiersprachen stellen eine vordefinierte Datenstruktur für lineare Listen zur Verfügung. Im Vergleich zu unseren mathematischen Notationen weichen aber die Bezeichnungen und auch die Angaben konkreter Listen oft sehr ab. Wir geben nachfolgend die Syntax für lineare Listen für zwei sehr bekannte funktionale Programmiersprachen an, nämlich für die Sprache Scheme (die insbesonders zu Lehrzwecken eingesetzt wird<sup>6</sup>) und die Sprache Haskell (benannt nach dem amerikanischen Mathematiker Haskell Curry (1900-1982)).

| Mathematik          | Scheme                        | Haskell                    |
|---------------------|-------------------------------|----------------------------|
| $(a_1, \dots, a_n)$ | <code>(list a1 ... an)</code> | <code>[a1, ..., an]</code> |
| $()$                | <code>empty</code>            | <code>[]</code>            |
| $\text{kopf}(s)$    | <code>(first s)</code>        | <code>head s</code>        |
| $\text{rest}(s)$    | <code>(rest s)</code>         | <code>tail s</code>        |
| $s \& t$            | <code>(append s t)</code>     | <code>s ++ t</code>        |
| $ s $               | <code>(length s)</code>       | <code>length s</code>      |
| $a : s$             | <code>(cons a s)</code>       | <code>a : s</code>         |
| $s_i$               | <code>(list-ref s i)</code>   | <code>s !! i</code>        |

Der Vorteil der eckigen Klammern ist, dass man genau zwischen den Klammern zur Listenbildung und den Klammern zur Strukturierung von Ausdrücken und Formeln unterscheidet. Man vergleiche etwa den Haskell-Ausdruck `(1 : [2,3]) ++ [3,4]` mit den Ausdruck `(1 : (2,3)) & (3,4)` in unserer Notation. Im zweiten Ausdruck dient ein Klammerpaar der Strukturierung und zwei Klammerpaare definieren Listen.

In der Sprache Scheme werden alle Funktionsanwendungen  $f(a_1, \dots, a_n)$  konsequent in der Form  $(f\ a_1 \dots a_n)$  notiert und in Haskell durch das Hintereinanderstellen von Funktionsbezeichnung und Argument(tupel), was im Fall der einstelligen Operationen `head` und `tail` zu den obigen Schreibweisen führt. Allerdings zählen sowohl Scheme als auch Haskell die Komponenten von Listen ab dem Index 0, nehmen also  $s$  von der Form  $(s_0, \dots, s_{n-1})$  an und nicht von der Form  $(s_1, \dots, s_n)$  wie wir. In solch einem Szenario ist die obige Operation  $\text{elem}$  geeignet umzudefinieren.

Jedes Wort einer natürlichen Sprache ist eine Liste von Zeichen (z.B. Buchstaben). Jedoch werden in diesem Zusammenhang die Klammern und trennenden Kommata weggelassen. Beispielsweise schreibt man *Haus* statt  $(H, a, u, s)$ . Das gleiche Vorgehen ist in

---

<sup>6</sup>Bei Scheme verwenden wir nicht die Originalnotationen, sondern die eines Sprachdialekt, welcher auch an der Universität Kiel bei der Einführung in die Programmierung verwendet wird.

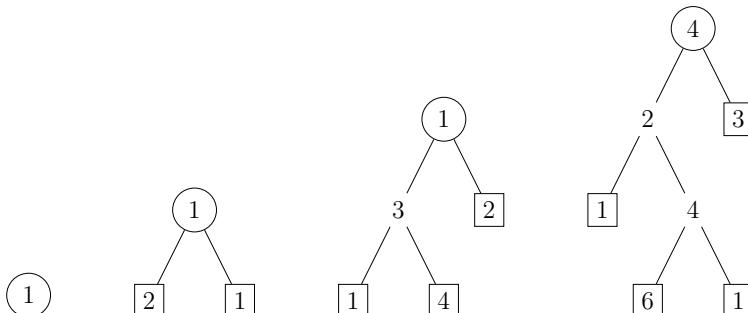
der Informatik bei formalen Sprachen üblich. Auch hier schreibt man  $a_1a_2\dots a_n$  statt  $(a_1, a_2, \dots, a_n)$  und nennt  $a_1a_2\dots a_n$  ein Wort und jedes einzelne  $a_i$  ein Zeichen. Weiterhin wird die Konkatenation durch das Hintereinanderschreiben notiert. Dabei wird zwischen einzelnen Zeichen und Wörtern nicht unterschieden. Es kann also  $aw$  sowohl die Konkatenation der Wörter  $a$  und  $w$  bedeuten als auch das Linksanfügen des Zeichens  $a$  an das Wort  $w$  als auch das Rechtsanfügen des Zeichens  $w$  an das Wort  $a$ . Was gemeint ist, wird in diesem Zusammenhang normalerweise durch Zusatzbedingungen festgelegt, etwa, dass Zeichen immer mit dem Buchstaben  $a$  (gegebenenfalls auch mit einem Index versehen) bezeichnet werden und Wörter immer mit dem Buchstaben  $w$ . Nur das leere Wort, also unsere leere Liste  $()$ , wird normalerweise mit dem griechischen Buchstaben  $\varepsilon$  bezeichnet. All dies vereinfacht natürlich die entstehenden Ausdrücke. Die Vorgehensweise birgt aber, insbesondere für den Anfänger, die Gefahr des falschen Interpretierens. Wir gebrauchen deshalb in diesem Text immer die in diesem Abschnitt eingeführten Notationen.

### 3.3 Knotenmarkierte Binäräbäume

Neben den linearen Listen spielen noch Datenstrukturen mit Verzweigung, sogenannte Bäume, in der Informatik eine große Rolle. Es gibt viele Typen von Bäumen, beispielsweise beliebig verzweigte Bäume, binär verzweigte Bäume, knotenmarkierte Bäume, blattmarkierte Bäume und so fort. Wir behandeln in diesem Abschnitt nur einen speziellen Typ, nämlich **knotenmarkierte Binäräbäume**. Diese werden etwa zur Implementierung von Mengen eingesetzt, wenn es darum geht, schnelle Zugriffsoperationen zum Einfügen, Lösen und den Enthalteinstest zu bekommen. Wie solche speziellen Bäume aussehen, machen wir uns am besten zuerst anhand von einigen bildlichen Beispielen klar.

#### 3.3.1 Beispiele: knotenmarkierte Binäräbäume

In den nachfolgenden vier Bildern sind vier verschiedene knotenmarkierte Binäräbäume zeichnerisch dargestellt. Ein Binärbaum besteht danach aus **Knoten** und sie verbindende **Kanten** (gezeichnet als Linien). Zusätzlich hat man **Marken** (in den nachfolgenden Bildern natürliche Zahlen), die den Knoten zugeordnet sind. Jeder Knoten hat entweder genau zwei **Nachfolger**, das sind die unmittelbar unter ihm gezeichneten Knoten, zu denen jeweils eine Kante führt, oder keinen Nachfolger. Der einzige Knoten, der kein Nachfolger ist, heißt die **Wurzel** des Binärbaums.



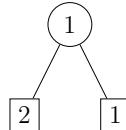
In den obigen vier Bildern sind die Wurzeln durch Kreise hervorgehoben. Die Knoten ohne Nachfolger nennt man die **Blätter** des Binärbaums. Mit Ausnahme des Bildes ganz

links sind in den obigen Bildern die Blätter durch Quadrate angezeigt. Der Binärbaum des Bildes ganz links besteht nur aus einem Knoten. Dieser ist sowohl die Wurzel als auch das einzige Blatt. Solche speziellen Binärbäume heißen **atomar**. Die **Höhe eines Binärbaums** ist die um Eins verminderte Anzahl der Schichten beim Zeichnen. Diese Zahl entspricht genau der größten Zahl von Kanten, die einen sogenannten **Weg** von der Wurzel zu einem Blatt bilden. Die oben gezeichneten Binärbäume haben, von links nach rechts, die Höhen 0, 1, 2 und 3.  $\square$

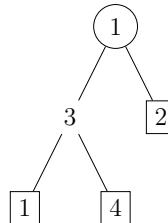
Die eben präsentierten vier Zeichnungen machen, nach einer jeweiligen Drehung um 180 Grad, auch sofort einsichtig, warum man von Binärbäumen spricht. Zur in der Informatik üblichen Darstellung von Bäumen mit der Wurzel als dem obersten Knoten und den Blättern an den unteren Enden der Verästelungen bemerkte der deutsche Mathematiker und Informatiker Klaus Samelson (1918-1980) einmal zweideutig: „In der Informatik wachsen die Bäume nicht in den Himmel“. Da Zeichnungen keine mathematischen Objekte sind, drückt man die Struktur (Hierarchie) der in Beispiel 3.3.1 gegebenen Bilder in der Regel durch Klammerungen aus, was zu Elementen von direkten Produkten führt. Bei knotenmarkierten Binärbäumen sind die Elemente der direkten Produkte 3-Tupel, also Tripel. Eine erste Möglichkeit ist dann, mit den Markierungen als den einfachsten Binärbäumen zu beginnen. Damit wird etwa der atomare Binärbaum



von Beispiel 3.3.1 zum Objekt 1, der Binärbaum



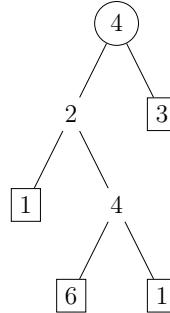
von Beispiel 3.3.1 mit drei Knoten zum Tripel  $(2, 1, 1)$  mit (teils gleichen) drei Zahlen und der Binärbaum



von Beispiel 3.3.1 mit fünf Knoten zum geschachtelten Tripel  $((1, 3, 4), 1, 2)$  mit (teils gleichen) fünf Zahlen.

Der Nachteil der eben aufgezeigten Vorgehensweise ist, dass man damit nicht alle Binärbäume modellieren kann. Beispielsweise ist es nicht möglich, auf diese Weise einen Binärbaum mit zwei oder mit vier Knoten darzustellen, weil es weder den ersten noch den zweiten Binärbaum in der bisherigen Auffassung gibt. Deshalb beginnt man nicht mit den Markierungen als den einfachsten Binärbäumen, sondern, analog zu den linearen Listen,

mit dem sogenannten **leeren Binärbaum**. Wenn wir diesen mit dem speziellen Symbol „ $\diamond$ “ bezeichnen, dann wird der gezeichnete Binärbaum



von Beispiel 3.3.1, wo man sich in der Zeichnung an jedem Blatt noch zusätzlich zwei unsichtbare leere Binärbäume vorstellen muss, durch die mathematische Klammerstruktur

$$(((\diamond, 1, \diamond), 2, ((\diamond, 6, \diamond), 4, (\diamond, 1, \diamond))), 4, (\diamond, 3, \diamond))$$

dargestellt, also durch ein (zugegeben kompliziertes) Objekt eines direkten Produkts. Vergleicht man das letzte Bild und diese Klammerstruktur, so erkennt man bei der gewählten Darstellungsart unmittelbar die folgenden Eigenschaften:

- (1) Die Blätter entsprechen genau den innersten Tripeln der Klammerstruktur. Sie haben die Form  $(\diamond, a, \diamond)$ , wobei  $a$  die Marke des Blattes ist.
- (2) Die Wurzel entspricht genau dem äußersten Tripel der Klammerstruktur und dessen zweite Komponente ist die Wurzelmarkierung.
- (3) Die Höhe eines Binärbaums ist die um Eins verminderte Maximalzahl von sich öffnenden Klammern, d.h. die **Klammertiefe** minus 1.

Ein Binärbaum mit zwei Knoten in der üblichen zeichnerischen Darstellung mit unsichtbaren leeren Binärbäumen ist nun etwa  $((\diamond, 2, \diamond), 1, \diamond)$ . Man beachte, dass den früheren atomaren Binärbäumen nun die Binärbäume der speziellen Gestalt  $(\diamond, a, \diamond)$  entsprechen. Die nächste Definition formalisiert die Umsetzung der graphischen Bilder in Schachtelungen von Tripeln nach der zweiten Vorgehensweise. Wir verwenden dazu, wie schon bei den aussagenlogischen und den prädikatenlogischen Formeln in Kapitel 2, ein entsprechendes Regelwerk.

### 3.3.2 Definition: knotenmarkierter Binärbaum

Es sei  $M$  eine Menge (von Marken). Dann ist die Menge  $\mathcal{B}(M)$  der **knotenmarkierten Binärbäume** über  $M$  durch die folgenden Regeln definiert:

- (1) Es gilt  $\diamond \in \mathcal{B}(M)$ .
- (2) Für alle  $a \in M$  und  $l \in \mathcal{B}(M)$  und  $r \in \mathcal{B}(M)$  gilt  $(l, a, r) \in \mathcal{B}(M)$ .
- (3) Es gibt keine Elemente in  $\mathcal{B}(M)$  außer denen, die durch die Regeln (1) und (2) zugelassen werden.

Ein Binärbaum der Gestalt  $(l, a, r)$  heißt **zusammengesetzt**, mit  $l$  als dem **linken Teilbaum**,  $r$  als dem **rechten Teilbaum** und  $a$  als der **Wurzelmarkierung**. Mit  $\mathcal{ZB}(M)$  bezeichnen wir die Menge der **zusammengesetzten knotenmarkierten Binärbäume** über  $M$ , also die Menge  $\mathcal{B}(M) \setminus \{\diamond\}$ .  $\square$

Die Definition der Gleichheit von Tupeln führt sofort zu der folgenden rekursiven Beschreibung der **Gleichheit von knotenmarkierten Binärbäumen**. Es sind  $b_1, b_2 \in \mathcal{B}(M)$  genau dann gleich, wenn  $b_1$  und  $b_2$  beide leer sind oder wenn  $b_1$  und  $b_2$  beide zusammengesetzt sind und sowohl ihre linken Teilbäume als auch ihre rechten Teilbäume als auch ihre Wurzelmarkierungen gleich sind. Bei linearen Listen konnten wir alle Listen aus der leeren Liste mit Hilfe der Operation des Linksanfügens erhalten. Analog dazu können wir jeden knotenmarkierten Binärbaum aus dem leeren Baum mit Hilfe der Konstruktionsoperation *baum* erhalten, wenn wir diese wie folgt definieren.

### 3.3.3 Definition: Baumkonstruktion

Die Funktion  $\text{baum} : \mathcal{B}(M) \times M \times \mathcal{B}(M) \rightarrow \mathcal{B}(M)$  zur **Konstruktion** von knotenmarkierten Binärbäumen ist definiert durch

$$\text{baum}(l, a, r) = (l, a, r). \quad \square$$

Dann gilt, wegen der Forderung (3) von Definition 3.3.2, für alle  $b \in \mathcal{ZB}(M)$  die folgende fundamentale Eigenschaft: Es gibt knotenmarkierte Binärbäume  $l, r \in \mathcal{B}(M)$  und ein Element  $a \in M$  mit der Eigenschaft, dass  $b = \text{baum}(l, a, r)$  gilt (d.h. der Baum  $b$  in der Tat „zusammengesetzt“ ist). Aufbauend auf die Konstruktion aller knotenmarkierten Binärbäume aus dem leeren Baum  $\diamond$  mittels der Konstruktoroperation *baum* können wir nun, analog zu den linearen Listen, weitere Operationen auf knotenmarkierten Binärbäumen definieren. Nachfolgend geben wir einige davon an. Die ersten drei Baumoperationen nennt man auch **Selektoren**. Damit diese überall definiert sind, ist es bei ihnen notwendig, die Menge  $\mathcal{ZB}(M)$  als deren Quelle zu definieren. Wir empfehlen der Leserin oder dem Leser zur Übung auch die oben schon erwähnte Gleichheit von knotenmarkierten Binärbäumen mittels der Operation *baum* und dem leeren Baum formal zu spezifizieren.

### 3.3.4 Definition: Baumoperationen

Es sei  $M$  eine Markenmenge.

- (1) Die Funktion  $\text{links} : \mathcal{ZB}(M) \rightarrow \mathcal{B}(M)$  zur Bestimmung des **linken Teilbaums** ist für alle  $l, r \in \mathcal{B}(M)$  und  $a \in M$  wie folgt definiert:

$$\text{links}(\text{baum}(l, a, r)) = l$$

- (2) Die Funktion  $\text{rechts} : \mathcal{ZB}(M) \rightarrow \mathcal{B}(M)$  zur Bestimmung des **rechten Teilbaums** ist für alle  $l, r \in \mathcal{B}(M)$  und  $a \in M$  wie folgt definiert:

$$\text{rechts}(\text{baum}(l, a, r)) = r$$

- (3) Die Funktion  $\text{wurzel} : \mathcal{ZB}(M) \rightarrow M$  zur Bestimmung der **Wurzelmarkierung** ist für alle  $l, r \in \mathcal{B}(M)$  und  $a \in M$  wie folgt definiert:

$$\text{wurzel}(\text{baum}(l, a, r)) = a$$

- (4) Die Funktion  $\|\cdot\| : \mathcal{B}(M) \rightarrow \mathbb{N}$ , die für jeden knotenmarkierten Binärbaum seine **Höhe** bestimmt, ist für alle  $l, r \in \mathcal{B}(M)$  und  $a \in M$  wie folgt definiert:

$$\|\diamond\| = 0 \quad \|baum(l, a, r)\| = \begin{cases} 0 & \text{falls } l = \diamond \text{ und } r = \diamond \\ 1 + \max\{\|l\|, \|r\|\} & \text{sonst} \end{cases}$$

- (5) Die Funktion  $marken : \mathcal{B}(M) \rightarrow \mathcal{P}(M)$ , die für jeden knotenmarkierten Binärbaum die **Menge der in ihm vorkommenden Marken** bestimmt, ist für alle  $l, r \in \mathcal{B}(M)$  und  $a \in M$  wie folgt definiert:

$$marken(\diamond) = \emptyset \quad marken(baum(l, a, r)) = marken(l) \cup \{a\} \cup marken(r)$$

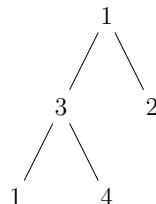
Dabei ist in der rechten Gleichung von (4) durch  $\max N$  das größte Element der endlichen und nichtleeren Teilmenge  $N$  von  $\mathbb{N}$  bezeichnet, also dasjenige Element  $x$ , welches  $x \in N$  und  $y \leq x$  für alle  $y \in N$  erfüllt.  $\square$

Wir haben schon früher bemerkt, dass die Höhe eines knotenmarkierten Binärbaums die um Eins verminderte Anzahl der Schichten beim Zeichnen ist. Unter Verwendung des Begriffs eines Wegs ist die Höhe eines knotenmarkierten Binärbaums die größte Zahl von Kanten, die einen Weg von der Wurzel zu einem Blatt bilden. Beim leeren Baum gibt es weder eine Schicht noch einen Weg mit Kanten. Aufgrund von (4) wird für diesen Ausnahmefall die Null als Höhe festgelegt. Wir haben uns bei der Definition der Höhe an die gängige Vorgehensweise gehalten, welche sich an der maximalen Kantenzahl zwischen der Wurzel und einem Blatt orientiert. Eigentlich wäre es wesentlich sinnvoller, die Anzahl der Schichten als Höhe festzulegen.

Nachfolgend demonstrieren wir anhand eines Beispielbaums von Beispiel 3.3.1, wie man mit diesen Operationen Ergebnisse termmäßig berechnen kann.

### 3.3.5 Beispiel: Baumoperationen

Wir betrachten den dritten der knotenmarkierten Binärbäume der Liste des einführenden Beispiels 3.3.1. Nachfolgend ist zur Erinnerung noch einmal seine Zeichnung angegeben, nun aber ohne die Hervorhebung der Wurzel und der Blätter.



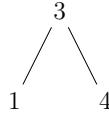
Die sich aus diesem Bild ergebende Klammerdarstellung ist  $((((\diamond, 1, \diamond), 3, (\diamond, 4, \diamond)), 1, (\diamond, 2, \diamond)))$  und daraus ergibt sich unmittelbar der Ausdruck

$$baum(baum(baum(\diamond, 1, \diamond), 3, baum(\diamond, 4, \diamond)), 1, baum(\diamond, 2, \diamond))$$

zur Konstruktion des Binärbaums mittels des leeren Baums und der Operation *baum* des Baumkonstruierens, indem man einfach vor jede öffnende Klammer der Klammerdarstellung den Operationsnamen *baum* schreibt. Nun berechnen wir, was die Baumoperationen liefern. Beginnen wir mit der Operation, welche den linken Teilbaum bestimmt. Hier haben wir die Rechnung

$$\begin{aligned} & \text{links}(\text{baum}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)), 1, \text{baum}(\diamond, 2, \diamond))) \\ &= \text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)) \\ &= ((\diamond, 1, \diamond), 3, (\diamond, 4, \diamond)) \end{aligned}$$

und die aus ihr resultierende Klammerstruktur ist genau die des folgenden bildlich angegebenen Binärbaums, welcher der linke Teilbaum der Eingabe ist.



Durch analoge Rechnungen bekommen wir

$$\begin{aligned} & \text{rechts}(\text{baum}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)), 1, \text{baum}(\diamond, 2, \diamond))) \\ &= \text{baum}(\diamond, 2, \diamond) \\ &= (\diamond, 2, \diamond) \end{aligned}$$

für den rechten Teilbaum,

$$\text{wurzel}(\text{baum}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)), 1, \text{baum}(\diamond, 2, \diamond))) = 1$$

für die Wurzelmarkierung und

$$\begin{aligned} & \| \text{baum}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)), 1, \text{baum}(\diamond, 2, \diamond)) \| \\ &= 1 + \max \{ \| \text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)) \|, \| \text{baum}(\diamond, 2, \diamond) \| \} \\ &= 1 + \max \{ 1 + \max \{ \| \text{baum}(\diamond, 1, \diamond) \|, \| \text{baum}(\diamond, 4, \diamond) \| \}, 0 \} \\ &= 1 + \max \{ 1 + \max \{ 0, 0 \}, 0 \} \\ &= 1 + \max \{ 1, 0 \} \\ &= 2 \end{aligned}$$

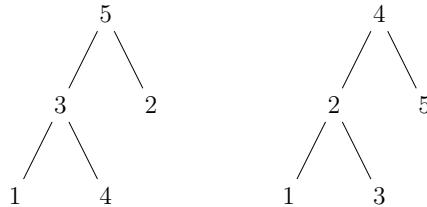
für die Höhe. Aus der Rechnung

$$\begin{aligned} & \text{marken}(\text{baum}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond)), 1, \text{baum}(\diamond, 2, \diamond))) \\ &= \text{marken}(\text{baum}(\text{baum}(\diamond, 1, \diamond), 3, \text{baum}(\diamond, 4, \diamond))) \cup \\ & \quad \{1\} \cup \text{marken}(\text{baum}(\diamond, 2, \diamond)) \\ &= \text{marken}(\text{baum}(\diamond, 1, \diamond)) \cup \{3\} \cup \text{marken}(\text{baum}(\diamond, 4, \diamond)) \cup \\ & \quad \{1\} \cup \text{marken}(\diamond) \cup \{2\} \cup \text{marken}(\diamond) \\ &= \text{marken}(\diamond) \cup \{1\} \cup \text{marken}(\diamond) \cup \{3\} \cup \text{marken}(\diamond) \cup \{4\} \cup \text{marken}(\diamond) \cup \\ & \quad \{1\} \cup \emptyset \cup \{2\} \cup \emptyset \\ &= \emptyset \cup \{1\} \cup \emptyset \cup \{3\} \cup \emptyset \cup \{4\} \cup \emptyset \cup \{1\} \cup \{2\} \\ &= \{1, 3, 4, 2\} \end{aligned}$$

ersehen wir schließlich noch, wie man die Menge aller Marken eines Binärbaums bestimmen kann.  $\square$

Wir haben am Anfang dieses Abschnitts schon bemerkt, dass knotenmarkierte Binäräbäume insbesondere zur Implementierung von Mengen eingesetzt werden. Besonders wichtig sind in diesem Zusammenhang die sortierten knotenmarkierten Binäräbäume, auch **Suchbäume** genannt. Bei diesen speziellen Bäumen ist eine Reihenfolge der Marken vorausgesetzt, ähnlich zur Ordnung auf den natürlichen Zahlen. Wir werden im sechsten Kapitel diesen Begriff als lineare Ordnung kennenlernen. Die geforderte Eigenschaft für Suchbäume ist, dass für jeden Knoten  $x$  eines Suchbaums alle Knoten links von  $x$  eine Marke tragen, die in der Reihenfolge echt vor der Marke von  $x$  steht, und alle Knoten rechts von  $x$  eine Marke tragen, die in der Reihenfolge echt nach der Marke von  $x$  steht.

Beispielsweise ist der linke der folgenden zwei Binäräbäume kein Suchbaum zur Implementierung der Menge  $\{1, 2, 3, 4, 5\}$ ; der rechte Baum ist hingegen ein Suchbaum zur Implementierung von  $\{1, 2, 3, 4, 5\}$ .



In Suchbäumen kann man oft sehr schnell nach bestimmten Marken  $a$  suchen, da bei jedem Knoten, falls er nicht mit  $a$  markiert ist, entweder nur links oder nur rechts weiter zu suchen ist. Besonders günstig sind hierbei die sogenannten „balancierten Suchbäume“, bei denen jedes Blatt von der Wurzel aus durch etwa gleich viele Kanten (d.h. Schritte) mittels eines Wegs erreichbar ist. Wie man sich leicht überlegt, kann man Wege mit gleich vielen Kanten von der Wurzel zu jedem Blatt aber nur für sehr spezielle Anzahlen von Knoten erhalten. Deshalb fordert man als schärfste Bedingung, dass sich die Kantenzahlen aller Wege von der Wurzel zu den Blättern maximal um Eins unterscheiden. Extrem ungünstig beim Suchen sind hingegen diejenigen Suchbäume, welche quasi zu einer linearen Liste entarten. Man nennt sie auch „gekämmte Suchbäume“. Genauer wird auf dieses Thema normalerweise in einer Vorlesung und in der Literatur über effiziente Algorithmen und Datenstrukturen eingegangen.

### 3.4 Zur induktiven Definition von Mengen

Wir haben in Kapitel 1 zwei Darstellungsarten für Mengen eingeführt. Aus so angegebenen Mengen kann man neue Mengen erzeugen; auch dies wurde im ersten Kapitel mittels entsprechender Konstruktionen gezeigt. Als Erweiterung dieser Möglichkeiten führen wir in Kapitel 2 bei den Formeln und in diesem Kapitel bei den knotenmarkierten Binäräbäumen die Definition von Mengen durch ein Regelsystem ein. Diese Vorgehensweise soll nachfolgend etwas allgemeiner behandelt werden.

Es seien  $M$  eine nichtleere Menge,  $B$  eine nichtleere Teilmenge von  $M$  und  $K$  eine Menge von Funktionen  $f : M^{s(f)} \rightarrow M$ , wobei  $s(f)$  die Stelligkeit von  $f$  bezeichne, also die Anzahl der Argumente. Dann heißt  $M$  **induktiv definiert** mittels der **Basiselemente** aus  $B$  und der **Konstruktorfunktionen** aus  $K$ , falls die folgenden Bedingungen gelten:

- (1) Es gilt  $B \subseteq M$ .
- (2) Für alle  $f \in K$  und  $x_1, \dots, x_{s(f)} \in M$  gilt  $f(x_1, \dots, x_{s(f)}) \in M$ .
- (3) Es gibt keine Elemente in  $M$  außer denen, die durch die Regeln (1) und (2) zugelassen werden.

Man kann die durch Regel (3) formulierte Bedingung auch wie folgt beschreiben: Für alle Objekte  $a \in M$  gibt es einen Ausdruck, der nur mittels der Elemente aus  $B$  und der Funktionen aus  $K$  aufgebaut ist, dessen Wert  $a$  ergibt. Da Ausdrücke in der Mathematik und der Informatik auch als Terme bezeichnet werden, nennt man  $M$  wegen dieser Formulierung auch **termerzeugt**. Gibt es für alle  $a \in M$  genau einen Ausdruck (Term), der nur mittels der Basiselemente und der Konstruktorfunktionen aufgebaut ist und dessen Wert  $a$  ergibt, so nennt man  $M$  **frei induktiv definiert**.

Beispielsweise ist die Menge der natürlichen Zahlen frei induktiv definiert mittels  $B := \{0\}$  und  $K := \{\text{nachf}\}$ , wobei  $\text{nachf}$  die Nachfolgerfunktion aus Abschnitt 1.4 ist:

$$\text{nachf} : \mathbb{N} \rightarrow \mathbb{N} \quad \text{nachf}(x) = x + 1$$

Es gelten nämlich die Gleichungen

$$1 = \text{nachf}(0), 2 = \text{nachf}(\text{nachf}(0)), 3 = \text{nachf}(\text{nachf}(\text{nachf}(0))), \dots,$$

und andere Ausdrücke über 0 und  $\text{nachf}$  zur Darstellung der natürlichen Zahlen gibt es nicht. Auch die Menge  $\mathcal{B}(M)$  der knotenmarkierten Binäräbäume über  $M$  ist frei induktiv definiert, wenn man  $B := \{\diamond\}$  und  $K := \{b_a \mid a \in M\}$  wählt, wobei alle Konstruktorfunktionen  $b_a : \mathcal{B}(M)^2 \rightarrow \mathcal{B}(M)$  definiert sind durch

$$b_a(l, r) = (l, a, r) = \text{baum}(l, a, r).$$

Die Leserin oder der Leser mache sich klar, durch welche Basismenge und Menge von Konstruktorfunktionen man jeweils die Formelmengen von Kapitel 2 und die Menge der linearen Listen  $M^*$  frei induktiv definieren kann, wenn man bei den Formeln immer eine vollständige Klammerung voraussetzt, also etwa  $(A_1 \vee (A_2 \vee (\neg A_3)))$  statt  $A_1 \vee A_2 \vee \neg A_3$  schreibt. Eine induktive Definition, die nicht frei ist, ist die der Menge  $\mathbb{Z}$  der ganzen Zahlen mit Basismenge  $B := \{0\}$  und Konstruktorfunktionenmenge  $K := \{\text{nachf}, \text{vorg}\}$ , wobei

$$\text{nachf} : \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{nachf}(x) = x + 1$$

die Nachfolgerfunktion auf den ganzen Zahlen sei und

$$\text{vorg} : \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{vorg}(x) = x - 1$$

die Vorgängerfunktion. Beispielsweise ist nun die Null der Wert sowohl des Ausdrucks 0 als auch der Wert des Ausdrucks  $\text{nachf}(\text{vorg}(0))$ .

Im Fall einer mittels der zwei Mengen  $B$  und  $K$  frei induktiv definierten Menge  $M$  kann man Funktionen durch den Aufbau ihrer Argumente festlegen, wobei man in der Regel eine Argumentposition nimmt, die, wie man sagt, die Definition steuert. Ist dies beispielsweise

die erste Position, so spezifiziert man im Fall einer Funktion  $g : M \times A_1 \times \dots \times A_n \rightarrow B$  wie folgt, was Aufrufe von  $g$  bewirken. Man wählt  $y_i \in A_i$ ,  $1 \leq i \leq n$ , als beliebige Objekte. Dann definiert man die Basisfälle

$$g(a, y_1, \dots, y_n) = E_1(a, y_1, \dots, y_n)$$

durch die Angabe eines entsprechenden Ausdrucks  $E_1(a, y_1, \dots, y_n)$  auf der rechten Seite in Abhängigkeit von  $a$  und den  $y_1, \dots, y_n$  für alle Basiselemente  $a$ , legt also fest, was  $g$  bewirkt, wenn das erste Argument ein Basiselement ist. Und schließlich betrachtet man noch die Konstruktorfälle, wo das erste Argument von  $g$  kein Basiselement, sondern ein zusammengesetztes (konstruiertes) Element ist. Das führt zu Gleichungen

$$g(f(x_1, \dots, x_{s(f)}), y_1, \dots, y_n) = E_2(g, x_1, \dots, x_{s(f)}, y_1, \dots, y_n)$$

für alle Konstruktorfunktionen  $f \in K$ , wobei die rechte Seite  $E_2(g, x_1, \dots, x_{s(f)}, y_1, \dots, y_n)$  wiederum ein entsprechender Ausdruck ist, nun aber nur von  $g$ , den  $x_1, \dots, x_{s(f)}$  und den  $y_1, \dots, y_n$  abhängend<sup>7</sup>. Jeder Konstruktorfall führt bei seiner Berechnung schließlich zu den Basisfällen und dort hängt alles nur mehr von den  $y_1, \dots, y_n$  ab. Wenn, wie im Fall von *kopf* und *rest* bei den linearen Listen oder im Fall von *links*, *rechts* und *wurzel* bei den knotenmarkierten Binärbäumen, eine Funktion nur für Nichtbasiselemente definiert ist, dann können die Basisfälle auch fehlen. Als Erweiterung des obigen Vorgehens sind bei den Konstruktorfällen schließlich nicht nur einzelne Aufrufe  $f(x_1, \dots, x_{s(f)})$  von Konstruktorfunktionen erlaubt, sondern ganze **Konstruktorausdrücke**, die mehrere solche Aufrufe enthalten können. Damit kann man etwa das Testen auf Geradesein bei den natürlichen Zahlen als Funktion *gerade* :  $\mathbb{N} \rightarrow \mathbb{B}$  wie folgt spezifizieren:

$$\text{gerade}(0) = \mathbf{W} \quad \text{gerade}(\text{nachf}(0)) = \mathbf{F} \quad \text{gerade}(\text{nachf}(\text{nachf}(x))) = \text{gerade}(x)$$

Dann zeigt etwa die folgende Rechnung, dass 5 keine gerade Zahl ist.

$$\begin{aligned} \text{gerade}(5) &= \text{gerade}(\text{nachf}(\text{nachf}(\text{nachf}(\text{nachf}(\text{nachf}(\text{nachf}(0))))))) \\ &= \text{gerade}(\text{nachf}(\text{nachf}(\text{nachf}(0)))) \\ &= \text{gerade}(\text{nachf}(0)) \\ &= \mathbf{F} \end{aligned}$$

In funktionalen Programmiersprachen, wie den schon erwähnten Sprachen ML und Haskell, entsprechen die Deklarationen von rekursiven Datentypen genau den freien induktiven Definitionen der entsprechenden Mengen und die Deklarationen von Funktionen durch, wie man sagt, Musteranpassung genau der eben beschriebenen Vorgehensweise der Festlegung von Funktionen durch den Aufbau ihrer Argumente.

## 3.5 Übungsaufgaben

### Aufgabe

Spezifizieren Sie die folgenden Eigenschaften mittels Formeln:

---

<sup>7</sup>Er darf sogar noch von  $f$  abhängen, aber nur in einer bestimmten Weise, welche bewirkt, dass alle Berechnungen terminieren. Weil dies Abhängigkeit von  $f$  in der Praxis aber kaum vorkommt, beachten wir diesen Fall hier nicht.

- (1) Das  $n$ -Tupel  $(x_1, \dots, x_n) \in \mathbb{N}^n$  ist von links nach rechts aufsteigend der Größe nach sortiert.
- (2) Alle Komponenten des  $n$ -Tupels  $(x_1, \dots, x_n) \in \mathbb{N}^n$  sind paarweise verschieden.
- (3) Alle Komponenten des  $n$ -Tupels  $(x_1, \dots, x_n) \in \mathbb{N}^n$  sind identisch.

### Aufgabe

Gegeben seien die Mengen  $M_1 := \{1, 2, 3\}$ ,  $M_2 := \{2, 3\}$  und  $M_3 := \{3\}$ .

- (1) Geben Sie das direkte Produkt  $\prod_{i=1}^3 M_i$  explizit an.
- (2) Zu  $x \in M_1$ ,  $y \in M_2$  und  $z \in M_3$  betrachten wir die folgenden Formeln:

$$(a) \quad x \leq y \wedge y \leq z \quad (b) \quad x \neq y \wedge y \neq z \wedge z \neq x \quad (c) \quad x = y \wedge y = z$$

Kennzeichnen Sie in der Lösung von (1) die Tripel  $(x, y, z)$ , welche (a) bzw. (b) bzw. (c) erfüllen.

- (3) Beschreiben Sie die durch (a), (b) und (c) spezifizierten Eigenschaften umgangssprachlich.

### Aufgabe

Wir betrachten eine Menge  $M := \{a_1, \dots, a_n\}$  mit  $n$  Elementen. Berechnen Sie die Kardinalitäten der folgenden Teilmengen von  $M^k$ :

$$\{(x_1, \dots, x_k) \in M^k \mid x_1 = a_1\} \quad \{(x_1, \dots, x_k) \in M^k \mid x_k \neq a_k\}$$

### Aufgabe

Aufbauend auf die Mengen  $M := \{a, b\}$  und  $N := \{c\}$  betrachten wir die Konstruktionen  $M \times N^1$ ,  $(M^2 \times M) \times N$ ,  $((M \times M) \times M) \times N$ ,  $M^2 \times (M \times N)$  und  $(M \times M) \times (M \times N^2)$ . Geben Sie zu den Tupeln  $((b, b), b), c)$ ,  $(a, (c))$ ,  $((b, b), (b, (c, c)))$ ,  $((b, b), b)$ ,  $(c, (c, b))$  und  $((b, b), (b, c))$ , jeweils an, zu welcher Menge sie gehören.

### Aufgabe

Transformieren Sie die Formel

$$(a) \quad \neg \exists i \in \mathbb{N} : 1 \leq i \leq |s| \wedge s_i = x$$

durch logische Umformungen in eine äquivalente Formel, in der kein Negationssymbol mehr auftritt. Was besagt (a) umgangssprachlich für  $s \in M^*$  und  $x \in M$ ?

### Aufgabe

Zeigen Sie, aufbauend auf die Definitionen der Operationen *kopf*, *rest* und *&* der linearen Listen, für alle  $a \in M$  und  $s, t \in M^*$  die folgenden Gleichungen:

$$(a) \quad \text{kopf}((a : s) \& t) = a \quad (b) \quad \text{rest}((a : s) \& t) = s \& t$$

### Aufgabe

Eine lineare Liste  $s \in M^*$  heißt Anfangsstück der linearen Liste  $t \in M^*$ , falls ein  $r \in M^*$  mit  $s \& r = t$  existiert.

- (1) Ist  $s$  ein Anfangsstück von  $t$  und  $t$  ein Anfangsstück von  $u$ , so ist  $s$  ein Anfangsstück von  $u$ . Beweis!
- (2) Gibt es eine lineare Liste, die ein Anfangsstück von allen linearen Listen aus  $M^*$  ist (mit Begründung)?

### Aufgabe

Die Aussage  $A(f)$ , in der  $f$  eine Variable für Funktionen von  $\mathbb{N}^n$  nach  $\mathbb{N}^n$  ist, sei wie folgt definiert:

$$\forall s \in \mathbb{N}^n, i \in \mathbb{N} : (1 \leq i \leq n) \Rightarrow f(s)_i = s_{n+1-i}$$

- (1) Welche Eigenschaft von  $f$  wird durch  $A(f)$  spezifiziert?
- (2) Zeigen Sie: Sind  $g, h : \mathbb{N}^n \rightarrow \mathbb{N}^n$  Funktionen, für die  $A(g)$  und  $A(h)$  gelten, so gilt  $g = h$ .
- (3) Beweisen Sie für alle Funktionen  $f : \mathbb{N}^n \rightarrow \mathbb{N}^n$ , dass aus  $A(f)$  für alle  $t \in \mathbb{N}^n$  die Gleichheit  $f(f(t)) = t$  folgt.

### Aufgabe

Es sei  $M$  eine Menge und  $s \in M^*$  eine lineare Liste.

- (1) Definieren Sie mit Hilfe der Operationen auf den linearen Listen eine Funktion  $\text{rev} : M^* \rightarrow M^*$ , welche das Argument umkehrt, z. B.  $\text{rev}(a : b : c : ()) = c : b : a : ()$ .
- (2) Demonstrieren Sie die Arbeitsweise von  $\text{rev}$  an den linearen Listen  $(o, t, t, o)$  und  $(r, e, n, t, n, e, r)$ .

### Aufgabe

Ein lineare Liste  $s \in M^*$  heißt ein Palindrom genau dann, wenn  $s$  von vorne und hinten gelesen gleich bleibt. Definieren Sie eine Aussage  $\text{palindrom}(s)$ , die genau dann gilt, wenn  $s$  ein Palindrom ist.

### Aufgabe

Es sei  $M$  eine Menge.

- (1) Geben Sie eine Funktion  $\text{anz} : \mathcal{B}(M) \rightarrow \mathbb{N}$  an, welche die Anzahl der Markierungen eines knotenmarkierten Binärbaums zählt.
- (2) Geben Sie eine Funktion  $\text{einmal} : \mathcal{B}(M) \rightarrow \mathbb{N}$  an, welche die Anzahl derjenigen Markierungen zählt, die genau einmal in einem knotenmarkierten Binärbaum vorkommen.

## 4 Mathematische Beweise

Beweise zu führen ist das Kerngeschäft der Mathematik. In ihnen wird mit logischen Mitteln nachgewiesen, dass eine mathematische Aussage gültig ist. Es gibt verschiedene Stile, um mathematische Beweise aufzuschreiben. Früher, als die Formelsprache der Mathematik noch nicht oder noch nicht so weit wie heute entwickelt war, waren Beweise hauptsächlich Argumentationen in der Umgangssprache; ein Argumentieren, wie es sich aus der Philosophie entwickelt hat. Heutzutage sind mathematische Beweise in der Regel viel formaler, insbesondere dann, wenn sie durch Computerprogramme überprüft werden sollen. Auf den Gebrauch der Umgangssprache wird aber nicht völlig verzichtet, da umgangssprachliche Formulierungen die Verständlichkeit und Lesbarkeit oft sehr verbessern. In diesem Kapitel wollen wir die wichtigsten Beweistechniken vorstellen und anhand von ausgewählten Beispielen demonstrieren. Dabei gehen wir auch auf die den Beweistechniken zugrundeliegenden logischen Regeln ein.

### 4.1 Direkte Beweise

Bei einem **direkten Beweis** einer mathematischen Aussage  $A$  wird das Problem direkt und ohne Umwege angegangen. Man verwendet bei der Argumentation der Richtigkeit nur die Voraussetzungen, schon bewiesene Aussagen und logische Regeln, um  $A$  zu beweisen. Alle bisherigen Beweise der ersten drei Kapitel waren direkt. Hier ist ein weiteres sehr berühmtes Beispiel für einen Satz mit einem direkten Beweis.

#### 4.1.1 Satz: Summenformel von C.F. Gauß

Für alle  $n \in \mathbb{N} \setminus \{0\}$  gilt  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ .

**Beweis:** Wir starten mit der Rechnung

$$\begin{aligned}(1 + \dots + n) + (1 + \dots + n) &= (1 + 2 + \dots + n) + (n + (n - 1) + \dots + 1) \\&= (1 + n) + (2 + n - 1) + \dots + (n + 1) \\&= (n + 1) + (n + 1) + \dots + (n + 1) \quad n\text{-mal} \\&= n(n + 1).\end{aligned}$$

Also gilt  $2(1 + 2 + \dots + n) = n(n + 1)$  und ein Umstellen dieser Gleichung durch eine Division beider Seiten durch 2 bringt die Behauptung.  $\square$

Wir haben diesen Beweis in der informellen Notation mit den drei Punkten geführt, damit die Idee, die ihm zugrunde liegt, ganz deutlich hervortritt. Diese Beweisidee soll der große deutsche Mathematiker Carl Friedrich Gauß (1777–1855) schon als Schüler gehabt haben, als er in Sekundenschule die Aufgabe löste, alle Zahlen von 1 bis 100 zu addieren. Wir haben schon früher die Summe  $\sum_{i=1}^n k_i$  einer Liste  $k_1, \dots, k_n$  von  $n > 0$  Zahlen rekursiv definiert. Unter Verwendung dieser Schreibweise besagt Satz 4.1.1, dass

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

für alle  $n \in \mathbb{N} \setminus \{0\}$  gilt. Man kann diese Aussage auch ohne Verwendung der Schreibweise mit den drei Punkten beweisen. Wie dies geht, werden wir in Abschnitt 4.4 demonstrieren.

Typische direkte Beweise sind solche durch logische Umformungen oder arithmetische bzw. mengentheoretische Abschätzungen. Hier ist ein Beispiel für eine Abschätzung, welches wir als Vorbereitung für ein wichtigeres Resultat bringen.

#### 4.1.2 Lemma

Es seien  $M$  eine Menge und  $\mathcal{M}$  eine nichtleere Menge von Mengen. Gilt  $M \subseteq X$  für alle  $X \in \mathcal{M}$ , so gilt auch  $M \subseteq \bigcap \mathcal{M}$ .

**Beweis:** Es sei  $a$  ein beliebiges Objekt. Weiterhin gelte die Aussage  $a \in M$ . Dann folgt daraus  $a \in X$  für alle  $X \in \mathcal{M}$ , da  $M \subseteq X$  für alle  $X \in \mathcal{M}$  gilt. Nach der Definition von  $\bigcap \mathcal{M}$  zeigt dies  $a \in \bigcap \mathcal{M}$ .

Also haben wir  $M \subseteq \bigcap \mathcal{M}$  nach der Definition der Inklusion von Mengen gezeigt.  $\square$

Ein Beweis einer Aussage, welche eine Existenzquantifizierung darstellt, heißt **konstruktiv**, wenn die behauptete Existenz eines bestimmten Objekts dadurch gezeigt wird, dass es angegeben oder sogar algorithmisch konstruiert wird. Konstruktive Beweise sind oftmals auch direkt. Hier ist ein bekanntes Beispiel. Wir beweisen einen sogenannten Fixpunktsatz, der auf die polnischen Mathematiker Bronislaw Knaster (1893-1990) und Alfred Tarski (1901-1983) zurückgeht und von Knaster im Jahr 1927 publiziert wurde. Mit ihm werden wir im nächsten Kapitel einen berühmten Satz der Mengenlehre zeigen.

#### 4.1.3 Satz: Fixpunktsatz von B. Knaster

Eine Funktion  $f : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$  auf der Potenzmenge einer Menge  $M$  erfülle die folgende Eigenschaft (genannt **Monotonie**):

$$\forall X, Y \in \mathcal{P}(M) : X \subseteq Y \Rightarrow f(X) \subseteq f(Y)$$

Dann gibt es eine Menge  $N \in \mathcal{P}(M)$  mit den folgenden zwei Eigenschaften:

- (1)  $f(N) = N$
- (2) Für alle  $X \in \mathcal{P}(M)$  gilt: Aus  $f(X) = X$  folgt  $N \subseteq X$ .

**Beweis:** Wir betrachten die (wegen  $f(M) \subseteq M$  nichtleere) Menge

$$\mathcal{M} := \{X \in \mathcal{P}(M) \mid f(X) \subseteq X\}$$

und definieren die Menge  $N$  mittels  $N := \bigcap \mathcal{M}$ . Für diese Menge zeigen wir nun die behaupteten Eigenschaften (1) und (2).

Beweis von (1): Es sei die Menge  $X$  beliebig angenommen. Gilt  $X \in \mathcal{M}$ , so gilt auch  $\bigcap \mathcal{M} \subseteq X$  nach Satz 1.2.6. Als Konsequenz erhalten wir aufgrund der vorausgesetzten Monotonie und weil  $X \in \mathcal{M}$ , dass

$$f(\bigcap \mathcal{M}) \subseteq f(X) \subseteq X.$$

Folglich ist  $f(\bigcap \mathcal{M}) \subseteq X$  für alle  $X \in \mathcal{M}$  wahr. Das eben bewiesene Lemma 4.1.2 und die Definition von  $N$  implizieren

$$f(N) = f(\bigcap \mathcal{M}) \subseteq \bigcap \mathcal{M} = N.$$

Nun verwenden wir wiederum die Monotonie und erhalten daraus  $f(f(N)) \subseteq f(N)$ . Also gilt  $f(N) \in \mathcal{M}$  und eine nochmalige Anwendung von Satz 1.2.6 bringt  $\bigcap \mathcal{M} \subseteq f(N)$ . Schließlich folgt die noch fehlende Inklusion

$$N = \bigcap \mathcal{M} \subseteq f(N)$$

zum Beweis von (1) aus der Definition von  $N$ .

Beweis von (2): Es sei  $X \in \mathcal{P}(M)$  beliebig vorgegeben. Gilt  $f(X) = X$ , so folgt daraus  $f(X) \subseteq X$ . Dies ist logisch äquivalent zu  $X \in \mathcal{M}$ . Damit erhalten wir

$$N = \bigcap \mathcal{M} \subseteq X$$

aufgrund der Definition von  $N$  und einer nochmaligen Anwendung von Satz 1.2.6.  $\square$

In der Sprechweise der Mathematik sagt Satz 4.1.3: Monotone Funktionen auf Potenzmengen besitzen einen kleinsten Fixpunkt. Es wird ein Element  $x \in X$  nämlich als **Fixpunkt** einer Funktion  $g : X \rightarrow X$  bezeichnet, falls  $g(x) = x$  gilt. Die Menge  $N$  des Satzes 4.1.3 ist also ein Fixpunkt der vorgegebenen Funktion  $f : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$  und, im Inklusionssinne, kleiner als jeder andere Fixpunkt von  $f$ . Oft schreibt man  $\mu(g)$  für kleinste Fixpunkte.

Bei konstruktiven Beweisen von Aussagen ist eine Aufgabe, die immer wieder auftritt, zu zeigen, dass, in einer formalen Schreibweise mit Formeln, die logische Implikation

$$\exists x : A_1(x) \implies \exists y : A_2(y)$$

gilt. Zu deren Beweis nimmt man an, dass die linke Seite  $\exists x : A_1(x)$  wahr ist. Also gibt es ein Objekt  $a$ , für das die Aussage  $A_1(a)$  gilt. Mit Hilfe dieses Objekts berechnet man ein weiteres Objekt  $b$  mit der Eigenschaft  $A_2(b)$ . Durch die Existenz von  $b$  ist bewiesen, dass die rechte Seite  $\exists y : A_2(y)$  der zu zeigenden Implikation ebenfalls wahr ist. Damit gilt auch die Implikation. Wir kommen auf diese Beweistechnik, die natürlich auch bei Blöcken von Existenzquantoren angewendet werden kann, später noch zurück.

Direkte Beweise werden oft auch durch Fallunterscheidungen geführt. Wir haben in Kapitel 1 schon solche Beweise erbracht. Ihnen liegt die logische Äquivalenz

$$(B \Rightarrow A) \wedge (\neg B \Rightarrow A) \iff A$$

für alle aussagenlogischen Formeln  $A$  und  $B$  zugrunde, welche man sehr einfach mit Hilfe der in Abschnitt 2.2 angegebenen Umformungen nachrechnen kann.

## 4.2 Indirekte Beweise

In Satz 2.2.9 wurde für alle beliebigen Aussagen  $A_1$  und  $A_2$  gezeigt, dass die Implikationen  $A_1 \Rightarrow A_2$  und  $\neg A_2 \Rightarrow \neg A_1$  logisch äquivalent sind. Um  $A_1 \Rightarrow A_2$  zu zeigen, kann

man also auch  $\neg A_2 \Rightarrow \neg A_1$  beweisen, denn aus einem solchen Beweis folgt dann mittels der obigen logischen Äquivalenz die ursprünglich zu zeigende Aussage. Man nennt dieses indirekte Vorgehen einen **indirekten Beweis**. Oft spricht man auch von einem **Beweis durch Kontraposition**, weil  $\neg A_2 \Rightarrow \neg A_1$  die durch eine Kontraposition aus  $A_1 \Rightarrow A_2$  entstehende Aussage ist. Nachfolgend ist ein einfaches Beispiel für einen indirekten Beweis einer zahlentheoretischen Eigenschaft angegeben.

#### 4.2.1 Satz: ungerade Summen

Für alle  $m, n \in \mathbb{N}$  gilt: Ist  $m + n$  ungerade, so ist  $m$  ungerade oder es ist  $n$  ungerade.

**Beweis (indirekt):** Wenn wir die Behauptung etwas formaler aufschreiben, so haben wir für alle  $m, n \in \mathbb{N}$  die folgende logische Implikation zu beweisen:

$$m + n \text{ ungerade} \implies m \text{ ungerade} \vee n \text{ ungerade}$$

Bei einem indirekten Beweis dieser Aussage starten wir mit der Negation der rechten Seite. Nach einer Regel von de Morgan ist diese äquivalent zu

$$m \text{ gerade} \wedge n \text{ gerade}.$$

Also gibt es  $a, b \in \mathbb{N}$  mit  $m = 2a$  und  $n = 2b$ . Daraus folgt

$$m + n = 2a + 2b = 2(a + b) = 2c,$$

mit  $c \in \mathbb{N}$  definiert als  $c := a + b$ . Folglich ist  $m + n$  gerade und dies ist genau die Negation der linken Seite der zu beweisenden logischen Implikation.  $\square$

Indirekte Beweise werden, wie im letzten Beispiel demonstriert, der Leserin oder dem Leser oft dadurch angezeigt, dass man nach dem Schlüsselwort „**Beweis**“ einen entsprechenden Hinweis gibt. Wichtig bei indirekten Beweisen ist das korrekte Negieren der beiden Seiten der ursprünglichen Implikation. Eine nicht korrekte Negation der rechten Seite als Ausgangspunkt, insbesondere im Fall von vorhandenen Quantoren, ist die häufigste Fehlerquelle bei indirekten Beweisen. Für Anfänger ist es ratsam, gegebenenfalls die Negationen mittels logischer Umformungen formal auszurechnen.

Häufig werden Beweisprinzipien auch gemischt, insbesondere in umfangreichen Beweisen. Nachfolgend geben wir einen Beweis einer Äquivalenz an, wobei eine Richtung direkt und die andere Richtung indirekt bewiesen wird. In dem Satz verwenden wir die schon aus früheren Abschnitten bekannte Operation *max* zur Bestimmung des größten Elements einer nichtleeren und endlichen Menge von natürlichen Zahlen.

#### 4.2.2 Satz: ganzzahliger Anteil der Quadratwurzel

Für alle  $m, n \in \mathbb{N}$  gilt  $m = \max\{x \in \mathbb{N} \mid x^2 \leq n\}$  genau dann, wenn  $m^2 \leq n < (m+1)^2$ .

**Beweis:** Die Richtung „ $\implies$ “ zeigen wir direkt. Es folgt der Beweis aus der Rechnung

$$\begin{aligned} m = \max\{x \in \mathbb{N} \mid x^2 \leq n\} &\implies m \in \{x \in \mathbb{N} \mid x^2 \leq n\} \\ &\iff m^2 \leq n, \end{aligned}$$

die verwendet, dass das größte Element einer Menge in dieser als Element enthalten ist, und der Rechnung

$$\begin{aligned} m = \max \{x \in \mathbb{N} \mid x^2 \leq n\} &\implies m+1 \notin \{x \in \mathbb{N} \mid x^2 \leq n\} \\ &\iff \neg((m+1)^2 \leq n) \\ &\iff n < (m+1)^2, \end{aligned}$$

die verwendet, dass der Nachfolger des größten Elements nicht in der Menge liegt.

Die Richtung „ $\Leftarrow$ “ zeigen wir indirekt. Es gelte also  $m \neq \max \{x \in \mathbb{N} \mid x^2 \leq n\}$ . Dann gibt es zwei Fälle.

- (a) Es ist  $m$  kein Element der Menge  $\{x \in \mathbb{N} \mid x^2 \leq n\}$ . Dann ist dies gleichwertig zu  $\neg(m^2 \leq n)$ , also auch zu  $n < m^2$ .
- (b) Es ist  $m$  ein Element von  $\{x \in \mathbb{N} \mid x^2 \leq n\}$ . Weil  $m$  nicht das größte Element dieser Menge ist, muss es ein  $k \in \{x \in \mathbb{N} \mid x^2 \leq n\}$  geben mit  $m < k$ . Also gelten sowohl  $k^2 \leq n$  als auch  $m < k$ . Aus  $m < k$  folgt  $m+1 \leq k$ , also  $(m+1)^2 \leq k^2 \leq n$ .

Aufgrund dieser zwei Fälle haben wir gezeigt, dass die Formel  $n < m^2 \vee (m+1)^2 \leq n$  wahr ist. Nun formen wir diese Formel wie folgt um:

$$\begin{aligned} n < m^2 \vee (m+1)^2 \leq n &\iff \neg(m^2 \leq n) \vee \neg(n < (m+1)^2) \\ &\iff \neg(m^2 \leq n \wedge n < (m+1)^2) \\ &\iff \neg(m^2 \leq n < (m+1)^2) \end{aligned}$$

Damit ist der indirekte Beweis erbracht, denn die letzte Formel dieser Rechnung ist genau die zu zeigende Eigenschaft.  $\square$

In der Mathematik wird eine Formel des Typs  $x \leq y \wedge y \leq z$ , wie schon erwähnt, normalerweise zu  $x \leq z$  abgekürzt. Gleiches gilt für die Relation „ $<$ “ und, wie oben gezeigt, Mischungen von beiden. Bei einer Negation wird aus der Kurzschreibweise immer eine Disjunktion; dies wird von Anfängern oft übersehen und führt dann zu falschen Beweisen.

### 4.3 Beweise durch Widerspruch

Es sei  $A_1$  eine vorgegebene Aussage. Um  $A_1$  zu zeigen, nimmt man die negierte Aussage  $\neg A_1$  als wahr an und folgert daraus eine Aussage  $A_2$  und auch deren Negation  $\neg A_2$ . Wegen der logischen Äquivalenz

$$\begin{aligned} (\neg A_1 \Rightarrow A_2) \wedge (\neg A_1 \Rightarrow \neg A_2) &\iff (\neg\neg A_1 \vee A_2) \wedge (\neg\neg A_1 \vee \neg A_2) \\ &\iff (A_1 \vee A_2) \wedge (A_1 \vee \neg A_2) \\ &\iff A_1 \vee (A_2 \wedge \neg A_2) \\ &\iff A_1 \vee \text{falsch} \\ &\iff A_1 \end{aligned}$$

hat man damit  $A_1$  gezeigt. Dieses Vorgehen nennt man einen **Beweis durch Widerspruch**, weil sich die beiden aus  $\neg A_1$  bewiesenen Aussagen  $A_2$  und  $\neg A_2$  gegenseitig widersprechen. Ein wichtiger Spezialfall liegt vor, wenn  $A_2$  eine zu **falsch** logisch äquivalente

Aussage ist, man also die Implikation  $\neg A_1 \Rightarrow \text{falsch}$  bewiesen hat. Dann ist  $\neg A_2$  zu **wahr** logisch äquivalent und, da  $\neg A_1 \Rightarrow \text{wahr}$  immer wahr ist, braucht man sich nicht mehr mit ihr zu befassen. Auch eine Implikation  $\neg(B_1 \Rightarrow B_2)$  kommt oft als  $A_1$  vor. Hier ist dann  $B_1 \wedge \neg B_2$  die negierte Form, mit der man den Beweis durch Widerspruch beginnt.

Der Widerspruchsbeweis ist eines der wirksamsten Mittel des mathematischen Beweisens. Er war schon den alten Griechen bekannt und wird in Euklids bekanntem Werk „Die Elemente“, in dem das gesamte mathematische Wissen der griechischen Antike in 13 Büchern zusammengefasst ist, fortlaufend verwendet. Die folgenden berühmten Beispiele stammen alle aus diesem Werk. Wie schon bei den indirekten Beweisen, so zeigt man auch bei den Widerspruchsbeweisen oft durch einen Hinweis am Beweisanfang an, dass man dieses Beweisprinzip verwendet.

#### 4.3.1 Satz (Euklid)

Es gilt  $\sqrt{2} \notin \mathbb{Q}$ , d.h.  $\sqrt{2}$  ist eine irrationale Zahl.

**Beweis (durch Widerspruch):** Angenommen, es sei  $\sqrt{2} \in \mathbb{Q}$  wahr. Dann gibt es Zahlen  $p, q \in \mathbb{Z}$  mit  $q \neq 0$  so, dass die folgenden Eigenschaften gelten:

(a)  $p$  und  $q$  sind teilerfremd.

(b)  $\sqrt{2} = \frac{p}{q}$

Aus (b) folgt  $2 = (\sqrt{2})^2 = (\frac{p}{q})^2 = \frac{p^2}{q^2}$ , also  $p^2 = 2q^2$ , und damit ist  $p^2$  gerade. Folglich ist auch  $p$  gerade. Da  $p$  gerade ist, gibt es  $a \in \mathbb{N}$  mit  $p = 2a$ . Aus  $p^2 = 2q^2$  folgt  $(2a)^2 = 2q^2$ , also  $4a^2 = 2q^2$ , also  $q^2 = 2a^2$ . Damit ist auch  $q^2$  gerade und folglich ist auch  $q$  gerade. Insgesamt sind nun  $p$  und  $q$  nicht teilerfremd. Das ist ein Widerspruch zu (a).  $\square$

Im Vergleich zur schematischen Beschreibung am Anfang des Abschnitts entspricht nun  $\sqrt{2} \notin \mathbb{Q}$  der zu beweisenden Aussage  $A_1$  und die aus deren Negation  $\sqrt{2} \in \mathbb{Q}$  bewiesenen Aussagen  $A_2$  und  $\neg A_2$  sind „ $p$  und  $q$  sind teilerfremd“ und „ $p$  und  $q$  sind nicht teilerfremd“. Normalerweise taucht  $A_2$  irgendwann im Laufe des Beweises als bewiesene (Teil-)Aussage auf und man erwähnt erst nach dem Beweis von  $\neg A_2$ , dass dies ein Widerspruch zu  $A_2$  ist.

Von der weiterbildenden Schule her ist sicherlich bekannt, dass man jede natürliche Zahl  $n$  mit  $n \geq 2$  als ein Produkt  $p_1 \cdot \dots \cdot p_k$  von  $k \geq 1$  Primzahlen darstellen (also in  $k$  Primzahlen faktorisieren) kann. Gleiche Primzahlen fasst man dann zu Primzahlpotenzen zusammen. Etwa gelten die folgenden Gleichungen:

$$\begin{aligned} 5 &= 5 = 5^1 \\ 45 &= 3 \cdot 3 \cdot 5 = 3^2 \cdot 5^1 \\ 240 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^4 \cdot 3^1 \cdot 5^1 \end{aligned}$$

Diese Darstellung von natürlichen Zahlen durch Produkte von Primzahlen bzw. deren Potenzen wird sogar eindeutig, wenn man die Primzahlen der Größe nach sortiert. Nachfolgend beweisen wir nun die Existenz der Zerlegung in Primfaktoren. Dabei verwenden wir die folgende Festlegung, da sie hilft, die Argumentation zu erleichtern.

### 4.3.2 Festlegung

Im Weiteren bezeichnet das Symbol  $\mathbb{P}$  die Menge aller Primzahlen.  $\square$

Hier ist nun der angekündigte Satz.

### 4.3.3 Satz (Euklid)

Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gibt es eine nichtleere lineare Liste  $s \in \mathbb{P}^+$  von Primzahlen mit  $n = \prod_{i=1}^{|s|} s_i$ .

**Beweis (durch Widerspruch):** Angenommen, es gelte die behauptete Aussage nicht. Dann gilt die Formel

$$\exists n \in \mathbb{N} : n \geq 2 \wedge \forall s \in \mathbb{P}^+ : n \neq \prod_{i=1}^{|s|} s_i$$

und somit ist die Menge  $M := \{n \in \mathbb{N} \mid n \geq 2 \wedge \forall s \in \mathbb{P}^+ : n \neq \prod_{i=1}^{|s|} s_i\}$  nicht leer.

Es sei  $n_0$  die kleinste Zahl in dieser Menge, im Zeichen  $n_0 := \min M$ . Dann ist  $n_0$  keine Primzahl, denn sonst hätte man die Darstellung  $n_0 = \prod_{i=1}^{|s|} s_i$ , mit der linearen Liste  $s := (n_0)$ . Folglich gibt es  $a, b \in \mathbb{N}$  mit  $n_0 = ab$  und  $2 \leq a, b \leq n_0 - 1$ . Aufgrund von  $a, b < n_0$  gilt  $a, b \notin M$  und wegen  $2 \leq a, b$  müssen die zwei Formeln  $\forall s \in \mathbb{P}^+ : a \neq \prod_{i=1}^{|s|} s_i$  und  $\forall s \in \mathbb{P}^+ : b \neq \prod_{i=1}^{|s|} s_i$  falsch sein. Also existieren lineare Listen  $t \in \mathbb{P}^+$  mit  $a = \prod_{i=1}^{|t|} t_i$  und  $u \in \mathbb{P}^+$  mit  $b = \prod_{i=1}^{|u|} u_i$ . Dies zeigt die Gleichung

$$n_0 = ab = \left( \prod_{i=1}^{|t|} t_i \right) \left( \prod_{i=1}^{|u|} u_i \right) = \prod_{i=1}^{|v|} v_i,$$

wenn wir die lineare Liste  $v$  durch  $v := t \& u$  definieren. Die Existenz von  $v$  impliziert  $n_0 \notin M$  und dies ein Widerspruch zu  $n_0 \in M$ .  $\square$

Mit Hilfe dieses Satzes kann man nun den folgenden Satz zeigen. Umgangssprachlich besagt er, dass es unendlich viele Primzahlen gibt.

### 4.3.4 Satz (Euklid)

- (1) Es sei  $M \subseteq \mathbb{P}$  eine endliche und nichtleere Menge von Primzahlen. Dann existiert eine Primzahl  $p$  mit  $p \notin M$ .
- (2) Für jedes  $n \in \mathbb{N} \setminus \{0\}$  gibt es eine Menge  $M \subseteq \mathbb{P}$  von Primzahlen mit  $|M| = n$ .

**Beweis:** (1) Es habe die Menge  $M$  die explizite Darstellung  $M = \{p_1, \dots, p_k\}$  mit  $k \geq 1$  Primzahlen  $p_1, \dots, p_k$ . Wir definieren eine Zahl  $n \in \mathbb{N}$  wie folgt:

$$n := 1 + \prod_{i=1}^k p_i$$

Fall 1: Es ist  $n$  eine Primzahl. Dann gilt  $n \neq p_i$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$ . Wir beweisen dies durch Widerspruch. Gäbe es ein  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$  und  $n = p_i$ , so gibt es auch ein

$a \in \mathbb{N}$  mit  $n = 1 + an$ . Dies folgt aus der Definition von  $n$  mit  $a := p_1 \dots p_{i-1} p_{i+1} \dots p_k$ . Aus  $n = 1 + an$  folgt  $a = \frac{n-1}{n}$ , d.h.  $a \notin \mathbb{N}$ . Das ist ein Widerspruch zu  $a \in \mathbb{N}$ . Also ist  $n$  eine gesuchte Primzahl  $p$ .

Fall 2: Es ist  $n$  keine Primzahl. Nach Satz 4.3.3 gibt es dann eine Primzahl  $p$  und  $a \in \mathbb{N}$  mit  $n = ap$  (aus der Definition von  $n$  folgt nämlich  $n \geq 2$ ). Für diese Primzahl  $p$  gilt  $p \neq p_i$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$ . Auch dies beweisen wir durch Widerspruch. Gäbe es ein  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$  und  $p = p_i$ , so gilt  $n = ap_i$ . Aus der Definition von  $n$  folgt aber auch, analog zum ersten Fall, dass es ein  $b \in \mathbb{N}$  gibt mit  $n = 1 + bp_i$ . Dies bringt

$$ap_i = n = 1 + bp_i$$

und daraus folgt  $1 = ap_i - bp_i = p_i(a - b)$ , d.h.  $p_i = 1$  oder  $p_i \notin \mathbb{N}$ . Das ist ein Widerspruch zur Primzahleigenschaft von  $p_i$ . Also hat man wieder das gesuchte  $p$  gefunden.

(2) Wir zeigen auch diesen Teil des Satzes durch Widerspruch. Angenommen, es gäbe ein  $n \in \mathbb{N} \setminus \{0\}$  so, dass keine Menge  $M$  von  $n$  Primzahlen existiert. Es sei  $n_0$  das kleinste  $n$  mit dieser Eigenschaft. Dann gilt  $n_0 \neq 1$ , da  $\{2\}$  eine Menge mit einer Primzahl ist. Folglich gibt es eine Menge  $N \subseteq \mathbb{P}$  mit der Kardinalität  $|N| = n_0 - 1$ , die nur aus Primzahlen besteht. Wegen  $n_0 > 1$  gilt  $n_0 - 1 > 0$  und somit ist  $N$  nicht leer. Nach (1) gibt es eine Primzahl  $p$  mit  $p \notin N$ . Also ist  $N \cup \{p\} \subseteq \mathbb{P}$  eine Menge von  $n_0 - 1 + 1 = n_0$  Primzahlen. Das ist ein Widerspruch zur Annahme, dass es keine Menge mit genau  $n_0$  Primzahlen als ihre Elemente gibt.  $\square$

Die in den Beweisen der Sätze 4.3.3 und 4.3.4 (2) verwendeten speziellen Zahlen  $n_0$  werden manchmal auch die **kleinsten Verbrecher** genannt. Die Wahl von kleinsten Verbrechern bei Widerspruchsbeweisen ist eine oft verwendete Technik. Sie wird uns im Laufe des Texts noch mehrfach begegnen.

Wichtig bei Beweisen durch Widerspruch ist, wie schon bei indirekten Beweisen, dass die Behauptung korrekt negiert wird. Werden dabei Fehler gemacht, so ist der gesamte Beweis falsch. Der Beweis des nachfolgenden Satzes ist ein letztes Beispiel für einen Widerspruchsbeweis. Wir demonstrieren noch einmal, wie hilfreich formales Vorgehen beim Negieren sein kann, wenn man unsicher ist. Das folgende Prinzip wird dem deutschen Mathematiker Peter Gustav Lejeune Dirichlet (1805-1859) zugeschrieben, der Nachfolger von Gauß in Göttingen war.

#### 4.3.5 Satz: Schubfachprinzip

Es seien  $n_1, \dots, n_k$  natürliche Zahlen, wobei  $k \geq 1$  gilt, und  $\bar{X} := \frac{1}{k} \sum_{l=1}^k n_l$  der arithmetische Mittelwert ist. Dann gibt es  $i, j \in \mathbb{N}$  mit  $1 \leq i, j \leq k$  und  $n_i \leq \bar{X} \leq n_j$ .

**Beweis (durch Widerspruch):** Wir bereiten den eigentlichen Beweis etwas vor. Als Formel mit zwei durch einen Existenzquantor gebundenen Variablen  $i$  und  $j$  sieht die Aussage des Satzes wie folgt aus:

$$\exists i, j \in \mathbb{N} : 1 \leq i \leq k \wedge 1 \leq j \leq k \wedge n_i \leq \bar{X} \wedge \bar{X} \leq n_j.$$

Zur Negation dieser Formel empfiehlt es sich, sie erst in die nachstehende logisch äquivalente Formel umzuformen, in der einzeln über  $i$  und  $j$  quantifiziert wird:

$$(\exists i \in \mathbb{N} : 1 \leq i \leq k \wedge n_i \leq \bar{X}) \wedge (\exists j \in \mathbb{N} : 1 \leq j \leq k \wedge \bar{X} \leq n_j)$$

Die Negation dieser Formel ist dann, nach einer der de Morganschen Regeln, logisch äquivalent zur Disjunktion

$$\neg(\exists i \in \mathbb{N} : 1 \leq i \leq k \wedge n_i \leq \bar{X}) \vee \neg(\exists j \in \mathbb{N} : 1 \leq j \leq k \wedge \bar{X} \leq n_j)$$

und diese ist offensichtlich wiederum logisch äquivalent zu

$$(\forall i \in \mathbb{N} : 1 \leq i \leq k \Rightarrow n_i > \bar{X}) \vee (\forall j \in \mathbb{N} : 1 \leq j \leq k \Rightarrow \bar{X} > n_j).$$

Nun gelte also die Negation der ursprünglichen Aussage/Formel, also die eben hergeleitete Disjunktion. Dann gibt es zwei Fälle.

(a) Der linke Teil der Disjunktion ist wahr. Hier folgt

$$k\bar{X} = k\left(\frac{1}{k} \sum_{i=1}^k n_i\right) = \sum_{i=1}^k n_i > \sum_{i=1}^k \bar{X} = k\bar{X}$$

und dies ist ein Widerspruch zur immer geltenden Aussage  $k\bar{X} = k\bar{X}$ .

(b) Der rechte Teil der Disjunktion ist wahr. Hier folgt analog zum ersten Fall, dass

$$k\bar{X} = k\left(\frac{1}{k} \sum_{i=1}^k n_i\right) = \sum_{i=1}^k n_i < \sum_{i=1}^k \bar{X} = k\bar{X},$$

und dies ist wieder ein Widerspruch zu  $k\bar{X} = k\bar{X}$ . □

Will man zu einer mathematischen Aussage einen Beweis finden, ist aber nicht erfolgreich, so gibt es im Prinzip drei Gründe hierfür:

- (1) Der Beweis ist **zu schwierig** und etwa mit den derzeitig vorhandenen Erfahrungen, Kenntnissen, Techniken usw. nicht zu erbringen.
- (2) Es ist aus **prinzipiellen Gründen nicht möglich**, solch einen Beweis zu finden. Von Kurt Gödel (1906-1978), einem österreichischen Logiker und Mathematiker, wurde im Jahr 1932 in einer epochalen Arbeit gezeigt, dass es wahre mathematische Aussagen gibt, die nicht beweisbar sind.
- (3) Die Aussage **ist falsch**, kann also nicht bewiesen werden.

Um zu zeigen, dass eine Aussage falsch ist, muss man sie durch ein Gegenbeispiel widerlegen. Das ist etwas anderes als ein Beweis durch Widerspruch. Normalerweise widerlegt man Aussagen, die in einer formalisierten Form einer allquantifizierten Formel  $\forall x : A(x)$  entsprechen. Um zu zeigen, dass die Formel  $\forall x : A(x)$  falsch ist, muss man zeigen, dass die negierte Formel  $\neg\forall x : A(x)$  wahr ist. Wegen der logischen Äquivalenz von  $\neg\forall x : A(x)$  und  $\exists x : \neg A(x)$  genügt es, dazu ein Objekt  $a$  mit  $\neg A(a)$  anzugeben, also eines, für das  $A(a)$  falsch ist. Wir beschließen diesen Abschnitt mit Beispielen zu Widerlegungen durch Gegenbeispiele.

### 4.3.6 Beispiele: Widerlegen durch Gegenbeispiele

Wir betrachten die umgangssprachlich formulierte Aussage „zwischen den natürlichen Zahlen  $n$  und  $2n$  liegen in Fall  $n \geq 4$  mindestens zwei Primzahlen“, welche als prädikatenlogische Formel wie folgt aussieht:

$$\forall n \in \mathbb{N} : n \geq 4 \Rightarrow \exists p, q \in \mathbb{N} : p, q \text{ Primzahlen } \wedge n < p < q < 2n$$

Diese Formel gilt nicht. Ein Gegenbeispiel ist  $n := 5$ , denn zwischen den natürlichen Zahlen 5 und 10 liegt nur eine Primzahl.

Eine reelle Folge  $(f_n)_{n \in \mathbb{N}}$  im Sinne von Definition 3.1.7 heißt eine **Nullfolge**, falls die folgende Formel gilt, in der  $|f_m|$  der **Absolutbetrag** der reellen Zahl  $f_m$  im Sinne von Abschnitt 1.5 ist:

$$\forall \varepsilon \in \mathbb{R}_{>0} : \exists n \in \mathbb{N} : \forall m \in \mathbb{N} : m \geq n \Rightarrow |f_m| < \varepsilon$$

In Worten besagt die Formel, dass jeder noch so kleine Abstand  $\varepsilon$  von der Null ab einem bestimmten Folgenglied echt unterboten wird und dies ab da immer so bleibt. Wir betrachten die folgende Aussage:

Zu einer Nullfolge  $(f_n)_{n \in \mathbb{N}}$  ist die Folge  $(\sum_{i=0}^n f_i)_{n \in \mathbb{N}}$  der sogenannten  $n$ -ten Partialsummen ebenfalls eine Nullfolge.

Auch diese Aussage gilt nicht. Ein Gegenbeispiel ist die reelle Folge  $(\frac{1}{n+1})_{n \in \mathbb{N}}$ . Sie ist eine Nullfolge, wie wir in Abschnitt 4.5 formal zeigen werden. Die (etwas lesbarer mit Punkten hingeschriebene) Folge

$$(1, 1 + \frac{1}{2}, 1 + \frac{1}{2} + \frac{1}{3}, \dots, \sum_{i=1}^n \frac{1}{i+1}, \dots)$$

ihrer Partialsummen ist hingegen keine Nullfolge. Die Folgenglieder werden immer größer und übersteigen sogar irgendwann jede noch so große vorgegebene Zahl. Wir verzichten hier auf den zugehörigen Beweis.  $\square$

## 4.4 Induktionsbeweise

Wie wir schon erwähnt haben, besitzen sehr viele Sätze der Mathematik die folgende Form. „Gegeben sei  $x \in M$  mit  $A_1(x)$ . Dann gilt  $A_2(x)$ .“ Überführt man dies nun in die formale Sprache der Prädikatenlogik, so bekommt man die allquantifizierte Formel  $\forall x \in M : A(x)$ , die es zu beweisen gilt. Die Formel  $A(x)$  ist dann im obigen Fall gegeben durch die Implikation  $A_1(x) \Rightarrow A_2(x)$ , wobei in  $A_1(x)$  die Annahmen an  $x$  formuliert sind und in  $A_2(x)$  die Eigenschaften von  $x$ , an denen man eigentlich interessiert ist. Zum Beweis von sogenannten Allaussagen der obigen Form ist die Induktion ein häufig verwendetes Mittel. Es gibt davon zwei Arten:

- (1) Induktion über den **Aufbau**: Hier verwendet man, dass alle Elemente der Menge  $M$  aus gegebenen Basiselementen durch gewisse Operationen erzeugt werden können und dieses Erzeugen die Gültigkeit der Aussage  $A(x)$  erhält.

- (2) Induktion durch **Rückgriff**: Hier verwendet man, dass auf der Menge  $M$  eine Relation  $R$  so existiert, dass man, wenn man  $R$  als Pfeildiagramm auffasst, nur endlich viele Schritte entgegen den Pfeilrichtungen machen kann, wie etwa im Diagramm der Relation *nachf* in Abschnitt 1.4. Für diejenigen Elemente, von denen aus kein Rückwärtsgehen möglich ist, muss die Aussage  $A(x)$  gelten und weiterhin muss sich die Gültigkeit von  $A(x)$  gemäß den Pfeilen vererben.

In diesem Abschnitt betrachten wir nur Induktion über den Aufbau. Die Induktion durch Rückgriff verschieben wir auf das sechste Kapitel. Wir beginnen mit den natürlichen Zahlen als Menge  $M$ . Man kann diese durch die Null und die Nachfolgerbildung  $nachf(n) = n + 1$  erzeugen. Dies ist der Hintergrund des im nächsten Satz formulierten Beweisprinzips. Im Beweis verwenden wir als entscheidende Eigenschaft, dass jede nichtleere Menge von natürlichen Zahlen eine kleinste natürliche Zahl enthält.

#### 4.4.1 Satz: vollständige Induktion

Es sei  $n$  eine Variable für natürliche Zahlen und  $A(n)$  eine Aussage (über  $n$ ). Sind die beiden (mit (IB) und (IS) bezeichneten) Formeln

$$(IB) \quad A(0) \qquad (IS) \quad \forall n \in \mathbb{N} : A(n) \Rightarrow A(n + 1)$$

wahr, so ist auch die Formel  $\forall n \in \mathbb{N} : A(n)$  wahr.

**Beweis (durch Widerspruch):** Unter der Verwendung der Abkürzungen (IB) und (IS) wird die Aussage des Satzes zur Implikation

$$(IB) \wedge (IS) \Rightarrow \forall n \in \mathbb{N} : A(n).$$

Diese gilt es als wahr zu beweisen. Einige einfache logische Umformungen ergeben, dass die Negation der obigen Implikation logisch äquivalent zu

$$(IB) \wedge (IS) \wedge \exists n \in \mathbb{N} : \neg A(n)$$

ist. Diese Formel nehmen wir nun für den Widerspruchsbeweis als wahr an. Wir nehmen also (IB) und (IS) als wahr an und, dass es ein  $n \in \mathbb{N}$  gibt mit  $\neg A(n)$ . Weil (IB) wahr ist, muss  $n$  ungleich 0 sein. Nun wählen wir wieder das kleinste  $n_0$  mit  $\neg A(n_0)$ , formal  $n_0 := \min \{n \in \mathbb{N} \mid \neg A(n)\}$ . Folglich gilt  $A(n_0 - 1)$ . Weil aber auch (IS) wahr ist, folgt daraus  $A(n_0 - 1 + 1)$ , also  $A(n_0)$ . Das ist ein Widerspruch zur Gültigkeit von  $\neg A(n_0)$ .  $\square$

Bei der vollständigen Induktion haben sich gewisse Sprechweisen herausgebildet, die wir nun vorstellen. Sie werden auch in Verbindung mit anderen Induktionsmethoden gebraucht, etwa der Listeninduktion oder der Bauminduktion, welche wir beide am Ende dieses Abschnitts noch behandeln werden.

#### 4.4.2 Sprechweisen

Man nennt die Formel (IB) in Satz 4.4.1 den **Induktionsbeginn** (manchmal auch **Induktionsanfang**) und die Formel (IS) im gleichen Satz den **Induktionsschluss**. In der Implikation von (IS) nennt man die linke Seite  $A(n)$  die **Induktionshypothese** oder **Induktionsvoraussetzung**.  $\square$

Das Beweisprinzip von Satz 4.4.1 ist eigentlich sehr einleuchtend. Es gilt die Aussage  $A(0)$  aufgrund der Voraussetzung (IB). Aus  $A(0)$  folgt  $A(1)$  wegen der Voraussetzung (IS), indem man  $n$  als 0 wählt, aus  $A(1)$  folgt dann  $A(2)$ , wiederum wegen (IS), indem man  $n$  als 1 wählt, aus  $A(2)$  folgt dann  $A(3)$ , wiederum wegen (IS), indem man  $n$  als 2 wählt und so fort. Es wird also durch vollständige Induktion ein Beweis von unendlich vielen Aussagen zur Rechtfertigung einer Allaussage der Form  $\forall n \in \mathbb{N} : A(n)$  zurückgeführt auf einen Beweis von nur zwei Aussagen, nämlich vom Induktionsbeginn (IB) und vom Induktionsschluss (IS).

Man kann bei der vollständigen Induktion statt mit der Null auch mit einer anderen natürlichen Zahl  $n_0$  beginnen. Natürlich gilt dann die Aussage, an der man interessiert ist, erst ab der Zahl  $n_0$ . Wir geben den entsprechenden Satz ohne Beweis an, denn dieser ist nur eine leichte Variation des Beweises von Satz 4.4.1.

#### 4.4.3 Satz: vollständige Induktion, variabler Induktionsbeginn

Es seien die Variable  $n$  und die Aussage  $A(n)$  wie in Satz 4.4.1 angenommen. Weiterhin sei  $n_0 \in \mathbb{N}$  beliebig. Sind die beiden Formeln

$$(IB) \quad A(n_0) \qquad (IS) \quad \forall n \in \mathbb{N} : n \geq n_0 \wedge A(n) \Rightarrow A(n+1)$$

wahr, so ist auch die Formel  $\forall n \in \mathbb{N} : n \geq n_0 \Rightarrow A(n)$  wahr.  $\square$

Die Anwendung der vollständigen Induktion beim Beweis eines Satzes besteht aus drei Schritten. Zuerst bestimmt man aus der Formulierung des zu beweisenden Satzes die Aussage  $A(n)$  im Sinne des allgemeinen Prinzips. Dann beweist man den Induktionsbeginn, also die Aussage  $A(0)$  oder die Aussage  $A(n_0)$ , falls man nicht mit der Null beginnt. Und schließlich beweist man noch den Induktionsschluss. Dazu wählt man eine beliebige natürliche Zahl  $n \in \mathbb{N}$ , gegebenenfalls mit der zusätzlichen Annahme  $n \geq n_0$ , wenn man die Induktion bei  $n_0$  beginnt, und zeigt dann, dass die Aussage  $A(n+1)$  aus der Induktionshypothese  $A(n)$  folgt. Es ist üblich, wie auch bei indirekten Beweisen und Widerspruchsbeweisen, einen Induktionsbeweis am Beweisanfang durch einen entsprechenden Vermerk anzugeben. Weiterhin ist es üblich, im Beweis durch Induktion zu erwähnen, wo man mit dem Induktionsbeginn und dem Induktionsschluss startet und wo genau man im letztgenannten Teil die Induktionshypothese anwendet.

In den folgenden Sätzen demonstrieren wir einige Anwendungen des Beweisprinzips der vollständigen Induktion. Im ersten Beispielbeweis verwenden wir die Teilbarkeitsrelation „|“, wie sie in Abschnitt 1.4 eingeführt wurde.

#### 4.4.4 Satz: Teilbarkeit durch 6

Für alle  $n \in \mathbb{N}$  gilt  $6 | (n^3 + 5n)$ .

**Beweis (durch vollständige Induktion):** Die Aussage  $A(n)$  analog zu Satz 4.4.1 ist hier  $6 | (n^3 + 5n)$ . Um durch vollständige Induktion zu zeigen, dass  $A(n)$  für alle  $n \in \mathbb{N}$  gilt, haben wir zwei Teilebeweise zu führen.

Induktionsbeginn: Es ist  $A(0)$  zu zeigen, also  $6 \mid (0^3 + 5 \cdot 0)$ , also  $6 \mid 0$ . Dies gilt aber, da es ein  $a \in \mathbb{N}$  gibt, nämlich  $a := 0$ , mit  $6a = 0$ .

Induktionsschluss: Es sei  $n \in \mathbb{N}$  so gegeben, dass die Induktionshypothese  $A(n)$  gilt, also die Beziehung  $6 \mid (n^3 + 5n)$ . Wir haben  $A(n+1)$  zu zeigen, also  $6 \mid ((n+1)^3 + 5(n+1))$ . Wegen  $6 \mid (n^3 + 5n)$  gibt es ein  $a \in \mathbb{N}$  mit  $6a = n^3 + 5n$ . Nun rechnen wir wie folgt:

$$\begin{aligned}
(n+1)^3 + 5(n+1) &= (n+1)(n^2 + 2n + 1) + 5(n+1) && \text{Potenz, binomische Formel} \\
&= n^3 + 3n^2 + 3n + 1 + 5n + 5 && \text{durch Ausmultiplikation} \\
&= n^3 + 5n + 3n^2 + 3n + 6 \\
&= 6a + 3n^2 + 3n + 6 && \text{siehe oben} \\
&= 6a + 3n(n+1) + 6 \\
&= 6(a+1) + 3n(n+1)
\end{aligned}$$

Es ist  $n(n+1)$  stets eine gerade Zahl. Also gibt es  $b \in \mathbb{N}$  mit  $n(n+1) = 2b$ . Dies bringt

$$(n+1)^3 + 5(n+1) = 6(a+1) + 6b = 6(a+b+1) = 6c,$$

wenn man  $c \in \mathbb{N}$  durch  $c := a+b+1$  definiert. Folglich gilt auch  $6 \mid ((n+1)^3 + 5(n+1))$  und wir sind fertig.  $\square$

Im nächsten Satz geben wir einen Induktionsbeweis für den Satz von Gauß (Satz 4.1.1) an. Da dieser eine Aussage macht für alle  $n \in \mathbb{N} \setminus \{0\}$ , ist hier Satz 4.4.3 das richtige Mittel zum Beweis.

#### 4.4.5 Satz: Summenformel von C.F. Gauß

Für alle  $n \in \mathbb{N}$  gilt: Aus  $n \geq 1$  folgt  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ .

**Beweis (durch vollständige Induktion):** Die Aussage  $A(n)$  analog zu Satz 4.4.3 ist hier  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$  und das dortige  $n_0$  ist hier 1.

Induktionsbeginn: Es ist  $A(1)$  wahr, da

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

Induktionsschluss: Es sei  $n \in \mathbb{N}$  so gegeben, dass  $n \geq 1$  und die Induktionshypothese  $A(n)$  gelten. Zum Beweis von  $A(n+1)$  starten wir mit der linken Seite dieser Gleichung und bekommen die Gleichheit

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

aufgrund der Definition des Summensymbols im ersten Schritt und der Induktionshypothese  $A(n)$  im zweiten Schritt. Nun starten wir mit der rechten Seite von  $A(n+1)$  und berechnen durch einfache arithmetische Umformungen die Gleichheit

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

Also gilt  $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+1+1)}{2}$ , was  $A(n+1)$  zeigt.  $\square$

Wenn man das Summensymbol in einer offensichtlichen Weise auf die Summation von 0 bis  $n$ , also auf  $\sum_{i=0}^n k_i$ , erweitert, so gilt auch  $\sum_{i=0}^n i = \frac{n(n+1)}{2}$  für alle  $n \in \mathbb{N}$ . Diese Aussage kann man mit dem Prinzip von Satz 4.1.1 beweisen, indem man im letzten Beweis nur den Induktionsbeginn an den Fall  $n = 0$  anpasst.

Bei vielen mathematischen Sätzen wird über mehr als ein Objekt allquantifiziert. Ist nur eines dieser Objekte eine natürliche Zahl, sagen wir  $n$ , und will man vollständige Induktion zum Beweis verwenden, so ist die abstrakte Form der Sätze  $\forall n \in \mathbb{N} : A(n)$ , wobei alle anderen Allquantifizierungen Teil von  $A(n)$  sind. Tauchen hingegen mehrere allquantifizierte natürliche Zahlen in der Formulierung des Satzes auf, so muss man sich bei der Überführung in die abstrakte Form für die richtige Zahl entscheiden. Ist diese  $n$ , so sagt man auch, dass man Induktion nach  $n$  macht. Die Wahl der richtigen Zahl kann entscheidend für das Gelingen des Beweises sein. Ist diese nicht sofort ersichtlich, so müssen gegebenenfalls mehrere Beweisversuche unternommen werden. Wie dann solche Beweise formal geführt werden, zeigen wir im nächsten Beispiel. Dazu sei die **Potenzierung** vorausgesetzt, definiert durch  $a^0 := 1$  und  $a^{n+1} := aa^n$  für alle  $a \in \mathbb{R}$  und  $n \in \mathbb{N}$ . Die Wahl der richtigen Zahl  $m$  im Beweis von Satz 4.4.6 ist durch die Definition der Potenzierung motiviert.

#### 4.4.6 Satz: Potenzierungsregel

Für alle  $a \in \mathbb{R}$  und alle  $m, n \in \mathbb{N}$  gilt  $a^{m+n} = a^m a^n$ .

**Beweis (durch vollständige Induktion):** Wenn wir die Aussage des Satzes als Formel hinschreiben, so erhalten wir:

$$\forall a \in \mathbb{R}, m, n \in \mathbb{N} : a^{m+n} = a^m a^n$$

Diese Formel ist logisch äquivalent zu der nachfolgend angegebenen, da nur die abkürzende Schreibweise des Quantorenblocks teilweise rückgängig gemacht wurde und dann die zwei Allquantoren umsortiert wurden:

$$\forall m \in \mathbb{N} : \forall a \in \mathbb{R}, n \in \mathbb{N} : a^{m+n} = a^m a^n$$

Nun setzen wir  $A(m)$  für die Aussage  $\forall a \in \mathbb{R}, n \in \mathbb{N} : a^{m+n} = a^m a^n$ . Dann hat die letzte Formel die Gestalt  $\forall m \in \mathbb{N} : A(m)$  und dies ist genau das, was wir für einen Induktionsbeweis brauchen. Wir führen, wie man sagt, Induktion nach  $m$ .

Induktionsbeginn: Es ist  $A(0)$  wahr, denn für alle  $a \in \mathbb{R}$  und  $n \in \mathbb{N}$  gilt

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

Induktionsschluss. Es sei  $m \in \mathbb{N}$  so vorausgesetzt, dass  $A(m)$  wahr ist. Zum Beweis von  $A(m+1)$  seien  $a \in \mathbb{R}$  und  $n \in \mathbb{N}$  beliebig vorgegeben. Dann können wir wie folgt rechnen:

$$a^{(m+1)+n} = a^{(m+n)+1} = aa^{m+n} = aa^m a^n = a^{m+1} a^n$$

Dabei benutzen wir die Definition der Potenzierung im zweiten und vierten Schritt und die Induktionshypothese  $A(m)$  im dritten Schritt. Also gilt  $a^{(m+1)+n} = a^{m+1} a^n$  für alle

$a \in \mathbb{R}$  und  $n \in \mathbb{N}$  und dies ist genau die Gültigkeit von  $A(m + 1)$ .  $\square$

Wie schon erwähnt, sind viele mathematische Sätze in der Umgangssprache wie folgt formuliert: „Es sei  $x \in M$ . Dann gilt  $A(x)$ .“ Hier wird der Allquantor unterdrückt. Bisher kam diese Unterdrückung nicht zur Geltung. Bei Induktionsbeweisen muss man in der Formulierung aber oft konkret sein, d.h. die Allquantifizierung explizit hinschreiben, damit der Beweis formal geführt werden kann. Wir demonstrieren dies anhand von Satz 1.3.9. Hier sind die explizit allquantifizierte Formulierung und deren Beweis.

#### 4.4.7 Satz: Kardinalität der Potenzmenge

Für alle Mengen  $M$  gilt: Ist  $M$  endlich, so folgt daraus  $|\mathcal{P}(M)| = 2^{|M|}$ .

**Beweis (durch vollständige Induktion):** Eine Menge  $M$  ist genau dann endlich, wenn es ein  $n \in \mathbb{N}$  gibt mit  $|M| = n$ . Also hat die umgangssprachliche Behauptung des Satzes als prädikatenlogische Formel die folgende Gestalt:

$$\forall M : (\exists n \in \mathbb{N} : |M| = n) \Rightarrow |\mathcal{P}(M)| = 2^{|M|}$$

Da  $n$  in  $|\mathcal{P}(M)| = 2^{|M|}$  nicht vorkommt, gilt diese Formel nach der Regel (7) von Satz 2.3.7 genau dann, wenn die folgende Formel gilt:

$$\forall M : \forall n \in \mathbb{N} : |M| = n \Rightarrow |\mathcal{P}(M)| = 2^{|M|}$$

Nun stellen wir die Quantoren noch um und erhalten die logisch äquivalente Formel

$$\forall n \in \mathbb{N} : \forall M : |M| = n \Rightarrow |\mathcal{P}(M)| = 2^{|M|},$$

bzw.  $\forall n \in \mathbb{N} : A(n)$ , wenn  $A(n)$  der Formel  $\forall M : |M| = n \Rightarrow |\mathcal{P}(M)| = 2^{|M|}$  entspricht. Zum Beweis, dass  $A(n)$  für alle  $n \in \mathbb{N}$  gilt, verwenden wir nun vollständige Induktion.

Induktionsbeginn, d.h. Beweis von  $A(0)$ . Es sei  $M$  eine Menge mit der Eigenschaft  $|M| = 0$ . Dann gilt  $M = \emptyset$  und die Behauptung folgt aus

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

Induktionsschluss, d.h. Beweis von  $A(n + 1)$  aus  $A(n)$  für alle  $n \in \mathbb{N}$ . Es sei also  $n \in \mathbb{N}$  mit  $A(n)$  gegeben. Zum Beweis von  $A(n + 1)$  sei  $M$  eine beliebige Menge mit  $|M| = n + 1$ . Wegen  $n + 1 \neq 0$  gilt  $M \neq \emptyset$ . Also kann man ein Element  $a \in M$  auswählen. Nach Satz 1.3.3 gilt die Gleichung

$$\begin{aligned} \mathcal{P}(M) &= \mathcal{P}((M \setminus \{a\}) \cup \{a\}) \\ &= \mathcal{P}(M \setminus \{a\}) \cup \{X \cup \{a\} \mid X \in \mathcal{P}(M \setminus \{a\})\} \end{aligned}$$

und damit, nach Satz 1.3.7,

$$\begin{aligned} |\mathcal{P}(M)| &= |\mathcal{P}(M \setminus \{a\}) \cup \{X \cup \{a\} \mid X \in \mathcal{P}(M \setminus \{a\})\}| \\ &= |\mathcal{P}(M \setminus \{a\})| + |\{X \cup \{a\} \mid X \in \mathcal{P}(M \setminus \{a\})\}| \\ &= |\mathcal{P}(M \setminus \{a\})| + |\mathcal{P}(M \setminus \{a\})| \\ &= 2 \cdot |\mathcal{P}(M \setminus \{a\})|, \end{aligned}$$

denn die Mengen  $\mathcal{P}(M \setminus \{a\})$  und  $\{X \cup \{a\} \mid X \in \mathcal{P}(M \setminus \{a\})\}$  sind disjunkt und in der zweiten Menge gibt es genau so viele Elemente wie in  $\mathcal{P}(M \setminus \{a\})$ . Es gilt

$$|M \setminus \{a\}| = |M| - 1 = n + 1 - 1 = n.$$

Wegen der Gültigkeit von  $A(n)$ , wo über alle Mengen der Kardinalität  $n$  eine Aussage gemacht wird, gilt also für die Menge  $M \setminus \{a\}$  der Kardinalität  $n$  die Gleichung

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

Setzen wir das oben ein, so folgt

$$|\mathcal{P}(M)| = 2 \cdot 2^{|M \setminus \{a\}} = 2 \cdot 2^{|M|-1} = 2^{|M|}.$$

Damit ist der Beweis des Induktionsschlusses beendet.  $\square$

Wenn Beweise von der Argumentationsstruktur her komplexer werden, dann ist eine Formulierung in der Umgangssprache oft hinderlich. Die explizite Verwendung von Formeln und insbesondere das Hinschreiben der auftauchenden Quantoren zeigt viel besser auf, was formal beim logischen Argumentieren eigentlich geschieht. Wir glauben, dass dies insbesondere durch das letzte Beispiel eindrucksvoll demonstriert wird.

Bei den Beweisen der Sätze 4.4.1 und 4.4.3 wird als entscheidende Eigenschaft verwendet, dass jedes  $n \in \mathbb{N}$  entweder gleich der Null ist oder von der Form  $m + 1$ , mit  $m \in \mathbb{N}$ , also alle natürlichen Zahlen aus der Null mittels der Nachfolgerbildung erzeugt werden können. Bei den linearen Listen werden in analoger Weise durch die leere Liste und die Linksanfügeoperation „;“ alle Listen erzeugt. Also sollte auch hier ein analoges Induktionsprinzip gelten. Das tut es auch, wie wir durch den nachfolgenden Satz zeigen.

#### 4.4.8 Satz: Listeninduktion

Es sei  $M$  eine Menge und  $A(s)$  eine Aussage, in der die Variable  $s$  für lineare Listen über  $M$  stehe. Sind die beiden Formeln

$$(IB) \quad A(\emptyset) \qquad (IS) \quad \forall a \in M, s \in M^* : A(s) \Rightarrow A(a : s)$$

wahr, so ist auch die Formel  $\forall s \in M^* : A(s)$  wahr.

**Beweis (durch Widerspruch):** Formulieren wir die Aussage des Satzes als

$$(IB) \wedge (IS) \Rightarrow \forall s \in M^* : A(s),$$

so ist die Negation dieser Formel logisch äquivalent zu

$$(IB) \wedge (IS) \wedge \exists s \in M^* : \neg A(s).$$

Angenommen, es gelte diese Formel. Dann gibt es eine lineare Liste  $s \in M^*$  mit  $\neg A(s)$ . Weil (IB) gilt, muss  $s \neq \emptyset$  zutreffen. Nun wählen wir eine lineare Liste  $t \neq \emptyset$  mit  $\neg A(t)$ , welche eine kleinste Länge hat. Also gilt insbesondere  $A(u)$  für alle  $u \in M^*$  mit  $|u| < |t|$ . Aufgrund von  $t \neq \emptyset$  existieren  $a \in M$  und  $u \in M^*$  mit  $t = a : u$ . Für dieses  $u$  haben wir

$|t| = |u| + 1$ , also  $|u| < |t|$ , und folglich gilt  $A(u)$ . Nun zeigt die Gültigkeit von (IS), dass auch  $A(a : u)$  gilt, d.h.  $A(t)$  wahr ist. Dies ist ein Widerspruch zur Gültigkeit von  $\neg A(t)$ .  $\square$

Die Leserin oder der Leser vergleiche diesen Beweis mit dem Beweis von Satz 4.4.1. Wir sind in der vollkommen gleichen Art und Weise vorgegangen. Der kleinste Verbrecher  $t$  ist natürlich nicht eindeutig, da es viele lineare Listen gleicher minimaler Länge geben kann, die die zu zeigende Aussage nicht erfüllen. Deshalb spricht man hier auch von einem **minimalen Verbrecher**. Den Unterschied in den Sprechweisen „kleinst“ und „minimal“ werden wir später in Abschnitt 6.2 bei den Ordnungen und den geordneten Mengen genau klären.

Mit Hilfe von Listeninduktionen kann man nun für die in Abschnitt 3.2 betrachteten Operationen auf Listen viele der fundamentalen Eigenschaften zeigen. Wir behandeln als einziges Beispiel die Konkatenation.

#### 4.4.9 Satz: Eigenschaften der Konkatenation

Für die Konkatenationsoperation „ $\&$ “ auf jeder Menge  $M^*$  von linearen Listen gelten die folgenden drei Eigenschaften:

- (1)  $\forall s \in M^* : s \& () = s$  (Rechtsneutralität der leeren Liste)
- (2)  $\forall t \in M^* : () \& t = t$  (Linksneutralität der leeren Liste)
- (3)  $\forall s, t, u \in M^* : (s \& t) \& u = s \& (t \& u)$  (Assoziativität)

**Beweis (durch Listeninduktion):** Zum Beweis von (1) verwenden wir  $s \& () = s$  als Aussage  $A(s)$  des Prinzips der Listeninduktion.

Induktionsbeginn, d.h. Beweis von  $A(()).$  Es gilt aufgrund der Definition der Konkatenation, dass

$$() \& () = () .$$

Induktionsschluss, d.h. Beweis von  $A(a : s)$  aus  $A(s)$  für alle  $a \in M$  und  $s \in M^*$ . Es seien also  $a \in M$  und  $s \in M^*$  mit  $A(s)$  gegeben. Dann gilt:

$$\begin{aligned} (a : s) \& () &= a : (s \& ()) && \text{Definition Konkatenation} \\ &= a : s && \text{wegen } A(s) \end{aligned}$$

Die Eigenschaft (2) gilt nach der Definition der Konkatenation.

Zum Beweis von (3) durch Listeninduktion verwenden wir

$$\forall t, u \in M^* : (s \& t) \& u = s \& (t \& u)$$

als Aussage  $A(s)$ , denn es ist  $\forall s \in M^* : A(s)$  genau die Behauptung.

Induktionsbeginn, d.h. Beweis von  $A(()).$  Für alle  $t, u \in M^*$  bekommt man die Gleichung

$$() \& t \& u = t \& u = () \& (t \& u)$$

durch zweimaliges Anwenden der Definition der Konkatenation.

Induktionsschluss, d.h. Beweis von  $A(a : s)$  aus  $A(s)$  für alle  $a \in M$  und  $s \in M^*$ . Hier gilt für alle  $t, u \in M^*$  die folgende Gleichung.

$$\begin{aligned}
 ((a : s) \& t) \& u &= (a : (s \& t)) \& u && \text{Definition Konkatenation} \\
 &= a : ((s \& t) \& u) && \text{Definition Konkatenation} \\
 &= a : (s \& (t \& u)) && \text{wegen } A(s) \\
 &= (a : s) \& (t \& u) && \text{Definition Konkatenation}
 \end{aligned}$$

Dies beendet den Beweis von allen drei Eigenschaften.  $\square$

Die knotenmarkierten Binärbaume  $\mathcal{B}(M)$  von Abschnitt 3.3 werden aus dem leeren Baum „ $\diamond$ “ durch die Konstruktionsoperation *baum* erzeugt. Dies führt unmittelbar zu dem folgenden Induktionsprinzip, welches wir kurz Bauminduktion nennen. Wir verzichten auf den Beweis des Satzes und merken nur an, dass diesmal ein minimaler Verbrecher mit kleinster Höhe benutzt wird.

#### 4.4.10 Satz: Bauminduktion

Es sei  $M$  eine Menge und  $A(b)$  eine Aussage, in der die Variable  $b$  für knotenmarkierte Binärbäume über  $M$  stehe. Sind die beiden Formeln

$$(\text{IB}) \quad A(\diamond) \qquad (\text{IS}) \quad \forall a \in M, l, r \in \mathcal{B}(M) : A(l) \wedge A(r) \Rightarrow A(\text{baum}(l, a, r))$$

wahr, so ist auch die Formel  $\forall b \in \mathcal{B}(M) : A(b)$  wahr.  $\square$

Neben der Listeninduktion und der Bauminduktion kann man auch vollständige Induktion verwenden, um zu zeigen, dass alle Elemente von  $M^*$  bzw. von  $\mathcal{B}(M)$  eine gewisse Eigenschaft erfüllen. Im Fall von linearen Listen gilt etwa die folgende logische Äquivalenz; sie verwendet, neben der Regel (7) von Satz 2.3.7, noch die offensichtliche logische Äquivalenz von  $A$  und **wahr**  $\Rightarrow A$  für alle Aussagen  $A$ :

$$\begin{aligned}
 \forall s \in M^* : A(s) &\iff \forall s \in M^* : \mathbf{wahr} \Rightarrow A(s) \\
 &\iff \forall s \in M^* : (\exists n \in \mathbb{N} : n = |s|) \Rightarrow A(s) \\
 &\iff \forall s \in M^* : \forall n \in \mathbb{N} : n = |s| \Rightarrow A(s) \\
 &\iff \forall n \in \mathbb{N} : \forall s \in M^* : n = |s| \Rightarrow A(s)
 \end{aligned}$$

Um  $\forall s \in M^* : A(s)$  zu zeigen, kann man also gleichwertigerweise auch durch vollständige Induktion  $\forall n \in \mathbb{N} : B(n)$  zeigen, mit  $B(n)$  als Formel  $\forall s \in M^* : n = |s| \Rightarrow A(s)$ . Letzteres heißt konkret: Man zeigt zuerst, dass  $A(s)$  für alle Listen der Länge 0 gilt. Dann beweist man für alle  $n \in \mathbb{N}$ , dass, wenn  $A(s)$  für alle Listen  $s$  der Länge  $n$  wahr ist, dies impliziert, dass  $A(s)$  auch für alle Listen  $s$  der Länge  $n + 1$  wahr ist. Man führt, wie man sagt, eine **Induktion über die Listenlänge**. Im Fall von knotenmarkierten Binärbäumen kann man in analoger Weise die Gültigkeit von  $\forall b \in \mathcal{B}(M) : A(b)$  durch eine **Induktion über die Baumhöhe** beweisen. Die letztgenannten Vorgehensweisen kann man auch für Listen einer bestimmten Mindestlänge und Bäume einer bestimmten Mindesthöhe verwenden. Dem liegt im Fall von Listen etwa die logische Äquivalenz

$$\forall s \in M^* : |s| \geq n_0 \Rightarrow A(s) \iff \forall n \in \mathbb{N} : n \geq n_0 \Rightarrow \forall s \in M^* : n = |s| \Rightarrow A(s)$$

zugrunde, welche man durch eine leichte Abänderung der obigen logischen Umformungen bekommt.

Die bisher bewiesenen Induktionsprinzipien können auch auf induktiv definierte Mengen wie folgt verallgemeinert werden. Es sei  $M$  induktiv definiert mittels der Basismenge  $B$  und der Menge  $K$  der Konstruktorfunktionen. Weiterhin sei  $A(x)$  eine Aussage, in der die Variable  $x$  für Elemente aus  $M$  stehe. Gilt  $A(b)$  für alle  $b \in B$  und gilt die Implikation

$$\forall x_1, \dots, x_{s(f)} \in M : A(x_1) \wedge \dots \wedge A(x_{s(f)}) \Rightarrow A(f(x_1, \dots, x_{s(f)}))$$

für alle  $f \in K$ , wobei  $s(f)$  die Stelligkeit von  $f$  bezeichnet, so gilt  $A(m)$  für alle  $m \in M$ . In Worten besagt dies: Gilt eine Eigenschaft für alle Basiselemente und bleibt sie beim Aufbau der Elemente mittels der Konstruktorfunktionen gültig, so gilt sie für alle Elemente der induktiv definierten Menge. Man vergleiche dies noch einmal mit den Ausführungen in Abschnitt 3.4 zur induktiven Erzeugung der Mengen  $\mathbb{N}$ ,  $M^*$  und  $\mathcal{B}(M)$  und den oben bewiesenen Induktionsprinzipien. Auch mache man sich beispielsweise klar, wie man durch solch ein allgemeines Induktionsprinzip zeigen kann, dass eine Eigenschaft für alle aussagenlogischen Formeln gilt.

## 4.5 Einige Hinweise zum Finden von Beweisen

Alle bisher im vorliegenden Text gebrachten Sätze stellen irgendwie gewonnene mathematische Einsichten dar. Erst durch einen nachfolgend gegebenen Beweis wird aus einer Einsicht ein allgemeingültiger mathematischer Satz. Wie findet man nun aber einen Beweis zu einer gewonnenen Einsicht? Der deutsche Mathematiker David Hilbert (1862-1943) meinte dazu: „Da ist das Problem, suche die Lösung dazu. Du kannst sie durch reines Denken finden.“ Was so einfach klingt, ist in der Praxis oft ungeheuer schwierig. Und in der Tat gibt es eine Vielzahl von mathematischen Einsichten, deren Beweise erst Jahrhunderte später erbracht wurden bzw. immer noch nicht erbracht sind. Die **Goldbachsche Vermutung** gehört zur letzten Klasse. Sie besagt in der Originalversion, dass jede ungerade natürliche Zahl größer als 5 die Summe von drei Primzahlen ist, und wurde vom deutschen Mathematiker Christian Goldbach (1690-1764) im Jahr 1742 in einem Brief an den schweizer Mathematiker Leonhard Euler (1707-1783) formuliert. Heutzutage ist man an der folgenden stärkeren Variante interessiert, genannt **binäre Goldbachsche Vermutung**: Jede gerade natürliche Zahl größer als 2 ist die Summe von zwei Primzahlen.

Die Schwierigkeit, einen mathematischen Beweis zu finden, hängt oft eng mit der Aufgabenstellung zusammen und der Komplexität der verwendeten Begriffe. Anfänger in der Mathematik haben häufig schon bei relativ einfachen Aufgabenstellungen und elementaren Begriffen große Schwierigkeiten, einen Beweis zu finden und diesen dann so aufzuschreiben, dass der entstehende Text als logische Rechtfertigung der Richtigkeit einer Aussage, also als ein mathematischer Beweis, akzeptiert wird. Was in so einem Fall hilfreich sein kann, ist die Einhaltung gewisser Schemata und die Anwendung gewisser Vorgehensweisen. Nachfolgend werden einige von ihnen angegeben und mittels Beispielen demonstriert. In diesem Zusammenhang ist aber unbedingt zu betonen, dass es sich nur um eine kleine Auswahl von sehr allgemeinen Hilfestellungen handelt und dass es auch nicht sinnvoll ist, ihnen immer blind zu folgen. Allgemein sollte man, wie der ungarische Mathematiker George Polya (1887-1985) fordert, erst die Idee eines Beweises erschließen, bevor man die

Details ausformuliert. Polya spricht hier das an, was man oft die Aufteilung eines Beweises in die **Findungsphase** und **Formulierungsphase** nennt. Wir konzentrieren uns in diesem Abschnitt also auf die Findungsphase. Wie man Beweise als Texte formuliert, sollte der Leserin oder dem Leser mittlerweile einigermaßen klar geworden sein.

Nachfolgend geben wir eine erste allgemeine Vorgehensweise an, die helfen kann, einen Beweis zu finden. Diese kann natürlich, wie auch die, welche noch folgen werden, mit allen in den vorangegangenen Abschnitten besprochenen Beweisprinzipien kombiniert werden. Bei umfangreicheren Beweisen ist es oft so, dass sogar mehrere Beweisprinzipien und Vorgehensweisen kombiniert werden müssen, um erfolgreich zu sein. Weiterhin kommen hier in der Regel auch Techniken zum Einsatz, die typisch sind für den speziellen Zweig der Mathematik, aus dem das zu lösende Problem stammt, oder die Begriffe, mit denen man es in seinem Zusammenhang zu tun hat. Die Leserin oder der Leser vergleiche hierzu später mit den Beweisen aus den noch kommenden Kapiteln.

#### 4.5.1 Von beiden Seiten her rechnen

Im Rahmen von Beweisen tauchen oft gewisse Rechnungen auf, die in Form von Ketten geführt werden. Dies ist insbesondere bei Beweisen von Gleichungen und Ungleichungen und bei Umformungen aussagenlogischer und prädikatenlogischer Formeln der Fall. Ein Fehler, der dabei oft gemacht wird, ist, stur von einer Seite zur anderen Seite zu rechnen. Dabei kann es nämlich vorkommen, dass man an einer Stelle stecken bleibt, weil etwa eine nicht offensichtliche Umformung auszuführen ist. Startet man hingegen in einer Nebenrechnung die Rechnung auch von der anderen Seite, so bekommt man die nicht offensichtliche Umformung oft als simplen Vereinfachungsschritt geschenkt.  $\square$

Wir haben dieses Vorgehen explizit beispielsweise schon beim Beweis von Satz 4.4.5 demonstriert. Implizit wurde es oft verwendet, um die Beweise dieses Texts zu finden, insbesondere die des zweiten Kapitels. Nachfolgend behandeln wir nochmals ein Beispiel aus der Aussagenlogik.

#### 4.5.2 Beispiel: Aussagenlogik

Es sei die Aufgabe gestellt, zu zeigen, dass die beiden folgenden Formeln der Aussagenlogik logisch äquivalent sind (man nennt dies die **Selbstdistributivität** der Implikation):

$$A_1 \Rightarrow (A_2 \Rightarrow A_3) \quad (A_1 \Rightarrow A_2) \Rightarrow (A_1 \Rightarrow A_3)$$

Zur Lösung starten wir mit der linken Formel und transformieren sie wie folgt, indem wir alle Implikationen durch Negationen und Disjunktionen ausdrücken:

$$A_1 \Rightarrow (A_2 \Rightarrow A_3) \iff \neg A_1 \vee \neg A_2 \vee A_3$$

Irgendwie muss nun  $A_1$  nochmals eingeführt werden, damit man die rechte der obigen Formeln erreichen kann. An dieser Stelle ist aber nicht klar, wie man dies zu tun hat. Es bietet sich deshalb an, die obigen Umformungen auch mit der rechten Ausgangsformel zu machen. Dies bringt:

$$(A_1 \Rightarrow A_2) \Rightarrow (A_1 \Rightarrow A_3) \iff \neg(\neg A_1 \vee A_2) \vee \neg A_1 \vee A_3$$

Wenn wir nun auf der rechten Seite dieser Äquivalenz eines der Gesetze von de Morgan anwenden, so wird eine Konjunktion eingeführt. Diese muss aber wieder beseitigt werden, damit wir, wie beabsichtigt, auf der rechten Seite der ersten Äquivalenz ankommen. Wie dies geht, wird nun gezeigt:

$$\begin{aligned}
 \neg(\neg A_1 \vee A_2) \vee \neg A_1 \vee A_3 &\iff (\neg\neg A_1 \wedge \neg A_2) \vee \neg A_1 \vee A_3 \\
 &\iff (A_1 \wedge \neg A_2) \vee \neg A_1 \vee A_3 \\
 &\iff ((A_1 \vee \neg A_1) \wedge (\neg A_2 \vee \neg A_1)) \vee A_3 \\
 &\iff (\text{wahr} \wedge (\neg A_2 \vee \neg A_1)) \vee A_3 \\
 &\iff (\neg A_2 \vee \neg A_1) \vee A_3
 \end{aligned}$$

Wenn wir nun die überflüssige Klammerung weglassen und die Kommutativität der Disjunktion verwenden, so erhalten wir aus der letzten Formel dieser Kette von Äquivalenzumformungen genau die rechte Seite der ersten logischen Äquivalenz des Beispiels. Damit sind wir fertig und können sofort alles auch in eine einzige Rechnung zusammenfassen. Die Umformung, welche es erlaubt weiterzurechnen, wird uns durch die Rechnung mit der rechten Ausgangsformel als Start geschenkt.  $\square$

Man kann die Selbstdistributivität natürlich auch anders beweisen. Wir wissen aufgrund der Definition der logischen Äquivalenz, dass die beiden Formeln  $A_1 \Rightarrow (A_2 \Rightarrow A_3)$  und  $(A_1 \Rightarrow A_2) \Rightarrow (A_1 \Rightarrow A_3)$  genau dann logisch äquivalent sind, wenn sie für alle Belegungen ihrer atomaren Aussagen durch jeweils gleiche Wahrheitswerte den gleichen Wert besitzen. Also genügt es, eine beliebige Belegung anzunehmen, die explizit gar nicht Verwendung findet, da auch die atomaren Aussagen nicht explizit genannt sind, und durch eine Wahrheitstabelle alle 8 möglichen Kombinationen der Werte von  $A_1$ ,  $A_2$  und  $A_3$  systematisch zu überprüfen. Hier ist die entsprechende Tabelle.

| $A_1$ | $A_2$ | $A_3$ | $A_1 \Rightarrow (A_2 \Rightarrow A_3)$ | $(A_1 \Rightarrow A_2) \Rightarrow (A_1 \Rightarrow A_3)$ |
|-------|-------|-------|---|---|
| F     | F     | F     | W                                       | W   |
| F     | F     | W     | W                                       | W   |
| F     | W     | F     | W                                       | W   |
| F     | W     | W     | W                                       | W   |
| W     | F     | F     | W                                       | W   |
| W     | F     | W     | W                                       | W   |
| W     | W     | F     | F                                       | F   |
| W     | W     | W     | W                                       | W   |

Damit hat man auch die Behauptung gezeigt. Für viele Anfänger ist solch ein Beweis sicherlich einfacher als der oben angegebene, da er nur das Nachsehen in der Wahrheitstabelle der Implikation erfordert und nicht das logisch korrekte Umformen. Das Folgende kann man sich daher als eine weitere allgemeine Vorgehensweise merken, auch wenn sie nicht immer zu den elegantesten Beweisen führt.

#### 4.5.3 Einfache Lösungen bevorzugen

Hat man bei mehreren Ansätzen zu einem Beweis einen zur Verfügung, der aus einer systematischen und algorithmisch einfach durchführbaren Überprüfung einer nicht zu großen Anzahl von Fällen besteht, so nehme man diesen.  $\square$

Wenn ein mathematischer Beweis in einem Buch oder einer anderen Publikation (Zeitschrift, Tagungsband, Technischer Bericht etc.) präsentiert wird, so werden hierbei in ihm oft zuerst eine Reihe von Hilfsaussagen bewiesen, aus denen sich letztendlich der gesamte Beweis ergibt. Diese Art der Aufschreibung dient dazu, das Verstehen der Argumentationen zu erleichtern. Gefunden werden Beweise in der Mathematik in der Regel aber anders, insbesondere dann, wenn man eine Aussage als wahr vermutet, aber noch nicht genau weiß, was die dazu erforderlichen Voraussetzungen sind. Man startet in so einer Situation sehr oft mit der zu beweisenden Aussage und reduziert diese dann schrittweise solange auf einfache Aussagen, bis man letztendlich bei Aussagen landet, die trivialerweise wahr sind, schon woanders als wahr bewiesen wurden oder sinnvolle Voraussetzungen darstellen. Eine Reduktion einer Aussage  $A$  auf Aussagen  $A_1$  bis  $A_n$  bedeutet dabei, dass die Implikation  $A_1 \wedge \dots \wedge A_n \Rightarrow A$  als wahr bewiesen wird oder als zutreffend bekannt ist. Man nennt bei einer Implikation die linke Seite stärker als die rechte Seite. Gilt die umgekehrte Implikation nicht, so heißt sie sogar echt stärker. Falsche Aussagen sind die stärksten Aussagen, denn man kann aus ihnen alles folgern. Damit ist das folgende allgemeine Vorgehen beim Beweisen oft sinnvoll.

#### 4.5.4 Reduzierend vorgehen und dabei so wenig wie möglich verstärken

Sind die Voraussetzungen einer Behauptung unklar, so ist das reduzierende Vorgehen oft sehr hilfreich. Beim Finden von mathematischen Beweisen durch Reduktionen sollte man weiterhin versuchen, so viel wie möglich mit Reduktionen auf logisch äquivalente Aussagen zu arbeiten. Eine Reduktion auf eine logisch echt stärkere Aussage birgt nämlich immer die Gefahr, dass jene falsch ist oder ihre Konjunktion mit den (vermuteten) Voraussetzungen des Satzes zu einer falschen Aussage führt. Da aus einer falschen Aussage nach Definition der Implikation alles folgt, ist so ein Reduktionsschritt wertlos und hilft beim Beweis nicht weiter.  $\square$

Nachfolgend geben wir zwei Beispiele für eine reduzierende Vorgehensweise beim Beweisen an, wobei in den Reduktionsschritten nur verstärkt wird, wenn es sinnvoll ist. Dabei vermeiden wir die Umgangssprache so weit wie möglich, damit die verwendeten logischen Schlussweisen klar ersichtlich werden. Wir starten mit zwei Eigenschaften der Potenzmenge im Hinblick auf beliebige Vereinigungen und Durchschnitte.

#### 4.5.5 Beispiel: Potenzmenge

Wir wollen nachfolgend zeigen, dass  $\bigcup \mathcal{P}(M) = M$  und  $\bigcap \mathcal{P}(M) = \emptyset$  für alle Mengen  $M$  gelten. Dazu starten wir mit  $\bigcup \mathcal{P}(M) = M$  und verwenden zuerst zum Beweis dieser Gleichung die Definition der Mengengleichheit und erhalten

$$\bigcup \mathcal{P}(M) = M \iff \bigcup \mathcal{P}(M) \subseteq M \wedge M \subseteq \mathcal{P}(M).$$

Wir haben also die Aufgabe auf die Beweise von  $\bigcup \mathcal{P}(M) \subseteq M$  und von  $M \subseteq \bigcup \mathcal{P}(M)$  reduziert, und weil die obige Umformung eine logische Äquivalenz ist, haben wir eine echte Verstärkung vermieden.

Die Gültigkeit von  $\bigcup \mathcal{P}(M) \subseteq M$  beweisen wir durch die nachfolgende Rechnung. In ihr ist nur der drittletzte Schritt ein echt verstärkender; die Verwendung des linksgerichteten Pfeils für die logische Implikation ergibt sich hier in einer natürlichen Weise

aus der Aufschreibung von oben nach unten. Die dem Schritt entsprechende Eigenschaft  $A(a) \Rightarrow (\exists x : A(x))$  des Existenzquantors haben wir schon in Abschnitt 2.1 kennengelernt.

$$\begin{aligned}\cup\mathcal{P}(M) \subseteq M &\iff \forall a : a \in \cup\mathcal{P}(M) \Rightarrow a \in M \\ &\iff \forall a : (\exists X : X \in \mathcal{P}(M) \wedge a \in X) \Rightarrow a \in M \\ &\iff \forall a : M \in \mathcal{P}(M) \wedge a \in M \Rightarrow a \in M \\ &\iff \forall a : \text{wahr} \\ &\iff \text{wahr}\end{aligned}$$

Die verbleibende Inklusion  $M \subseteq \cup\mathcal{P}(M)$  folgt unmittelbar aus Satz 1.2.6, der Einschließungseigenschaft, indem man  $\mathcal{P}(M)$  als Menge  $\mathcal{M}$  des Satzes verwendet, sowie die Eigenschaft  $M \in \mathcal{P}(M)$ . Damit ist der gesamte Beweis von  $\cup\mathcal{P}(M) = M$  erbracht. Auf eine sehr ähnliche Art zeigt man durch die Rechnung

$$\begin{aligned}\cap\mathcal{P}(M) = \emptyset &\iff \neg\exists a : a \in \cap\mathcal{P}(M) \\ &\iff \forall a : \neg(\forall X : X \in \mathcal{P}(M) \Rightarrow a \in X) \\ &\iff \forall a : \exists X : X \in \mathcal{P}(M) \wedge a \notin X \\ &\iff \forall a : \emptyset \in \mathcal{P}(M) \wedge a \notin \emptyset \\ &\iff \forall a : \text{wahr} \\ &\iff \text{wahr}\end{aligned}$$

die verbleibende Gleichung  $\cap\mathcal{P}(M) = \emptyset$ , wobei wiederum nur der drittletzte Schritt echt verstärkend ist.  $\square$

Wir haben schon den arithmetischen Mittelwert behandelt. Daneben gibt es etwa noch den geometrischen Mittelwert. Als ein zweites Beispiel für die Anwendung der reduzierenden Vorgehensweise wollen wir nun zeigen, dass für alle nichtnegativen reellen Zahlen ihr geometrischer Mittelwert immer kleiner oder gleich dem arithmetischen Mittelwert ist. Dabei beschränken wir uns der Einfachheit halber auf zwei Zahlen.

#### 4.5.6 Beispiel: Mittelwerte

Es sei für alle nichtnegativen reellen Zahlen  $a$  und  $b$  zu zeigen, dass  $\sqrt{ab} \leq \frac{a+b}{2}$  gilt. Der Beweis dieser Ungleichung wird durch die nachfolgende Rechnung erbracht, in der kein echt verstärkender Reduktions schritt verwendet wird; die verwendeten elementaren Eigenschaften sollten alle von der weiterbildenden Schule her bekannt sein.

$$\begin{aligned}\sqrt{ab} \leq \frac{a+b}{2} &\iff (\sqrt{ab})^2 \leq \left(\frac{a+b}{2}\right)^2 \\ &\iff ab \leq \frac{a^2+2ab+b^2}{4} \\ &\iff 4ab \leq a^2 + 2ab + b^2 \\ &\iff 0 \leq a^2 - 2ab + b^2 \\ &\iff 0 \leq (a - b)^2\end{aligned}$$

Da Quadratzahlen immer größer oder gleich der Null sind, ist die letzte Aussage dieser Rechnung wahr. Also gilt auch ihre erste Aussage und dies ist genau die zu zeigende Ungleichung.  $\square$

Wie wir im Laufe dieses Texts schon oft gesehen haben, werden in vielen konkreten mathematischen Beweissituationen Definitionen oder schon bewiesene Eigenschaften (Sätze,

Lemmata und so fort) angewendet. Auch in Beispiel 4.5.5 gingen wir etwa so vor. Hier haben wir die Inklusion  $M \subseteq \bigcup \mathcal{P}(M)$  durch eine Anwendung von Satz 1.2.6 bewiesen. Dabei entspricht die Menge  $\mathcal{M}$  des Satzes der Menge  $\mathcal{P}(M)$  der konkreten Anwendung und die Menge  $M$  des Satzes der Menge  $M$  der konkreten Anwendung. Solche Kollisionen von Bezeichnungen beim Anwenden von Definitionen und schon bewiesenen Eigenschaften sind oft eine Quelle von Fehlern. Deshalb sollte man den folgenden Ratschlag beim mathematischen Beweisen beherzigen:

#### 4.5.7 Bezeichnungskollisionen auflösen

Die Einführung von Bezeichnungen (Variablen, Symbolen und so fort) ist ein wesentliches Hilfsmittel der Mathematik beim Niederschreiben von Sachverhalten. Wird dann im Rahmen eines mathematischen Beweises eine Definition oder eine schon bewiesene Tatsache verwendet, so muss man eine Beziehung herstellen zwischen den Bezeichnungen der Definition und des Satzes (oder Lemmas usw.) und den Bezeichnungen der konkreten Anwendung von diesen. Treten hier gleiche Bezeichnungen auf, so ist es sinnvoll, zuerst die der Definition oder des Satzes konsistent so umzubenennen, dass alle insgesamt betrachteten Bezeichnungen verschieden sind. In komplizierteren Situationen kann es sogar sinnvoll sein, die Entsprechungen der so entstehenden Bezeichnungen in Form einer Zuordnungstabelle zu formulieren, um schematisch vorgehen zu können.  $\square$

Schon bewiesene Eigenschaften können natürlich insbesondere auch Regeln sein, die als Gleichungen, Äquivalenzen oder Implikationen formuliert sind. Bei einem komplizierteren Ausdruck wie  $2(xy)^{n+2} \left( \frac{3}{x^2y^2} + \frac{1}{(xy)^{n+1}} \right) + 2x$  ist es dann sicher sinnvoll, sich bei der Anwendung des Distributivgesetzes  $x(y+z) = xy + xz$  klar zu machen, welcher Teilausdruck welcher Variablen des Gesetzes entspricht. Im nachfolgenden Beispiel greifen wir eine der beiden Gleichungen von Beispiel 4.5.5 noch einmal auf. Dabei erklären wir auch einmal sehr genau, was bei der Anwendung eines Satzes im Rahmen eines Beweises eigentlich vonstatten geht.

#### 4.5.8 Beispiel: nochmals Potenzmenge

Es sei  $M$  eine beliebige Menge. Wir wollen noch einmal die Eigenschaft  $\bigcap \mathcal{P}(M) = \emptyset$  zeigen, nun aber auf eine andere Weise. Statt der Einschließungseigenschaft verwenden wir nachfolgend Satz 1.2.7. Da in diesem Satz ebenfalls die Bezeichnung  $M$  vorkommt, formulieren wir ihn zuerst einmal wie folgt um:

Es sei  $\mathcal{M}$  eine Menge von Mengen. Dann gelten, falls  $\mathcal{M} \neq \emptyset$  zutrifft, für alle Mengen  $N \in \mathcal{M}$  die folgenden Gleichungen:

- (1)  $\bigcup \mathcal{M} = N \cup \bigcup (\mathcal{M} \setminus \{N\})$
- (2)  $\bigcap \mathcal{M} = N \cap \bigcap (\mathcal{M} \setminus \{N\})$

Weiterhin gilt im Fall der leeren Menge von Mengen die Eigenschaft  $\bigcup \emptyset = \emptyset$ .

Es wurde also im Vergleich zum Original nur der Buchstabe  $M$  in  $N$  umbenannt. Um die beabsichtigte Gleichung  $\bigcap \mathcal{P}(M) = \emptyset$  zu zeigen, wählen wir für die nun insgesamt vorkommenden „interessanten“ vier Objekte (das  $M$  ist irrelevant) die folgenden Entsprechungen:

$$\mathcal{M} \triangleq \mathcal{P}(M) \quad N \triangleq \emptyset$$

Durch diese Zuordnung werden auch die Bedingungen des umformulierten Satzes und der konkreten Anwendung einander wie folgt zugeordnet:

$$\mathcal{M} \neq \emptyset \stackrel{\wedge}{=} \mathcal{P}(M) \neq \emptyset \quad N \in \mathcal{M} \stackrel{\wedge}{=} \emptyset \in \mathcal{P}(M)$$

Offensichtlich sind die beiden Aussagen  $\mathcal{P}(M) \neq \emptyset$  und  $\emptyset \in \mathcal{P}(M)$  wahr und aus der Gleichung (2) des umformulierten Satzes folgt somit durch die entsprechende Ersetzung von  $\mathcal{M}$  durch  $\mathcal{P}(M)$  und von  $N$  durch  $\emptyset$  die Gleichung

$$\bigcap \mathcal{P}(M) = \emptyset \cap \bigcap (\mathcal{M} \setminus \{\emptyset\}).$$

Nun können wir noch die Eigenschaft  $\emptyset \subseteq \bigcap (\mathcal{M} \setminus \{\emptyset\})$  und die Äquivalenz der Formeln (1) und (2) von Satz 1.2.3 verwenden. Die Leserin oder der Leser mache sich hier zur Übung ebenfalls die Entsprechungen der Bezeichnungen klar. Wir erhalten dann  $\emptyset \cap \bigcap (\mathcal{M} \setminus \{\emptyset\}) = \emptyset$ , was es erlaubt, die obige Rechnung zur Gleichungskette

$$\bigcap \mathcal{P}(M) = \emptyset \cap \bigcap (\mathcal{M} \setminus \{\emptyset\}) = \emptyset$$

zu vervollständigen. Durch sie ist der Beweis erbracht.  $\square$

Der weitaus größte Teil der mathematischen Sätze hat die Form einer Allaussage. Es wird also ausgesagt, dass alle Objekte, die man in Betracht zieht, eine gewisse Eigenschaft besitzen. Wenn man solch einen Satz als prädikatenlogische Formel hinschreibt, so tauchen in dieser oftmals, neben dem äußersten Allquantor, weitere Quantoren auf. Daraus leitet sich das folgende schematische Vorgehen ab.

#### 4.5.9 Der Quantorenreihenfolge folgen

Diese Vorgehensweise besteht darin, dass man bei einem Beweis genau der Reihenfolge der Quantoren folgt, wie sie sich beim Aufschreiben der Behauptung als Formel ergibt. Beim Beweis einer Allquantifizierung nimmt man dabei ein beliebiges Objekt an und zeigt für dieses die geforderte Eigenschaft; beim Beweis einer Existenzquantifizierung versucht man ein ihre Gültigkeit bezeugendes Objekt aus den gegebenen Objekten des bisherigen Beweistextes zu berechnen bzw. Bedingungen herzuleiten, aus denen man leicht ein bezeugendes Objekt bekommen kann.  $\square$

Wir haben dieses Vorgehen etwa schon im Beweis von Satz 4.2.1 und im Induktionschluss von Satz 4.4.4 verwendet. Nachfolgend geben wir ein weiteres Beispiel an, das im Rahmen der Analysis in das Gebiet „Grenzwerte von Folgen“ fällt. Konkret zeigen wir, dass eine bestimmte Folge eine Nullfolge im Sinne der Beispiele 4.3.6 ist.

#### 4.5.10 Beispiel: Grenzwert einer Folge

Wir betrachten die Folge  $(\frac{1}{n+1})_{n \in \mathbb{N}}$  und behaupten, dass es zu jeder (noch so kleinen) positiven reellen Zahl  $\varepsilon$  ein  $m \in \mathbb{N}$  gibt mit  $\frac{1}{n+1} < \varepsilon$  für alle  $n \in \mathbb{N}$  mit  $n \geq m$ . Als Formel der Prädikatenlogik sieht die Behauptung wie folgt aus:

$$\forall \varepsilon \in \mathbb{R}_{>0} : \exists m \in \mathbb{N} : \forall n \in \mathbb{N} : n \geq m \Rightarrow \frac{1}{n+1} < \varepsilon$$

Bezüglich dieser Formel arbeiten wir nun zum Beweis der Behauptung die Quantifizierungen von links nach rechts ab. Wegen „ $\forall \varepsilon \in \mathbb{R}_{>0}$ “ starten wir wie folgt: Es sei ein beliebiges  $\varepsilon$  aus der Menge  $\mathbb{R}_{>0}$  gegeben. Nun haben wir, bedingt durch den nächsten Quantor „ $\exists m \in \mathbb{N}$ “, eine Zahl  $m$  zu finden, die eine gewisse Eigenschaft erfüllt. Welche, das wird durch die innerste Quantifizierung „ $\forall n \in \mathbb{N}$ “ festgelegt. Weil diese eine Allquantifizierung ist, nehmen wir also  $n \in \mathbb{N}$  beliebig an. Die Aussage, die  $n$  im Fall  $n \geq m$  zu erfüllen hat, verwenden wir nun als Startpunkt der folgenden Herleitung einer Bedingung, aus der man leicht ein  $m$  bekommt:

$$\frac{1}{n+1} < \varepsilon \iff \frac{1}{\varepsilon} < n+1 \iff \frac{1}{\varepsilon} - 1 < n \iff \frac{1}{\varepsilon} \leq n$$

Aufgrund der rechten Formel würde  $m := \frac{1}{\varepsilon}$  das Gewünschte leisten. Leider gibt es hier die Schwierigkeit, dass  $\frac{1}{\varepsilon}$  keine natürliche Zahl sein muss,  $m$  jedoch schon. Aber der Ausdruck und die Bedingung  $\frac{1}{\varepsilon} \leq n$  geben einen Hinweis, wie man  $m$  wählen kann. Jedes  $m$  mit  $\frac{1}{\varepsilon} \leq m$  ist möglich, denn aus  $\frac{1}{\varepsilon} \leq m$  folgt für das angenommene  $n$  aus  $n \geq m$  sofort  $\frac{1}{\varepsilon} \leq n$  und den Rest bewerkstelligt dann die obige logische Implikation. Eine konkrete Wahl von  $m$  ist etwa gegeben durch die Festlegung  $m := \min \{x \in \mathbb{N} \mid \frac{1}{\varepsilon} \leq x\}$ .

Normalerweise werden die eben erbrachten Rechnungen in Form einer Nebenrechnung auf einem Schmierzettel durchgeführt. Im eigentlichen Beweistext gibt man dann nach der Einführung von  $\varepsilon$  das errechnete  $m$  konkret an und zeigt, dass jeweils  $\frac{1}{n+1} < \varepsilon$  für jedes beliebige  $n \in \mathbb{N}$  mit  $n \geq m$  gilt.  $\square$

Die Angabe eines konkreten Objekts  $a$ , welches beim Aufschreiben eines Beweises die Richtigkeit einer Existenzaussage  $\exists x : A(x)$  bezeugen soll, nennt man in der Mathematik oft eine **Setzung**. Auf die Setzung von  $a$  folgt im Beweisablauf normalerweise sofort die Verifikation der Aussage  $A(a)$ , womit insgesamt  $\exists x : A(x)$  bewiesen ist.

In dem obigen Beispiel erstreckt sich der Bereich jeder der durch einen Quantor eingebrachten Variablen  $\varepsilon$ ,  $m$  und  $n$  bis zum Ende der Formel. Es kommt aber auch vor, dass dem nicht so ist, wie beispielsweise in der folgenden Formel, die wir beim indirekten Beweis von Satz 4.2.1 für alle  $m, n \in \mathbb{N}$  bewiesen haben:

$$(\exists x \in \mathbb{N} : m = 2x) \wedge (\exists x \in \mathbb{N} : n = 2x) \implies (\exists x \in \mathbb{N} : m + n = 2x)$$

Hier tauchen drei gleiche Variablenbezeichnungen  $x$  auf. Wo sie gelten, ist durch die Klammerung angegeben, wobei die Klammerung rechts des Implikationspfeils eigentlich überflüssig ist. Aus schon besprochenen Gründen sollte man Kollisionen von Bezeichnungen vermeiden, also auch in Formeln, folglich hier gleichbezeichnete gebundene Variablen entsprechend umbenennen. Statt der obigen Formel bietet sich an, die gleichwertige Version

$$(\exists x \in \mathbb{N} : m = 2x) \wedge (\exists y \in \mathbb{N} : n = 2y) \implies (\exists z \in \mathbb{N} : m + n = 2z)$$

zu verwenden. Dann kann man zum Beweis ein  $x \in \mathbb{N}$  mit  $m = 2x$  und ein  $y \in \mathbb{N}$  mit  $n = 2y$  annehmen und bekommt aus der Rechnung  $m + n = 2x + 2y = 2(x + y)$  ein  $z \in \mathbb{N}$  mit  $m + n = 2z$ , indem man die Setzung  $z := x + y$  verwendet.

Wir besprechen nun eine Vorgehensweise, die auch schon häufig im Laufe des Texts Anwendung fand, beispielsweise im Beweis von Satz 1.2.7.

#### 4.5.11 Sinnvolle Fallunterscheidungen einführen

In der Praxis kommt es vor, dass man den Beweis einer Behauptung nur unter der Verwendung einer zusätzlichen Bedingung  $B$  an die gegebenen Objekte erbringen kann. Hier bietet es sich an, aufgrund von  $B$  eine Fallunterscheidung zu treffen und zu versuchen, auch den Fall, dass  $B$  nicht gilt, unter Verwendung dieser Annahme zu verifizieren. Es sind sogar mehrere Bedingungen  $B_1$  bis  $B_n$  sinnvoll; dann ist aber darauf zu achten, dass ihre Disjunktion  $B_1 \vee \dots \vee B_n$  alle möglichen Fälle abdeckt, also wahr ist. Der Vorteil der Einführung von Fallunterscheidungen ist, dass durch die zusätzlichen Bedingungen der einzelnen Fälle mehr Information zur Beweisführung zur Verfügung steht.  $\square$

Fallunterscheidungen ergeben sich in einer natürlichen Weise, wenn man bei der reduzierenden Vorgehensweise auf eine Disjunktion  $A_1 \vee A_2$  stößt. Da man hier in der Regel nicht weiß, welche der beiden Formeln wahr ist, muss man beide Möglichkeiten in Betracht ziehen. Fallunterscheidungen sind insbesondere auch dann angebracht, wenn man es mit Objekten zu tun hat, die durch Fallunterscheidungen definiert sind. Beispiele hierzu sind etwa der Absolutbetrag einer Zahl und das Maximum bzw. Minimum von zwei Zahlen. Nachfolgend behandeln wir den Absolutbetrag.

#### 4.5.12 Beispiel: Absolutbetrag

Wir wollen zeigen, dass für alle reellen Zahlen  $x$  und  $y$  die folgende Aussage gilt, welche auch als **Dreiecksungleichung** bekannt ist:

$$|x + y| \leq |x| + |y|$$

Da der Absolutbetrag mittels einer Fallunterscheidung definiert ist und  $x$  und  $y$  beliebige reelle Zahlen sind, bietet sich an, nach dem Vorzeichen von  $x + y$  statt derer von  $x$  und von  $y$  zu unterscheiden.

- Gilt  $x + y \geq 0$ , so ist die zu zeigende Eigenschaft äquivalent zu  $x + y \leq |x| + |y|$ , und diese Ungleichung gilt, weil offensichtlich  $x \leq |x|$  und  $y \leq |y|$  wahr sind.
- Gilt  $x + y < 0$ , so ist die zu zeigende Eigenschaft äquivalent zu  $-(x + y) \leq |x| + |y|$ , also zu  $(-x) + (-y) \leq |x| + |y|$ , und diese letzte Ungleichung gilt wiederum, weil offensichtlich auch  $-x \leq |x|$  und  $-y \leq |y|$  zutreffen.

Damit ist die Dreiecksungleichung bewiesen.  $\square$

Insbesondere bei Rekursionen bieten sich Fallunterscheidungen zur Beweisführung an. Als ein Beispiel zeigen wir nachfolgend, wie aus der in Abschnitt 1.5 gegebenen impliziten Definition des ganzzahligen Anteils des dualen Logarithmus die im gleichen Abschnitt auch angegebene Rekursion folgt.

#### 4.5.13 Beispiel: ganzzahliger Anteil des dualen Logarithmus

Wir erinnern an die implizite Definition des ganzzahligen Anteils des dualen Logarithmus als eine Funktion  $glog_2 : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$  mit der Eigenschaft

$$glog_2(x) = y \iff 2^y \leq x < 2^{y+1}$$

für alle  $x \in \mathbb{N} \setminus \{0\}$  und  $y \in \mathbb{N}$ . Zum Beweis der in Abschnitt 1.5 angegebenen rekursiven Darstellung sei  $x \in \mathbb{N} \setminus \{0\}$  beliebig vorausgesetzt. Nach der oben angegebenen Definition gilt für alle  $y \in \mathbb{N}$  die Gleichung  $glog_2(x) = y$  genau dann, wenn  $2^y \leq x < 2^{y+1}$  gilt. Wir unterscheiden zum Beweis der Rekursion der Funktion  $glog_2$  nun die drei in ihr angegebenen Fälle.

- (a) Es gelte  $x = 1$  und  $glog_2(x) = y$ . Dann erhalten wir  $2^y \leq 1 < 2^{y+1}$  und dies bringt  $y = 0$ , also  $glog_2(x) = 0$ .
- (b) Nun gelte  $x \neq 1$  und  $x$  sei gerade. Wiederum sei  $glog_2(x) = y$ . Unter diesen Annahmen bekommen wir  $2^y \leq x < 2^{y+1}$  und eine Division durch 2 bringt  $2^{y-1} \leq \frac{x}{2} < 2^y$ . Man beachte, dass  $y \geq 1$  wegen der Voraussetzungen gilt. Aus  $2^{y-1} \leq \frac{x}{2} < 2^y$  folgt aufgrund der impliziten Definition von  $glog_2$  sofort  $glog_2(\frac{x}{2}) = y - 1$  und die Voraussetzung  $glog_2(x) = y$  zeigt  $glog_2(x) = glog_2(\frac{x}{2}) + 1$ .
- (c) Im verbleibenden Fall gelte wiederum  $x \neq 1$ , aber  $x$  sei nun eine ungerade Zahl. Ist  $glog_2(x) = y$ , so gilt  $2^y \leq x < 2^{y+1}$  und dies impliziert  $2^y \leq x - 1 < 2^{y+1}$ , denn  $2^y$  und  $2^{y+1}$  sind gerade. Eine Division durch 2 bringt hier  $2^{y-1} \leq \frac{x-1}{2} < 2^y$  und, analog zu (b), folgt daraus letztendlich  $glog_2(x) = glog_2(\frac{x-1}{2}) + 1$ .

Wenn wir den Beweis auf die eben gezeigte Art und Weise gefunden haben, so kann man sogar ohne die Hilfsbezeichnung  $y$  auskommen, wie der nachstehende Beweis des zweiten Falls durch reine Äquivalenztransformationen für gerade  $x \in \mathbb{N} \setminus \{0\}$  zeigt:

$$\begin{aligned} glog_2(x) = glog_2(x) &\iff 2^{glog_2(x)} \leq x < 2^{glog_2(x)+1} && \text{Definition von } glog_2 \\ &\iff 2^{glog_2(x)-1} \leq \frac{x}{2} < 2^{glog_2(x)} && \text{Division durch 2} \\ &\iff glog_2(\frac{x}{2}) = glog_2(x) - 1 && \text{Definition von } glog_2 \\ &\iff glog_2(x) = glog_2(\frac{x}{2}) + 1 \end{aligned}$$

Weil die erste Formel dieser Rechnung trivialerweise wahr ist, gilt dies auch für ihre letzte Formel. Ob man den Beweis wie oben oder wie eben gerade demonstriert aufschreibt, ist eine reine Frage des Geschmacks.  $\square$

Zum Schluss dieses Abschnitts behandeln wir noch eine Vorgehensweise, die insbesondere oft bei Induktionsbeweisen anwendbar ist.

#### 4.5.14 Behauptung gegebenenfalls verallgemeinern

Eine häufig auftretende Situation beim Beweis von Aussagen ist, dass der Beweis wesentlich einfacher wird, wenn man die Behauptung verallgemeinert. So eine Verallgemeinerung besteht oft darin, dass eine Konstante (z.B. eine fest vorgegebene Zahl) der Aussage als ein beliebiges Objekt (also eine beliebige Zahl) angenommen wird. Eigentlich möchte man denken, dass allgemeinere Aufgaben immer schwieriger zu lösen sind als speziellere. Aber durch eine Verallgemeinerung ist es oft so, dass zusätzliche Informationen und Eigenschaften benutzbar werden, die im ursprünglichen spezielleren Fall nicht sichtbar sind.  $\square$

Als Anwendung der eben beschriebenen Vorgehensweise betrachten wir zwei rekursiv beschriebene Funktionen  $f$  und  $g$  auf den natürlichen Zahlen und eine Eigenschaft, die zeigt, wie man die Werte der Funktion  $f$  durch spezielle Aufrufe der Funktion  $g$  berechnen kann.

Die Rekursionsstruktur von  $g$  ist von der Art, dass die Abarbeitung mittels einer Schleife im Sinne von Programmiersprachen wie Java oder C erfolgen kann. Sind  $f$  und  $g$  in einer funktionalen Programmiersprache implementiert, beispielsweise in Haskell, so nennt man den Schritt von  $f$  zu  $g$  auch Entrekursivierung oder Übergang zu einer endständigen Rekursion.

#### 4.5.15 Beispiel: Entrekursivierung

Wir betrachten zwei Funktionen  $f : \mathbb{N}^2 \rightarrow \mathbb{N}$  und  $g : \mathbb{N}^3 \rightarrow \mathbb{N}$ , welche für alle  $x, y, n \in \mathbb{N}$  wie folgt rekursiv spezifiziert sind:

$$f(x, n) = \begin{cases} x f(x, n - 1) & \text{falls } n \neq 0 \\ 1 & \text{falls } n = 0 \end{cases} \quad g(x, y, n) = \begin{cases} g(x, yx, n - 1) & \text{falls } n \neq 0 \\ y & \text{falls } n = 0 \end{cases}$$

Es sei nun die Aufgabe gestellt, zu beweisen, dass die Gleichung  $f(x, n) = g(x, 1, n)$  für alle  $x, n \in \mathbb{N}$  gilt. Dazu bietet sich natürlich eine vollständige Induktion nach  $n$  an, da in beiden Fällen  $n$ , wie man sagt, die Rekursion steuert. Als Aussage  $A(n)$ , die wir für alle  $n \in \mathbb{N}$  zeigen wollen, nehmen wir also die folgende Formel:

$$\forall x \in \mathbb{N} : f(x, n) = g(x, 1, n)$$

Der Induktionsbeginn ist einfach. Es gilt  $A(0)$  wegen  $f(x, 0) = 1 = g(x, 1, 0)$  für alle  $x \in \mathbb{N}$ . Zum Beweis des Induktionsschlusses sei ein  $n \in \mathbb{N}$  mit  $A(n)$  vorgegeben. Weiterhin sei  $x \in \mathbb{N}$  als beliebig angenommen. Dann liefern die Rekursion von  $f$  und  $A(n)$  die Gleichung  $f(x, n + 1) = x f(x, n) = x g(x, 1, n)$ . Wenn wir mit der anderen Seite der zu beweisenden Gleichung starten, so bekommen wir  $g(x, 1, n + 1) = g(x, x, n)$  wegen der rekursiven Beschreibung von  $g$ . Hier kommen wir aber offensichtlich nicht weiter.

Um den Beweis zu schaffen, ist es notwendig zu wissen, was die Beziehung von  $f(x, n)$  und  $g(x, y, n)$  für alle natürlichen Zahlen  $y$  und nicht nur für die spezielle Wahl  $y = 1$  ist. In unserem Fall haben wir  $y f(x, n) = g(x, y, n)$  für alle  $x, y, n \in \mathbb{N}$ , woraus wir sofort den oben behaupteten Spezialfall bekommen. Der Beweis der Verallgemeinerung der Originalaussage erfolgt ebenfalls durch eine vollständige Induktion nach  $n$ , nun aber mit

$$\forall x, y \in \mathbb{N} : y f(x, n) = g(x, y, n)$$

als  $A(n)$ . Den Induktionsbeginn  $A(0)$  zeigt man wie folgt. Es seien  $x, y \in \mathbb{N}$  beliebig vorgegeben. Dann gilt  $y f(x, 0) = y = g(x, y, 0)$ . Und auch der Beweis des Induktionsschlusses geht nun glatt vonstatten. Es sei  $n \in \mathbb{N}$  mit der Eigenschaft  $A(n)$  angenommen. Dann gilt für alle  $x, y \in \mathbb{N}$  die Gleichung

$$y f(x, n + 1) = yx f(x, n) = g(x, yx, n) = g(x, y, n + 1)$$

unter Verwendung der Rekursion von  $f$  im ersten Schritt, der Induktionshypothese  $A(n)$  im zweiten Schritt und der Rekursion von  $g$  im dritten Schritt. Insgesamt gilt also  $A(n+1)$ .  $\square$

Das eigentliche Problem bei einer Verallgemeinerung ist, diese zu finden. Hier kann Experimentieren sehr hilfreich sein. Im obigen Beispiel findet man etwa durch termmäßiges Rechnen im Fall von  $f$ , dass

$$f(x, n) = x f(x, n - 1) = x^2 f(x, n - 2) = x^3 f(x, n - 3) = \dots$$

gilt, was die Vermutung  $f(x, n) = x^n f(x, n - n) = x^n$  nahe legt. Bei der Funktion  $g$  bekommt man auf die gleiche Weise das Resultat

$$g(x, y, n) = g(x, yx, n - 1) = g(x, yx^2, n - 2) = g(x, yx^3, n - 3) = \dots$$

und dieses kann man zur Vermutung  $g(x, y, n) = g(x, yx^n, n - n) = yx^n$  verallgemeinern. Nun ist der Bezug zur im Beispiel verwendeten Verallgemeinerung  $g(x, y, n) = yx^n = y f(x, n)$  der originalen Aufgabe klar.

Neben den bisher vorgestellten Vorgehensweisen gibt es noch viele weitere, insbesondere solche, die mit speziellen mathematischen Teilgebieten zu tun haben, etwa der Algebra, der Analysis, der Graphentheorie oder der Ordnungstheorie. In diesen Gebieten wurden spezielle Techniken entwickelt, die oftmals erfolgreich eingesetzt werden können und deren Kenntnisse damit beim Suchen von Beweisen hilfreich sind. Wegen des einführenden Charakters dieses Texts können wir nicht genauer auf solche Techniken eingehen. Einige immer wiederkehrende Argumentationen wird die Leserin oder der Leser vielleicht in den kommenden Kapiteln erkennen.

Schließlich soll noch ein letzter Rat gegeben werden. Zwar ist es in mathematischen Beweisen verboten, auf der Ebene der Anschauung zu argumentieren, also etwa mit Venn-Diagrammen, Pfeil-Diagrammen, baumartigen Darstellungen von logischen Reduktionen und sonstigen Zeichnungen, aber zum Finden von Beweisen ist diese Ebene oft sehr wertvoll. Die Anschauung kann nämlich die entscheidenden Hinweise geben, wie ein Beweis eventuell weitergeführt werden kann, wenn man steckengeblieben ist, oder wie er sogar als Ganzes aufgebaut sein kann. Anschauliche Darstellungen sind auch ein wertvolles Mittel zur Kommunikation. Beim Beweisen geht es ja viel um Kommunikation mit anderen Personen, die man von der Richtigkeit eines Sachverhalts überzeugen will. Dabei helfen in einem geschriebenen mathematischen Text vor oder nach der Darstellung eines formalen Beweises oft motivierende Beispiele, Skizzen und ähnliche Dinge bei der Veranschaulichung und Verdeutlichung dessen, was das formale Vorgehen zeigt. Im Rahmen eines mündlichen Vortrags, beispielsweise einer Vorlesung, kann man die formale und die anschauliche Ebene sogar gewinnbringend verbinden und dies ist der große Vorteil solcher Präsentationen.

## 4.6 Übungsaufgaben

### Aufgabe

Eine Funktion  $f : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$  auf der Potenzmenge einer Menge  $M$  erfülle die folgende Eigenschaft:

$$(a) \quad \forall X, Y \in \mathcal{P}(M) : f(X \cup Y) = f(X) \cup f(Y)$$

Zeigen Sie, dass es eine Menge  $N \in \mathcal{P}(M)$  mit den folgenden zwei Eigenschaften gibt:

- (1)  $f(N) = N$
- (2) Für alle  $X \in \mathcal{P}(M)$  gilt: Aus  $f(X) = X$  folgt  $N \subseteq X$ .

Gilt diese Aussage auch, wenn in (a) die Vereinigung durch den Durchschnitt ersetzt wird (mit Begründung)?

### Aufgabe

Beweisen Sie die folgenden Aussagen jeweils indirekt:

- (1) Für alle  $n \in \mathbb{N}$  gilt: Ist  $n^2$  gerade, dann ist auch  $n$  gerade.
- (2) Für alle  $n \in \mathbb{N}$  gilt: Ist 9 kein Teiler von  $n^2$ , so ist 6 kein Teiler von  $n$ .
- (3) Für alle  $m, n \in \mathbb{Z}$  gilt: Sind  $m + n$  und  $m - n$  teilerfremd, so sind auch  $m$  und  $n$  teilerfremd.
- (4) Ist  $(a_1, \dots, a_k) \in \mathbb{N}^k$  eine nichtleere lineare Liste natürlicher Zahlen und  $\sum_{i=1}^k a_i$  gerade, so ist auch die Listenlänge  $k$  gerade.

### Aufgabe

Für alle  $m, n \in \mathbb{Z}$  gilt: Ist eine der Zahlen  $m, n$  nicht durch 3 teilbar, so ist auch eine der Zahlen  $m+n, m-n$  nicht durch 3 teilbar. Weisen Sie diese Aussage durch einen indirekten Beweis nach.

### Aufgabe

Zeigen Sie die folgenden Aussagen jeweils durch einen Widerspruchsbeweis.

- (1) Für alle  $n \in \mathbb{N}$  mit  $n > 1$  gilt  $n^2 < n^3$ :
- (2) Für alle  $n \in \mathbb{N}$  gilt: Ist  $n$  gerade und gilt  $\sqrt{n} \in \mathbb{N}$ , so ist  $\sqrt{n}$  gerade.
- (3) Für alle  $m, n \in \mathbb{N}$  gilt  $m^2 \neq 3n + 2$ .

### Aufgabe

Gegeben seien  $a, b, c \in \mathbb{N}$  mit  $a^2 + b^2 = c^2$ . Weiterhin seien  $a, b$  und  $c$  teilerfremd. Dann ist  $c$  ungerade und genau eine der Zahlen  $a, b$  ist gerade. Zeigen Sie diese Eigenschaft, indem Sie die folgenden Aussagen nacheinander durch Widerspruch beweisen.

- (1) Mindestens eine der Zahlen  $a, b, c$  ist ungerade.
- (2) Mindestens eine der Zahlen  $a, b, c$  ist gerade.
- (3) Genau eine der Zahlen  $a, b, c$  ist gerade.
- (4) Die gerade Zahl ist ungleich  $c$ .

### Aufgabe

Für alle  $n \in \mathbb{N}$  und  $a \in \mathbb{R}$  mit  $a \neq 1$  gilt

$$\sum_{i=0}^n a^i = \frac{a^{n+1} - 1}{a - 1}.$$

Beweisen Sie diese sogenannte Summenformel der geometrischen Reihe durch vollständige Induktion.

### Aufgabe

Beweisen Sie die folgenden Behauptungen durch vollständige Induktion, wobei der Induktionsbeginn geeignet festzulegen ist.

- (1) Für alle  $n \in \mathbb{N}$  mit  $n \geq 1$  ist  $3^n - 3$  durch 6 teilbar.
- (2) Für alle  $n, x \in \mathbb{N}$  mit  $n \geq 2$  und  $x \geq 1$  gilt  $1 + nx < (1 + x)^n$ .

### Aufgabe

Zeigen Sie durch vollständige Induktion, dass für alle  $a, b, n \in \mathbb{N}$  mit  $n \geq 1$  die Ungleichung

$$(a) \quad a^n + b^n \leq (a + b)^n$$

gilt. Bleibt (a) auch wahr, wenn  $a$  und  $b$  reelle Zahlen sein dürfen (mit Begründung)?

### Aufgabe

Die Funktion  $\text{rev} : M^* \rightarrow M^*$  zum Revertieren von linearen Listen über einer Menge  $M$  kann induktiv wie folgt beschrieben werden:

$$\text{rev}(()) = () \quad \text{rev}(a : s) = \text{rev}(s) \& (a)$$

Beweisen Sie durch Listeninduktion, dass für alle  $s \in M^*$  die folgenden Gleichungen gelten:

$$(a) \quad \text{rev}(\text{rev}(s)) = s \quad (b) \quad |\text{rev}(s)| = |s|$$

Hinweis: Zum Beweis von (a) benötigen Sie, neben der Assoziativität der Operation  $\&$  und den Gesetzen  $(a) = a : ()$  und  $s \& () = s$  für alle  $a \in M$  und  $s \in M^*$ , noch eine Hilfsaussage, die ebenfalls durch Listeninduktion bewiesen werden kann.

### Aufgabe

Beweisen Sie durch Listeninduktion, dass für alle linearen Listen  $s, t \in M^*$  die folgende Gleichung gilt:

$$|s \& t| = |s| + |t|$$

### Aufgabe

Beweisen Sie die Aussage der letzten Aufgabe auch durch eine Induktion nach der Listenlänge.

### Aufgabe

Die Funktion  $f : \mathcal{B}(M) \rightarrow \mathcal{B}(M)$  erfülle die folgenden Gleichungen für alle  $a \in M$  und  $b_1, b_2 \in \mathcal{B}(M)$ .

$$f(\diamond) = \diamond \quad f(\text{baum}(b_1, a, b_2)) = \text{baum}(f(b_2), a, f(b_1))$$

- (1) Beweisen Sie durch Bauminduktion, dass  $f(f(b)) = b$  für alle  $b \in \mathcal{B}(M)$  gilt.
- (2) Beschreiben Sie umgangssprachlich die Wirkung von  $f$ .

## 5 Spezielle Funktionen

In Abschnitt 1.4 haben wir Funktionen als spezielle Relationen eingeführt und auch einige Sprech- und Schreibweisen festgelegt. Bisher haben wir Funktionen aber nur zu Beispielszwecken verwendet, etwa um Sachverhalte zu beschreiben oder Möglichkeiten zu schaffen, vorgegebene Objekte zu manipulieren. Insbesondere bei den zweiten Anwendungen sprachen wir dann oftmals von Operationen statt von Funktionen, um diesen Charakter zu betonen. Man vergleiche mit den Operationen auf den linearen Listen oder den knotenmarkierten Binärbäumen. In diesem Kapitel studieren wir nun den Funktionsbegriff näher. Zuerst befassen wir uns mit einigen grundlegenden Eigenschaften von Funktionen. Dann vergleichen wir mit Hilfe von speziellen Funktionen die Kardinalitäten beliebiger (also auch nichtendlicher) Mengen. Und schließlich untersuchen wir noch einige Klassen von speziellen konkreten Funktionen, die für die Informatik wichtig sind, wenn man sich etwa mit der Laufzeit von Algorithmen beschäftigt.

### 5.1 Injektivität, Surjektivität und Bijektivität

Wir haben in Abschnitt 1.4 Funktionen  $f : M \rightarrow N$  als eindeutige und totale Relationen  $f \subseteq M \times N$  eingeführt und den Ausdruck  $f(x)$  für dasjenige eindeutig gegebene Element aus  $N$  geschrieben, welches mit dem Element  $x$  aus  $M$  in der Relation  $f$  steht. Über die beiden Mengen  $M$  und  $N$ , die Quelle und das Ziel von  $f$ , haben wir nichts ausgesagt. Insbesondere wurde bisher  $\emptyset$  als Quelle und/oder Ziel nicht ausgeschlossen. Für die leere Menge ergibt sich das folgende erstaunliche Resultat. In ihm wenden wir die für Relationen eingeführte Schreibweise  $x R y$  auch für die leere Relation an, also für die leere Menge von Paaren. Die Beweise zeigen, dass abkürzende Schreibweisen nicht immer hilfreich sind.

#### 5.1.1 Satz: leere Relation als Funktion

- (1) Für alle Mengen  $M$  gilt  $\emptyset \times M = \emptyset$  und auch  $M \times \emptyset = \emptyset$ .
- (2) Die leere Relation  $\emptyset \subseteq \emptyset \times M$  ist für alle Mengen  $M$  eine Funktion und für jede weitere Funktion  $f : \emptyset \rightarrow M$  gilt  $f = \emptyset$ .
- (3) Für alle Mengen  $M$  ist die leere Relation  $\emptyset \subseteq M \times \emptyset$  eindeutig und sie ist dann und nur dann total, wenn  $M = \emptyset$  gilt.

**Beweis:** (1) Nachfolgend ist der Beweis der ersten Gleichung angegeben, wobei wir im zweiten Schritt der Rechnung die zur Definition des direkten Produkts in Abschnitt 1.4 verwendete Zermelo-Mengenkomprehension rückgängig machen, damit Regel (6) von Satz 2.3.7 anwendbar wird.

$$\begin{aligned}\emptyset \times M &= \{(x, y) \mid x \in \emptyset \wedge y \in M\} \\&= \{u \mid \exists x : x \in \emptyset \wedge \exists y : y \in M \wedge u = (x, y)\} \\&= \{u \mid \exists x : \text{falsch}\} \\&= \{u \mid \text{falsch}\} \\&= \emptyset\end{aligned}$$

Auf die gleiche Weise kann man die zweite Gleichung nachrechnen.

(2) Weil alle Allquantifizierungen über die leere Menge wahr sind, ist die leere Relation  $\emptyset \subseteq \emptyset \times M$  nach den folgenden logischen Umformungen eindeutig:

$$\emptyset \text{ eindeutig} \iff \forall x \in \emptyset, y, z \in M : x \emptyset y \wedge x \emptyset z \Rightarrow y = z \iff \mathbf{wahr}$$

Durch einen ähnlichen Beweis mit dem gleichen Argument rechnet man wie folgt nach, dass die leere Relation  $\emptyset \subseteq \emptyset \times M$  auch total ist:

$$\emptyset \text{ total} \iff \forall x \in \emptyset : \exists y \in M : x \emptyset y \iff \mathbf{wahr}$$

Also ist per Definition eine Funktion gegeben. Ist  $f$  eine weitere Funktion von  $\emptyset$  nach  $M$ , so gilt, da Funktionen Relationen sind,  $f \subseteq \emptyset \times M$ , also  $f \subseteq \emptyset$  nach (1). Dies zeigt  $f = \emptyset$ , denn  $\emptyset \subseteq f$  gilt immer.

(3) Die leere Relation  $\emptyset \subseteq M \times \emptyset$  ist aufgrund der folgenden Rechnung eindeutig:

$$\emptyset \text{ eindeutig} \iff \forall x \in M, y, z \in \emptyset : x \emptyset y \wedge x \emptyset z \Rightarrow y = z \iff \mathbf{wahr}$$

Wieder wurde verwendet, dass Allquantifizierungen über die leere Menge wahr sind. Durch die Rechnung

$$\begin{aligned} \emptyset \text{ total} &\iff \forall x \in M : \exists y \in \emptyset : x \emptyset y \\ &\iff \forall x : x \in M \Rightarrow \exists y : y \in \emptyset \wedge x \emptyset y \\ &\iff \forall x : x \in M \Rightarrow \exists y : \mathbf{falsch} \wedge x \emptyset y \\ &\iff \forall x : x \in M \Rightarrow \exists y : \mathbf{falsch} \\ &\iff \forall x : x \in M \Rightarrow \mathbf{falsch} \\ &\iff \forall x : \neg(x \in M) \\ &\iff M = \emptyset \end{aligned}$$

ist schließlich der noch verbleibende Teil bewiesen. Hier wurde Satz 2.3.7 (6) benutzt.  $\square$

Der Beweis dieses Satzes demonstriert noch einmal, wie wichtig es ist, Quantifizierungen mit typisierten Variablen als Abkürzungen aufzufassen, so wie dies in der Festlegung 2.1.2 eingeführt wurde. Wesentlich für den Beweis war nämlich, dass diese Abkürzungen teilweise wieder rückgängig gemacht wurden. Genau genommen haben wir in den obigen Beweisen implizit auch benutzt, dass Quantorenblöcke mehrfachen geschachtelten Quantifizierungen entsprechen und haben auch diese rückgängig gemacht. So haben wir etwa im Beweis von Teil (2) benutzt, dass die Formel

$$\forall x \in \emptyset, y, z \in M : x \emptyset y \wedge x \emptyset z \Rightarrow y = z$$

eine Kurzschreibweise für die Formel

$$\forall x \in \emptyset : \forall y \in M : \forall z \in M : x \emptyset y \wedge x \emptyset z \Rightarrow y = z$$

ist. Erst dadurch konnten wir formal durch das Betrachten der äußersten Quantifizierung „ $\forall x \in \emptyset$ “ das logische Argument verwenden, dass die letzte Formel logisch äquivalent zu **wahr** ist, weil über die leere Menge quantifiziert wird. Normalerweise geht man beim Aufschreiben von Beweisen davon aus, dass die Leserin oder der Leser mit diesen Argumenten

hinreichend vertraut ist, und erwähnt sie und die entsprechenden Beweisschritte deshalb nicht eigens. Der eben bewiesene Satz zeigt auch, dass es bei Relationen und Funktionen nicht reicht, nur die Menge von Paaren anzugeben. Quelle und Ziel sind auch wesentlich. So ist etwa die leere Relation  $\emptyset$  mit Quelle  $\emptyset$  und Ziel  $\mathbb{N}$ , also  $\emptyset : \emptyset \rightarrow \mathbb{N}$ , eine Funktion. Vertauscht man hingegen Quelle und Ziel, betrachtet also  $\emptyset : \mathbb{N} \rightarrow \emptyset$ , so gilt dies nicht mehr.

Die **leere Funktion**  $\emptyset : \emptyset \rightarrow M$  (mit leerer Quelle und beliebigem Ziel) ist oft nützlich. Beispielsweise erlaubt sie, das leere Tupel zu modellieren, wenn wir  $n$ -Tupel als Funktionen  $f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n M_i$  auffassen. Sie ist aber insofern pathologisch, da für sie der Ausdruck  $\emptyset(x)$  nicht definiert ist – es gibt ja kein  $x$  in der Menge  $\emptyset$ . Aus diesem Grund wird in der Literatur, leider oft implizit, die folgende Bedingung unterstellt.

### 5.1.2 Festlegung: nichtleere Quellen

Für alle Funktionen  $f : M \rightarrow N$  wird **implizit**  $M \neq \emptyset$  angenommen. Dies impliziert  $N \neq \emptyset$  aufgrund der Totalitätsforderung und  $f$  ist somit nicht leer.  $\square$

Somit gilt von nun an in diesem Text, **wenn nicht explizit anders vermerkt**: Für alle Funktionen  $f : M \rightarrow N$  sind Quelle und Ziel nicht leer, für jedes Element  $x \in M$  ist der Ausdruck  $f(x)$  definiert und für alle Elemente  $x \in M$  und  $y \in M$  ist  $y = f(x)$  genau dann wahr, wenn die Aussage  $x \neq y$  in der relationalen Schreibweise von  $f$  zutrifft. In der Praxis, wo man mit konkreten Funktionen arbeitet, bedeutet die Festlegung 5.1.2 keinerlei Einschränkung. Sie bereitet aber manchmal in der Theorie Probleme, beispielsweise wenn man Tupel modellieren will. Wir werden auch in Abschnitt 5.2 auf so ein Problem stoßen. Nach diesen Vorbereitungen können wir nun die wesentlichen beiden Begriffe dieses Abschnitts einführen.

### 5.1.3 Definition: Injektivität und Surjektivität

Eine Funktion  $f : M \rightarrow N$  heißt

- (1) **injektiv**, falls für alle  $x, y \in M$  aus  $f(x) = f(y)$  folgt  $x = y$ ,
- (2) **surjektiv**, falls für alle  $y \in N$  ein  $x \in M$  mit  $f(x) = y$  existiert.  $\square$

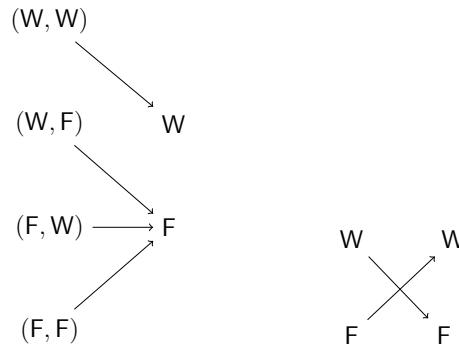
Man beachte im Hinblick auf Eigenschaft (1) dieser Definition, dass aus  $x = y$  immer folgt  $f(x) = f(y)$ . Gleiche Objekte liefern gleiche Werte. Dies gilt in analoger Weise auch für Ausdrücke, bei denen sich der Wert nicht ändert, wenn ein Teilausdruck durch einen Ausdruck mit einem gleichen Wert ersetzt wird, und Aussagen, bei denen sich die Gültigkeit nicht ändert, wenn eine Teilformel durch eine logisch äquivalente Formel ersetzt wird. Dieses fundamentale logische Prinzip wird nach dem deutschen Universalgelehrten Gottfried Wilhelm Leibniz (1646-1716) auch **Leibniz-Gesetz** oder **Identitätsprinzip von Leibniz** genannt.

In Abschnitt 1.4 haben wir aufgezeigt, wie man Relationen zeichnerisch durch Pfeildiagramme darstellen kann. Da Funktionen spezielle Relationen sind, kann man damit auch sie so darstellen. Alle Pfeildiagramme der Beispiele von Abschnitt 1.4 betreffen Relationen auf einer Menge. Die gezeigten Pfeildiagramme enthalten jedes Element dieser Menge

genau einmal. In Verbindung mit Funktionen sind oft sogenannte **bipartite Pfeildiagramme** hilfreicher. Hier zeichnet man zuerst links die Elemente der Quelle und rechts die Elemente des Ziels der vorgegebenen Relation  $R$ ; in der Regel werden die Elemente senkrecht übereinander gestellt. Dann verbindet man ein Element  $x$  der Quelle mit einem Element  $y$  des Ziels durch einen Pfeil von  $x$  nach  $y$  genau dann, wenn die Beziehung  $x R y$  gilt. In so einem Pfeildiagramm erkennt man nun die Eindeutigkeit (Totalität) daran, dass höchstens (mindestens) ein Pfeil in jedem linken Objekt beginnt und die Injektivität (Surjektivität) daran, dass höchstens (mindestens) ein Pfeil in jedem rechten Objekt endet. Nachfolgend geben wir zwei Beispiele an.

### 5.1.4 Beispiele: bipartite Pfeildiagramme

Wir betrachten die Pfeildiagramme zu den beiden Funktionen  $und : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$  und  $nicht : \mathbb{B} \rightarrow \mathbb{B}$ , welche die Konjunktion und die Negation auf den Wahrheitswerten beschreiben:



Aus dem linken Diagramm kann man sofort erkennen, dass die Funktion *und* nicht injektiv ist. Im Element  $F$  des Ziels enden drei Pfeile. Sie ist jedoch surjektiv, da auch im Element  $W$  des Ziels ein Pfeil endet. Das rechte Diagramm zeigt, dass die Funktion *nicht* sowohl injektiv als auch surjektiv ist.  $\square$

Dass Funktionen die Eigenschaften von Definition 5.1.3 nicht besitzen, belegt man im Normalfall durch die Angabe von Gegenbeispielen. Etwa ist  $f : \mathbb{R} \rightarrow \mathbb{R}$  mit der Definition  $f(x) = x^2$  nicht injektiv, da  $f(1) = 1 = f(-1)$ , aber  $1 \neq -1$ . Sie ist auch nicht surjektiv. Wegen  $f(x) \geq 0$  für alle  $x \in \mathbb{R}$  kann es etwa zum Zielement  $y := -1$  kein Quellelement  $x$  mit  $f(x) = y$  geben. Eine große Klasse von injektiven Funktionen auf den reellen Zahlen ist in der nachfolgenden Definition gegeben.

### 5.1.5 Definition: strenge Monotonie

Es seien  $M$  und  $N$  (nichtleere) Mengen von reellen Zahlen. Eine Funktion  $f : M \rightarrow N$  heißt **strenge monoton**, falls für alle  $x, y \in M$  mit  $x < y$  gilt  $f(x) < f(y)$ .  $\square$

Manchmal spricht man deutlicher von streng monoton wachsenden oder streng monoton aufsteigenden Funktionen. Fordert man für die Funktion  $f$  in Definition 5.1.5 nur, dass  $f(x) \leq f(y)$  für alle  $x, y \in M$  mit  $x \leq y$  gilt, so heißt  $f$  **monoton** oder monoton wachsend oder monoton aufsteigend. Statt monoton sagt man auch isoton. Leider ist insgesamt die

Bezeichnungsweise im Zusammenhang mit solchen Funktionen nicht einheitlich. Neben den (strenge) monotonen Funktionen gibt es noch die (strenge) antitonen Funktionen. Diese werden auch (strenge) monoton fallend oder (strenge) monoton absteigend genannt. Aus diesen Bezeichnungen wird klar, was gemeint ist. Etwa ist  $f : M \rightarrow N$  streng antiton, falls für alle  $x, y \in M$  mit  $x < y$  gilt  $f(y) < f(x)$ . Wir betrachten nachfolgend aber nur die streng monotonen Funktionen. Für diese Klasse von Funktionen gilt das folgende Resultat:

### 5.1.6 Satz: strenge Monotonie impliziert Injektivität

Sind  $M$  und  $N$  Teilmengen von  $\mathbb{R}$  und ist  $f : M \rightarrow N$  eine streng monotone Funktion, so ist  $f$  auch injektiv.

**Beweis (indirekt):** Es sei  $f$  nicht injektiv. Dann gibt es  $x, y \in M$  mit  $f(x) = f(y)$  und  $x \neq y$ . Aus  $x \neq y$  folgt  $x < y$  oder  $y < x$ . Nun unterscheiden wir zwei Fälle:

(a) Es sei  $x < y$ . Wegen  $f(x) = f(y)$  ist dann  $f$  nicht streng monoton.

(b) Es sei  $y < x$ . Wegen  $f(y) = f(x)$  ist dann  $f$  wiederum nicht streng monoton.  $\square$

Beispielsweise sind also alle Funktionen  $f : \mathbb{R} \rightarrow \mathbb{R}$  mit der Definition  $f(x) = x^k$ , wobei  $k \in \mathbb{N}$  eine ungerade Zahl ist, injektiv. Ist  $k$  gerade, so ist die Injektivität verletzt. Die Umkehrung von Satz 5.1.6 gilt offensichtlich nicht. Es gibt Funktionen auf den reellen Zahlen, die injektiv sind, aber nicht streng monoton. Man kann die Injektivität und die Surjektivität beliebiger Funktionen anhand der Definition 5.1.3 feststellen. Manchmal ist aber auch die Anwendung der Kriterien des folgenden Satzes sehr hilfreich.

### 5.1.7 Satz: hinreichende Kriterien für Injektivität und Surjektivität

Es sei  $f : M \rightarrow N$  eine Funktion. Dann gelten die folgenden zwei Eigenschaften:

- (1) Gibt es eine Funktion  $g : N \rightarrow M$  mit  $g(f(x)) = x$  für alle  $x \in M$ , so ist  $f$  injektiv.
- (2) Gibt es eine Funktion  $g : N \rightarrow M$  mit  $f(g(y)) = y$  für alle  $y \in N$ , so ist  $f$  surjektiv.

**Beweis:** (1) Existiert eine Funktion  $g : N \rightarrow M$  mit der geforderten Eigenschaft, so gilt für alle  $x, y \in M$  die folgende logische Implikation, welche die Injektivität von  $f$  beweist:

$$f(x) = f(y) \implies g(f(x)) = g(f(y)) \iff x = y$$

(2) Existiert wiederum eine Funktion  $g : N \rightarrow M$  mit der geforderten Eigenschaft, so gilt für alle  $y \in N$ , dass  $f(x) = f(g(y)) = y$ , falls man das Element  $x \in M$  durch  $x := g(y)$  festlegt. Dies zeigt die Surjektivität von  $f$ .  $\square$

Nachfolgend geben wir einige Beispiele für Anwendungen dieses Satzes an.

### 5.1.8 Beispiele: Injektivität und Surjektivität

Es sei  $\mathbb{R}_{\geq 0}$  die Menge der positiven reellen Zahlen. Die Funktion  $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ , mit  $f(x) = x^2 + 2$ , ist injektiv, denn für die Funktion

$$g : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0} \quad g(y) = \begin{cases} \sqrt{y-2} & \text{falls } y \geq 2 \\ 0 & \text{sonst} \end{cases}$$

gilt  $g(f(x)) = x$  für alle  $x \in \mathbb{R}_{\geq 0}$ , da  $x^2 + 2 \geq 2$  in Verbindung mit den Definitionen von  $f$  und  $g$  impliziert, dass

$$g(f(x)) = g(x^2 + 2) = \sqrt{x^2 + 2 - 2} = \sqrt{x^2} = |x| = x.$$

Würde man  $\mathbb{R}$  als Quelle von  $f$  wählen, so wäre die Injektivität verletzt.

Man kann die Funktion  $g$  des Satzes 5.1.7 oft sogar ausrechnen. Dies ist besonders wichtig, wenn die Funktion  $f$  nicht explizit durch eine definierende Gleichung gegeben ist, sondern implizit durch Eigenschaften spezifiziert wird. Hier ist ein Beispiel für solch eine implizite Spezifikation durch eine Formel (in Abschnitt 4.2 haben wir die rechte Konstruktion der Äquivalenz der Formel schon einmal betrachtet):

$$f : \mathbb{N} \rightarrow \mathbb{N} \quad \forall x, y \in \mathbb{N} : f(x) = y \Leftrightarrow y^2 \leq x < (y+1)^2$$

Um zu zeigen, dass  $f$  surjektiv ist, nimmt man eine Funktion  $g : \mathbb{N} \rightarrow \mathbb{N}$  mit der Eigenschaft  $f(g(y)) = y$  für alle  $y \in \mathbb{N}$  an. Dann folgt wie folgt um, wobei sich die abschließende logische Implikation aufgrund des Rechnens von links nach rechts konsequenterweise in der Form „ $\Leftarrow$ “ ergibt:

$$f(g(y)) = y \Leftrightarrow y^2 \leq g(y) < (y+1)^2 \Leftrightarrow g(y) = y^2$$

Dies zeigt, dass die Festlegung  $g(y) = y^2$  das Gewünschte leistet.

Analog kommt man bei der von reellen Zahlen  $a$  und  $b$  abhängenden Funktion

$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = ax + b$$

im Fall  $a \neq 0$  zum Ziel. Es sei  $g : \mathbb{R} \rightarrow \mathbb{R}$  unbekannterweise vorgegeben. Dann zeigt

$$f(g(y)) = y \Leftrightarrow ag(y) + b = y \Leftrightarrow g(y) = \frac{y-b}{a},$$

dass  $g$ , nun mit der ausgerechneten Definition  $g(y) = \frac{y-b}{a}$ , dazu führt, dass  $f$  surjektiv ist. Mit der gleichen Funktion  $g$  bekommt man für alle  $x \in \mathbb{R}$  zusätzlich

$$g(f(x)) = \frac{f(x)-b}{a} = \frac{ax+b-b}{a} = \frac{ax}{a} = x,$$

also, dass die Funktion  $f$  aufgrund der Existenz von  $g$  auch injektiv ist.  $\square$

Vermutet man Injektivität und Surjektivität einer gegebenen Funktion  $f$ , so empfiehlt sich, beim Ausrechnen einer entsprechenden Funktion  $g$  mit  $f(g(y)) = y$  zu arbeiten, da man  $f$  kennt, also  $g(y)$  in die Definition  $f(x) = \dots$  einsetzen kann. Der obige Satz 5.1.7 lässt sich mit den folgenden drei Begriffen wesentlich eleganter formulieren. Wir werden insbesondere den ersten Begriff noch oft verwenden.

### 5.1.9 Definition: Komposition und identische Funktion

- (1) Zu zwei Funktionen  $f : M \rightarrow N$  und  $g : N \rightarrow P$  ist ihre **Komposition** wie folgt definiert:

$$g \circ f : M \rightarrow P \quad (g \circ f)(x) = g(f(x))$$

- (2) Die **identische Funktion** auf einer Menge  $M$  ist wie folgt definiert:

$$id_M : M \rightarrow M \quad id_M(x) = x$$

- (3) Erfüllen zwei Funktionen  $f : M \rightarrow N$  und  $g : N \rightarrow M$  die Gleichung  $g \circ f = id_M$ , so heißt  $g$  eine **Linksinverse** von  $f$  und  $f$  eine **Rechtsinverse** von  $g$ .  $\square$

Man beachte, dass diese Definition in (1) ausnutzt, dass die Quelle  $M$  von  $f$  aufgrund der Festlegung 5.1.2 nicht leer ist. Nach Satz 5.1.1 (3) muss damit auch das Ziel  $N$  von  $f$  nicht leer sein und folglich auch das Ziel  $P$  von  $g$ , weil dessen Quelle  $N$  nicht leer ist. In Definition 5.1.9 (1) sind also aufgrund der Festlegung 5.1.2 beide Funktionen ungleich der leeren Relation. Würde man auf die Festlegung 5.1.2 verzichten, so hätte man den Fall  $\emptyset \circ g$  mit  $\emptyset : \emptyset \rightarrow N$  eigens zu betrachten. Da  $\emptyset \circ g$  die Funktionalität  $\emptyset \rightarrow N$  besitzen muss, ist nur  $\emptyset : \emptyset \rightarrow P$  als das Resultat von  $\emptyset \circ g$  sinnvoll. Mit dieser Erweiterung von Definition 5.1.9 kann man alle folgenden Resultate auch ohne Festlegung 5.1.2 beweisen, indem man den Fall der leeren Relation als erstes Argument der Funktionskomposition „ $\circ$ “ immer noch eigens betrachtet. Wir verzichten aber auf dies und bleiben der Einfachheit halber bei der getroffenen Festlegung.

In Abschnitt 1.4 haben wir die Gleichheit  $f = g$  von Funktionen gleicher Funktionalität charakterisiert. Es gilt  $f = g$  genau dann, wenn  $f(x) = g(x)$  für alle Elemente  $x$  der gemeinsamen Quelle gilt. Somit ist etwa  $g \circ f = id_M$  äquivalent zu  $g(f(x)) = id_M(x) = x$  für alle  $x \in M$ . In der Sprechweise von Definition 5.1.9 lautet also Satz 5.1.7 wie folgt:

- (1) Hat  $f$  eine Linksinverse, so ist  $f$  injektiv.
- (2) Hat  $f$  eine Rechtsinverse, so ist  $f$  surjektiv.

Bevor wir auf eine dritte wichtige Eigenschaft von Funktionen eingehen, wollen wir noch wichtige Eigenschaften für die Komposition von Funktionen festhalten. Der Beweis des folgenden Satzes ist so einfach, dass wir darauf verzichten, ihn anzugeben.

### 5.1.10 Satz: Eigenschaften Funktionskomposition

- (1) Für alle Funktionen  $f : M \rightarrow N$ ,  $g : N \rightarrow P$  und  $h : P \rightarrow Q$  gilt die Gleichung  $h \circ (g \circ f) = (h \circ g) \circ f$ .
- (2) Für alle Funktionen  $f : M \rightarrow N$  gelten die beiden Gleichungen  $f \circ id_M = f$  und  $id_N \circ f = f$ .  $\square$

Wegen der in Punkt (1) dieses Satzes angegebenen Assoziativität lässt man bei mehrfachen Funktionskompositionen die Klammern weg, schreibt also etwa  $i \circ h \circ g \circ f$ . Und hier ist nun der dritte uns in diesem Abschnitt interessierende wichtige Begriff für Funktionen, der die beiden Begriffe von Definition 5.1.3 kombiniert.

### 5.1.11 Definition: Bijektion

Eine injektive und surjektive Funktion heißt **bijektiv** oder eine **Bijektion**.  $\square$

Hat die Funktion  $f$  also eine Linksinverse und eine Rechtsinverse, so ist  $f$  bijektiv. Der folgende Satz zeigt, dass sogar die Umkehrung dieser Implikation gilt und dann alle inversen Funktionen von  $f$  zusätzlich noch identisch sind.

### 5.1.12 Satz: Bijektivität und Links- bzw. Rechtsinverse

Es sei  $f : M \rightarrow N$  eine Funktion. Dann gelten die folgenden Aussagen:

- (1) Ist  $f$  bijektiv, so gibt es eine Funktion  $f^{-1} : N \rightarrow M$  mit den beiden Eigenschaften

$$f^{-1} \circ f = id_M \quad f \circ f^{-1} = id_N,$$

d.h. es gilt  $f^{-1}(f(x)) = x$  für alle  $x \in M$  und es gilt  $f(f^{-1}(y)) = y$  für alle  $y \in N$ .

- (2) Gibt es eine Funktion  $g : N \rightarrow M$  mit den beiden Eigenschaften

$$g \circ f = id_M \quad f \circ g = id_N,$$

so ist die Funktion  $f$  bijektiv und es gilt die Gleichheit  $g = f^{-1}$ , mit der Funktion  $f^{-1}$  aus dem Teil (1).

- (3) Ist  $f$  bijektiv, so ist die Funktion  $f^{-1}$  aus Teil (1) die einzige Linksinverse und auch die einzige Rechtsinverse von  $f$ .

**Beweis:** (1) Wir definieren  $f^{-1}$  als Relation von  $N$  nach  $M$  wie folgt:

$$f^{-1} := \{(y, x) \in N \times M \mid f(x) = y\}$$

Es ist  $f^{-1}$  eindeutig. Zum Beweis seien  $y \in N$  und  $x, z \in M$  beliebig vorgegeben. Dann gilt die folgende logische Implikation:

$$\begin{aligned} y f^{-1} x \wedge y f^{-1} z &\iff f(x) = y \wedge f(z) = y && \text{Definition } f^{-1} \\ &\implies f(x) = f(z) \\ &\implies x = z && f \text{ injektiv} \end{aligned}$$

Es ist  $f^{-1}$  auch total. Zum Beweis sei  $y \in N$  beliebig gewählt. Da  $f$  surjektiv ist, gibt es ein  $x \in M$  mit  $f(x) = y$ . Dies zeigt

$$y f^{-1} x \iff f(x) = y \iff \mathbf{wahr}.$$

Wenden wir nun die bei Funktionen eingeführte Schreibweise  $f^{-1}(y) = x$  für die relationale Beziehung  $y f^{-1} x$  an, so folgt daraus

$$f^{-1}(y) = x \iff f(x) = y \tag{*}$$

für alle  $x \in M$  und  $y \in N$ . Dies zeigt für alle  $x \in M$ , dass

$$f^{-1}(f(x)) = x \iff f(x) = f(x) \iff \mathbf{wahr}$$

zutrifft (das Element  $y$  der Äquivalenz (\*) ist hier  $f(x)$ ), also die Gleichheit  $f^{-1} \circ f = id_M$  gilt, und für alle  $y \in M$ , dass

$$f(f^{-1}(y)) = y \iff f^{-1}(y) = f^{-1}(y) \iff \mathbf{wahr}$$

zutrifft (das Element  $x$  der Äquivalenz (\*) ist hier  $f^{-1}(y)$ ), also auch die Gleichheit  $f \circ f^{-1} = id_N$  gilt.

(2) Die Bijektivität der Funktion  $f$  folgt aus Satz 5.1.7 (1) und (2). Es bleibt noch die Gleichheit  $g = f^{-1}$  zu verifizieren. Die folgende Rechnung zeigt, dass dazu etwa die Gleichung  $g \circ f = id_M$  genügt:

$$\begin{aligned} g \circ f = id_M &\implies g \circ f = f^{-1} \circ f && \text{nach (1)} \\ &\implies g \circ f \circ f^{-1} = f^{-1} \circ f \circ f^{-1} \\ &\iff g \circ id_N = id_M \circ f^{-1} && \text{nach (1)} \\ &\iff g = f^{-1} && \text{nach Satz 5.1.10 (2)} \end{aligned}$$

(3) In Teil (2) wurde gezeigt, dass jede Linksinverse  $g$  von  $f$  gleich der Funktion  $f^{-1}$  aus Teil (1) ist. Hier ist nun der Beweis für jede Rechtsinverse  $g$  von  $f$ :

$$\begin{aligned} f \circ g = id_N &\implies f \circ g = f \circ f^{-1} && \text{nach (1)} \\ &\implies f^{-1} \circ f \circ g = f^{-1} \circ f \circ f^{-1} \\ &\iff id_M \circ g = id_M \circ f^{-1} && \text{nach (1)} \\ &\iff g = f^{-1} && \text{nach Satz 5.1.10 (2)} \end{aligned}$$

Damit ist der gesamte Beweis erbracht.  $\square$

Eine Funktion  $f : M \rightarrow N$  ist also bijektiv genau dann, wenn es genau eine Funktion gibt, welche zugleich eine Linksinverse und eine Rechtsinverse von ihr ist. Diese eindeutig bestimmte Funktion, oben mit  $f^{-1} : N \rightarrow M$  bezeichnet, hat einen eigenen Namen.

### 5.1.13 Definition: Umkehrfunktion

Ist  $f : M \rightarrow N$  eine bijektive Funktion, so nennt man die Funktion  $f^{-1} : N \rightarrow M$  von Satz 5.1.12 (1) ihre **Umkehrfunktion** oder **Inverse**.  $\square$

Umkehrfunktionen  $f^{-1} : N \rightarrow M$  sind offensichtlich ebenfalls bijektiv. Also hat  $f^{-1}$ , wiederum nach dem eben bewiesenen Satz, eine eindeutig bestimmte Umkehrfunktion, nun mit  $(f^{-1})^{-1} : M \rightarrow N$  oder einfacher mit  $f^{-1-1} : M \rightarrow N$  bezeichnet. Es gilt die Eigenschaft  $f^{-1-1} = f$ .

Aufgrund des obigen Satzes 5.1.12 bekommen wir beispielsweise auch, dass für alle  $a, b \in \mathbb{R}$  mit der Eigenschaft  $a \neq 0$  die Funktion

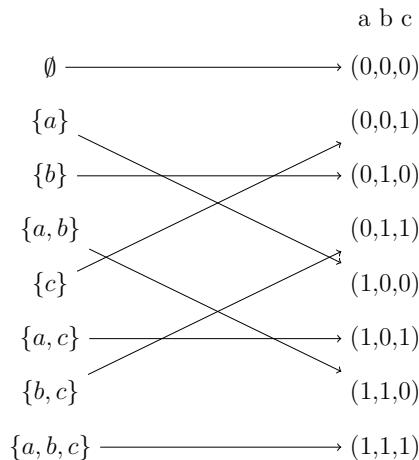
$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = ax + b$$

von Beispiel 5.1.8 bijektiv ist und ihre Umkehrfunktion  $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$  bestimmt ist durch die Gleichung  $f^{-1}(x) = \frac{x-b}{a}$ .

In bipartiten Pfeildiagrammen stellen sich bijektive Funktionen so dar, dass von jedem Element der linken Menge zu genau einem Element der rechten Menge ein Pfeil führt. Man spricht aufgrund dieser Bilder beim Vorliegen einer bijektiven Funktion auch von einer **eineindeutigen Beziehung** oder einer **Eins-zu-Eins-Beziehung** zwischen den Mengen der Funktionalität dieser Funktion. Umkehrfunktionen bijektiver Funktionen sind ebenfalls bijektiv. In bipartiten Pfeildiagrammen bekommt man sie, indem man einfach die Pfeilrichtung umkehrt und dann das Diagramm horizontal spiegelt.

### 5.1.14 Beispiel: Bijektivität im Pfeildiagramm

Wir betrachten Potenzmengen und lineare 0/1-Listen. Es sei die Menge  $M$  definiert durch  $M := \{a, b, c\}$ . Dann werden die Mengen  $\mathcal{P}(M)$  und  $\{0, 1\}^3$  beispielsweise bijektiv aufeinander abgebildet durch eine Funktion, die durch das folgende bipartite Pfeildiagramm graphisch darstellt wird:



Wir haben in diesem Bild die erste Komponente der Liste dem Element  $a$  zugeordnet, die zweite Komponente dem Element  $b$  und die dritte Komponente dem Element  $c$ . Andere Komponentenzuordnungen führen zu anderen Bildern bzw. bijektiven Funktionen. Das oben angegebene Beispiel zeigt auch auf, wie man allgemein für endliche Mengen  $M$  eine bijektive Funktion von  $\mathcal{P}(M)$  nach  $\{0, 1\}^{|M|}$  konstruieren kann.  $\square$

Eine Funktion ist genau dann bijektiv, wenn sie eine Linksinverse und eine Rechtsinverse besitzt. Es gibt jeweils nur eine davon und diese beiden Funktionen sind sogar noch identisch. Wie sieht es nun mit den allgemeineren Eigenschaften der Injektivität und der Surjektivität aus? Als erste unmittelbare Folgerungen aus Satz 5.1.7 und Satz 5.1.12 bekommen wir für alle Funktionen  $f$  die folgende Eigenschaft: Existieren zu  $f$  mehrere Linksinverse, so ist  $f$  injektiv, aber nicht surjektiv, und existieren zu  $f$  mehrere Rechtsinverse, so ist  $f$  surjektiv, aber nicht injektiv. Unser ultimatives Ziel ist, zu zeigen, dass eine Funktion genau dann injektiv ist, wenn sie eine Linksinverse besitzt, und genau dann surjektiv ist, wenn sie eine Rechtsinverse besitzt. Bisher haben wir von diesen Aussagen jeweils nur eine Richtung bewiesen. Für das weitere Vorgehen führen wir in der nachfolgenden Definition zwei neue Begriffe ein.

### 5.1.15 Definition: Bild(menge) und Urbild(menge)

Es sei  $f : M \rightarrow N$  eine Funktion. Zu einer Menge  $X \subseteq M$  heißt

$$f(X) := \{f(x) \mid x \in X\} = \{y \mid \exists x \in X : y = f(x)\} \subseteq N$$

das **Bild** oder die **Bildmenge** von  $X$  unter  $f$  und zu  $Y \subseteq N$  heißt

$$f^{-1}(Y) := \{x \in M \mid f(x) \in Y\} \subseteq M$$

das **Urbild** oder die **Urbildmenge** von  $Y$  unter  $f$ .

□

Manchmal schreibt man auch  $f[X]$  und  $f^{-1}[X]$  um Verwechslungen mit Funktionsanwendungen zu vermeiden, wie etwa in  $f^{-1}(f(X))$  bei beliebigen (auch nicht bijektiven) Funktionen, wo  $f^{-1}[f[X]]$  den Unterschied klar aufzeigt. Offensichtlich gilt  $f(\emptyset) = \emptyset = f^{-1}(\emptyset)$  für alle Funktionen  $f$ . Für die spezielle Funktion  $f : \mathbb{N} \rightarrow \mathbb{N}$  mit der Definition  $f(x) = x^2$  gelten beispielsweise die Gleichungen  $f(\{1, 2\}) = \{1, 4\}$  und  $f^{-1}(\{9, 16\}) = \{3, 4\}$ . Urbilder von einelementigen Mengen erlauben im Fall endlicher Quellen mit Hilfe der Kardinalitäten die früheren Begriffe zu charakterisieren. Wie dies möglich ist, wird nun angegeben.

### 5.1.16 Satz: Urbilder einelementiger Mengen

Es sei  $f : M \rightarrow N$  eine Funktion, deren Quelle  $M$  endlich ist. Dann gelten die folgenden Eigenschaften:

- (1) Es ist  $f$  injektiv genau dann, wenn für alle  $y \in N$  gilt  $|f^{-1}(\{y\})| \leq 1$ .
- (2) Es ist  $f$  surjektiv genau dann, wenn für alle  $y \in N$  gilt  $|f^{-1}(\{y\})| \geq 1$ .
- (3) Es ist  $f$  bijektiv genau dann, wenn für alle  $y \in N$  gilt  $|f^{-1}(\{y\})| = 1$ .

**Beweis:** Es ist (3) eine unmittelbare Folgerung von (1) und (2). Für einen Beweis von (1) bietet es sich an, die rechte Seite der zu zeigenden Äquivalenz als logische Formel hinzuschreiben. Dann führen die folgenden Umformungen zum Ziel:

$$\begin{aligned} & \forall y \in N : |f^{-1}(\{y\})| \leq 1 \\ \iff & \forall y \in N : \forall x, z \in M : x \in f^{-1}(\{y\}) \wedge z \in f^{-1}(\{y\}) \Rightarrow x = z \\ \iff & \forall y \in N : \forall x, z \in M : f(x) \in \{y\} \wedge f(z) \in \{y\} \Rightarrow x = z \\ \iff & \forall y \in N : \forall x, z \in M : f(x) = y \wedge f(z) = y \Rightarrow x = z \\ \iff & \forall x, z \in M : f(x) = f(z) \Rightarrow x = z \\ \iff & f \text{ injektiv} \end{aligned}$$

In der gleichen Art und Weise wird durch die Rechnung

$$\begin{aligned} \forall y \in N : |f^{-1}(\{y\})| \geq 1 & \iff \forall y \in N : \exists x \in M : x \in f^{-1}(\{y\}) \\ & \iff \forall y \in N : \exists x \in M : f(x) \in \{y\} \\ & \iff \forall y \in N : \exists x \in M : f(x) = y \\ \iff & f \text{ surjektiv.} \end{aligned}$$

die Äquivalenz von Teil (2) bewiesen. □

Das nächste Resultat zeigt, wie man Injektivität und Surjektivität durch Bild- und Urbildmengen charakterisieren kann.

### 5.1.17 Satz: Charakterisierung von Injektivität und Surjektivität

Gegeben sei eine Funktion  $f : M \rightarrow N$ . Dann gelten die folgenden Eigenschaften:

- (1) Es ist  $f$  injektiv genau dann, wenn für alle  $X \subseteq M$  gilt  $f^{-1}(f(X)) = X$ .

(2) Es ist  $f$  surjektiv genau dann, wenn für alle  $Y \subseteq N$  gilt  $f(f^{-1}(Y)) = Y$ .

**Beweis:** Wir beginnen mit der Aussage (1) und hier mit der Richtung „ $\Rightarrow$ “. Dazu sei  $X \subseteq M$  beliebig vorgegeben. Dann gilt:

$$\begin{aligned} f^{-1}(f(X)) &= f^{-1}(\{f(x) \mid x \in X\}) \\ &= \{y \in M \mid f(y) \in \{f(x) \mid x \in X\}\} \\ &= \{y \in M \mid f(y) \in \{u \mid \exists x \in X : u = f(x)\}\} \\ &= \{y \in M \mid \exists x \in X : f(y) = f(x)\} \\ &= \{y \in M \mid \exists x \in X : y = x\} \\ &= \{y \in M \mid y \in X\} \\ &= X \end{aligned}$$

Neben der Definition der Bild- und Urbildmenge werden im fünften Schritt die Injektivität von  $f$  und das Identitätsprinzip von Leibniz verwendet. Wesentlich ist auch der dritte Schritt, welcher die Zermelo-Mengenkomprehension rückgängig macht. Der Rest folgt aus bekannten logischen und mengentheoretischen Gesetzen.

Die verbleibende Richtung „ $\Leftarrow$ “ von (1) beweisen wir wie folgt, wobei die entscheidende Idee die Spezialisierung der Allquantifizierung auf einelementige Mengen im ersten Schritt ist. Neben der Definition der Bild- und Urbildmenge werden wieder nur bekannte Tatsachen aus der Logik und der Mengenlehre verwendet.

$$\begin{aligned} &\forall X \in \mathcal{P}(M) : f^{-1}(f(X)) = X \\ \iff &\forall x \in M : f^{-1}(f(\{x\})) = \{x\} \\ \iff &\forall x \in M : \{y \in M \mid f(y) \in f(\{x\})\} = \{x\} \\ \iff &\forall x \in M : \{y \in M \mid f(y) \in \{f(x)\}\} = \{x\} \\ \iff &\forall x \in M : \{y \in M \mid f(y) = f(x)\} = \{x\} \\ \iff &\forall x, u \in M : u \in \{y \in M \mid f(y) = f(x)\} \Leftrightarrow u \in \{x\} \\ \iff &\forall x, u \in M : f(u) = f(x) \Leftrightarrow u = x \\ \Rightarrow &\forall x, u \in M : f(u) = f(x) \Rightarrow u = x \end{aligned}$$

Die letzte Formel dieser Rechnung beschreibt genau, dass  $f$  eine injektive Funktion ist.

Auch bei (2) ist es vorteilhaft, zwei Richtungen zu beweisen. Dies geht ziemlich ähnlich zu den Beweisen von (1), wobei im Fall der Richtung „ $\Leftarrow$ “ der entscheidende erste Schritt wiederum eine Spezialisierung der Allquantifizierung ist. Deshalb verzichten wir auf die Beweise. Wir empfehlen aber der Leserin oder dem Leser, sie zu Übungszwecken durchzuführen.  $\square$

Nach diesen Vorbereitungen können wir damit beginnen, die Umkehrungen von Satz 5.1.7 zu beweisen. Wir starten mit Punkt (1).

### 5.1.18 Satz: Injektivität und Linksinverse

Für alle Funktionen  $f : M \rightarrow N$  gilt: Es ist  $f$  injektiv genau dann, wenn es eine Linksinverse  $g : N \rightarrow M$  zu  $f$  gibt.

**Beweis:** Wir beginnen mit dem Beweis von „ $\implies$ “. Dazu betrachten wir die folgende Funktion, die aus  $f$  entsteht, indem man das Ziel auf die Bildmenge der Quelle einschränkt:

$$f_1 : M \rightarrow f(M) \quad f_1(x) = f(x)$$

Durch diese Festlegung ist  $f_1$  nicht nur injektiv, sondern auch surjektiv, also bijektiv. Somit existiert die Umkehrfunktion  $f_1^{-1} : f(M) \rightarrow M$ . Wegen  $M \neq \emptyset$  können wir irgendein Element  $a \in M$  wählen und damit die folgende Funktion festlegen:

$$g : N \rightarrow M \quad g(y) = \begin{cases} f_1^{-1}(y) & \text{falls } y \in f(M) \\ a & \text{falls } y \notin f(M) \end{cases}$$

Dann gilt für alle  $x \in M$  die Gleichung

$$g(f(x)) = f_1^{-1}(f(x)) = f_1^{-1}(f_1(x)) = x$$

aufgrund von  $f(x) \in f(M)$  und  $f(x) = f_1(x)$  (da  $x \in M$ ) und  $f_1^{-1} \circ f_1 = id_M$ . Also ist die Funktion  $g$  eine Linksinverse von  $f$ .

Die verbleibende Richtung „ $\Leftarrow$ “ brauchen wir nicht zu zeigen, denn sie entspricht genau Satz 5.1.7 (1).  $\square$

Für die Umkehrung von Teil (2) von Satz 5.1.7 müssen wir etwas genauer über Mengenlehre reden. Wir betreiben, wie in Kapitel 1 erwähnt, in diesem Text naive Mengenlehre, gehen also nicht auf die Axiome der Mengenlehre ein. Implizit haben wir diese Axiome natürlich immer wieder verwendet, etwa das **Axiome der Existenz der leeren Menge**, welches besagt, dass es eine Menge ohne Elemente gibt, das **Axiom der Mengengleichheit**, welches genau unserer Definition von  $M = N$  entspricht, und das **Aussonderungsaxiom**, welches zu jeder Menge  $M$  und jeder logischen Aussage  $A(x)$ , in der die Variable  $x$  für Objekte steht, die Existenz der Menge  $\{x \mid x \in M \wedge A(x)\}$  zusichert. Nun brauchen wir ein weiteres Axiom der Mengenlehre explizit. Es wird Auswahlaxiom genannt und geht auf den schon erwähnten deutschen Mathematiker Zermelo zurück. Er entdeckte es im Jahr 1904, als er, zusammen mit seinem Kollegen Erhard Schmidt (1876-1959), über einen Beweis eines fundamentalen Satzes diskutierte, der heutzutage als **Zermeloscher Wohlordnungssatz** bekannt ist.

### 5.1.19 Auswahlaxiom (E. Zermelo)

Ist  $\mathcal{M}$  eine Menge nichtleerer Mengen, so existiert eine (Auswahl-)Funktion  $\alpha : \mathcal{M} \rightarrow \bigcup \mathcal{M}$  mit  $\alpha(X) \in X$  für alle  $X \in \mathcal{M}$ .  $\square$

Durch die Funktion  $\alpha$  wird also gleichzeitig aus jeder der Mengen von  $\mathcal{M}$  ein Element ausgewählt. Ist  $\mathcal{M}$  endlich, so ist dies durch einen Algorithmus offenbar möglich. Im Unendlichen kann man über so eine Möglichkeit jedoch diskutieren und es gibt durchaus ernst zu nehmende Mathematikerinnen und Mathematiker, die das Auswahlaxiom als Beweismittel ablehnen. Man spricht dann von konstruktiver oder intuitionistischer Mathematik. Von der überwiegenden Mehrheit der Mathematikerinnen und Mathematiker wird das Auswahlaxiom akzeptiert. Mit seiner Hilfe zeigen wir nun das noch fehlende Resultat.

### 5.1.20 Satz: Surjektivität und Rechtsinverse

Für alle Funktionen  $f : M \rightarrow N$  gilt: Es ist  $f$  genau dann surjektiv, wenn es eine Rechtsinverse  $g : N \rightarrow M$  zu  $f$  gibt.

**Beweis:** Die Richtung „ $\Leftarrow$ “ ist genau Satz 5.1.7, Teil (2).

Beweis von „ $\Rightarrow$ “: Wegen der Surjektivität von  $f$  gilt  $f^{-1}(\{y\}) \neq \emptyset$  für alle  $y \in N$ . Wir betrachten nun die folgende Menge  $\mathcal{M}$  von Mengen:

$$\mathcal{M} := \{f^{-1}(\{y\}) \mid y \in N\}$$

Dann ist  $\mathcal{M}$  eine Menge von nichtleeren Mengen und jede dieser Mengen ist in  $M$  als Teilmenge enthalten. Nach dem Auswahlaxiom 5.1.19 gibt es also eine Auswahlfunktion  $\alpha : \mathcal{M} \rightarrow \bigcup \mathcal{M}$ , mit  $\alpha(X) \in X$  für alle  $X \in \mathcal{M}$ . Nun formen wir wie folgt logisch um:

$$\begin{aligned} \forall X \in \mathcal{M} : \alpha(X) \in X &\iff \forall y \in N : \alpha(f^{-1}(\{y\})) \in f^{-1}(\{y\}) \\ &\iff \forall y \in N : f(\alpha(f^{-1}(\{y\}))) \in \{y\} \\ &\iff \forall y \in N : f(\alpha(f^{-1}(\{y\}))) = y \end{aligned}$$

Die unterste Formel dieser Rechnung legt es nahe, die folgende Funktion zu betrachten:

$$g : N \rightarrow M \quad g(y) = \alpha(f^{-1}(\{y\}))$$

Wegen  $\alpha(f^{-1}(\{y\})) \in M$  für alle  $y \in N$  ist jedes Resultat tatsächlich in der Menge  $M$  enthalten, diese Funktion also hinsichtlich des Ziels „wohldefiniert“. Weiterhin gilt

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

für alle  $y \in N$  und somit ist die Funktion  $g$  eine Rechtsinverse von  $f$ .  $\square$

Man kann nun natürlich fragen, ob ein solch schweres Geschütz für den Beweis von Satz 5.1.20 notwendig ist, oder es nicht doch einen Beweis ohne das Auswahlaxiom (oder eine dazu gleichwertige mathematische Aussage) gibt. Die Antwort ist negativ, denn es kann gezeigt werden, dass das Auswahlaxiom aus Satz 5.1.20 bewiesen werden kann, indem man nur die restlichen Axiome der axiomatischen Mengenlehre verwendet.

## 5.2 Kardinalitätsvergleich von Mengen

Mit den Begriffen von Abschnitt 5.1 kann man nun die Endlichkeit von Mengen und den Vergleich der Kardinalität von Mengen ohne Rückgriff auf natürliche Zahlen spezifizieren. Von Bernhard Bolzano (1781-1848), einem österreichisch-böhmischem Philosophen und Mathematiker, stammt die folgende Beobachtung: Die Menge  $M$  ist genau dann endlich, wenn es keine bijektive Funktion  $f : M \rightarrow N$  gibt, deren Ziel  $N$  eine echte Teilmenge von  $M$  ist. Ein Beweis, der auf den naiven Endlichkeitsbegriff von Abschnitt 1.3 aufbaut, ist nicht schwierig. Für alle endlichen Mengen  $M$  und  $N$  gelten weiterhin die folgenden Beziehungen zwischen den Kardinalitäten und der Existenz von speziellen Funktionen:

- (1) Es gilt  $|M| = |N|$  genau dann, wenn es eine bijektive Funktion  $f : M \rightarrow N$  gibt.
- (2) Es gilt  $|M| \leq |N|$  genau dann, wenn es eine injektive Funktion  $f : M \rightarrow N$  gibt.

Wir haben (1) etwa implizit im Beweis von Satz 1.4.3 verwendet. Die dortige Gleichheit  $|\{(a_i, b) \mid b \in N\}| = |N|$  gilt aufgrund der Zuordnung  $(a_i, b) \mapsto b$ , die eine bijektive Funktion von  $\{a_i\} \times N$  nach  $N$  definiert. Auch der Beweis von Satz 4.4.7 verwendet z.B. implizit, dass (1) gilt. Die entsprechende bijektive Funktion wird hier durch die Zuordnung  $X \mapsto X \cup \{a\}$  definiert. Cantors Idee war, die Eigenschaften (1) und (2) zur Definition für einen allgemeinen Vergleich von Kardinalitäten von Mengen zu verwenden, also auch im unendlichen Fall. Ihm folgend definiert man heutzutage wie nachstehend gegeben:

### 5.2.1 Definition: Kardinalitätsvergleiche

Es seien  $M$  und  $N$  beliebige Mengen. Dann legt man drei Kardinalitätsvergleiche zwischen diesen Mengen wie folgt fest:

- (1) Es sind  $M$  und  $N$  **gleich mächtig** (oder:  $M$  und  $N$  haben die **gleiche Kardinalität**), im Zeichen  $|M| = |N|$ , falls es eine bijektive Funktion  $f : M \rightarrow N$  gibt.
- (2) Es ist  $M$  **höchstens so mächtig** wie  $N$  (oder:  $M$  hat **höchstens die Kardinalität** von  $N$ ), im Zeichen  $|M| \leq |N|$ , falls es eine injektive Funktion  $f : M \rightarrow N$  gibt.
- (3) Es ist  $N$  **echt mächtiger** als  $M$  (oder:  $N$  ist **von echt größerer Kardinalität** als  $M$ ), im Zeichen  $|M| < |N|$ , falls  $|M| \leq |N|$  gilt und  $|M| = |N|$  nicht gilt (also  $\neg(|M| = |N|)$  gilt).  $\square$

Man beachte, dass in den Aussagen  $|M| = |N|$ ,  $|M| \leq |N|$  und  $|M| < |N|$ , welche in dieser Definition eingeführt werden, beim Vorliegen von mindestens einer unendlichen Menge die Ausdrücke  $|M|$  und  $|N|$  nicht mehr die in Definition 1.3.6 gegebenen Bedeutungen haben, also nicht mehr für die Anzahlen der Elemente von  $M$  und  $N$  stehen. Was soll in so einem Fall auch etwa bei  $M := \{1\}$  und  $N := \mathbb{N}$  die Gültigkeit von  $|M| = |N|$  sein, wo doch  $|N|$  im Sinne der in Definition 1.3.6 gegebenen Bedeutung nicht erklärt ist? Für eine unendliche Menge  $M$  ist der Ausdruck  $|M|$  für sich allein stehend nicht mehr zulässig. Er darf nur als Teil eines Kardinalitätsvergleichs vorkommen, also nur in Verbindung mit den in Definition 5.2.1 eingeführten Schreibweisen. Ist eine der Mengen  $M$  und  $N$  in  $|M| = |N|$ ,  $|M| \leq |N|$  und  $|M| < |N|$  unendlich, so sind die Aussagen genau dann gültig, wenn es eine bijektive Funktion  $f : M \rightarrow N$  gibt bzw. wenn es eine injektive Funktion  $f : M \rightarrow N$  gibt bzw. wenn es eine injektive Funktion  $f : M \rightarrow N$  gibt, aber keine bijektive Funktion  $g : M \rightarrow N$  existiert.

Aufgrund der Festlegung 5.1.2 haben wir genau genommen die drei Kardinalitätsvergleiche  $|M| = |N|$ ,  $|M| \leq |N|$  und  $|M| < |N|$  in Definition 5.2.1 nur für nichtleere Mengen definiert. Es ist aber klar, wie wir sie auf die leere Menge zu erweitern haben. Es sei  $M$  eine beliebige (auch leere) Menge. Dann legen wir definierend fest:

$$\begin{array}{lll} |\emptyset| = |M| & :\iff & M = \emptyset \\ |M| = |\emptyset| & :\iff & M = \emptyset \end{array} \quad \begin{array}{lll} |\emptyset| \leq |M| & :\iff & \text{wahr} \\ |M| \leq |\emptyset| & :\iff & M = \emptyset \end{array}$$

Diese Festlegungen sind im Fall einer endlichen Menge  $M$  offensichtlich verträglich mit der bisherigen naiven Definition der Kardinalität. Im Fall einer unendlichen Menge  $M$  wären sie auch verträglich mit Definition 5.2.1, wenn dieser ein Funktionsbegriff ohne die Einschränkung auf nichtleere Quellen zugrunde liegen würde. Analog zu Satz 5.1.1 kann

man nämlich zeigen, dass die leere Relation  $\emptyset \subseteq \emptyset \times M$  auch injektiv ist und sie surjektiv genau dann ist, wenn  $M = \emptyset$  gilt.

Im nächsten Satz formulieren wir einige fundamentale Eigenschaften der eben eingeführten Begriffe. Bei den Relationen im nächsten Kapitel werden uns diese Eigenschaften wieder begegnen.

### 5.2.2 Satz: fundamentale Eigenschaften

Es seien  $M$ ,  $N$  und  $P$  beliebige Mengen. Dann gelten die folgenden Eigenschaften:

- (1) Aus  $|M| = |N|$  und  $|N| = |P|$  folgt  $|M| = |P|$ , aus  $|M| \leq |N|$  und  $|N| \leq |P|$  folgt  $|M| \leq |P|$  und aus  $|M| < |N|$  und  $|N| < |P|$  folgt  $|M| < |P|$ .
- (2) Es sind  $|M| = |N|$  und  $|N| = |M|$  logisch äquivalent.
- (3) Sind  $|M| = |N|$  und  $|N| \leq |P|$  wahr, so ist auch  $|M| \leq |P|$  wahr.
- (4) Es gelten  $|M| = |M|$  und  $|M| \leq |M|$  und  $\neg(|M| < |M|)$ .

**Beweis:** Weil die Komposition bijektiver Funktionen bijektiv ist und die Komposition injektiver Funktionen injektiv ist, gilt (1). Wir zeigen zuerst, dass die Komposition  $f \circ g$  von injektiven Funktionen injektiv ist, indem wir für alle  $x$  und  $y$  aus der Quelle von  $g$  unter der Verwendung der Injektivität von  $f$  und dann von  $g$  nachrechnen, dass

$$(f \circ g)(x) = (f \circ g)(y) \iff f(g(x)) = f(g(y)) \implies g(x) = g(y) \implies x = y$$

gilt. Dass die Komposition bijektiver Funktionen bijektiv ist, folgt nun aus der Tatsache, dass die Komposition  $f \circ g$  von surjektiven Funktionen surjektiv ist. Zum Beweis sei  $z$  aus dem Ziel von  $f$ . Dann gibt es ein  $y$  aus der Quelle von  $f$  mit  $f(y) = z$ , denn  $f$  ist surjektiv. Weiterhin gibt es zu dem  $y$  nun ein  $x$  aus der Quelle von  $g$  mit  $g(x) = y$ , denn auch  $g$  ist surjektiv und  $y$  ist aus dem Ziel von  $g$ . Insgesamt haben wir also

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

Die restlichen Punkte (2) bis (4) kann man in analoger Weise zeigen.  $\square$

Nachfolgend geben wir einige Beispiele für Kardinalitätsvergleiche an. Dabei verwenden wir, wie auch bei den üblichen Ordnungen auf Zahlen, die Abkürzung  $|M| < |N| < |P|$  für die Konjunktion  $|M| < |N| \wedge |N| < |P|$ . Dies ist durch den obigen Satz gerechtfertigt.

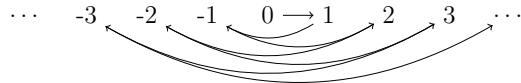
### 5.2.3 Beispiele: Kardinalitätsvergleiche

In der Potenzmenge der natürlichen Zahlen haben wir etwa die folgende Kette von immer echt größer werdenden Kardinalitäten:

$$|\emptyset| < |\{0\}| < |\{0, 1\}| < |\{0, 1, 2\}| < \dots$$

Weiterhin gilt  $|X| \leq |\mathbb{N}|$  für alle  $X \subseteq \mathbb{N}$ . Schließlich gilt noch  $|\mathbb{G}| = |\mathbb{N}|$ , wenn  $\mathbb{G}$  die Menge der geraden natürlichen Zahlen bezeichnet. Dies zeigt, dass  $\mathbb{N}$  eine unendliche Menge im Sinne der von Bolzano gegebenen Definition von Endlichkeit ist.

Es gilt  $|\mathbb{N}| = |\mathbb{Z}|$ . Zum Beweis dieser Aussage zählt man etwa die ganzen Zahlen der Reihe nach auf, wie in dem folgenden Bild zeichnerisch dargestellt.



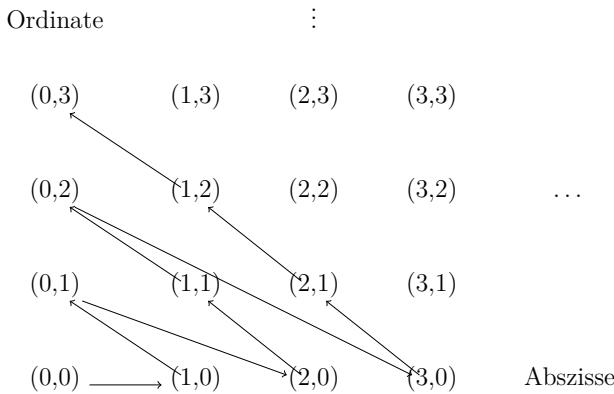
Man benötigt also eine Funktion, für welche die Eigenschaften  $f(0) = 0$ ,  $f(1) = 1$ ,  $f(-1) = 2$ ,  $f(2) = 3$ ,  $f(-2) = 4$ ,  $f(3) = 5$ ,  $f(-3) = 6$  usw. gelten. Es ist sehr einfach zu verifizieren, dass die Funktion

$$f : \mathbb{Z} \rightarrow \mathbb{N} \quad f(x) = \begin{cases} 2x - 1 & \text{falls } x \in \mathbb{N} \setminus \{0\} \\ |2x| & \text{falls } x \notin \mathbb{N} \setminus \{0\} \end{cases}$$

das Gewünschte leistet. Auch der formale Bijektivitätsbeweis ist nicht schwierig.

Ist man mit der Mathematik nicht sehr vertraut, so wirken diese eben gebrachten Ergebnisse auf den ersten Blick überraschend. Es gibt doch beispielsweise echt weniger gerade natürliche Zahlen als insgesamt natürliche Zahlen, denn beispielsweise ist die Eins nicht gerade. Aber trotzdem kann man jeder natürlichen Zahl in einer eindeutigen Weise durch ihre Verdopplung eine gerade natürliche Zahl zuordnen. Solche Paradoxien sind aber nur bei unendlichen Mengen möglich und dies hat Bolzano zu seiner Definition von Endlichkeit geführt.

Von Cantor wurde als ein bedeutendes Resultat bewiesen, dass die Eigenschaft  $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$  gilt. Hierzu zählte er alle Paare der Menge  $\mathbb{N} \times \mathbb{N}$  in der Art und Weise auf, wie es das nachfolgende Bild zeigt. Man nennt diese Aufzählung heutzutage das **erste Cantorsche Diagonalargument**.



Aufgrund dieser Zeichnung gilt es, eine Funktion  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  zu finden, welche den Gleichungen  $f(0,0) = 0$ ,  $f(1,0) = 1$ ,  $f(0,1) = 2$ ,  $f(2,0) = 3$  usw. genügt. Durch einfache geometrische Überlegungen kommt man auf die bijektive Funktion  $f(x, y) = y + \sum_{i=0}^{x+y} i$  als Lösung. Die Injektivität von  $f$  kann man durch Fallunterscheidungen verifizieren, die Surjektivität, indem man durch Induktion  $n \in f(\mathbb{N} \times \mathbb{N})$  für alle  $n \in \mathbb{N}$  zeigt.  $\square$

Mengen  $M$  mit  $|M| = |\mathbb{N}|$  heißen **abzählbar (unendlich)**; solche mit  $|\mathbb{N}| < |M|$  heißen **überabzählbar (unendlich)**. Von Cantor wurde auch das folgende wichtige Resultat gefunden. Es erlaubt, die Kette  $|\emptyset| < |\{0\}| < |\{0, 1\}| < \dots < |\mathbb{N}|$  der Kardinalitäten des letzten Beispiels nach der abzählbar unendlichen Menge  $\mathbb{N}$  beliebig „ins Überabzählbare“ fortzusetzen. Man nennt die entscheidende Idee der Definition von  $Y$  im Beweis von Satz 5.2.4 heutzutage das **zweite Cantorsche Diagonalargument**.

#### 5.2.4 Satz (G. Cantor)

Für alle Mengen  $M$  gilt  $|M| < |\mathcal{P}(M)|$ .

**Beweis:** Um  $|M| < |\mathcal{P}(M)|$  zu beweisen, müssen wir  $|M| \leq |\mathcal{P}(M)|$  und  $\neg(|M| = |\mathcal{P}(M)|)$  verifizieren. Für  $|M| \leq |\mathcal{P}(M)|$  genügt es, eine injektive Funktion von  $M$  nach  $\mathcal{P}(M)$  anzugeben. Hier ist eine; auf den offensichtlichen Injektivitätsbeweis verzichten wir:

$$f : M \rightarrow \mathcal{P}(M) \quad f(x) = \{x\}$$

Um zu zeigen, dass  $|M| = |\mathcal{P}(M)|$  nicht gilt, führen wir einen Beweis durch Widerspruch. Angenommen, es gelte  $|M| = |\mathcal{P}(M)|$ . Dann gibt es eine bijektive Funktion

$$g : M \rightarrow \mathcal{P}(M).$$

Als bijektive Funktion ist  $g$  insbesondere auch surjektiv. Also hat die Menge

$$Y := \{x \in M \mid x \notin g(x)\},$$

die ein Element von  $\mathcal{P}(M)$  ist, ein Urbild  $a \in M$ . Folglich gilt  $Y = g(a)$ . Unter Verwendung dieser Eigenschaft bekommt man die logische Äquivalenz

$$\begin{aligned} a \in Y &\iff a \notin g(a) && \text{nach der Definition von } Y \\ &\iff a \notin Y && Y = g(a) \text{ gilt nach Annahme.} \end{aligned}$$

Also haben wir einen Widerspruch, denn eine Aussage ist niemals logisch äquivalent zu ihrer Negation.  $\square$

Cantor stellte nun im Zusammenhang mit Mengenkardinalitäten drei entscheidende Fragen, die sehr bedeutend für die Weiterentwicklung der Mathematik wurden. Diese sind nachfolgend angegeben.

- (1) Sind beliebige Mengen bezüglich der Kardinalität immer vergleichbar, d.h. gilt für alle Mengen  $M$  und  $N$  die Aussage  $|M| \leq |N| \vee |N| \leq |M|$ ?
- (2) Gibt es eine Menge  $M$  mit der Eigenschaft  $|\mathbb{N}| < |M| < |\mathcal{P}(\mathbb{N})|$ ?
- (3) Gilt für alle Mengen  $M$  und  $N$  die logische Äquivalenz der zwei Aussagen  $|M| = |N|$  und  $|M| \leq |N| \wedge |N| \leq |M|$ ?

Zermelo zeigte, dass die Frage (1) mit „ja“ zu beantworten ist. Genau zu dem Zweck wurde das Auswahlaxiom eingeführt. Gödel und der amerikanische Mathematiker Paul Cohen (1934-2007) bewiesen durch zwei Arbeiten aus den Jahren 1938 und 1963, dass die

der Frage (2) entsprechende Aussage mit den Axiomen der Mengenlehre weder widerlegbar noch beweisbar ist. Das Problem (2) ist auch als die **Kontinuumshypothese** bekannt. Es gilt nämlich  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$  und somit fragt (2) nach einer Menge, die hinsichtlich des Kardinalitätsvergleichs echt zwischen den natürlichen Zahlen und den reellen Zahlen (dem Kontinuum) liegt. Die deutschen Mathematiker Ernst Schröder (1841-1902) und Felix Bernstein (1878-1956) zeigten schließlich, dass die Antwort zu Frage (3) ebenfalls „ja“ ist. Wir geben nachfolgend einen Beweis für die positive Beantwortung von (3) an, die Beweise zu den Antworten zu (1) und (2) sind wesentlich komplizierter und können mit den derzeitigen Mitteln nicht erbracht werden.

### 5.2.5 Satz (E. Schröder und F. Bernstein)

Es seien  $M$  und  $N$  beliebige Mengen. Dann gelten die folgenden zwei Aussagen:

- (1) Gibt es eine bijektive Funktion  $f : M \rightarrow N$ , so gibt es eine injektive Funktion  $g_1 : M \rightarrow N$  und eine injektive Funktion  $g_2 : N \rightarrow M$ .
- (2) Gibt es injektive Funktionen  $g_1 : M \rightarrow N$  und  $g_2 : N \rightarrow M$ , so gibt es eine bijektive Funktion  $f : M \rightarrow N$ .

**Beweis:** (1) Dies ist die einfache Richtung der durch (1) und (2) beschriebenen Äquivalenz. Man wählt die Funktion  $g_1$  als  $f$  und die Funktion  $g_2$  als die Umkehrfunktion  $f^{-1}$ . Dann sind  $g_1$  und  $g_2$  bijektiv, also auch injektiv.

(2) Wir betrachten die nachfolgend gegebene Funktion; dabei verwenden wir die Definition 5.1.15, in der das Bild einer Menge festgelegt ist:

$$\Phi : \mathcal{P}(M) \rightarrow \mathcal{P}(M) \quad \Phi(X) = M \setminus g_2(N \setminus g_1(X))$$

Nun gilt für alle Mengen  $X, Y \in \mathcal{P}(M)$  die folgende logische Implikation:

$$\begin{aligned} X \subseteq Y &\implies g_1(X) \subseteq g_1(Y) && \text{Eigenschaft Bild} \\ &\implies N \setminus g_1(X) \supseteq N \setminus g_1(Y) && \text{Eigenschaft Differenz} \\ &\implies g_2(N \setminus g_1(X)) \supseteq g_2(N \setminus g_1(Y)) && \text{Eigenschaft Bild} \\ &\implies M \setminus g_2(N \setminus g_1(X)) \subseteq M \setminus g_2(N \setminus g_1(Y)) && \text{Eigenschaft Differenz} \\ &\iff \Phi(X) \subseteq \Phi(Y) \end{aligned}$$

Nach Satz 4.1.3, dem Fixpunktsatz von Knaster, gibt es also eine Menge  $X^\circ \in \mathcal{P}(M)$  mit der Eigenschaft  $\Phi(X^\circ) = X^\circ$ . Die Definition der Funktion  $\Phi$  bringt diese Gleichung in die Form  $M \setminus g_2(N \setminus g_1(X^\circ)) = X^\circ$ . Wenden wir auf beide Seiten dieser Gleichung noch die Differenzbildung  $A \mapsto M \setminus A$  an, so folgt schließlich

$$g_2(N \setminus g_1(X^\circ)) = M \setminus X^\circ.$$

Damit liegt die folgende Situation vor:

- (a) Die Menge  $M$  ist die disjunkte Vereinigung von  $M \setminus X^\circ$  und  $X^\circ$ .
- (b) Die Menge  $N$  ist die disjunkte Vereinigung von  $N \setminus g_1(X^\circ)$  und  $g_1(X^\circ)$ .

- (c) Die Mengen  $X^\circ$  und  $g_1(X^\circ)$  stehen in einer eindeutigen Beziehung zueinander durch die folgende bijektive Funktion:

$$h_1 : X^\circ \rightarrow g_1(X^\circ) \quad h_1(x) = g_1(x)$$

- (d) Die Mengen  $N \setminus g_1(X^\circ)$  und  $M \setminus X^\circ$  stehen in einer eindeutigen Beziehung zueinander durch die folgende bijektive Funktion:

$$h_2 : N \setminus g_1(X^\circ) \rightarrow M \setminus X^\circ \quad h_2(y) = g_2(y)$$

Mit Hilfe der Umkehrfunktion  $h_2^{-1} : M \setminus X^\circ \rightarrow N \setminus g_1(X^\circ)$  definieren wir nun die folgende Funktion (welche genau die ist, die wir suchen):

$$f : M \rightarrow N \quad f(x) = \begin{cases} g_1(x) & \text{falls } x \in X^\circ \\ h_2^{-1}(x) & \text{falls } x \notin X^\circ \end{cases}$$

Wir zeigen zuerst, dass die Funktion  $f$  injektiv ist. Zum Beweis seien  $x, y \in M$  beliebig vorgegeben. Wir unterscheiden vier Fälle:

- (a) Es gelte  $x, y \in X^\circ$ . Dann rechnen wir wie folgt unter der Verwendung der Definition von  $f$  und der Injektivität von  $g_1$ :

$$f(x) = f(y) \iff g_1(x) = g_1(y) \implies x = y$$

- (b) Es sei  $x \notin X^\circ$  und  $y \notin X^\circ$ . Hier haben wir aufgrund der Definition von  $f$  und der Injektivität von  $h_2^{-1}$ , dass

$$f(x) = f(y) \iff h_2^{-1}(x) = h_2^{-1}(y) \implies x = y.$$

- (c) Es sei  $x \in X^\circ$  und  $y \notin X^\circ$ . Wegen  $f(x) \in g_1(X^\circ)$  und  $f(y) = h_2^{-1}(y) \in N \setminus g_1(X^\circ)$  ist dann die Gleichung  $f(x) = f(y)$  falsch. Also gilt die zu verifizierende Implikation

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

- (d) Es sei  $x \notin X^\circ$  und  $y \in X^\circ$ . Hier geht man wie in Fall (c) vor.

Es ist  $f$  auch surjektiv, also insgesamt bijektiv. Zum Beweis der Surjektivität sei  $y \in N$  beliebig vorgegeben. Wir unterscheiden zwei Fälle:

- (a) Es sei  $y \in g_1(X^\circ)$ . Dann gibt es  $x \in X^\circ$  mit  $g_1(x) = y$ . Diese Eigenschaft impliziert mittels der Definition von  $f$  die Gleichung

$$f(x) = g_1(x) = y.$$

- (b) Es sei  $y \in N \setminus g_1(X^\circ)$ . Weil die Funktion  $h_2^{-1}$  surjektiv ist, gibt es ein  $x \in M \setminus X^\circ$  mit  $h_2^{-1}(x) = y$ . Dies bringt schließlich, wiederum mittels der Definition von  $f$ , dass

$$f(x) = h_2^{-1}(x) = y.$$

Damit ist der gesamte Beweis erbracht.  $\square$

Der eben bewiesene Satz zeigt, dass die bei endlichen Mengen  $M$  und  $N$  und der ursprünglichen Festlegung der Kardinalität (siehe Definition 1.3.6) gültige logische Äquivalenz

$$|M| \leq |N| \wedge |N| \leq |M| \iff |M| = |N|$$

gültig bleibt, wenn  $M$  und  $N$  beliebige Mengen sind und Definition 5.2.1 zum Vergleich der Kardinalitäten verwendet wird. Der Satz ist ein sehr wichtiges Hilfsmittel beim Nachweis der Gleichmächtigkeit von Mengen. Wir skizzieren nachfolgend zwei Anwendungen und empfehlen der Leserin oder dem Leser zu Übungszwecken, die Beweise im Detail auszuformulieren.

### 5.2.6 Beispiele: Anwendungen des Satzes von Schröder-Bernstein

Zuerst kann mit der Hilfe von Satz 5.2.5 sofort die folgende logische Implikation für alle Mengen  $M$ ,  $N$  und  $P$  bewiesen werden:

$$M \subseteq N \subseteq P \wedge |M| = |P| \implies |M| = |N| = |P|$$

Man muss dazu nur bedenken, dass eine Teilmengenbeziehung durch ein identisches Abbilden eine injektive Funktion nach sich zieht.

Weiterhin kann man mit dem Satz von Schröder und Bernstein beweisen, dass es eine Bijektion zwischen der Potenzmenge der Menge  $\mathbb{N}$  und der Menge aller Funktionen auf der Menge  $\mathbb{N}$  gibt. Solch ein Beweis wird nachfolgend skizziert, wobei  $\mathbb{N}^{\mathbb{N}}$  die Menge aller Funktionen auf  $\mathbb{N}$  bezeichne. Zuerst verwenden wir  $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$  und, dass daraus folgt  $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N} \times \mathbb{N})|$ . Weil jede Funktion per Definition eine Relation ist, haben wir  $|\mathbb{N}^{\mathbb{N}}| \leq |\mathcal{P}(\mathbb{N} \times \mathbb{N})|$ . Das eben erwähnte Resultat zeigt folglich  $|\mathbb{N}^{\mathbb{N}}| \leq |\mathcal{P}(\mathbb{N})|$ . Zum Beweis von  $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{N}^{\mathbb{N}}|$  ordnen wir jeder Menge  $M \in \mathcal{P}(\mathbb{N})$  die sogenannte **charakteristische Funktion** zu, welche wie folgt definiert ist:

$$\chi_M : \mathbb{N} \rightarrow \mathbb{N} \quad \chi_M(x) = \begin{cases} 1 & \text{falls } x \in M \\ 0 & \text{falls } x \notin M \end{cases}$$

Die Zuordnung  $M \mapsto \chi_M$  von  $M$  zu  $\chi_M$  liefert, wie man leicht verifiziert, eine injektive Funktion von  $\mathcal{P}(\mathbb{N})$  nach  $\mathbb{N}^{\mathbb{N}}$ . Den Rest erledigt der Satz von Schröder-Bernstein.  $\square$

Mit dem zuletzt skizzierten Ansatz kann man durch einige weitere Überlegungen auch die schon erwähnte Beziehung  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$  herleiten. Man fasst dazu jede Funktion  $f : \mathbb{N} \rightarrow \{0, 1\}$  in der Folgenschreibweise  $(f_n)_{n \in \mathbb{N}}$  als eine reelle Zahl in der Binärdarstellung  $0.f_0f_1f_2\dots$  auf und zeigt, mit der Definition  $[0, 1] := \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ , dass  $[0, 1]$  in einer Eins-zu-Eins-Beziehung zu der Menge  $\{0, 1\}^{\mathbb{N}}$  der Funktionen von  $\mathbb{N}$  nach  $\{0, 1\}$  steht. Doppelte Darstellungen, wie  $0.1000\dots$  und  $0.0111\dots$ , sind dabei gesondert zu behandeln; wir wollen darauf aber nicht eingehen. Wenn man das Ziel von  $\chi_M$  auf  $\{0, 1\}$  einschränkt, so zeigt dies, dass auch  $\mathcal{P}(\mathbb{N})$  mittels  $M \mapsto \chi_M$  in einer Eins-zu-Eins-Beziehung zur Menge  $\{0, 1\}^{\mathbb{N}}$  steht. Nun brauchen wir nur noch eine bijektive Funktion von  $\mathbb{R}$  nach  $[0, 1]$ , um  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$  zu erhalten. Formal werden solche in jeder Analysis-Vorlesung und jedem Analysis-Lehrbuch definiert.

Die Bezeichnung in der Literatur hinsichtlich des Satzes von Schröder-Bernstein ist leider etwas uneinheitlich. Manchmal wird Satz 5.2.5 auch als Satz von Cantor-Bernstein oder Satz von Cantor-Bernstein-Schröder bezeichnet. Sonderbarerweise wird bei der Namensgebung nirgendwo der deutsche Mathematiker Richard Dedekind (1831-1916) erwähnt, der den Satz 1887 erstmals bewies, den Beweis aber nicht publizierte.

## 5.3 Wachstum spezieller Funktionen

In der Informatik werden die von einem Algorithmus (oder einem Programm, welches ihn implementiert) verwendeten Ressourcen, in der Regel der notwendige Speicherplatz und die Anzahl der benötigten Rechenschritte, normalerweise in Abhängigkeit von der Eingabegröße nach oben abgeschätzt. Ist  $n \in \mathbb{N}$  die Eingabegröße, etwa die Länge einer zu sortierenden linearen Liste oder die Tiefe eines Suchbaums, in dem ein bestimmtes Element gesucht wird, so wird die Abschätzung oftmals umgangssprachlich in der folgenden Form gegeben: Der Algorithmus braucht größtenteils  $f(n)$  Schritte und  $g(n)$  Speicherplatz. Genau wird dies normalerweise in der Lehrbuch-Literatur über Datenstrukturen und effiziente Algorithmen behandelt; wir gehen am Ende dieses Abschnitts kurz auf den dem zugrunde liegenden entscheidenden Begriff ein. Bei Angaben der obigen Form spielen in  $f(n)$  und  $g(n)$  die folgenden Funktionen eine entscheidende Rolle:

- (1) Potenzfunktionen und Wurzelfunktionen
- (2) Exponentialfunktionen und Logarithmusfunktionen

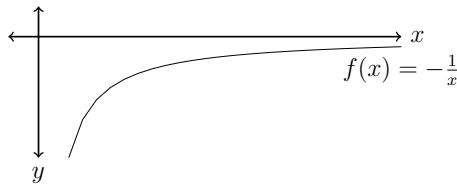
Diesen speziellen Funktionen und deren Wachstumsverhalten wollen wir uns nun widmen. Wenn man sie auf den reellen Zahlen betrachtet, so sind alle diese Funktionen **stetig**. Was dies genau heißt, ist vielleicht von der höheren Schule her bekannt, in der Regel dort aber nicht (mathematisch) formal definiert worden. Man kann die Stetigkeit einer Funktion auf reellen Zahlen formal auch nur erklären, wenn man die reellen Zahlen im Hinblick auf Grenzwertbildungen genau kennt, sie also diesbezüglich auch formal erklärt hat. Dieser Stoff wird normalerweise in jedem Lehrbuch über Analysis behandelt. Eine naive und anschauliche Beschreibung der Stetigkeit bei Funktionen  $f : M \rightarrow \mathbb{R}$ , mit einer zusammenhängenden Teilmenge  $M$  von  $\mathbb{R}$  (etwa dem Intervall  $[0, 1]$ ) als Quelle, ist etwa dadurch gegeben, dass die graphische Darstellung von  $f$  im üblichen Koordinatensystem keine Sprünge besitzt, also der Graph ohne Absetzen des Zeichenstifts gezeichnet werden kann. Wichtig für unsere Zwecke ist die folgende Eigenschaft.

### 5.3.1 Lemma

Es seien  $M$  und  $N$  Teilmengen von  $\mathbb{R}$  und  $f : M \rightarrow N$  streng monoton und surjektiv. Dann ist  $f$  bijektiv.

**Beweis:** Aufgrund der strengen Monotonie ist  $f$  injektiv. Zusammen mit der Surjektivität bringt dies die Bijektivität.  $\square$

Aus der strengen Monotonie einer Funktion auf reellen Zahlen allein folgt noch nicht deren Bijektivität. Ein Beispiel, das diese Aussage belegt, ist etwa die Funktion  $f : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  mit der Definition  $f(x) = -\frac{1}{x}$ , wobei  $\mathbb{R}_{>0}$  die Menge der positiven reellen Zahlen bezeichnet. Nachfolgend ist  $f$  graphisch dargestellt.



Es ist  $f$  streng monoton. Für alle  $x, y \in \mathbb{R}_{>0}$  gilt nämlich:  $x < y$  impliziert  $\frac{1}{y} < \frac{1}{x}$ , also auch  $-\frac{1}{x} < -\frac{1}{y}$ , also auch  $f(x) < f(y)$ . Jedoch ist  $f$  nicht bijektiv, da  $f(x) < 0$  für alle  $x \in \mathbb{R}_{>0}$  zutrifft. Somit ist etwa 1 kein Bildelement von  $f$ .

Für Funktionen von  $\mathbb{R}$  nach  $\mathbb{R}$  (oder von einer Teilmenge  $M$  von  $\mathbb{R}$  nach einer Teilmenge  $N$  von  $\mathbb{R}$ ) ist im Fall der Bijektivität die Zeichnung der Umkehrfunktion dadurch gegeben, dass man die originale Funktion an der Hauptdiagonale durch den Nullpunkt spiegelt. Anschaulich ist damit die Aussage des folgenden Lemmas einsichtig. Wir geben natürlich auch einen formalen Beweis an.

### 5.3.2 Lemma

Es sei  $f : M \rightarrow N$  wie in Lemma 5.3.1 als streng monoton und surjektiv vorausgesetzt. Dann ist die bijektive Umkehrfunktion  $f^{-1} : N \rightarrow M$  auch streng monoton.

**Beweis:** Dass Umkehrfunktionen bijektiver Funktionen bijektiv sind, wissen wir bereits. Es ist also noch die strenge Monotonie von  $f^{-1} : N \rightarrow M$  zu beweisen. Dazu seien  $x, y \in N$  mit  $x < y$  vorgegeben. Es ist  $f^{-1}(x) < f^{-1}(y)$  zu zeigen. Dazu führen wir einen Beweis durch Widerspruch. Angenommen,  $f^{-1}(x) < f^{-1}(y)$  gelte nicht. Dann gilt  $f^{-1}(y) \leq f^{-1}(x)$ . Nun gibt es zwei Fälle:

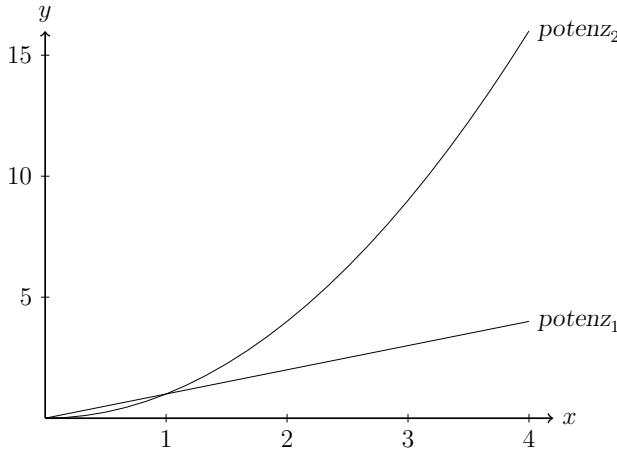
- (a) Es gelte  $f^{-1}(y) = f^{-1}(x)$ . Dann gilt  $y = f(f^{-1}(y)) = f(f^{-1}(x)) = x$  und das widerspricht  $x < y$ .
- (b) Es gelte  $f^{-1}(y) < f^{-1}(x)$ . Hier folgt  $y = f(f^{-1}(y)) < f(f^{-1}(x)) = x$  aus der strengen Monotonie von  $f$  und  $y < x$  widerspricht  $x < y$ .  $\square$

Umkehrfunktionen stetiger Funktionen sind nicht immer stetig. Dies wird normalerweise in Lehrbüchern über Analysis mittels eines Beispiels gezeigt. Wir beginnen unsere Untersuchungen spezieller Funktionen mit der Klasse der Potenzfunktionen. Im Sinne von Lemma 5.3.1 und Lemma 5.3.2 haben wir hier  $M = N = \mathbb{R}_{\geq 0}$ . Diese Wahl von Quelle und Ziel ist wesentlich für die Bijektivität. Da  $x^0 = 1$  für alle  $x \in \mathbb{R}_{\geq 0}$  gilt und konstantwertige Funktionen ziemlich uninteressant sind, betrachten wir nur positive Potenzen.

### 5.3.3 Definition: Potenzfunktion

Zu allen natürlichen Zahlen  $k \in \mathbb{N} \setminus \{0\}$  ist die **Potenzfunktion** mit dem Exponenten  $k$  definiert durch  $\text{potenz}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ , wobei  $\text{potenz}_k(x) = x^k$ .  $\square$

Nachfolgend sind die ersten zwei Potenzfunktionen  $\text{potenz}_1$  und  $\text{potenz}_2$  in einem Koordinatensystem graphisch angegeben.



Da Potenzfunktionen sehr schnell wachsen, sind in dem Bild die Einteilungen an den Achsen verschieden gewählt. Der Maßstab der Ordinate ist wesentlich kleiner als der der Abszisse. Schon aus den zwei Darstellungen des Bildes erkennt man die strenge Monotonie und Surjektivität der Potenzfunktionen. Beide Eigenschaften sind im Fall  $k = 0$ , also bei konstantwertigen Funktionen, offensichtlich nicht mehr gegeben. Wir beweisen nun formal die strenge Monotonie der Potenzfunktionen und gehen dabei auch auf die Probleme mit der Surjektivität ein.

#### 5.3.4 Satz: Eigenschaften Potenzfunktion

Für alle  $k \in \mathbb{N} \setminus \{0\}$  ist die Funktion  $\text{potenz}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  streng monoton und surjektiv, also bijektiv.

**Beweis:** Die strenge Monotonie zeigen wir durch Induktion nach  $k$  mit dem Induktionsbeginn 1. Formal zeigen wir also die Gültigkeit von  $\forall k \in \mathbb{N} : k \geq 1 \Rightarrow A(k)$ , wobei  $A(k)$  definiert ist als  $\forall x, y \in \mathbb{R}_{\geq 0} : x < y \Rightarrow x^k < y^k$ .

Induktionsbeginn, d.h. Beweis von  $A(1)$ . Für beliebige  $x, y \in \mathbb{R}_{\geq 0}$  ist die folgende Implikation wahr:

$$x < y \Rightarrow x^1 < y^1.$$

Induktionsschluss, d.h. Beweis von  $A(k+1)$  aus  $A(k)$ , wobei  $k \geq 1$  beliebig vorgegeben ist. Es seien wiederum  $x, y \in \mathbb{R}_{\geq 0}$  irgendwelche positive reelle Zahlen. Dann können wir aufgrund bekannter Eigenschaften der Potenzen wie folgt rechnen:

$$\begin{aligned} x < y &\implies x^k < y^k && \text{Induktionshypothese } A(k) \\ &\implies x x^k < y y^k && \text{weil } x, y, x^k, y^k \in \mathbb{R}_{\geq 0} \\ &\iff x^{k+1} < y^{k+1} \end{aligned}$$

Diese logische Implikation zeigt die Gültigkeit von  $x < y \Rightarrow x^{k+1} < y^{k+1}$ .

Die Surjektivität der Potenzfunktionen können wir mit unseren Mitteln nicht behandeln.

Sie wird üblicherweise in jedem Analysis-Lehrbuch bewiesen. Dort wird unter der Verwendung einer speziellen Eigenschaft der Menge der reellen Zahlen formal gezeigt, dass für alle  $y \in \mathbb{R}_{\geq 0}$  ein  $x \in \mathbb{R}_{\geq 0}$  mit der Eigenschaft  $x^k = y$  existiert (sogenannte Existenz der  $k$ -ten Wurzel von  $y$ ).

Die Bijektivität der Potenzfunktionen folgt dann aus der strengen Monotonie und der Surjektivität aufgrund von Lemma 5.3.1.  $\square$

Nach Satz 5.3.4 besitzt die Potenzfunktion  $\text{potenz}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ , mit  $k > 0$ , eine Umkehrfunktion  $\text{potenz}_k^{-1} : \mathbb{R}_{>0} \rightarrow \mathbb{R}_{\geq 0}$ , die bijektiv und, wegen Lemma 5.3.2, auch streng monoton ist. Diese Umkehrfunktion wird eigens bezeichnet.

### 5.3.5 Definition: Wurzelfunktion

Die Umkehrfunktion  $\text{potenz}_k^{-1} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ , wobei  $k > 0$ , heißt die  $k$ -te **Wurzelfunktion**. Sie wird mit  $\text{wurzel}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  bezeichnet und statt  $\text{wurzel}_k(x)$  schreibt man auch  $\sqrt[k]{x}$ . Im Fall  $k = 2$  kürzt man  $\sqrt[2]{x}$  zu  $\sqrt{x}$  ab.  $\square$

Aufgrund dieser Festlegung bekommen wir sofort die folgenden (aus der höheren Schule bekannten) zwei Rechenregeln für das Potenzieren und das Wurzelziehen (oder: Radizieren). Für alle  $k \in \mathbb{N} \setminus \{0\}$  und alle  $x \in \mathbb{R}_{\geq 0}$  gilt

- (1)  $\sqrt[k]{x^k} = x$ , was  $\text{potenz}_k^{-1}(\text{potenz}_k(x)) = x$  entspricht, und
- (2)  $(\sqrt[k]{x})^k = x$ , was  $\text{potenz}_k(\text{potenz}_k^{-1}(x)) = x$  entspricht.

Bezüglich des Wachstums von Potenzfunktionen und Wurzelfunktionen hat man die folgenden drei Beziehungen, welche ebenfalls aus der höheren Schule bekannt sind. Sie zeigen, dass das Wachstumsverhalten dieser Funktionen abhängig ist von der Größe der Eingabe. Es seien  $k \in \mathbb{N} \setminus \{0\}$  und  $x \in \mathbb{R}_{\geq 0}$  gegeben. Dann gelten:

- (3)  $\sqrt[k+1]{x} < \sqrt[k]{x} < x < x^k < x^{k+1}$ , falls  $x > 1$ .
- (4)  $\sqrt[k+1]{x} = \sqrt[k]{x} = x = x^k = x^{k+1}$ , falls  $x = 1$  oder  $x = 0$ .
- (5)  $\sqrt[k+1]{x} > \sqrt[k]{x} > x > x^k > x^{k+1}$ , falls  $0 < x < 1$ .

Bei diesen drei Beziehungen ist die Voraussetzung  $k \neq 0$  nötig, da  $x < x^0 = 1$  natürlich für  $x > 1$  nicht gilt und auch  $x > x^0 = 1$  für  $x < 1$  falsch ist.

Nach den  $k$ -ten Potenzfunktionen  $\text{potenz}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  und deren Umkehrfunktionen, den  $k$ -ten Wurzelfunktionen  $\text{wurzel}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ , welche alle auf den positiven reellen Zahlen definiert sind, kommen wir nun zu den Exponentialfunktionen und deren Umkehrfunktionen, den Logarithmusfunktionen. Exponentialfunktionen lassen beliebige reelle Eingaben zu, haben also  $\mathbb{R}$  als Quelle. Sie liefern aber nur positive Werte. Damit haben sie  $\mathbb{R}_{>0}$  als Ziel. Logarithmusfunktionen lassen hingegen nur positive Eingaben zu. Dafür liefern sie beliebige Werte. Wir behandeln nachfolgend nur den Spezialfall zur Basis 2, da dieser für die Informatik der wichtigste Fall ist. Die Funktionalität der entsprechenden Exponentialfunktion ergibt sich aus der obigen Beobachtung. Sie ist wesentlich, da sonst die gewünschte Bijektivität nicht erhalten wird.

### 5.3.6 Definition: Exponentialfunktion

Die **Exponentialfunktion**  $\exp_2 : \mathbb{R} \rightarrow \mathbb{R}_{>0}$  zur Basis 2 (oder duale Exponentialfunktion) ist definiert durch  $\exp_2(x) = 2^x$ .  $\square$

Die Bildung von Exponentialausdrücken der Form  $a^b$  ist sicher auch von der höheren Schule her bekannt. Wir setzen für das Folgende das dadurch gegebene intuitive Verständnis des Ausdrucks  $2^x$  voraus. Was bedeutet aber nun  $2^x$  genau? Für  $x \in \mathbb{N}$  kann man  $2^x$  formal rekursiv festlegen durch die Gleichungen  $2^0 := 1$  und  $2^{x+1} := 2 \cdot 2^x$ . Dadurch bekommt man etwa durch termmäßiges Auswerten

$$2^3 = 2 \cdot 2^2 = 2 \cdot 2 \cdot 2^1 = 2 \cdot 2 \cdot 2 \cdot 2^0 = 2 \cdot 2 \cdot 2 \cdot 1 = 8.$$

Auch den Fall einer negativen ganzen Zahl, also  $x \in \mathbb{Z} \setminus \mathbb{N}$ , kann man formal erklären. Mittels der (hoffentlich von der höheren Schule her) bekannten Regel  $2^x = \frac{1}{2^{-x}}$  führt man ihn auf den ersten Fall zurück. Für  $2^{-3}$  ergibt sich also

$$2^{-3} = \frac{1}{2^3} = \frac{1}{8} = 0.125$$

als Wert. Gleichermaßen gilt auch noch für rationale Zahlen, also für  $x \in \mathbb{Q}$ . Für  $m, n \in \mathbb{N}$  und  $n \neq 0$  ergibt sich nämlich, nach bekannten (Schul-)Regeln, dass  $2^{\frac{m}{n}} = \sqrt[n]{2^m}$  und dass  $2^{-\frac{m}{n}} = \frac{1}{\sqrt[n]{2^m}}$ . Also bekommen wir etwa

$$2^{\frac{3}{4}} = \sqrt[4]{2^3} = \sqrt[4]{8} = 1.6817$$

(gerundet). Den verbleibenden Fall  $x \in \mathbb{R} \setminus \mathbb{Q}$ , also etwa  $2^{\sqrt{2}}$ , können wir in diesem Text wiederum aufgrund von fehlenden Mitteln nicht formal erklären. Hier benötigt man zur Definition von  $2^x$  die Exponentialfunktion zur Basis  $e$  (der Eulerschen Zahl  $2.7182\dots$ ); dies ist normalerweise wiederum Stoff von Analysis-Lehrbüchern. Auch der folgende Satz wird in so einem Buch bewiesen.

### 5.3.7 Satz: Eigenschaften Exponentialfunktion

Die Funktion  $\exp_2 : \mathbb{R} \rightarrow \mathbb{R}_{>0}$  ist streng monoton und surjektiv, also bijektiv.  $\square$

Als Konsequenz haben wir, dass die Exponentialfunktion  $\exp_2 : \mathbb{R} \rightarrow \mathbb{R}_{>0}$  zur Basis 2 eine Umkehrfunktion  $\exp_2^{-1} : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  besitzt. Wir legen fest:

### 5.3.8 Definition: Logarithmusfunktion

Die Umkehrfunktion  $\exp_2^{-1} : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  wird als **Logarithmusfunktion zur Basis 2** bezeichnet (oder als dualer Logarithmus). Man schreibt  $\log_2 : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  und kürzt  $\log_2(x)$  auch zu  $\log x$  oder  $\text{ld } x$  (logarithmus dualis) ab.  $\square$

Bezüglich der Exponentiation und der Logarithmisierung, also der Anwendungen der Funktionen  $\exp_2$  und  $\log_2$ , gelten die Eigenschaften

- (1)  $\log_2(2^x) = x$  für alle  $x \in \mathbb{R}$ , was  $\exp_2^{-1}(\exp_2(x)) = x$  entspricht, und
- (2)  $2^{\log_2(x)} = x$  für alle  $x \in \mathbb{R}_{>0}$ , was  $\exp_2(\exp_2^{-1}(x)) = x$  entspricht.

Im nächsten Satz 5.3.11, der das Hauptresultat dieses Abschnitts darstellt, vergleichen wir nun das Wachstum von allen Potenzfunktionen und der Exponentialfunktion zur Basis 2. Wir tun dies aber nur für **Argumente aus der Menge  $\mathbb{N}$  der natürlichen Zahlen**, da dies für die Aufwandsabschätzungen von Algorithmen in der Informatik wesentlich ist, weil deren Eingaben immer eine natürliche Zahl als Größe zugeordnet wird. Unser ultimatives Ziel ist zu zeigen, dass bezüglich des Wachstums jede Potenzfunktion schließlich irgendwann von der Exponentialfunktion zur Basis 2 übertroffen wird – man muss nur die Argumente groß genug wählen. Zur Vereinfachung des Beweises dieses Resultats formulieren wir zuerst zwei Hilfsaussagen in der Form von zwei Lemmata. Hier ist das erste davon, welches nur natürliche Zahlen behandelt.

### 5.3.9 Lemma

Für alle  $n \in \mathbb{N}$  gilt  $2^{n+1} \geq n^2 + n$ .

**Beweis:** Für  $n \in \{0, 1\}$  gilt das Lemma aufgrund von  $2 \geq 0$  und  $4 \geq 2$ . Nun zeigen wir durch vollständige Induktion, dass die Aussage  $2^{n+1} \geq n^2 + n$  für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  wahr ist. Es ist also die das Lemma zu  $\forall n \in \mathbb{N} : A(n)$  formalisierende Aussage  $A(n)$  gleich  $2^{n+1} \geq n^2 + n$ .

Induktionsbeginn: Der Beweis von  $A(2)$  folgt aus  $8 \geq 6$ .

Induktionsschluss: Zum Beweis von  $A(n+1)$  aus  $A(n)$  sei  $n \in \mathbb{N}$  beliebig vorausgesetzt. Weiterhin seien  $n \geq 2$  und  $A(n)$  angenommen. Dann gilt die Ungleichung

$$2^{n+2} = 2 \cdot 2^{n+1} \geq 2(n^2 + n) = 2n^2 + 2n = n^2 + 2n + n^2$$

aufgrund der Induktionshypothese  $A(n)$ . Rechnen wir von der anderen Seite der zu beweisenden Abschätzung her, so bekommen wir die Gleichung

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

Wegen  $n \geq 2$  gilt schließlich noch

$$2 + n \leq n + n \leq n^2$$

und diese Ungleichung zeigt mit den obigen Rechnungen die gewünschte Abschätzung  $2^{n+2} \geq (n+1)^2 + (n+1)$ , also  $A(n+1)$ .  $\square$

Wie schon erwähnt, beweisen wir noch eine weitere Hilfsaussage, bevor wir den eigentlichen Satz formulieren und beweisen. In dieser wird eine Aussage gemacht, die natürliche Zahlen und reelle Zahlen aus  $[0, 1]$  betrifft.

### 5.3.10 Lemma

Für alle  $n \in \mathbb{N}$  und  $a \in \mathbb{R}$  mit  $0 \leq a \leq 1$  gilt  $(1+a)^n \leq 1 + (2^n - 1)a$ .

**Beweis:** Wir beweisen durch vollständige Induktion die Aussage  $\forall n \in \mathbb{N} : A(n)$ , wobei  $A(n)$  die Formel  $\forall a \in \mathbb{R} : 0 \leq a \leq 1 \Rightarrow (1+a)^n \leq 1 + (2^n - 1)a$  abkürzt.

Induktionsbeginn, d.h. Beweis von  $A(0)$ . Dies folgt daraus, dass für alle  $a \in \mathbb{R}$  mit  $0 \leq a \leq 1$  die folgende Gleichung gilt:

$$(1+a)^0 = 1 = 1 + 0 \cdot a = 1 + (2^0 - 1)a$$

Induktionsschluss, d.h. Beweis von  $A(n+1)$  aus  $A(n)$  für alle  $n \in \mathbb{N}$ . Es sei dazu  $a \in \mathbb{R}$  mit  $0 \leq a \leq 1$  vorgegeben. Dann rechnen wir wie folgt:

$$\begin{aligned} (1+a)^{n+1} &= (1+a)^n(1+a) && \text{Potenzdefinition} \\ &\leq (1+(2^n-1)a)(1+a) && \text{Induktionshypothese } A(n) \\ &= 1+a+(2^n-1)a+(2^n-1)a^2 && \text{Distributivit\"at} \\ &\leq 1+a+(2^n-1)a+(2^n-1)a && a \leq 1 \text{ impliziert } a^2 \leq a \\ &= 1+a+2(2^n-1)a \\ &= 1+a+2^{n+1}a-2a \\ &= 1+2^{n+1}a-a \\ &= 1+(2^{n+1}-1)a \end{aligned}$$

Dies zeigt die gew\"unschte Absch\"atzung des Induktionsschlusses und damit ist der gesamte Beweis beendet.  $\square$

Nun k\"onnen wir endlich den schon angek\"undigten Satz beweisen, der besagt, dass jede  $k$ -te Potenzfunktion  $\text{potenz}_k : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  schlie\l{}lich durch die Exponentialfunktion  $\exp_2 : \mathbb{R} \rightarrow \mathbb{R}_{>0}$  \"ubertroffen wird. Die Exponentialfunktion w\"achst also insgesamt st\"arker als jede Potenzfunktion.

### 5.3.11 Satz: Exponentiation \"ubertrifft irgendwann Potenzierung

Es sei die Zahl  $k \in \mathbb{N} \setminus \{0\}$  beliebig vorgegeben. Dann gilt f\"ur alle  $n \in \mathbb{N}$  mit der Eigenschaft  $n \geq 2^{k+1}$ , dass  $2^n \geq n^k$ .

**Beweis:** Wir betrachten zu der vorgegebenen Zahl  $k \in \mathbb{N} \setminus \{0\}$  die folgende allquantifizierte Formel, in der  $k$  als Konstante aufgefasst wird:

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

Der Beweis ist erbracht, wenn diese Formel als g\"ultig bewiesen ist. Letzteres bewerkstelligen wir nachfolgend durch eine vollst\"andige Induktion, wobei  $A(n)$  der Formel  $2^n \geq n^k$  entspricht und  $2^{k+1}$  der Induktionsbeginn ist. Dabei machen wir explizit Gebrauch von der in Abschnitt 4.5 beschriebenen reduzierenden Vorgehensweise.

Induktionsbeginn: Zum Beweis von  $A(2^{k+1})$  starten wir mit der folgenden Kette von logischen \\"Aquivalenzen:

$$\begin{aligned} 2^{2^{k+1}} \geq (2^{k+1})^k &\iff 2^{2^{k+1}} \geq 2^{(k+1)k} && \text{Potenzgesetz} \\ &\iff 2^{k+1} \geq (k+1)k && \text{Monotonie von } \log_2 \text{ und } \exp_2 \\ &\iff 2^{k+1} \geq k^2 + k \end{aligned}$$

Wegen Lemma 5.3.9 ist die letzte Formel wahr, also ist auch die erste Formel wahr, die es zu beweisen gilt.

Induktionsschluss von  $A(n)$  nach  $A(n + 1)$  für  $n \in \mathbb{N}$  mit  $n \geq 2^{k+1}$  beliebig vorgegeben. Hier bekommen wir unter Verwendung der Induktionshypothese  $A(n)$  die Eigenschaft

$$2^{n+1} = 2 \cdot 2^n \geq 2n^k$$

und wir müssen deshalb nur noch  $2n^k \geq (n + 1)^k$  beweisen, damit  $A(n + 1)$  wahr wird. Es gilt die logische Äquivalenz

$$2n^k \geq (n + 1)^k \iff 2 \geq \frac{(n + 1)^k}{n^k} \iff 2 \geq \left(1 + \frac{1}{n}\right)^k$$

wegen  $\frac{(n+1)^k}{n^k} = \left(\frac{n+1}{n}\right)^k$ . Aufgrund dieser Reduktion haben wir nur noch  $\left(1 + \frac{1}{n}\right)^k \leq 2$  zu verifizieren. Wegen  $0 \leq \frac{1}{n} \leq 1$  kommt nun Lemma 5.3.10 zur Anwendung. Mit dessen Hilfe erhalten wir

$$\begin{aligned} \left(1 + \frac{1}{n}\right)^k &\leq 1 + (2^k - 1) \cdot \frac{1}{n} && \text{Lemma 5.3.10} \\ &\leq 1 + (2^k - 1) \cdot \frac{1}{2^{k+1}} && n \geq 2^{k+1} \text{ impliziert } \frac{1}{n} \leq \frac{1}{2^{k+1}} \\ &= 1 + \frac{2^k}{2^{k+1}} - \frac{1}{2^{k+1}} && \text{da } \frac{1}{2^{k+1}} \geq 0 \\ &\leq 1 + \frac{2^k}{2 \cdot 2^k} && \\ &= 1 + \frac{1}{2} \\ &\leq 2 \end{aligned}$$

und durch diesen Beweis von  $\left(1 + \frac{1}{n}\right)^k \leq 2$  sind wir fertig.  $\square$

Unter Verwendung der ursprünglichen Schreibweisen für Potenzfunktionen und Exponentialfunktionen erhalten wir Satz 5.3.11 als folgende Formel:

$$\forall k \in \mathbb{N} \setminus \{0\}, n \in \mathbb{N} : n \geq \exp_2(k + 1) \Rightarrow \exp_2(n) \geq \text{potenz}_k(n)$$

Diese Eigenschaft ist insbesondere in der Informatik bei der Bewertung von Algorithmen von Bedeutung, wie sie am Anfang dieses Abschnitts schon skizziert wurde. Schätzt man den Aufwand eines vorgegebenen Algorithmus nach oben durch eine **Aufwandsfunktion** ab, deren Eingabe die Problemgröße ist, so spricht man im Jargon von einer **Worst-case** oder **pessimistischen Analyse**. Da man in der Regel über die konkret vorliegenden Problemgrößen nichts aussagen kann, lässt man diese im Prinzip gegen Unendlich gehen. Dies nennt man dann eine **asymptotische Abschätzung**. Theoretisch liegt dieser Vorgehensweise der folgende Begriff zugrunde.

### 5.3.12 Definition: asymptotische Beschränkung

Die Funktion  $g : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  wird von der Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  **asymptotisch beschränkt**, falls ein  $c \in \mathbb{R}_{>0}$  und ein  $m \in \mathbb{N}$  so existieren, dass  $g(n) \leq c f(n)$  für alle

$n \in \mathbb{N}$  mit  $n \geq m$  gilt. Mit  $\mathcal{O}(f)$  bezeichnet man die Menge aller von  $f$  asymptotisch beschränkten Funktionen.  $\square$

Die Notation  $\mathcal{O}(f)$  geht auf die deutschen Mathematiker Paul Bachmann (1837-1920) und Edmund Landau (1877-1938) zurück, welche sie bei zahlentheoretischen Untersuchungen einführten. Man nennt  $\mathcal{O}$  heutzutage ein **Landau-Symbol**. Es gibt noch weitere Landau-Symbole, auf die wir aber nicht eingehen wollen.

Ist die Aufwandsfunktion eines Algorithmus etwa aus  $\mathcal{O}(\text{potenz}_2)$ , wobei die Quelle von  $\text{potenz}_2$  auf  $\mathbb{N}$  eingeschränkt ist, so wächst der Aufwand bei der Berechnung um das Vierfache, wenn sich die Eingabegröße verdoppelt. Bei einer Aufwandsfunktion aus  $\mathcal{O}(\exp_2)$ , wobei die Quelle wiederum  $\mathbb{N}$  sei und das Ziel nun  $\mathbb{R}_{\geq 0}$ , wächst der Aufwand um das Doppelte, wenn sich die Eingabegröße nur um 1 erhöht. Unter der Verwendung der Varianten  $\text{potenz}_k : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  und  $\exp_2 : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  der Originalfunktionen der Definitionen 5.3.3 und 5.3.6 lautet Satz 5.3.11 wie folgt:

### 5.3.13 Korollar

Für alle  $k \in \mathbb{N} \setminus \{0\}$  gilt  $\text{potenz}_k \in \mathcal{O}(\exp_2)$ .  $\square$

Natürlich gilt für die Varianten  $\text{potenz}_k : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  und  $\text{potenz}_{k+1} : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  auch  $\text{potenz}_k \in \mathcal{O}(\text{potenz}_{k+1})$  für alle  $k \in \mathbb{N} \setminus \{0\}$ . Es ist nämlich beispielsweise  $n^k \leq 1 \cdot n^{k+1}$  für alle  $n \geq 0$ . Hingegen gilt etwa  $\text{potenz}_2 \in \mathcal{O}(\text{potenz}_1)$  nicht. Dazu ist zu zeigen, dass die Formel

$$\exists c \in \mathbb{R}_{>0}, m \in \mathbb{N} : \forall n \in \mathbb{N} : n \geq m \Rightarrow n^2 \leq cn$$

nicht gilt, also die Formel

$$\forall c \in \mathbb{R}_{>0}, m \in \mathbb{N} : \exists n \in \mathbb{N} : n \geq m \wedge n^2 > cn$$

gilt. Letzteres ist aber einfach. Sind  $c \in \mathbb{R}_{>0}$  und  $m \in \mathbb{N}$  beliebig vorgegeben, so wählt man  $n := m$  im Fall  $m > c$  und  $n := \min\{x \in \mathbb{N} \mid c < x\}$  im Fall  $m \leq c$ . Dann gilt in beiden Fällen  $n \geq m \wedge n > c$ , also auch  $n \geq m \wedge n^2 > cn$ .

Formal hat beim Verwenden des Landau-Symbols die Funktionalität wie in Definition 5.3.12 gefordert vorzuliegen. Dies bedingt, wie eben gezeigt, oftmals die Anpassung von Quellen- und Zielmengen von Funktionen. In der mathematischen Praxis werden solche Anpassungen in der Regel implizit vorgenommen, also nicht eigens erwähnt. Normalerweise verwendet man beim Landau-Symbol auch eine vereinfachende Schreibweise und setzt statt Bezeichner für Funktionen direkt die sie beschreibenden Ausdrücke ein. Beim Korollar schreibt man also kürzer  $n^k \in \mathcal{O}(2^n)$ . Oft wird das Landau-Symbol zur Verkürzung der Schreibweisen auch im Rahmen von Ausdrücken verwendet. Beispielsweise bedeutet  $n + \mathcal{O}(\frac{1}{n+1})$  eigentlich  $n + f(n)$ , mit  $f \in \mathcal{O}(\frac{1}{n+1})$ . Dadurch drückt man in dem vorliegenden Fall aus, dass der Wert von  $n + \mathcal{O}(\frac{1}{n+1})$  sich immer mehr  $n$  nähert, wenn  $n$  gegen Unendlich strebt. Wegen dieser Auffassung ist statt  $g \in \mathcal{O}(f)$  auch die Schreibweise  $g = \mathcal{O}(f)$  üblich. Hier ist unbedingt zu beachten, dass dadurch keine Gleichheit im korrekten mathematischen Sinne definiert ist, denn sonst würde aus dem obigen Korollar ja die Gleichheit von allen Potenzfunktionen folgen – was schlichtweg Unsinn ist.

In der Praxis tauchen auch Fälle auf, bei denen es sinnvoll ist, der Eingabe eines Algorithmus mehr als eine Größe zuzuordnen. Dies bedingt dann eine Erweiterung des Landau-Symbols  $\mathcal{O}$  auf mehrstellige Funktionen. Einzelheiten hierzu findet die Leserin oder der Leser beispielsweise in der einschlägigen Informatik-Literatur.

Wir wollen zum Abschluss dieses Kapitels das Wachstumsverhalten der betrachteten Funktionen anhand eines Beispiels demonstrieren und auch die praktischen Auswirkungen ansprechen.

### 5.3.14 Beispiel: Aufwand und Laufzeiten

Wir betrachten drei Algorithmen  $\mathcal{A}_1$ ,  $\mathcal{A}_2$  und  $\mathcal{A}_3$  und die vier verschiedenen Problemgrößen  $n = 10, 30, 60, 100$ , die etwa vier verschiedene Listenlängen im Fall von Sortieralgorithmen sein können. Weiterhin betrachten wir die folgenden drei Aufwandsfunktionen, welche Größenordnungsmäßig die Zahlen der benötigten Rechenschritte in Abhängigkeit von den Eingabegrößen angeben:

$$\text{Algorithmus } \mathcal{A}_1 : \text{potenz}_2 \quad \text{Algorithmus } \mathcal{A}_2 : \text{potenz}_3 \quad \text{Algorithmus } \mathcal{A}_3 : \exp_2$$

Nun nehmen wir an, dass ein einzelner elementarer Rechenschritt eines jeden der vorliegenden Algorithmen genau  $10^{-6}$  Sekunden Rechenzeit benötigt. Dann ergeben sich die in der nachfolgenden Tabelle zusammengestellten Gesamtrechenzeiten:

| Algorithmus     | $n = 10$       | $n = 30$       | $n = 60$    | $n = 100$               |
|-----------------|----------------|----------------|-------------|-------------------------|
| $\mathcal{A}_1$ | $10^{-4}$ Sek. | $10^{-3}$ Sek. | 0.004 Sek.  | 0.01 Sek.               |
| $\mathcal{A}_2$ | $10^{-3}$ Sek. | 0.03 Sek.      | 0.2 Sek.    | 1 Sek.                  |
| $\mathcal{A}_3$ | $10^{-3}$ Sek. | 17 Min.        | 36000 Jahre | $4 \cdot 10^{15}$ Jahre |

Dabei stehen die Abkürzungen „Sek.“ bzw. „Min“ für Sekunden bzw. Minuten. Zwischen den Begriffen „Potenzierung“ und „Exponentiation“ liegt also ein Qualitätssprung. Diese Diskrepanz kann auch durch Technologiesprünge nicht behoben werden. Eine Verbesserung der Schnelligkeit eines Rechners um den Faktor 1000 bewirkt beispielsweise bei einer Aufwandsfunktion  $\text{potenz}_2$  sehr viel, bei einer Aufwandsfunktion  $\exp_2$  hingegen fast gar nichts.  $\square$

Eine heutzutage weitgehend akzeptierte Arbeitshypothese der Informatik, die vom kanadischen Mathematiker Jack Edmonds (geb. 1934) im Jahre 1964 aufgestellt wurde, besagt, dass ein Algorithmus praktikabel ist, falls es eine Zahl  $k \in \mathbb{N} \setminus \{0\}$  so gibt, dass seine Aufwandsfunktion in  $O(\text{potenz}_k)$  liegt. Praktisch relevant sind dabei nur kleine natürliche Zahlen  $k$ , etwa  $k = 0$  (konstanter Aufwand, der unabhängig ist von der Größe der Eingabe),  $k = 1$  (linearer Aufwand),  $k = 2$  (quadratischer Aufwand) und  $k = 3$  (kubischer Aufwand). Viele wichtige Probleme der Informatik können durch praktikable Algorithmen gelöst werden, beispielsweise das schon mehrfach erwähnte Sortieren von linearen Listen. Hier gibt es einfache Algorithmen mit einer Laufzeit in  $O(\text{potenz}_2)$ , also mit quadratischem Aufwand, wobei als Problemgröße die Listenlänge genommen wird. Das Suchen in linearen Listen erfordert normalerweise einen linearen Aufwand in der Listenlänge. Will man eine lineare Liste revertieren, so führt dies zu Zugriffen an beiden Listenenden. Der

Aufwand in der Listenlänge hängt dann vom Aufwand dieser Zugriffe ab.

Es gibt jedoch ebenfalls viele wichtige praktische Probleme, zu deren Lösung man bisher noch keine praktikablen Algorithmen kennt und sogar vermutet, dass es solche aus prinzipiellen Gründen gar nicht geben kann. Eines der wichtigsten davon ist das sogenannte **Erfüllbarkeitsproblem der Aussagenlogik**. Man hat hier eine aussagenlogische Formel  $A$  der speziellen Gestalt  $A_1 \wedge A_2 \wedge \dots \wedge A_n$  vorgegeben, wobei  $n > 0$  und jede Formel  $A_i$  eine Disjunktion  $D_1^{(i)} \vee D_2^{(i)} \vee \dots \vee D_k^{(i)}$  von  $k > 0$  Formeln ist, mit den  $D_j^{(i)}$  als Aussagenvariablen oder negierten Aussagenvariablen. Die Aufgabe ist, festzustellen, ob es eine Belegung der Aussagenvariablen gibt, zu welcher  $A$  den Wahrheitswert  $W$  besitzt (man sagt: erfüllbar ist). Mit der Anzahl der in  $A$  vorkommenden Aussagenvariablen als Problemgröße kennt man bisher noch keine praktikablen Algorithmen für so einen Test.

## 5.4 Einige Bemerkungen zur Berechenbarkeit von Funktionen

Bei den Funktionen, die man heutzutage üblicherweise von der höheren Schule her kennt, handelt es sich oft um ganzrationale oder rationale Funktionen. Berechnen des Funktionswerts  $f(a)$  heißt hier, dass man an Stelle des Argument-Bezeichners  $x$  (normalerweise Parameter genannt) in der Funktionsdefinition  $f(x) = \dots$  das aktuelle Argument  $a$  einsetzt und dann die so entstehende rechte Seite (den  $f(a)$  definierenden Ausdruck) soweit wie möglich auswertet. So wird beispielsweise der Wert von  $f(3)$  mit der Definition

$$f : \mathbb{Z} \rightarrow \mathbb{Z} \quad f(x) = 2x^3 - x^2 - x - 1$$

von  $f$  ausgerechnet durch

$$f(3) = 2 \cdot 3^3 - 3^2 - 3 - 1 = 54 - 9 - 3 - 1 = 41.$$

Neben den ganzrationalen oder rationalen Funktionen lernt man in der Regel auch einige trigonometrische Funktionen kennen, etwa den Sinus oder den Cosinus. Wie man solche Funktionen auf vorgegebene  $n$  Stellen nach dem Dezimalkomma genau ausrechnet, etwa  $\sin(0.123)$  bis auf 3 Stellen nach dem Komma, lernt man normalerweise nicht mehr. Da jeder noch so billige Taschenrechner dafür aber keine messbare Zeit braucht, sollte dies nicht allzu schwierig sein.

Wenn man eine bestimmte Funktion  $f$  zu einem Argument  $a$  ausrechnet, dann heißt dies genau genommen, dass man einen Algorithmus  $\mathcal{A}$  verwendet, der zur Eingabe  $a$  den Funktionswert  $f(a)$  als Ausgabe liefert. Konkret kann man sich  $\mathcal{A}$  immer als Programm in irgendeiner der derzeit gängigen Programmiersprachen vorstellen. Es gibt viele Funktionen, die sich effizient berechnen lassen, also mit praktikablen Programmen. Die Effizienz der Algorithmen und Programme hängt dabei von einigen Faktoren ab. Ein entscheidender Faktor ist z.B. die Darstellung der Daten. Eine gute Darstellung kann zu schnellen Algorithmen führen, eine weniger geeignete Darstellung zu langsameren Algorithmen. Die Darstellung von endlichen Mengen  $M$  ist ein Beispiel hierzu. Stellt man  $M$  durch eine lineare Liste dar, so benötigt die Suche nach einem Element  $\mathcal{O}(|M|)$  Schritte. Verwendet man hingegen einen Suchbaum, der ziemlich ausbalanciert ist, so sind nur  $\mathcal{O}(\log_2(|M|))$  Schritte erforderlich.

Neben den Funktionen, die sich effizient berechnen lassen, gibt es auch solche, wie schon am Ende von Abschnitt 5.3 angemerkt wurde, zu deren Berechnung man noch keine praktikablen Programme kennt und sogar vermutet, dass es solche aus prinzipiellen Gründen gar nicht geben kann. Für einige Funktionen hat man mittels mathematischer Argumentation sogar zeigen können, dass kein praktikables Programm existieren kann. Es würde den Rahmen sprengen, solch ein Beispiel hier anzugeben<sup>8</sup>. Festzuhalten ist aber, dass es bei den Funktionen eine Aufteilung gibt in diejenigen, welche sich effizient berechnen lassen, und diejenigen, welche sich nur ineffizient berechnen lassen. Eine sich daraus sofort ergebende fundamentale Frage ist: Gibt es vielleicht sogar Funktionen  $f : M \rightarrow N$ , welche sich gar nicht berechnen lassen, für die es also aus prinzipiellen Gründen kein Programm in irgendeiner Programmiersprache geben kann, das für alle Argumente  $a \in M$  als Eingabe den Funktionswert  $f(a)$  bestimmt?

Solche Fragen werden in einem Gebiet der Logik untersucht, welches sich Berechenbarkeitstheorie oder Rekursionstheorie nennt. Es stellte sich heraus, dass es solche Funktionen in der Tat gibt. Zum Beweis dieser Tatsache war es zuerst notwendig, den Begriff des Algorithmus mathematisch zu präzisieren. Eine Möglichkeit, dies zu bewerkstelligen, geht auf den englischen Mathematiker Alan Turing (1912–1954) zurück. Er entwarf eine hypothetische Maschine als, wie er meinte, Modell des „menschlichen Rechners“. Mit ihr, heute Turing-Maschine genannt, war er in der Lage, die negative Beantwortung der obigen Frage mathematisch präzise zu beweisen. Das Resultat, welches Turing im Jahr 1936 publizierte, kann gut veranschaulicht werden, wenn man Algorithmen als Programme einer Programmiersprache ansieht.

In Programmiersprachen geschriebene Programme werden heutzutage im Prinzip immer noch als Texte abgefasst – trotz aller grafischen und sonstigen Hilfsmittel. Somit kann ein Programm  $P$  als eine lineare Liste (ein Wort) aus  $A^*$  interpretiert werden, wobei  $A$  genau die Zeichen (wie `+`), zusammengesetzten Symbole (wie `<=`) und Schlüsselwörter (wie `begin`, `while`) enthält, die man beim Schreiben von Programmen in der vorgegebenen Programmiersprache verwenden darf. Man vergleiche dazu noch einmal mit den Bemerkungen am Ende von Abschnitt 3.2 zu den formalen Sprachen und ihren Wörtern als speziellen Darstellungen von linearen Listen. Auch Daten werden normalerweise als Texte abgefasst und damit kann auch die Eingabe  $a$  zu einem Programm  $P$  als eine lineare Liste (ein Wort)  $a$  aus  $A^*$  angesehen werden. Nun können Programme zu Eingaben terminieren (also nach einer endlichen Anzahl von Rechenschritten stoppen), aber auch nicht terminieren. Die von Turing betrachtete Funktion ist bei dieser Auffassung die Terminierungstest-Funktion  $t : A^* \times A^* \rightarrow \{0, 1\}$  mit der folgenden Festlegung:

$$t(P, a) = \begin{cases} 1 & \text{falls das Programm } P \text{ zur Eingabe } a \text{ terminiert} \\ 0 & \text{falls das Programm } P \text{ zur Eingabe } a \text{ nicht terminiert} \end{cases}$$

Durch Widerspruch konnte Turing zeigen, dass es, übertragen in unsere Terminologie mit Programmen als Algorithmen, kein Terminierungstest-Programm  $\mathcal{T}$  geben kann, welches für alle Eingaben  $P$  und  $a$  den Wert von  $t(P, a)$  berechnet, also 1 ausgibt, falls  $P$  zur Eingabe  $a$  terminiert, und 0 sonst ausgibt. Die Terminierung von Programmen ist also, wie man sagt, algorithmisch nicht entscheidbar.

---

<sup>8</sup>Das Teilgebiet der theoretischen Informatik, in dem dies geschieht, nennt sich Komplexitätstheorie.

Man beachte, dass gerade eine Aussage über ein Programm gemacht wurde, das mit allen nur vorstellbaren Programmen und allen nur vorstellbaren Eingaben zurecht käme. Für Spezialfälle ist es oftmals sogar sehr leicht, die Terminierung nachzuweisen. Es gibt aber auch immer noch ungelöste Terminierungsprobleme. Ein Beispiel, welches auf den deutschen Mathematiker Lothar Collatz (1910-1990) zurückgeht, ist das folgende:

```
while n > 1 do
    if even(n) then n := n/2
    else n := 3*n+1
```

Bis heute ist nicht bekannt, ob dieses Programm terminiert, falls der Eingabewert der Variablen  $n$  eine beliebige natürliche Zahl ungleich der Null ist.

## 5.5 Übungsaufgaben

### Aufgabe

Zu einer gegebenen bijektiven Funktion  $f : \mathbb{R} \rightarrow \mathbb{R}$  sei die Funktion  $g : \mathbb{R} \rightarrow \mathbb{R}$  definiert durch  $g(x) = 2 + 3f(x)$ . Zeigen Sie:

(1)  $g$  ist injektiv.

(2)  $g$  ist surjektiv.

### Aufgabe

Die Funktion  $f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$  sei durch  $f(n) = \{x \in \mathbb{N} \mid x \leq n\}$  definiert.

- (1) Beweisen Sie, dass für alle  $m, n \in \mathbb{N}$  die Eigenschaften  $m \leq n$  und  $f(m) \subseteq f(n)$  äquivalent sind.
- (2) Zeigen Sie mit Hilfe von (1) die Injektivität von  $f$ .
- (3) Kann  $f$  auch surjektiv sein (mit Begründung)?

### Aufgabe

Die  $n$ -te Potenz  $f^n : M \rightarrow M$  einer Funktion  $f : M \rightarrow M$  ist erklärt durch  $f^0 := id_M$  (mit  $id_M$  als identische Funktion auf  $M$ ) und  $f^{n+1} := f \circ f^n$  für alle  $n \in \mathbb{N}$ .

- (1) Zeigen Sie, dass  $f^m \circ f^n = f^{m+n}$  für alle  $m, n \in \mathbb{N}$  gilt.
- (2) Beweisen Sie  $f \circ f^n = f^n \circ f$  für alle  $n \in \mathbb{N}$ .
- (3) Gibt es ein  $n \in \mathbb{N} \setminus \{0\}$  mit  $f^n = id_M$ , so ist  $f$  bijektiv. Beweis!
- (4) Geben Sie drei Beispiele für Funktionen an, bei denen eine  $n$ -te Potenz zur identischen Funktion wird.

### Aufgabe

Beweisen Sie, dass das Auswahlaxiom äquivalent zu folgender Aussage ist: Für alle Mengen  $M \neq \emptyset$  gibt es eine Funktion  $f : \mathcal{P}(M) \setminus \{\emptyset\} \rightarrow M$ , so dass  $f(X) \in X$  für alle  $X \in \mathcal{P}(M) \setminus \{\emptyset\}$  gilt.

### Aufgabe

Wir betrachten die Teilmengen  $M := \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$  und  $N := \{x \in \mathbb{R} \mid 4 \leq x \leq 7\}$  der Menge der reellen Zahlen.

- (1) Zeigen Sie  $|M| = |N|$ , indem Sie eine bijektive Funktion  $f : M \rightarrow N$  angeben (mit Beweis der Bijektivität).
- (2) Geben Sie die Umkehrfunktion zu  $f$  an. Die entsprechenden Eigenschaften von  $f^{-1}$  sind zu beweisen!

### Aufgabe

Im Folgenden verwenden wir den Begriff der Kardinalität  $|M|$  für endliche Mengen  $M$  als Zahl der Elemente von  $M$ , also wie in Definition 1.3.6 eingeführt. Beweisen Sie, dass für alle endlichen Mengen  $M$  und  $N$  die folgenden Beziehungen gelten:

- (1) Es gilt  $|M| = |N|$  genau dann, wenn es eine bijektive Funktion  $f : M \rightarrow N$  gibt.
- (2) Es gilt  $|M| \leq |N|$  genau dann, wenn es eine injektive Funktion  $f : M \rightarrow N$  gibt.
- (3) Es gilt  $|M| < |N|$  genau dann, wenn es eine injektive Funktion  $f : M \rightarrow N$  gibt, aber keine bijektive Funktion  $g : M \rightarrow N$ .

### Aufgabe

Es seien  $M, N, P$  und  $Q$  beliebige Mengen. Beweisen Sie:

- (1) Die zwei Mengen  $M \times N$  und  $N \times M$  haben die gleiche Kardinalität.
- (2) Die drei Mengen  $M \times (N \times P)$ ,  $(M \times N) \times P$  und  $M \times N \times P$  haben die gleiche Kardinalität.
- (3) Haben  $M$  und  $P$  die gleiche Kardinalität und  $N$  und  $Q$  die gleiche Kardinalität, so haben auch  $M \times N$  und  $P \times Q$  die gleiche Kardinalität.

### Aufgabe

Beweisen Sie die Punkte (2) bis (4) von Satz 5.2.2.

### Aufgabe

Die Funktion  $f : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{R}$  sei definiert durch  $f(n) = \sum_{i=1}^n \frac{1}{i}$ . Zeigen Sie für alle  $n \in \mathbb{N}$  mit  $n \geq 1$  die Abschätzung  $f(n) \leq 1 + \frac{n}{2}$ .

### Aufgabe

Die beiden Funktionen  $f : \mathbb{N} \rightarrow \mathbb{N}$  und  $g : \mathbb{N} \rightarrow \mathbb{N}$  seien durch  $f(x) = 2x+2$  und  $g(x) = x^2$  definiert.

- (1) Stellen Sie die Werte  $f(n)$  und  $g(n)$  für alle  $n \in \{0, \dots, 5\}$  tabellarisch dar.

- (2) Bestimmen Sie anhand der Tabelle von (1) die kleinste Zahl  $n \in \mathbb{N}$  mit der Eigenschaft  $f(n) < g(n)$ .
- (3) Es sei  $n_0$  das Resultat von Punkt (2). Zeigen Sie für alle  $k \in \mathbb{N}$  die Abschätzung  $f(n_0 + k) < g(n_0 + k)$ .

### Aufgabe

Beantworten Sie die folgenden Fragen, gegebenenfalls mit Hilfe eines in einer Programmiersprache Ihrer Wahl geschriebenen Programms. Was ist die kleinste natürliche Zahl  $m \in \mathbb{N}$ , so dass

- (1)  $\text{potenz}_2(n) \leq \exp_2(n)$  für alle  $n \in \mathbb{N}$  mit  $m \leq n$  gilt,
- (2)  $\text{potenz}_3(n) \leq \exp_2(n)$  für alle  $n \in \mathbb{N}$  mit  $m \leq n$  gilt,
- (3)  $\text{potenz}_4(n) \leq \exp_2(n)$  für alle  $n \in \mathbb{N}$  mit  $m \leq n$  gilt?

### Aufgabe

Wir betrachten die durch  $\text{fib}(0) = 1$ ,  $\text{fib}(1) = 1$  und  $\text{fib}(n) = \text{fib}(n - 1) + \text{fib}(n - 2)$ , falls  $n \geq 2$ , rekursiv definierte Funktion  $\text{fib} : \mathbb{N} \rightarrow \mathbb{N}$  der Fibonacci-Zahlen.

- (1) Berechnen Sie mit Hilfe dieser Festlegung die Funktionswerte (d.h. Fibonacci-Zahlen)  $\text{fib}(n)$  für alle  $n \in \mathbb{N}$  mit  $n \leq 10$ .
- (2) Beweisen Sie für alle  $n \in \mathbb{N}$  die Eigenschaft  $2^n \leq \text{fib}(2n) \leq \text{fib}(2n + 1)$ .
- (3) Zeigen Sie für alle  $n \in \mathbb{N}$  die Abschätzung  $\text{fib}(n) \leq 2^n$ .

### Aufgabe

Aufbauend auf die Funktion  $\text{fib} : \mathbb{N} \rightarrow \mathbb{N}$  betrachten wir die folgende Funktion:

$$F : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad F(n, a, b) = a \text{fib}(n) + b \text{fib}(n + 1)$$

- (1) Zeigen Sie für alle  $n, a, b \in \mathbb{N}$  die Gleichungen  $F(0, a, b) = a + b$  und  $F(n + 1, a, b) = F(n, b, a + b)$ .
- (2) Wie lässt sich der Wert  $\text{fib}(n)$  mittels  $F$  bestimmen und welchen Vorteil hat die Berechnung von  $\text{fib}(n)$  mittels  $F$  im Vergleich zu einer, welche die Rekursion von  $\text{fib}$  aus der letzten Aufgabe verwendet?

### Aufgabe

Beweisen Sie: Für alle  $k, p \in \mathbb{N} \setminus \{0\}$  mit  $k \leq p$  gilt  $\text{potenz}_k \in \mathcal{O}(\text{potenz}_p)$ .

### Aufgabe

Die Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$  sei durch  $f(x) = 4x^3 + 3x^2 + 2x + 1$  definiert. Zeigen Sie, dass  $f \in \mathcal{O}(\text{potenz}_3)$ .

# 6 Spezielle Relationen und gerichtete Graphen

Im letzten Kapitel haben wir einige Klassen und Eigenschaften von Funktionen im Detail behandelt, also, genau genommen, von speziellen Relationen, nämlich eindeutigen und totalen. Nun betrachten wir weitere wichtige Klassen von Relationen und einige ihrer Eigenschaften näher. Im Gegensatz zu den Funktionen, die in ihrer Urform Relationen des Typs  $f \subseteq M \times N$  mit zwei beliebigen Mengen  $M$  und  $N$  sind, betrachten wir in diesem Kapitel nur Relationen des Typs  $R \subseteq M \times M$ , also Relationen, bei denen Quelle und Ziel gleich sind. Solche Relationen auf einer Menge werden auch **homogen** genannt. Homogene Relationen kann man anschaulich gut durch Pfeildiagramme darstellen und zwar durch solche, wie wir sie in Abschnitt 1.4 ursprünglich eingeführt haben. In der Sprache der Mathematik werden diese Pfeildiagramme auch gerichtete Graphen genannt. Diesen Strukturen, die in der Informatik insbesondere zu Modellierungszwecken eingesetzt werden, ist der letzte Teil des Kapitels gewidmet.

## 6.1 Äquivalenzrelationen und Partitionen

Äquivalenzrelationen stellen eine der wichtigsten Klassen von homogenen Relationen dar. Sie werden häufig dazu verwendet, um durch einen Abstraktionsprozess vorgegebene Objekte gemäß einiger spezieller Merkmale in gewisse Typen (Klassen, Kategorien) einzuteilen. Ist man etwa am Rechenaufwand eines Algorithmus auf linearen Listen in Abhängigkeit von der Listenlänge interessiert, so kann man in diesem Zusammenhang alle linearen Listen als gleichwertig („äquivalent“) betrachten, welche dieselbe Länge besitzen. Wir beginnen nachfolgend mit der Definition der Klasse der Äquivalenzrelationen anhand von drei Eigenschaften.

### 6.1.1 Definition: Äquivalenzrelation

Eine Relation  $R \subseteq M \times M$  heißt

- (1) **reflexiv**, falls für alle  $x \in M$  gilt  $x Rx$ ,
- (2) **symmetrisch**, falls für alle  $x, y \in M$  aus  $x Ry$  folgt  $y Rx$ ,
- (3) **transitiv**, falls für alle  $x, y, z \in M$  aus  $x Ry$  und  $y Rz$  folgt  $x Rz$ .

Eine **Äquivalenzrelation** ist eine reflexive, symmetrische und transitive Relation. □

Man stellt sofort fest, dass eine Relation  $R \subseteq M \times M$  genau dann symmetrisch ist, wenn  $x Ry$  und  $y Rx$  für alle  $x, y \in M$  äquivalente Aussagen sind. Für Äquivalenzrelationen verwendet man statt des Buchstabens  $R$  oft Symbole wie „ $\equiv$ “ und „ $\approx$ “. Damit drücken  $x \equiv y$  und  $x \approx y$  aus, dass die Objekte  $x$  und  $y$  in einer Relationsbeziehung stehen. Nachfolgend geben wir einige Beispiele für Äquivalenzrelationen an.

### 6.1.2 Beispiele: Äquivalenzrelationen

Die **identische Relation**  $I_M \subseteq M \times M$ , definiert für alle  $x, y \in M$  durch

$$x I_M y \iff x = y,$$

ist für alle Mengen  $M$  eine Äquivalenzrelation. Sie ist sogar eindeutig und total, also auch eine Funktion. In der Auffassung als Funktion und bei der Verwendung von funktionalen Schreibweisen haben wird diese spezielle Relation bisher mit dem Symbol  $id_M$  bezeichnet. Beim Umgehen mit allgemeinen Relationen wird jedoch das Symbol  $\mathbf{I}_M$  bevorzugt, oder vereinfachend auch  $\mathbf{I}$ , wenn die Menge  $M$  aus dem Kontext klar erkennbar ist.

Es sei  $M$  eine beliebige Menge. Definiert man auf der Potenzmenge  $\mathcal{P}(M)$  eine Relation  $\equiv$  durch die Festlegung

$$X \equiv Y : \iff |X| = |Y|$$

für alle  $X, Y \in \mathcal{P}(M)$ , wobei  $|X| = |Y|$  erklärt ist durch Definition 5.2.1, so ist  $\equiv$  eine Äquivalenzrelation. Man sagt in der Umgangssprache: „Das Gleichsein der Kardinalitäten ist eine Äquivalenzrelation auf Mengen“.

Wiederum sei  $M$  eine Menge. Definiert man auf der Menge der linearen Listen über  $M$ , also auf  $M^*$ , eine Relation  $\equiv$  durch die Festlegung

$$s \equiv t : \iff |s| = |t|$$

für alle  $s, t \in M^*$ , so ist  $\equiv$  ebenfalls eine Äquivalenzrelation auf  $M^*$ . Hier sagt man kürzer: „Gleiche Länge zu haben ist eine Äquivalenzrelation auf Listen“.  $\square$

Gehen wir die obigen drei Beispiele noch einmal der Reihe nach durch, so fallen der Leserin oder dem Leser vielleicht die folgenden Eigenschaften auf; dabei nehmen wir in Gleichung (2) die Menge  $M$  als endlich an, damit die Kardinalität von  $M$  definiert ist.

- (1)  $M = \bigcup \{\{x\} \mid x \in M\}$
- (2)  $\mathcal{P}(M) = \bigcup \{\mathcal{P}_n(M) \mid n \leq |M|\}$ , wobei  $\mathcal{P}_n(M) := \{X \in \mathcal{P}(M) \mid n = |X|\}$ .
- (3)  $M^* = \bigcup \{M^n \mid n \in \mathbb{N}\}$ , wobei  $M^n = \{s \in M^* \mid n = |s|\}$ .

Es wird also die Grundmenge in jedem Fall als die Vereinigung von disjunkten und nichtleeren Mengen dargestellt. Weiterhin stehen alle Elemente der einzelnen Mengen der disjunktene Vereinigung immer bezüglich der dem Beispiel zugrundeliegenden Äquivalenzrelation in Beziehung. Und schließlich gilt noch, dass Elemente, die aus verschiedenen Mengen der disjunktene Vereinigung kommen, niemals bezüglich der zugrundeliegenden Äquivalenzrelation in Beziehung stehen. Man bekommt also in allen drei Fällen eine Partition (Zerlegung) der Grundmenge in Mengen von „äquivalenten Elementen“ im Sinne der folgenden Festlegung des Begriffs Partition.

### 6.1.3 Definition: Partition / Zerlegung

Eine Menge  $\mathcal{Z}$  von Mengen heißt eine **Partition** oder **Zerlegung** einer nichtleeren Menge  $M$ , falls die folgenden drei Eigenschaften gelten:

- (1) Für alle  $X \in \mathcal{Z}$  gilt  $X \neq \emptyset$ .
- (2) Für alle  $X, Y \in \mathcal{Z}$  folgt aus  $X \neq Y$ , dass  $X \cap Y = \emptyset$ .
- (3)  $M = \bigcup \mathcal{Z}$   $\square$

Alle Mengen einer Partition sind also nichtleer und paarweise disjunkt. Weiterhin ergibt ihre Vereinigung die zugrundeliegende Menge. Ist  $\mathcal{Z}$  eine Partition von  $M$ , so sollten in den Mengen von  $\mathcal{Z}$  nur Elemente von  $M$  vorkommen. Dies ist in Definition 6.1.3 nicht explizit gefordert worden. Es kann aber relativ einfach gezeigt werden, dass dem so ist.

#### 6.1.4 Satz: Partition ist Teilmenge der Potenzmenge

Es seien  $M$  eine nichtleere Menge und  $\mathcal{Z}$  eine Partition von  $M$ . Dann gilt die Inklusion  $\mathcal{Z} \subseteq \mathcal{P}(M)$ .

**Beweis:** Es sei  $X$  eine beliebige Menge. Dann haben wir

$$\begin{aligned} X \in \mathcal{Z} &\implies X \subseteq \bigcup \mathcal{Z} && \text{Satz 1.2.6} \\ &\iff X \subseteq M && \text{Partitionseigenschaft} \\ &\iff X \in \mathcal{P}(M) && \text{Definition } \mathcal{P}(M) \end{aligned}$$

und durch diese logische Implikation ist der Beweis erbracht.  $\square$

Wir haben anhand der obigen Beispiele schon festgestellt, dass spezielle Äquivalenzrelationen Mengen partitionieren. Im folgenden Satz zeigen wir nun, dass diese Eigenschaft für alle Äquivalenzrelationen gilt und auch sogar ihre Umkehrung wahr ist, d.h., dass Partitionen auch zu Äquivalenzrelationen führen. Unser ultimatives Ziel ist eine Eins-zu-Eins-Beziehung; dazu kommen wir aber erst später.

#### 6.1.5 Satz: Partitionen und Äquivalenzrelationen

Für alle nichtleeren Mengen  $M$  gelten die folgenden Eigenschaften:

- (1) Ist  $\equiv$  eine Äquivalenzrelation auf  $M$  und definiert man für alle Elemente  $x \in M$  die Menge  $[x]_\equiv := \{y \in M \mid y \equiv x\}$ , so ist eine Partition von  $M$  gegeben durch

$$\mathcal{Z} := \{[x]_\equiv \mid x \in M\}.$$

- (2) Ist  $\mathcal{Z} \subseteq \mathcal{P}(M)$  eine Partition von  $M$  und definiert man eine Relation  $\equiv$  auf  $M$  durch die Festlegung

$$x \equiv y : \iff \exists X \in \mathcal{Z} : x \in X \wedge y \in X$$

für alle  $x, y \in M$ , so ist  $\equiv$  eine Äquivalenzrelation.

**Beweis:** (1) Wir rechnen die drei Eigenschaften von Definition 6.1.3 nach.

- (a) Wegen der Gültigkeit von  $x \equiv x$  erhalten wir  $x \in [x]_\equiv$  für alle  $x \in M$ . Also haben wir, dass  $[x]_\equiv \neq \emptyset$  für alle  $[x]_\equiv \in \mathcal{Z}$  wahr ist.
- (b) Es seien  $[x]_\equiv \in \mathcal{Z}$  und  $[y]_\equiv \in \mathcal{Z}$  mit  $[x]_\equiv \neq [y]_\equiv$ . Dann gibt es  $a \in M$  mit  $a \in [x]_\equiv$  und  $a \notin [y]_\equiv$ . Aus  $a \in [x]_\equiv$  folgt  $a \equiv x$  und aus  $a \notin [y]_\equiv$  folgt  $\neg(a \equiv y)$ . Angenommen, es gelte  $[x]_\equiv \cap [y]_\equiv \neq \emptyset$  und es sei  $b \in [x]_\equiv \cap [y]_\equiv$ . Dann können wir wie folgt rechnen:

$$\begin{aligned} b \in [x]_\equiv \cap [y]_\equiv &\iff b \in [x]_\equiv \wedge b \in [y]_\equiv \\ &\iff b \equiv x \wedge b \equiv y && \text{Symmetrie, Transitivität} \\ &\implies x \equiv y && \text{Transitivität} \\ &\implies a \equiv y && a \equiv x, \text{ Transitivität} \end{aligned}$$

Und das bringt einen Widerspruch zu  $\neg(a \equiv y)$ .

- (c) Wegen  $\mathcal{Z} \subseteq \mathcal{P}(M)$  gilt  $X \subseteq M$  für alle  $X \in \mathcal{Z}$  und somit auch  $\bigcup \mathcal{Z} \subseteq M$ . Für die Umkehrung dieser Inklusion sei  $a$  ein beliebiges Objekt. Dann haben wir:

$$\begin{aligned} a \in M &\implies a \in [a]_{\equiv} && \text{Reflexivit\"at} \\ &\implies \exists X \in \mathcal{Z} : a \in X && \text{n\"amlich } X := [a]_{\equiv} \\ &\iff a \in \bigcup \mathcal{Z} && \text{Definition } \bigcup \mathcal{Z} \end{aligned}$$

Folglich gilt insgesamt  $M = \bigcup \mathcal{Z}$ .

- (2) Wir beweisen die in Definition 6.1.1 angegebenen drei Eigenschaften einer Äquivalenzrelation. Zum Beweis der Reflexivit\"at sei  $x \in M$  beliebig angenommen. Dann gilt:

$$\begin{aligned} x \equiv x &\iff \exists X \in \mathcal{Z} : x \in X \wedge x \in X && \text{Definition } \equiv \\ &\iff \exists X \in \mathcal{Z} : x \in X && \\ &\iff x \in \bigcup \mathcal{Z} && \text{Definition } \bigcup \mathcal{Z} \\ &\iff x \in M && \mathcal{Z} \text{ ist Partition} \end{aligned}$$

und die letzte Aussage  $x \in M$  ist per Annahme wahr. Also ist auch  $x \equiv x$  wahr. Um die Symmetrie zu beweisen, seien  $x, y \in M$  beliebig vorgegeben. Dann bekommen wir:

$$\begin{aligned} x \equiv y &\iff \exists X \in \mathcal{Z} : x \in X \wedge y \in X && \text{Definition } \equiv \\ &\iff \exists X \in \mathcal{Z} : y \in X \wedge x \in X && \\ &\iff y \equiv x && \text{Definition } \equiv \end{aligned}$$

Es verbleibt noch die Aufgabe, die Transitivit\"at zu zeigen. Dazu setzen wir  $x, y, z \in M$  beliebig voraus. Dann gilt:

$$\begin{aligned} x \equiv y \wedge y \equiv z & \\ \iff (\exists X \in \mathcal{Z} : x \in X \wedge y \in X) \wedge (\exists Y \in \mathcal{Z} : y \in Y \wedge z \in Y) & \quad \text{Definition } \equiv \\ \implies \exists Z \in \mathcal{Z} : x \in Z \wedge z \in Z & \quad \text{siehe unten} \\ \iff x \equiv z & \quad \text{Definition } \equiv \end{aligned}$$

Gelten n\"amlich die Eigenschaften  $x, y \in X$  und  $y, z \in Y$ , so folgt daraus  $y \in X \cap Y$ . Dies bringt  $X \cap Y \neq \emptyset$ , also haben wir  $X = Y$  und damit existiert das behauptete  $Z$  mit  $x, z \in Z$ , n\"amlich  $Z := X = Y$ .  $\square$

Die in Teil (1) dieses Satzes eingef\"uhrten Mengen spielen eine herausragende Rolle und werden deshalb eigens bezeichnet.

### 6.1.6 Definition: Äquivalenzklasse

Ist  $\equiv$  eine Äquivalenzrelation auf der Menge  $M$ , so heit zu dem Element  $x \in M$  die Menge  $[x]_{\equiv} := \{y \in M \mid y \equiv x\}$  die **Äquivalenzklasse** von  $x$ . Mit  $M/\equiv$  bezeichnet man die Menge aller Äquivalenzklassen von  $\equiv$ . Eine Teilmenge  $V$  von  $M$  mit der Eigenschaft  $M/\equiv = \{[x]_{\equiv} \mid x \in V\}$  heit ein **Vertretersystem** der Äquivalenzklassen.  $\square$

Es sind also  $x, y \in M$  in derselben Äquivalenzklasse genau dann, wenn  $(x, y)$  in der zugrundeliegenden Äquivalenzrelation enthalten ist. Ihre Klassen sind dann identisch und sowohl  $x$  als auch  $y$  ist jeweils ein Klassenvertreter. Bei Äquivalenzrelationen auf kleinen Mengen erkennt man die Reflexivität und die Symmetrie sehr einfach an den Kreuzentabellen. Die Diagonale ist mit Kreuzchen belegt und eine Spiegelung der Tabelle an ihr verändert die Tabelle nicht. Die Transitivität ist normalerweise nicht einfach erkennbar. Jedoch ist es möglich, die Zeilen und Spalten der Kreuzentabellen so zu permutieren, dass alle Kreuzchen in den Diagonalen in quadratischen „Kreuzchenblöcken“ zusammengefasst werden. Aus diesen Kreuzchenblöcken bekommt man dann sofort die Äquivalenzklassen.

Durch die beiden Konstruktionen des letzten Satzes ist sogar eine Eins-zu-Eins-Beziehung zwischen der Menge  $\mathfrak{A}_M$  aller Äquivalenzrelationen auf einer nichtleeren Menge  $M$  und der Menge  $\mathfrak{Z}_M$  aller Partitionen von  $M$  gegeben. Dazu betrachten wir die sich aus ihnen ergebenden Funktionen  $f : \mathfrak{A}_M \rightarrow \mathfrak{Z}_M$  und  $g : \mathfrak{Z}_M \rightarrow \mathfrak{A}_M$  mit den Definitionen

$$f(\equiv) = M/\equiv \quad g(\mathcal{Z}) = \bigcup\{X \times X \mid X \in \mathcal{Z}\}$$

für alle Äquivalenzrelationen  $\equiv \in \mathfrak{A}_M$  und alle Partitionen  $\mathcal{Z} \in \mathfrak{Z}_M$ . Die Definition von  $g$  ist offensichtlich äquivalent dazu, dass

$$x g(\mathcal{Z}) y \iff \exists X \in \mathcal{Z} : x \in X \wedge y \in X$$

für alle Partitionen  $\mathcal{Z} \in \mathfrak{Z}_M$  und alle  $x, y \in M$  gilt. Diese „elementweise“ Beschreibung der Äquivalenzrelation  $g(\mathcal{Z})$  verwenden wir im Beweis des nachfolgenden Resultats.

### 6.1.7 Satz: Eins-zu-Eins-Beziehung zwischen $\mathfrak{A}_M$ und $\mathfrak{Z}_M$

Die Funktionen  $f : \mathfrak{A}_M \rightarrow \mathfrak{Z}_M$  und  $g : \mathfrak{Z}_M \rightarrow \mathfrak{A}_M$  sind bijektiv und es gilt  $g = f^{-1}$ .

**Beweis:** Es sei  $\equiv \in \mathfrak{A}_M$  eine beliebige Äquivalenzrelation. Dann können wir für alle  $x, y \in M$  wie folgt rechnen:

$$\begin{aligned} x g(f(\equiv)) y &\iff \exists X \in f(\equiv) : x \in X \wedge y \in X && \text{Beschreibung } g \\ &\iff \exists X \in M/\equiv : x \in X \wedge y \in X && \text{Definition } f \\ &\iff x \equiv y. \end{aligned}$$

Dies zeigt  $g(f(\equiv)) = \equiv$  und somit ist  $g$  eine Linksinverse von  $f$ .

Nun sei  $\mathcal{Z} \in \mathfrak{Z}_M$  eine beliebige Partition von  $M$ . Nach dem Auswahlaxiom 5.1.19 gibt es eine Auswahlfunktion  $\alpha : \mathcal{Z} \rightarrow \bigcup \mathcal{Z}$ , also  $\alpha : \mathcal{Z} \rightarrow M$ , mit  $\alpha(X) \in X$  für alle  $X \in \mathcal{Z}$ . Daraus erhalten wir für alle  $X \in \mathcal{Z}$  die folgende Eigenschaft:

$$\begin{aligned} [\alpha(X)]_{g(\mathcal{Z})} &= \{y \in M \mid y g(\mathcal{Z}) \alpha(X)\} && \text{Definition Klassen} \\ &= \{y \in M \mid \exists Y \in \mathcal{Z} : y \in Y \wedge \alpha(X) \in Y\} && \text{Beschreibung } g \\ &= \{y \in M \mid y \in X\} && \text{siehe unten} \\ &= X \end{aligned}$$

Aus  $y \in Y$  und  $\alpha(X) \in Y$  folgt nämlich  $Y = X$  aufgrund von  $\alpha(X) \in X$  und der Partitionseigenschaft, also  $y \in X$ . Die andere Implikation ist offensichtlich; wähle  $Y := X$ .

Die obige Rechnung zeigt, dass jedes  $X \in \mathcal{Z}$  eine Äquivalenzklasse von  $g(\mathcal{Z})$  ist, also  $\mathcal{Z} \subseteq M/g(\mathcal{Z})$  gilt. Zum Beweis von  $M/g(\mathcal{Z}) \subseteq \mathcal{Z}$  sei  $[x]_{g(\mathcal{Z})} \in M/g(\mathcal{Z})$  beliebig angenommen. Weil  $\mathcal{Z}$  eine Partition von  $M$  ist, existiert ein  $X \in \mathcal{Z}$  mit  $x \in X$ . Für dieses  $X$  gilt  $[x]_{g(\mathcal{Z})} = X$ .

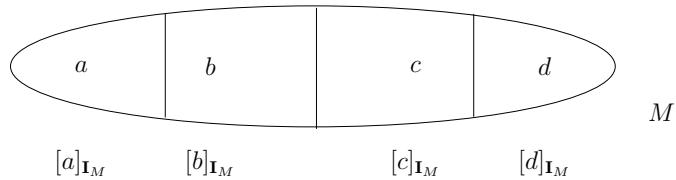
- Beweis von  $[x]_{g(\mathcal{Z})} \subseteq X$ : Es sei  $y \in [x]_{g(\mathcal{Z})}$  beliebig gewählt. Nach der elementweisen Beschreibung von  $g(\mathcal{Z})$  gibt es dann ein  $Y \in \mathcal{Z}$  mit  $x, y \in Y$ . Wegen  $x \in X$  und  $x \in Y$  und der Partitionseigenschaft von  $\mathcal{Z}$  bringt dies  $X = Y$ , also  $y \in X$ .
- Beweis von  $X \subseteq [x]_{g(\mathcal{Z})}$ : Es sei ein beliebiges  $y \in X$  gewählt. Dann gelten  $x, y \in X$  und dies bringt  $y \in g(\mathcal{Z})x$  wegen der elementweisen Beschreibung von  $g(\mathcal{Z})$ . Folglich gilt  $y \in [x]_{g(\mathcal{Z})}$ .

Insgesamt haben wir also  $M/g(\mathcal{Z}) = \mathcal{Z}$  gezeigt, was  $f(g(\mathcal{Z})) = M/g(\mathcal{Z}) = \mathcal{Z}$  impliziert. Damit ist  $g$  auch eine Rechtsinverse von  $f$  und wir sind fertig.  $\square$

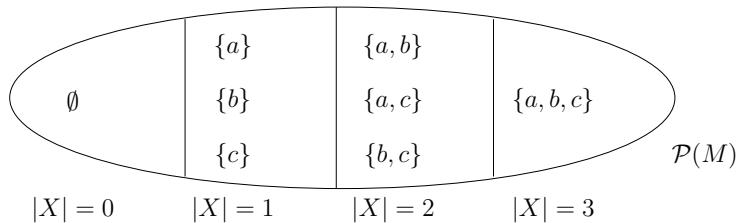
Nachfolgend stellen wir die Zerlegung einer Menge in Äquivalenzklassen anhand von drei Beispielen dar.

### 6.1.8 Beispiele: Äquivalenzklasse

Es sei die Menge  $M$  definiert durch  $M := \{a, b, c, d\}$  und weiterhin sei  $\mathbf{I}_M \subseteq M \times M$  die in Beispiel 6.1.2 eingeführte identische Relation auf  $M$ . Dann stellt sich die Zerlegung von  $M$  durch die Äquivalenzklassen von  $\mathbf{I}_M$  graphisch wie folgt dar:



Nun betrachten wir die Menge  $M := \{a, b, c\}$ . In diesem Fall bekommen wir für die in Beispiel 6.1.2 eingeführte Zerlegung der Potenzmenge von  $M$  gemäß der Kardinalität ihrer Elemente die folgende graphische Darstellung:



Schließlich sei  $M := \{a, b\}$ . Dann können wir die Zerlegung der linearen Listen über  $M$  aufgrund ihrer Längen, wie im dritten Teil von Beispiel 6.1.2 beschrieben, graphisch wie folgt darstellen:

|           |           |   |   |  |     |
|-----------|-----------|---|---|--|-----|
| ()        | $(a)$     | $(a, a)$<br>$(a, b)$<br>$(b)$<br>$(b, a)$<br>$(b, b)$ | $(a, a, a)$<br>$(a, a, b)$<br>$(b, a, a)$<br>$(a, b, a)$<br>$(a, b, b)$ | $(b, a, a)$<br>$(b, a, b)$<br>$(b, b, a)$<br>$(b, b, b)$ | ... |
| $ s  = 0$ | $ s  = 1$ | $ s  = 2$   | $ s  = 3$   | ...  |     |

Im Gegensatz zu den obigen zwei Mengen ist die zugrundeliegende Menge  $M^*$  nun nicht mehr endlich und wir haben deshalb drei Punkte verwendet, um anzudeuten, wie  $M^*$  partitioniert wird.  $\square$

Wir beenden diesen Abschnitt mit einer sehr wichtigen Äquivalenzrelation auf den ganzen Zahlen, die auf Gauß zurückgeht. Sie ist die Grundlage des sogenannten modularen Rechens und insbesondere für die Zahlentheorie und die Algebra von Bedeutung. Aber auch in der Informatik wird sie sehr häufig verwendet, beispielsweise in der Computeralgebra, bei Verschlüsselungstechniken der Kryptographie und der effizienten Speicherung von Daten durch sogenannte Hash-Tabellen.

### 6.1.9 Definition: Modulo-Relation

Es sei  $m \in \mathbb{Z}$ . Wir definieren die Menge der Vielfachen von  $m$  durch die Festlegung  $m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}$  und die Relation  $\equiv_m$  auf  $\mathbb{Z}$ , indem wir für alle  $x, y \in \mathbb{Z}$  setzen

$$x \equiv_m y \iff x - y \in m\mathbb{Z}.$$

Gilt die Aussage  $x \equiv_m y$ , so ist, per Definition,  **$x$  kongruent zu  $y$  modulo  $m$** .

$\square$

Die Eigenschaft

$$x \equiv_m y \iff \exists k \in \mathbb{Z} : x - y = mk \iff \exists k \in \mathbb{Z} : x = y + mk$$

folgt direkt aus der Definition der Vielfachen. Statt  $x \equiv_m y$  schreibt man in der Mathematik in der Regel  $x \equiv y \pmod{m}$ . Unsere Schreibweise ist durch die Tatsache motiviert, dass sich durch sie oft Beweise durch Umformungsketten  $x_1 \equiv_m x_2 \equiv_m x_3 \equiv_m \dots \equiv_m x_n$  führen lassen. Bei solchen Beweisen sind die dazwischengeschobenen Texte „( $\pmod{m}$ )“ sehr störend. Es gilt die folgende Eigenschaft:

### 6.1.10 Satz: Modulo-Relation ist Äquivalenzrelation

Die in Definition 6.1.9 eingeführte Relation  $\equiv_m$  auf den ganzen Zahlen  $\mathbb{Z}$  ist für alle  $m \in \mathbb{Z}$  eine Äquivalenzrelation.

**Beweis:** Wir verwenden im Folgenden die logische Äquivalenz der Relationsbeziehung  $x \equiv_m y$  und der Formel  $\exists k \in \mathbb{Z} : x = y + mk$  und starten mit der Reflexivität. Es gilt für alle  $x \in \mathbb{Z}$ , dass

$$x \equiv_m x \iff \exists k \in \mathbb{Z} : x = x + mk.$$

Die rechte Seite dieser Äquivalenz ist wahr, denn es gilt  $x = x + mk$  für  $k := 0 \in \mathbb{Z}$ . Folglich ist auch  $x \equiv_m x$  wahr.

Zur Verifikation der Symmetrie seien  $x, y \in \mathbb{Z}$  beliebig angenommen. Gilt  $x \equiv_m y$ , so gibt es ein  $k \in \mathbb{Z}$  mit  $x = y + mk$ . Wählt man  $k' := -k$ , dann gilt die Gleichung

$$y = x - mk = x + m(-k) = x + mk'.$$

Also gibt es ein  $k' \in \mathbb{Z}$  mit  $y = x + mk'$ . Dies bringt  $y \equiv_m x$ .

Es bleibt noch die Transitivität zu zeigen. Dazu seien  $x, y, z \in \mathbb{Z}$  beliebig gewählt. Gelten die Eigenschaften  $x \equiv_m y$  und  $y \equiv_m z$ , so gibt es  $k_1, k_2 \in \mathbb{Z}$  mit  $x = y + mk_1$  und  $y = z + mk_2$ . Daraus folgt, mit  $k := k_1 + k_2$ , dass

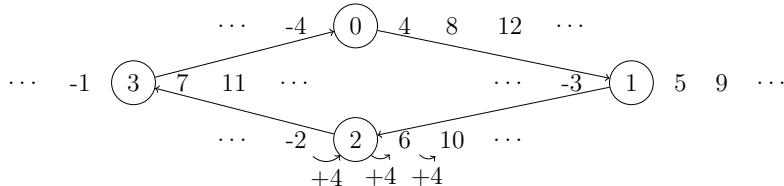
$$x = y + mk_1 = z + mk_2 + mk_1 = z + m(k_1 + k_2) = z + mk.$$

Also gibt es ein  $k \in \mathbb{Z}$  mit  $x = z + mk$ , d.h. es gilt  $x \equiv_m z$ .  $\square$

Wir wollen im Folgenden konkret die Äquivalenzklassen der eben behandelten Äquivalenzrelationen für zwei Beispiele bestimmen, da sich daraus dann der allgemeine Zusammenhang zwischen ihnen und der Teilbarkeit in den ganzen Zahlen ergibt.

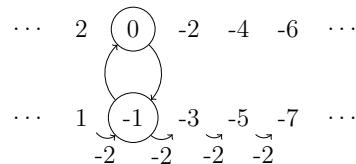
### 6.1.11 Beispiele: Rechnen modulo 4 und modulo -2

Wir betrachten zuerst die Äquivalenzrelation  $\equiv_4$  auf der Menge  $\mathbb{Z}$ . Aus der Festlegung von  $x \equiv_4 y$  genau dann, wenn es eine Zahl  $k \in \mathbb{Z}$  mit  $x = y + 4k$  gibt, bekommen wir durch ein „kreisförmiges“ Aufzählen aller ganzen Zahlen die folgenden Äquivalenzklassen:



Vier mögliche Klassenvertreter sind in diesem Bild eingerahmt angegeben, nämlich die Zahlen 0, 1, 2 und 3. Sie ergeben sich aus dem Startpunkt 0, indem man im Uhrzeigersinn zählt und jeweils das erste neue Element (bis zu 3, denn dann landet man ja wieder in der Ausgangsklasse) nimmt.

Man kann beim modularen Rechnen auch negative Zahlen  $m$  betrachten. Als Beispiel nehmen wir die Äquivalenzrelation  $\equiv_{-2}$ , d.h. es gilt  $x \equiv_{-2} y$  genau dann, wenn  $x = y - 2k$  mit einem  $k \in \mathbb{Z}$  gilt. Hier bekommen wir das folgende Bild:



Aufgrund der Art, wie man zu den Elementen der Äquivalenzklassen kommt, spricht man im Zusammenhang mit der Modulo-Relation manchmal auch von **Uhrenzahlen**. Die entsprechende Uhr besitzt  $m$  Stunden, die mit den Zahlen  $0, 1, \dots, m-1$  bezeichnet sind.  $\square$

Beim Rechnen modulo  $m$  mittels der Äquivalenzrelation  $\equiv_m$  empfiehlt es sich, die Zahlen zwischen  $0$  und  $m-1$  als Klassenvertreter zu wählen, falls  $m$  positiv ist. Ist  $m$  hingegen negativ, so ist es manchmal besser, die negativen Zahlen von  $m+1$  bis  $0$  als Klassenvertreter zu wählen. Dies erleichtert dann das Bestimmen der Äquivalenzklassen durch ein kreisförmiges Aufzählen ab der Null. Der Fall  $m=0$  ist uninteressant, da  $\equiv_0$  offensichtlich die identische Relation auf  $\mathbb{Z}$  ist. Man kann die in Definition 6.1.9 eingeführten Äquivalenzrelationen  $\equiv_m$  auch anders beschreiben. Dazu erinnern wir an die **ganzzahlige Division mit positivem Rest** in den ganzen Zahlen, die man von der höheren Schule her hoffentlich noch kennt (und deren Existenz wir später noch formal rechtfertigen werden). Gilt die Gleichung  $x = qy + r$  mit  $0 \leq r < |y|$ , so hat  $x \in \mathbb{Z}$  bei der ganzzahligen Division durch  $y \in \mathbb{Z} \setminus \{0\}$  den (positiven) Rest  $r \in \mathbb{N}$  und es „geht  $y$  in  $x$  maximal  $q$ -mal auf“, wobei für den Quotienten  $q \in \mathbb{Z}$  gefordert wird. Beispielsweise gilt  $12 = 2 \cdot 5 + 2$ , d.h.  $12$  hat bei der ganzzahligen Division durch  $5$  den Rest  $2$  und  $5$  geht in  $12$  maximal  $2$ -mal auf. Ein anderes Beispiel mit negativen Zahlen ist  $-12 = (-3) \cdot 5 + 3$ . Es hat also  $-12$  bei der ganzzahligen Division durch  $5$  den Rest  $3$  und  $5$  geht in  $-12$  maximal  $-3$ -mal auf. Damit gilt:

### 6.1.12 Satz: Modulo-Relation und ganzzahlige Division mit Rest

Es sei  $m \in \mathbb{Z} \setminus \{0\}$ . Dann sind für alle  $x \in \mathbb{Z}$  und  $y \in \mathbb{Z}$  die folgenden Aussagen äquivalent:

- (1)  $x \equiv_m y$
- (2) Es haben  $x$  und  $y$  bei der ganzzahligen Division durch  $m$  den gleichen Rest.

**Beweis:** Wir beweisen zuerst die Implikation „(1)  $\implies$  (2)“. Es gelte also die Beziehung  $x \equiv_m y$ . Dann folgt daraus, dass  $x - y = mk$  für ein  $k \in \mathbb{Z}$  zutrifft. Dies bringt im Falle der zwei Gleichungen  $x = pm + r_1$  und  $y = qm + r_2$ , wobei  $p, q \in \mathbb{Z}$  und  $r_1, r_2 \in \mathbb{N}$  mit  $r_1, r_2 < |m|$  angenommen sind, die folgende Eigenschaft:

$$\begin{aligned}
 r_1 - r_2 &= (x - pm) - (y - qm) && \text{Annahmen} \\
 &= x - y + qm - pm \\
 &= x - y + (q - p)m \\
 &= mk + (q - p)m && \text{Annahme} \\
 &= m(k + q - p)
 \end{aligned}$$

Weil  $r_1 < |m|$  und  $r_2 < |m|$  gelten, haben wir  $|r_1 - r_2| < |m|$ . Zusammen mit der eben bewiesenen Gleichung und  $k, p, q, r_1, r_2 \in \mathbb{Z}$  impliziert dies  $k + q - p = 0$ , also  $r_1 = r_2$ .

Nun zeigen wir „(2)  $\implies$  (1)“: Hierzu nehmen wir an, dass die Gleichungen  $x = pm + r$  und  $y = qm + r$  mit  $p, q \in \mathbb{Z}$  und  $r \in \mathbb{N}$  und  $r < |m|$  gelten. Dann bekommen wir

$$x - y = pm + r - (qm + r) = pm - qm + r - r = m(p - q),$$

also  $x - y \in m\mathbb{Z}$ , und damit trifft per Definition  $x \equiv_m y$  zu.  $\square$

Es seien  $m, x \in \mathbb{Z}$ . Dann kann man die Äquivalenzklasse von  $x$  bezüglich der Äquivalenzrelation  $\equiv_m$  durch die folgende Rechnung bestimmen:

$$\begin{aligned}[x]_{\equiv_m} &= \{y \in \mathbb{Z} \mid x - y \in m\mathbb{Z}\} \\ &= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x = y + mk\} \\ &= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = x + mk\} \\ &= \{x + mk \mid k \in \mathbb{Z}\}\end{aligned}$$

Die letzte Menge der eben durchgeführten Rechnung wird oft mit  $x + m\mathbb{Z}$  bezeichnet. Wir geben nun noch einige Beispiele dafür an, wie man mit Mengen dieser Form die Menge der ganzen Zahlen in disjunkte Mengen zerlegen kann.

### 6.1.13 Beispiel: Zerlegung von $\mathbb{Z}$

Für  $m = 1$  gilt  $1\mathbb{Z} = \mathbb{Z}$  und für alle  $x, y \in \mathbb{Z}$  gilt  $x \equiv_1 y$  genau dann, wenn  $x - y \in \mathbb{Z}$ . Also gilt  $x \equiv_1 y$  für alle  $x, y \in \mathbb{Z}$  und die Relation  $\equiv_1$  ist das direkte Produkt  $\mathbb{Z} \times \mathbb{Z}$ , in diesem Zusammenhang **Allrelation** auf  $\mathbb{Z}$  genannt. Es gibt nur eine Äquivalenzklasse:

$$\mathbb{Z} = [0]_{\equiv_1} = (0 + 1\mathbb{Z}) = \bigcup_{x=0}^0 x + 1\mathbb{Z}$$

Im Fall  $m = 2$  gilt  $x \equiv_2 y$  genau dann, wenn  $x - y$  gerade ist, also genau dann, wenn  $x$  und  $y$  beide gerade oder  $x$  und  $y$  beide ungerade sind. Dies zeigt, dass  $[0]_{\equiv_2}$  und  $[1]_{\equiv_2}$  die einzigen Äquivalenzklassen sind, wobei  $[0]_{\equiv_2} = \{0, 2, -2, 4, -4, \dots\}$  und  $[1]_{\equiv_2} = \{1, -1, 3, -3, 5, -5, \dots\}$  in einer informellen Schreibweise mit drei Punkten gilt. Weiterhin haben wir:

$$\mathbb{Z} = [0]_{\equiv_2} \cup [1]_{\equiv_2} = (0 + 2\mathbb{Z}) \cup (1 + 2\mathbb{Z}) = \bigcup_{x=0}^1 x + 2\mathbb{Z}$$

Für  $m = 3$  haben wir  $x \equiv_3 y$  genau dann, wenn beide bei der ganzzahligen Division durch 3 den gleichen Rest 0 oder den gleichen Rest 1 oder den gleichen Rest 2 haben. Dies bringt in der eben verwendeten informellen Schreibweise  $[0]_{\equiv_3} = \{0, 3, -3, 6, -6, 9, -9, \dots\}$ ,  $[1]_{\equiv_3} = \{1, 4, -2, 7, -5, 10, -8, 13, -11, \dots\}$  und  $[2]_{\equiv_3} = \{2, 5, -1, 8, -4, 11, -7, 14, -10, \dots\}$ . Also haben wir die Menge der ganzen Zahlen wie folgt in drei Mengen zerlegt:

$$\mathbb{Z} = [0]_{\equiv_3} \cup [1]_{\equiv_3} \cup [2]_{\equiv_3} = (0 + 3\mathbb{Z}) \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}) = \bigcup_{x=0}^2 x + 3\mathbb{Z}$$

Dies kann man für jede positive natürliche Zahl  $m$  durchführen und bekommt in jedem Fall eine Darstellung  $\mathbb{Z} = \bigcup_{x=0}^{m-1} x + m\mathbb{Z}$  der Menge der ganzen Zahlen, wobei die Mengen der Partition  $\{x + m\mathbb{Z} \mid 0 \leq x \leq m - 1\}$  jeweils aus genau den ganzen Zahlen bestehen, die bei der ganzzahligen Division durch  $m$  den Rest  $x$  besitzen.  $\square$

## 6.2 Ordnungsrelationen und geordnete Mengen

In Beispiel 1.4.5 haben wir angegeben, dass die übliche Ordnung  $\leq$  auf den natürlichen Zahlen formal eine Relation auf der Menge  $\mathbb{N}$  ist. Im gleichen Beispiel haben wir auch

die Teilbarkeitsrelation  $|$  auf der Menge  $\mathbb{N}$  betrachtet. Beide Relationen sind offensichtlich reflexiv und transitiv im Sinne der Definition 6.1.1. Symmetrisch sind beide nicht, also keine Äquivalenzrelationen. Sie sind jedoch beide antisymmetrisch im Sinne der folgenden Definition, und damit Ordnungsrelationen, ebenfalls im Sinne der folgenden Definition. Die in dieser Definition noch eingeführte Linearität trifft bei beiden Relationen nur für die Ordnungsrelation  $\leq$  zu.

### 6.2.1 Definition: Antisymmetrie, Linearität, Ordnung

Eine Relation  $R \subseteq M \times M$  heißt

- (1) **antisymmetrisch**, falls für alle  $x, y \in M$  aus  $x R y$  und  $y R x$  folgt  $x = y$ ,
- (2) **linear**, falls für alle  $x, y \in M$  gilt  $x R y$  oder  $y R x$ .

Eine **Ordnungsrelation** ist eine reflexive, antisymmetrische und transitive Relation und eine **lineare Ordnungsrelation** ist zusätzlich noch linear. Ist  $R$  eine (lineare) Ordnungsrelation auf der Menge  $M$  und  $M$  nicht leer, so heißt das Paar  $(M, R)$  eine (**linear**) geordnete Menge.  $\square$

Die in dieser Definition für Ordnungsrelationen gegebene axiomatische Definition scheint auf den deutschen Mathematiker Felix Hausdorff (1868-1942) zurückzugehen. Für Ordnungsrelationen verwendet man oft Symbole wie  $\leq$ ,  $\preceq$  oder  $\sqsubseteq$ . Statt Ordnungsrelationen sagt man kürzer auch **Ordnungen** oder sogar **Halbordnungen** oder **partielle Ordnungen**, um den Unterschied zu den **linearen Ordnungsrelationen** zu betonen, die vielfach auch **totale Ordnungsrelationen** genannt werden. In diesem Zusammenhang hat das Wort „total“ eine ganz andere Bedeutung als in Definition 1.4.7. Auch eine geordnete Menge  $(M, R)$  wird oft nur als Ordnung bezeichnet. Nachfolgend geben wir einige Beispiele für Ordnungen an.

### 6.2.2 Beispiele: Ordnungen

Die Paare  $(\mathbb{N}, \leq)$ ,  $(\mathbb{Z}, \leq)$ ,  $(\mathbb{Q}, \leq)$  und  $(\mathbb{R}, \leq)$  sind alle mit den von der höheren Schule her bekannten Ordnungsrelationen – ihren sogenannten Standardordnungen – linear geordnete Mengen.

Es ist, wie man sehr einfach nachrechnet, das Paar  $(\mathbb{N}, |)$  eine geordnete Menge. Die **Teilbarkeitsordnung**  $|$  auf  $\mathbb{N}$  ist jedoch nicht linear. Es gibt Zahlen, die bezüglich Teilbarkeit nicht vergleichbar sind. Beispielsweise gilt weder  $2 | 3$  noch  $3 | 2$ .

Für alle Mengen  $M$  ist das Paar  $(\mathcal{P}(M), \subseteq)$  ebenfalls eine geordnete Menge. Man vergleiche noch einmal mit Satz 1.1.11. Die **Inklusionsordnung**  $\subseteq$  auf  $\mathcal{P}(M)$  ist jedoch für alle Mengen  $M$  mit mindestens zwei Elementen nicht linear, da für alle  $a, b \in M$  mit  $a \neq b$  weder  $\{a\} \subseteq \{b\}$  noch  $\{b\} \subseteq \{a\}$  gilt. Hingegen ist das Paar  $(\mathcal{P}(M), \subseteq)$  im Fall  $|M| < 2$  eine lineare Ordnung.

Der **Kardinalitätenvergleich**  $|M| \leq |N|$  führt zu einer reflexiven und transitiven Relation auf Mengen. Man bekommt jedoch keine Antisymmetrie, da aus  $|M| \leq |N|$  und  $|N| \leq |M|$  nur  $|M| = |N|$  folgt, jedoch nicht  $M = N$ . Reflexive und transitive Relationen

heißen **Quasiordnungen**. Auch der Vergleich von linearen Listen nach der Länge und von knotenmarkierten Binärbäumen nach der Höhe führt nur zu Quasiordnungen, da lineare Listen gleicher Länge und knotenmarkierte Binärbäume gleicher Höhe nicht identisch sein müssen.  $\square$

Wenn wir in diesem Abschnitt beliebige geordnete Mengen untersuchen, dann bezeichnen wir die entsprechende Ordnungsrelation immer mit dem Symbol „ $\sqsubseteq$ “. Nachfolgend betrachten wir eine Variante des Ordnungsbegriffs. Wir kennen diese Konstruktion schon von den Zahlen und von der Mengeninklusion her.

### 6.2.3 Definition: Striktordnung

Ist  $(M, \sqsubseteq)$  eine geordnete Menge, so definiert man zur Ordnungsrelation  $\sqsubseteq$  auf  $M$  ihren **strikten Anteil**  $\sqsubset$  als Relation auf  $M$ , indem man für alle  $x, y \in M$  festlegt:

$$x \sqsubset y : \iff x \sqsubseteq y \wedge x \neq y$$

Die Relation  $\sqsubset$  heißt auch die **Striktordnungsrelation** zu  $\sqsubseteq$  und das Paar  $(M, \sqsubset)$  heißt **striktgeordnete Menge**.  $\square$

Striktordnungen sind genau die Relationen  $R$ , die transitiv sind und für alle Elemente  $x$  der Menge, auf der sie definiert sind,  $\neg(x R x)$  erfüllen. Die letzte Eigenschaft bezeichnet man als **Irreflexivität** einer Relation. Ist nun  $(M, \sqsubseteq)$  eine geordnete Menge und  $(M, \sqsubset)$  die zugehörige strukturgeordnete Menge, so schreibt man, wie von den Ordnungen auf Zahlen oder der Mengeninklusion her bekannt, statt  $x \sqsubseteq y$  auch  $y \sqsupseteq x$  und analog statt  $x \sqsubset y$  auch  $y \sqsupset x$ . Die üblichen Sprechweisen sind dann „kleiner oder gleich“, „größer oder gleich“, „echt kleiner“ und „echt größer“.

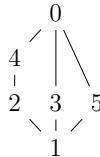
In Abschnitt 1.3 haben wir erklärt, wie man kleine Potenzmengen graphisch durch Diagramme darstellen kann. Diese Diagramme haben wir Ordnungs- oder Hassediagramme genannt. Sie sind auch für beliebige (kleine) geordnete Mengen ein übliches Darstellungsmittel. Dabei geht man bei der Erstellung des Diagramms im Fall einer geordneten Menge  $(M, \sqsubseteq)$  wie folgt vor:

- (1) Man zeichnet zuerst die Elemente von  $M$  in der Zeichenebene und ordnet sie dabei so an, dass ein Element  $x \in M$  unter einem Element  $y \in M$  liegt, falls die Beziehung  $x \sqsubset y$  gilt.
- (2) Dann zeichnet man eine Linie von jedem  $x \in M$  zu jedem  $y \in M$  genau dann, falls  $x \sqsubset y$  gilt und es kein  $z \in M$  mit  $x \sqsubset z$  und  $z \sqsubset y$  gibt.

Damit werden, wie im Fall der graphischen Darstellung von Potenzmengen, genau die Linien eingezeichnet, die man zur Rekonstruktion aller Ordnungsbeziehungen braucht. Nachfolgend ist ein Beispiel angegeben.

### 6.2.4 Beispiel: graphische Darstellung einer Ordnung

Wir betrachten die Teilbarkeitsrelation und reduzieren diese auf die Menge der natürlichen Zahlen von 0 bis 5, also auf  $M$ , definiert durch  $M := \{0, 1, 2, 3, 4, 5\}$ . Das folgende Bild zeigt das Hasse-Diagramm für die geordnete Menge  $(M, |)$ .



Man sieht auf diesem Bild, dass sich die Rolle der Null im Vergleich zur üblichen Ordnung stark verändert hat. Bezuglich der üblichen Ordnung ist 0 das kleinste Element. In der Teilbarkeitsrelation sind nun plötzlich alle Zahlen ungleich 0 echt kleiner als die Null, wobei hier „kleiner oder gleich“ der Beziehung „ist Teiler von“ entspricht.  $\square$

Liegt eine geordnete Menge vor, so gibt es eine Vielzahl von speziellen Elementen. Manche kennt man schon von den Ordnungen auf den Zahlen. Etwa ist 0 das kleinste Element der Menge  $\mathbb{N}$  bezüglich der üblichen Ordnung  $\leq$  und 5 das größte Element ihrer Teilmenge  $\{2, 3, 5\}$ . Manchmal sagt man in diesem Zusammenhang auch, dass 0 minimal und 5 maximal ist. Das ist nicht falsch. Bei beliebigen Ordnungsrelationen muss man jedoch zwischen kleinsten und minimalen und größten und maximalen Elementen im Sinne der folgenden Definition sorgfältig unterscheiden.

### 6.2.5 Definition: extreme Elemente

Es sei  $(M, \sqsubseteq)$  eine geordnete Menge und  $N \subseteq M$  sei eine Teilmenge von  $N$ . Ein Element  $x \in M$  heißt dann

- (1) **größtes Element** von  $N$ , falls  $x \in N$  und  $y \sqsubseteq x$  für alle  $y \in N$  gilt,
- (2) **kleinstes Element** von  $N$ , falls  $x \in N$  und  $x \sqsubseteq y$  für alle  $y \in N$  gilt,
- (3) **maximales Element** von  $N$ , falls  $x \in N$  und es kein  $y \in N$  gibt mit  $x \sqsubset y$ ,
- (4) **minimales Element** von  $N$ , falls  $x \in N$  und es kein  $y \in N$  gibt mit  $y \sqsubset x$ .  $\square$

Die eben festgelegten Elemente müssen nicht immer existieren. Dazu betrachten wir etwa das Paar  $(\mathbb{Z}, \leq)$  und die Teilmenge  $N \subseteq \mathbb{Z}$ , welche genau aus den geraden Zahlen besteht. Dann gibt es in  $N$  kein größtes, kein kleinstes, kein maximales und auch kein minimales Element. In der geordneten Menge  $(\mathbb{N}, \leq)$  hat  $N := \mathbb{N}$  die Null als kleinstes und als minimales Element. Größte und maximale Elemente gibt es hingegen nicht. Bevor wir ein weiteres Beispiel im Detail behandeln, stellen wir im nächsten Satz die wichtigsten Eigenschaften der Elemente von Definition 6.2.5 vor.

### 6.2.6 Satz: Eigenschaften extremer Elemente

Ist  $(M, \sqsubseteq)$  eine geordnete Menge, dann gelten für alle Teilmengen  $N \subseteq M$  die folgenden Eigenschaften:

- (1) Es hat  $N$  höchstens ein größtes und höchstens ein kleinstes Element.
- (2) Ist  $x \in N$  ein größtes (bzw. kleinstes) Element von  $N$ , so ist es auch ein maximales (bzw. minimales) Element von  $N$ .

- (3) Es ist  $x \in N$  genau dann ein maximales Element von  $N$ , falls für alle  $y \in N$  aus  $x \sqsubseteq y$  folgt  $x = y$ , und es ist  $x \in N$  genau dann ein minimales Element von  $N$ , falls für alle  $y \in N$  aus  $y \sqsubseteq x$  folgt  $x = y$ .

**Beweis:** (1) Sind  $x, y \in N$  größte Elemente von  $N$ , so gilt  $x \sqsubseteq y$  (da  $y$  ein größtes Element von  $N$  ist) und  $y \sqsubseteq x$  (da  $x$  ein größtes Element von  $N$  ist). Diese beiden Eigenschaften implizieren  $x = y$  wegen der Antisymmetrie. Die Eindeutigkeit des kleinsten Elements beweist man vollkommen analog.

(2) (Beweis durch Widerspruch.) Angenommen,  $x \in N$  sei ein größtes Element, aber nicht maximal. Dann gibt es  $y \in N$  mit  $x \sqsubset y$ , also mit  $x \sqsubseteq y$  und  $x \neq y$ . Weil  $x$  das größte Element von  $N$  ist, gilt  $y \sqsubseteq x$ . Die Antisymmetrie bringt nun  $x = y$  und dies ist ein Widerspruch zu  $x \neq y$ . Den Fall, dass  $x$  als kleinstes Element von  $N$  auch ein minimales Element von  $N$  ist, behandelt man wiederum vollkommen analog.

(3) Weil wir  $x \in N$  vorausgesetzt haben, ist  $x$  ein maximales Element von  $N$  genau dann, wenn die Formel  $\neg\exists y \in N : x \sqsubset y$  wahr ist. Die Rechnung

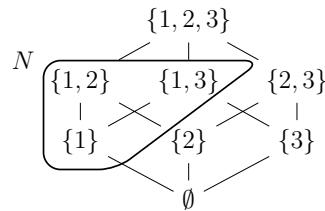
$$\begin{aligned} \neg\exists y \in N : x \sqsubset y &\iff \neg\exists y \in N : x \sqsubseteq y \wedge x \neq y && \text{Definition } \sqsubset \\ &\iff \forall y \in N : \neg(x \sqsubseteq y \wedge x \neq y) && \text{de Morgan} \\ &\iff \forall y \in N : \neg(x \sqsubseteq y) \vee x = y && \text{de Morgan} \\ &\iff \forall y \in N : x \sqsubseteq y \Rightarrow x = y \end{aligned}$$

zeigt nun die Behauptung. Analog behandelt man auch den verbleibenden Fall.  $\square$

Zur Verdeutlichung geben wir nun ein kleines Beispiel einer nicht linearen Ordnungsrelation an, wobei die Ordnungsbeziehungen zwischen den Elementen anhand des Hasse-Diagramms bildlich erklärt werden.

### 6.2.7 Beispiel: Extreme Elemente

Wir betrachten eine Menge  $M$  mit 3 Elementen, festgelegt durch  $M := \{1, 2, 3\}$ , und die durch die Inklusion geordnete Potenzmenge von  $M$ . Das Hasse-Diagramm von  $(\mathcal{P}(M), \subseteq)$  ist nachfolgend angegeben. In dieser Zeichnung ist die Teilmenge  $N := \{\{1\}, \{1, 2\}, \{1, 3\}\}$  von  $\mathcal{P}(M)$  durch eine Umrahmung gekennzeichnet.



Durch das Betrachten des Bildes erkennt man sehr schnell die folgenden Tatsachen: Die Teilmenge  $N$  von  $M$  hat kein größtes Element; sie hat aber zwei maximale Elemente, nämlich die Mengen  $\{1, 2\}$  und  $\{1, 3\}$ , ein kleinstes Element, nämlich die Menge  $\{1\}$ , und

genau ein minimales Element, nämlich die Menge  $\{1\}$ . □

Im Allgemeinen ist es beim Arbeiten mit geordneten Mengen sehr wichtig, zwischen größten und maximalen Elementen und kleinsten und minimalen Elementen genau zu unterscheiden. Werden diese fälschlicherweise identifiziert, so sind in der Regel falsche Aussagen und Beweise die Folge. Bei den Zahlen  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  mit den üblichen Ordnungen ist hingegen so eine Unterscheidung nicht wesentlich. Dem liegt der folgende Satz zugrunde. Die Richtungen „ $\Leftarrow$ “ in (1) und (2) gelten aufgrund von Satz 6.2.6 (2) für beliebige Ordnungsrelationen.

### 6.2.8 Satz: extreme Elemente und Linearität

Es sei  $(M, \sqsubseteq)$  eine linear geordnete Menge. Dann gelten für alle  $N \subseteq M$  und alle  $x \in N$  die folgenden zwei Aussagen:

- (1) Es ist  $x$  ein maximales Element von  $N$  genau dann, wenn  $x$  ein größtes Element von  $N$  ist.
- (2) Es ist  $x$  ein minimales Element von  $N$  genau dann, wenn  $x$  ein kleinstes Element von  $N$  ist.

**Beweis:** (1) Wir haben nur die Implikation „ $\Rightarrow$ “ zu beweisen. Dazu nehmen wir zu einem Widerspruchsbeweis an, dass es ein  $y \in N$  so gibt, dass  $y \sqsubseteq x$  nicht gilt. Weil  $(M, \sqsubseteq)$  linear geordnet ist, muss dann  $x \sqsubseteq y$  gelten. Da  $x$  maximal ist, folgt hieraus  $x = y$  nach Satz 6.2.6. Das bringt  $y = x$ , also  $y \sqsubseteq x$  wegen der Reflexivität. Das ist ein Widerspruch zur Annahme, dass  $y \sqsubseteq x$  nicht gilt.

(2) Auch hier ist nur die Implikation „ $\Rightarrow$ “ zu zeigen und dies ist analog zum Beweis von (1) möglich. □

In Definition 6.2.5 haben wir extreme Elemente von Teilmengen von geordneten Mengen eingeführt. Diese sind Elemente der gegebenen Teilmenge. Sie heißen extrem, weil sie bei zeichnerischen Darstellungen von Ordnungen immer am oberen oder unteren Rand der betrachteten Teilmenge liegen. Nun betrachten wir Schranken von Teilmengen. Diese müssen nicht unbedingt in den betrachteten Teilmengen liegen.

### 6.2.9 Definition: Schranken

Es seien  $(M, \sqsubseteq)$  eine geordnete Menge und  $N \subseteq M$ . Ein Element  $x \in M$  heißt

- (1) **obere Schranke** von  $N$ , falls  $y \sqsubseteq x$  für alle  $y \in N$  gilt,
- (2) **untere Schranke** von  $N$ , falls  $x \sqsubseteq y$  für alle  $y \in N$  gilt.

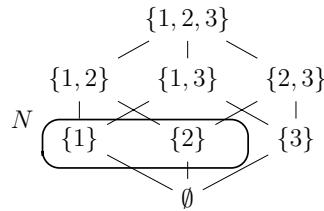
Hat die Menge  $N^\Delta$  der oberen Schranken von  $N$  ein kleinstes Element, so heißt dieses Element das **Supremum** von  $N$  und wird mit  $\sqcup N$  bezeichnet; hat die Menge  $N^\nabla$  der unteren Schranken von  $N$  ein größtes Element, so heißt dieses Element das **Infimum** von  $N$  und wird mit  $\sqcap N$  bezeichnet. □

Supremum und Infimum müssen nicht immer existieren. Wenn es sie aber gibt, so sind

sie nach Satz 6.2.6 als kleinste bzw. größte Elemente eindeutig bestimmt. Ordnungen, in denen zu je zwei Elementen  $x$  und  $y$  sowohl  $\sqcup\{x, y\}$  als auch  $\sqcap\{x, y\}$  existieren, nennt man **Verbände** oder **Verbandsordnungen**. Ihnen ist ein ganzer Zweig der Mathematik gewidmet, die Verbandstheorie. Wir betrachten nun noch einmal die geordnete Menge von Beispiel 6.2.7, nun aber mit einer anderen ausgewählten Teilmenge.

### 6.2.10 Beispiel: Supremum und Infimum

In der geordneten Menge  $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$  betrachten wir die Teilmenge  $N := \{\{1\}, \{2\}\}$ . Eingezeichnet in das Hasse-Diagramm ergibt sich das folgende Bild. Man macht sich anhand dieses Bildes sehr schnell die folgenden Tatsachen klar: Es hat die Teilmenge  $N$  zwei obere Schranken, nämlich  $\{1, 2\}$  und  $\{1, 2, 3\}$ . Das kleinste Element der Schrankenmenge  $N^\Delta = \{\{1, 2\}, \{1, 2, 3\}\}$  ist  $\{1, 2\}$ . Dies ist also das Supremum von  $N$ . Hingegen hat  $N$  nur eine untere Schranke, nämlich  $\emptyset$ . Das kleinste Element von  $N^\nabla = \{\emptyset\}$  ist ihr einziges Element  $\emptyset$ . Dies ist das Infimum von  $N$ .



Vielleicht hat manche Leserin oder mancher Leser schon an diesem Beispiel erkannt, dass die folgende Eigenschaft für alle Potenzmengen gilt: In der geordneten Menge  $(\mathcal{P}(M), \subseteq)$  gilt für alle Teilmengen  $\mathcal{N} \subseteq \mathcal{P}(M)$ , dass  $\bigcup \mathcal{N}$  das Supremum von  $\mathcal{N}$  ist und  $\bigcap \mathcal{N}$  das Infimum von  $\mathcal{N}$  ist. Dies ist auch der Grund dafür, dass die Symbole „ $\sqcup$ “ für das Supremum und „ $\sqcap$ “ für das Infimum verwendet werden. Leider sind auch noch andere Symbole gebräuchlich. Manchmal schreibt man etwa  $\sup N$  oder  $\inf N$  für das Supremum und  $\inf N$  oder  $\inf N$  für das Infimum von  $N$ .  $\square$

Im Rest dieses Abschnitts betrachten wir noch spezielle geordnete Mengen, die insbesondere für die Informatik von Bedeutung sind. Sie sind nach der deutschen Mathematikerin Emmy Noether (1882-1935) benannt.

### 6.2.11 Definition: Noethersche Ordnung

Eine geordnete Menge  $(M, \subseteq)$  heißt **Noethersch geordnet**, falls für alle nichtleeren Teilmengen  $N \subseteq M$  gilt: In  $N$  existiert ein minimales Element.  $\square$

Beispielsweise ist  $(\mathbb{N}, \leq)$  Noethersch geordnet, denn in  $(\mathbb{N}, \leq)$  besitzt jede nichtleere Teilmenge sogar ein kleinstes Element. Nach der Definition der Endlichkeit von Mengen in Abschnitt 1.3 haben wir Folgendes angemerkt:

Man kann die Endlichkeit einer Menge auch ohne Rückgriff auf natürliche Zahlen und die explizite Darstellung mittels der drei Punkte festlegen. Es ist nämlich  $M$  genau dann endlich, wenn für alle nichtleeren Teilmengen  $\mathcal{M}$  der

Potenzmenge  $\mathcal{P}(M)$  die folgende Eigenschaft gilt: Es gibt eine Menge  $X \in \mathcal{M}$  so, dass kein  $Y \in \mathcal{M}$  mit  $Y \subset X$  existiert.

Unter der Verwendung des neuen Begriffs von Definition 6.2.11 können wir dies nun wesentlich kompakter wie folgt formulieren:

Eine Menge  $M$  ist genau dann endlich, wenn die geordnete Menge  $(\mathcal{P}(M), \subseteq)$  Noethersch geordnet ist.

Dies ist eine Alternative zum Ansatz von Bolzano aus Abschnitt 5.2, wenn man ohne die explizite Darstellung und die natürlichen Zahlen auskommen will. Es ist  $\mathbb{N}$  nicht endlich, da  $(\mathcal{P}(\mathbb{N}), \subseteq)$  nicht Noethersch geordnet ist. Eine nichtleere Teilmenge ohne minimales Element in  $(\mathcal{P}(\mathbb{N}), \subseteq)$  ist etwa  $\{\{x \in \mathbb{N} \mid n \leq x \} \mid n \in \mathbb{N}\}$ , weil die bezüglich der Inklusion echt absteigende Folge  $\mathbb{N} \supset \mathbb{N} \setminus \{0\} \supset \mathbb{N} \setminus \{0, 1\} \supset \mathbb{N} \setminus \{0, 1, 2\} \supset \dots$  von echt ineinander enthaltenen Mengen niemals endet. Wir werden auf solche Folgen später noch zurückkommen. Zuvor wenden wir uns jedoch noch einem anderen wichtigen Thema zu. Der erste wichtige Grund für die Bedeutung Noethersch geordneter Mengen ist der folgende Satz, genannt das Prinzip der **Noetherschen Induktion**.

### 6.2.12 Satz: Noethersche Induktion

Es sei  $(M, \sqsubseteq)$  eine Noethersch geordnete Menge und  $A(x)$  eine Aussage, in der die Variable  $x$  für Elemente aus  $M$  steht. Sind die beiden Aussagen

- (IB) es gilt  $A(x)$  für alle minimalen Elemente von  $M$
- (IS) für alle nicht minimalen Elemente  $x$  von  $M$  gilt die Formel

$$(\forall y \in M : y \sqsubset x \Rightarrow A(y)) \Rightarrow A(x)$$

wahr, so ist auch die Formel  $\forall x \in M : A(x)$  wahr.

**Beweis (durch Widerspruch):** Es gelte also die Negation

$$(IB) \wedge (IS) \wedge \exists x \in M : \neg A(x)$$

der Behauptung. Dann gibt es ein also mindestens ein Element aus  $M$ , für das die Aussage nicht gilt. Wir betrachten nun die folgende nichtleere Menge:

$$S := \{x \in M \mid A(x) \text{ gilt nicht}\}$$

Weil  $(M, \sqsubseteq)$  Noethersch geordnet ist, gibt es in  $S$  ein minimales Element  $x_0 \in S$ . Wegen (IB) ist  $x_0$  nicht minimal in  $M$ . Für alle  $y \in M$  mit  $y \sqsubset x_0$  gilt weiterhin  $y \notin S$ . Nach der Definition von  $S$  gilt also für alle  $y \in M$  mit  $y \sqsubset x_0$ , dass  $A(y)$  gilt. Nun kommt (IS) zur Anwendung. Aus (IS) folgt nämlich  $A(x_0)$ , also  $x_0 \notin S$  nach Definition von  $S$ . Das ist ein Widerspruch zu  $x_0 \in S$ .  $\square$

Die bisher vorgestellte vollständige Induktion auf den natürlichen Zahlen erlaubt bei Beweisen nur Schritte von  $n - 1$  nach  $n$  oder von  $n$  nach  $n + 1$ . Wenn ein anderes Schema zum Beweis nötig ist, greift man in der Regel auf Noethersche Induktion zurück. Die Sprechweisen bei der Noetherschen Induktion sind dieselben wie in Abschnitt 4.4. Man spricht

also vom Induktionsbeginn (IB) und vom Induktionsschluss (IS) und nennt die linke Seite der Implikation von (IS) die Induktionshypothese. Wir geben nachfolgend ein Beispiel an, wo man sich mit vollständiger Induktion schwer tut, die Noethersche Induktion aber sehr rasch zum Ziel führt.

### 6.2.13 Beispiel: Noethersche Induktion

Wir betrachten die Funktion  $\text{fib} : \mathbb{N} \rightarrow \mathbb{N}$ , die wie folgt durch zwei Anfangswerte und rekursiv für alle  $n \in \mathbb{N}$  durch einen Rückgriff auf schon berechnete Werte definiert ist:

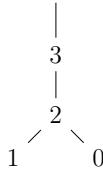
$$\text{fib}(0) = 1 \quad \text{fib}(1) = 1 \quad \text{fib}(n+2) = \text{fib}(n+1) + \text{fib}(n)$$

Es heißt, wie schon erwähnt,  $\text{fib}(n)$  die  $n$ -te Fibonacci-Zahl. Beispielsweise gelten

$$\text{fib}(2) = \text{fib}(1) + \text{fib}(0) = 1 + 1 = 2 \quad \text{fib}(3) = \text{fib}(2) + \text{fib}(1) = 2 + 1 = 3$$

und man bekommt 1, 1, 2, 3, 5, 8, 13, 21, 34 als Anfang der bekannten Fibonacci-Folge. Diese Folge wurde erstmals vom italienischen Mathematiker Leonardo Fibonacci (um 1180–1241) betrachtet, welcher auch unter dem Namen Leonardo di Pisa bekannt ist.

Wir behaupten nun, dass für alle  $n \in \mathbb{N}$  die Abschätzung  $\text{fib}(n) \leq 2^n$  gilt, d.h. die Formel  $\forall n \in \mathbb{N} : A(n)$  wahr ist, mit  $A(n)$  definiert als  $\text{fib}(n) \leq 2^n$ . Zum Beweis ist die übliche Ordnung  $\leq$  auf der Menge  $\mathbb{N}$  nicht geeignet. Wegen der Festlegung von 0 und 1 als Startpunkte der Fibonacci-Folge empfiehlt es sich, sie, anschaulich gesehen, am unteren Ende wie folgt abzuändern:



Wenn wir die so entstehende geordnete Menge mit  $(\mathbb{N}, \sqsubseteq)$  bezeichnen, so stimmen die Ordnungsrelationen  $\leq$  und  $\sqsubseteq$  auf den positiven natürlichen Zahlen überein. Weiterhin wird noch festgelegt, dass  $0 \sqsubseteq x$  genau dann gilt, wenn  $x = 0$  oder  $x \geq 2$  wahr ist. Es ist  $(\mathbb{N}, \sqsubseteq)$  Noethersch geordnet und minimal in der Menge  $\mathbb{N}$  sind 0 und 1.

Induktionsbeginn: Es gelten  $A(0)$  und auch  $A(1)$  aufgrund von  $\text{fib}(0) = 1 \leq 1 = 2^0$  und von  $\text{fib}(1) = 1 \leq 2 = 2^1$ .

Induktionsschluss: Wir haben  $A(n)$  für  $n \notin \{0, 1\}$  aus  $A(k)$  für alle  $k \sqsubset n$  zu beweisen. Wegen  $n \notin \{0, 1\}$  haben wir

$$A(n) \iff \text{fib}(n) \leq 2^n \iff \text{fib}(n-1) + \text{fib}(n-2) \leq 2^n.$$

Die letzte Eigenschaft gilt aber wegen  $A(n-1)$  und  $A(n-2)$  und der folgenden Rechnung:

$$\text{fib}(n-1) + \text{fib}(n-2) \leq 2^{n-1} + 2^{n-2} \leq 2^{n-1} + 2 \cdot 2^{n-2} = 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$$

Also gilt auch  $A(n)$  und damit ist der Beweis beendet.  $\square$

Mit Hilfe des Prinzips der Noetherschen Induktion können wir nun auch formal zeigen, dass die ganzzahlige Division mit positivem Rest tatsächlich für alle Paare  $(x, y)$  ganzer Zahlen mit  $y \neq 0$  definiert ist, also die entsprechenden Zahlen  $q$  und  $r$  existieren. Dies geschieht im folgenden Satz. Die ganzzahlige Division mit positivem Rest ist sogar eindeutig. Wir empfehlen der Leserin oder dem Leser, dies zur Übung zu beweisen.

#### 6.2.14 Satz: Existenz der ganzzahligen Division

Für alle  $x, y \in \mathbb{Z}$  mit der Eigenschaft  $y \neq 0$  gibt es ein  $q \in \mathbb{Z}$  und ein  $r \in \mathbb{N}$  so, dass  $x = qy + r$  und  $r < |y|$  gelten.

**Beweis (durch Noethersche Induktion):** Wir zeigen zuerst durch Noethersche Induktion unter Verwendung der Noetherschen geordneten Menge  $(\mathbb{N}, \leq)$  die Gültigkeit von  $\forall x \in \mathbb{N} : A(x)$ , wobei die Aussage  $A(x)$  steht für

$$\forall y \in \mathbb{N} \setminus \{0\} : \exists q \in \mathbb{Z}, r \in \mathbb{N} : x = qy + r \wedge r < |y|.$$

Induktionsbeginn: Es gilt  $A(0)$ , weil für alle  $y \in \mathbb{N} \setminus \{0\}$  die Gleichung  $0 = 0 \cdot y + 0$  wahr ist und auch  $0 < |y|$  zutrifft.

Induktionsschluss: Es sei  $x \in \mathbb{N}$  nicht minimal, also  $x \neq 0$ . Weiterhin sei  $y \in \mathbb{N} \setminus \{0\}$  beliebig vorgegeben. Wir unterscheiden zwei Fälle:

- (a) Es gelte  $x < y$ . Dann haben wir  $x = 0 \cdot y + x$ . Wählt man also  $q := 0$  und  $r := x$ , dann gelten  $x = qy + x$  und  $r < |y|$ .
- (b) Es gelte  $y \leq x$ . Da  $y \neq 0$  vorausgesetzt ist, gilt  $x - y < x$ . Wegen der Gültigkeit von  $A(x-y)$  nach der Induktionshypothese existieren  $q' \in \mathbb{Z}$  und  $r' \in \mathbb{N}$  mit  $x - y = q'y + r'$  und  $r' < |y|$ . Dies bringt  $x = q'y + r' + y = (q' + 1)y + r'$ . Wählt man  $q := q' + 1$  und  $r := r'$ , dann gelten  $x = qy + r$  und  $r < |y|$ .

Also gilt insgesamt  $A(x)$ , was zu zeigen war.

Mittels des eben geführten Induktionsbeweises ist nachgewiesen, dass die ganzzahlige Division für alle natürlichen Zahlen  $x$  und  $y$  mit  $y \neq 0$  existiert. Da aber  $x$  und  $y$  nach der Annahme des Satzes auch negativ sein dürfen, verbleiben noch drei weitere Fälle, die aber alle auf den eben gezeigten Fall reduziert werden können. Im Rest des Beweises gehen wir die drei Fälle der Reihe nach durch.

Es gelte  $x \in \mathbb{N}$  und  $y \in \mathbb{Z} \setminus \mathbb{N}$ . Dann ist  $-y \in \mathbb{N} \setminus \{0\}$  wahr. Nach dem obigen Fall gibt es  $q' \in \mathbb{Z}$  und  $r' \in \mathbb{N}$  so, dass  $x = q'(-y) + r'$  und  $r' < |-y| = |y|$  gelten. Daraus folgt die Gleichung  $x = (-q')y + r'$ . Nun wählt man  $q := -q'$  und  $r := r'$  und bekommt  $x = qy + r$  und  $r < |y|$ .

Es gelte  $x \in \mathbb{Z} \setminus \mathbb{N}$  und  $y \in \mathbb{N} \setminus \{0\}$ . Dann gilt  $-x \in \mathbb{N}$ . Also existieren, wiederum nach dem ersten Fall,  $q' \in \mathbb{Z}$  und  $r' \in \mathbb{N}$  mit  $-x = q'y + r'$  und  $r' < |y|$ . Im Fall  $r' > 0$  zeigt die Rechnung

$$x = -(-x) = -(q'y + r') = -q'y - r' = -q'y - y + y - r' = (-q' - 1)y + (y - r'),$$

dass die Wahl  $q := -q' - 1$  und  $r := y - r'$  die gewünschten Eigenschaften  $x = qy + r$  und  $r < |y|$  erfüllt; im Fall  $r' = 0$  kommen wir aufgrund von

$$x = -(-x) = -(q'y + 0) = -q'y + 0$$

mit der Wahl  $q := -q'$  und  $r := r' = 0$  zum Ziel  $x = qy + r$  und  $r < |y|$ .

Es gelte  $x \in \mathbb{Z} \setminus \mathbb{N}$  und  $y \in \mathbb{Z} \setminus \mathbb{N}$ . Hier geht man analog zum eben behandelten Fall vor und ersetzt in ihm  $y$  durch  $-y$ .  $\square$

In Definition 3.1.7 haben wir unendliche Folgen in Mengen eingeführt: Eine Folge  $(f_n)_{n \in \mathbb{N}}$  in  $M$  ist nichts anderes als eine andere Schreibweise für die Funktion  $f : \mathbb{N} \rightarrow M$ . Im Fall von geordneten Mengen kann man an Folgen zusätzliche Forderungen stellen. Bei Noethersch geordneten Mengen ist die nachfolgend angegebene wesentlich.

### 6.2.15 Definition: echt absteigende unendliche Kette

Es sei  $(M, \sqsubseteq)$  eine geordnete Menge. Eine unendliche Folge  $(f_n)_{n \in \mathbb{N}}$  in  $M$  heißt eine **echt absteigende unendliche Kette**, falls  $f_{n+1} \sqsubset f_n$  für alle  $n \in \mathbb{N}$  gilt.  $\square$

Beispielsweise ist die Kette  $(f_n)_{n \in \mathbb{N}}$  mit der Definition  $f_n := -n$  in  $(\mathbb{Z}, \leq)$  echt absteigend. Man schreibt die Kette auch in der Form  $0 > -1 > -2 > \dots$ , um dies lesbarer darzustellen. In der inklusionsgeordneten Potenzmenge von  $\mathbb{N}$  haben wir schon die echt absteigende unendliche Kette  $\mathbb{N} \supset \mathbb{N} \setminus \{0\} \supset \mathbb{N} \setminus \{0, 1\} \supset \mathbb{N} \setminus \{0, 1, 2\} \supset \dots$  kennengelernt. Hingegen gibt es in  $(\mathbb{N}, \leq)$  keine echt absteigenden unendlichen Ketten, denn  $(\mathbb{N}, \leq)$  ist Noethersch geordnet und es gilt das folgende Resultat.

### 6.2.16 Satz: Kettencharakterisierung Noethersch geordneter Mengen

Es sei  $(M, \sqsubseteq)$  eine geordnete Menge. Dann sind die beiden folgenden Aussagen äquivalent:

- (1) Es ist  $(M, \sqsubseteq)$  Noethersch geordnet.
- (2) Es gibt in  $(M, \sqsubseteq)$  keine echt absteigende unendliche Kette.

**Beweis:** Wir verwenden Kontraposition und beweisen, dass  $(M, \sqsubseteq)$  nicht Noethersch geordnet ist genau dann, wenn es in  $(M, \sqsubseteq)$  eine echt absteigende unendliche Kette gibt.

Beweis von „ $\Rightarrow$ “ der neuen Aussage: Es sei  $X \subseteq M$  die existierende nichtleere Menge ohne minimale Elemente. Man wählt  $f_0 \in X$  beliebig aus. Da  $f_0$  nicht minimal ist, gibt es ein  $f_1 \in X$  mit  $f_1 \sqsubset f_0$ . Auch  $f_1$  ist nicht minimal. Also gibt es ein  $f_2 \in X$  mit  $f_2 \sqsubset f_1 \sqsubset f_0$ . Durch vollständige Induktion kann man einfach beweisen, dass es für alle  $n \in \mathbb{N}$  eine echt absteigende Kette  $f_n \sqsubset f_{n-1} \sqsubset \dots \sqsubset f_1 \sqsubset f_0$  gibt. Also existiert insgesamt eine echt absteigende unendliche Kette  $(f_n)_{n \in \mathbb{N}}$ .

Beweis von „ $\Leftarrow$ “ der neuen Aussage: Ist  $(f_n)_{n \in \mathbb{N}}$  eine echt absteigende unendliche Kette, so gilt für die Menge  $X := \{f_n \mid n \in \mathbb{N}\}$  der Kettenglieder, dass  $X \neq \emptyset$  und  $X$  kein minimales Element besitzt. Wäre nämlich für ein  $i \in \mathbb{N}$  das Kettenglied  $f_i$  minimal in  $X$ , so muss  $f_{i+1} \notin X$  gelten, im Widerspruch zu  $f_n \in X$  für alle  $n \in \mathbb{N}$ .  $\square$

Satz 6.2.16 liegt der Namensgebung Noethersch geordneter Mengen zugrunde. Allerdings beschäftigte sich Emmy Noether mit algebraischen Strukturen (heutzutage Noethersche Ringe genannt), in denen echt aufsteigende unendliche Ketten von gewissen Teilmengen nicht existieren. Ihr österreichischer Kollege Emil Artin (1898-1962) studierte diese Teilmengen im Hinblick auf echt absteigende unendliche Ketten. Deshalb wird manchmal auch der Begriff **Artinsch geordnet** statt Noethersch geordnet verwendet.

Weil in Noethersch geordneten Mengen keine echt absteigenden unendlichen Ketten existieren, kann man sie dazu verwenden, die Terminierung von Rekursionen zu zeigen. Ist die Funktion  $f : N \rightarrow P$  durch rekursive Gleichungen beschrieben, dann definiert man eine sogenannte **Terminierungsfunktion**  $\delta : N \rightarrow M$  in einer Noethersch geordneten Menge  $(M, \sqsubseteq)$  und zeigt, dass in allen Gleichungen die  $\delta$ -Bilder aller Argumente aller rekursiven Aufrufe echt kleiner sind als das  $\delta$ -Bild des Arguments des Originalaufrufs. Ist  $N$  ein direktes Produkt, so werden Tupel als ein Argument aufgefasst. Aufgrund der Tatsache, dass keine echt absteigenden unendlichen Ketten existieren, kann es auch keine unendlichen Berechnungen geben. Denn eine unendliche Aufrufkette  $f(x_0) \rightsquigarrow f(x_1) \rightsquigarrow f(x_2) \rightsquigarrow \dots$  würde zur echt absteigenden unendlichen Kette  $\delta(x_0) \sqsupseteq \delta(x_1) \sqsupseteq \delta(x_2) \sqsupseteq \dots$  in der Noethersch geordneten Menge  $(M, \sqsubseteq)$  führen, was nicht möglich ist. Mit einer Anwendung dieser Technik auf ein Beispiel und ihrer Verallgemeinerung zu einem mathematischen Satz beenden wir diesen Abschnitt.

### 6.2.17 Beispiel: Terminierungsbeweis

Die **Ackermann-Peter-Funktion** ist eine rekursiv definierte mathematische Funktion, die extrem schnell wächst. Sie wurde ursprünglich vom deutschen Mathematiker Wilhelm Ackermann (1896-1962) aufgestellt; die folgende vereinfachte Variante geht auf die ungarische Mathematikerin Rozsa Peter (1905-1977) zurück. Peter definierte die Funktion  $a : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  für alle  $m, n \in \mathbb{N}$  durch die folgenden Gleichungen:

$$a(0, n) = n + 1 \quad a(m + 1, 0) = a(m, 1) \quad a(m + 1, n + 1) = a(m, a(m + 1, n))$$

Um zu zeigen, dass diese Funktion terminiert, betrachten wir die Noethersch geordnete Menge  $(\mathbb{N} \times \mathbb{N}, \leq_{lex})$ , wobei  $\leq_{lex}$  die lexikographische Ordnung ist, und die identische Funktion auf  $\mathbb{N} \times \mathbb{N}$  als Terminierungsfunktion. Für die Striktordnungsrelation  $<_{lex}$  und alle  $m_1, m_2, n_1, n_2 \in \mathbb{N}$  gilt

$$(m_1, n_1) <_{lex} (m_2, n_2) \iff m_1 < m_2 \vee (m_1 = m_2 \wedge n_1 < n_2).$$

Den Nachweis, dass die lexikographische Ordnung tatsächlich Noethersch ist, überlassen wir der Leserin oder dem Leser zur Übung.

Rekursive Aufrufe kommen nur in den letzten beiden Gleichungen der obigen Definition der Ackermann-Peter-Funktion  $a$  vor. Im Fall der Gleichung  $a(m + 1, 0) = a(m, 1)$  gilt für das Argument  $(m, 1)$  des rekursiven Aufrufs und das Argument  $(m + 1, 0)$  des Originalaufrufs die Abschätzung

$$\delta(m, 1) = (m, 1) <_{lex} (m + 1, 0) = \delta(m + 1, 0).$$

Die Gleichung  $a(m + 1, n + 1) = a(m, a(m + 1, n))$  beinhaltet zwei rekursive Aufrufe. Für das Argument  $(m + 1, n)$  des inneren rekursiven Aufrufs und das Argument  $(m + 1, n + 1)$

der Originalaufrufs gilt

$$\delta(m+1, n) = (m+1, n) <_{lex} (m+1, n+1) = \delta(m+1, n+1)$$

und für das Argument  $(m, a(m+1, n))$  des äußeren rekursiven Aufrufs und das Argument  $(m+1, n+1)$  der Originalaufrufs gilt

$$\delta(m, a(m+1, n)) = (m, a(m+1, n)) <_{lex} (m+1, n+1) = \delta(m+1, n+1).$$

Also werden in allen rekursiven Aufrufen die Argumente lexikographisch echt kleiner und nach der oben gemachten Bemerkung terminiert somit die Rekursion der Ackermann-Peter-Funktion.  $\square$

Weil Rekursionen nicht terminieren können, werden durch sie im Prinzip nur partielle Funktionen beschrieben. Es kann sogar der Fall auftreten, dass eine gegebene Rekursion durch mehrere partielle Funktionen erfüllt wird. In solch einem Fall ist es nicht einmal mehr offensichtlich, welche der partiellen Funktionen man durch die Rekursion eigentlich festlegt und ob jede andere Person dieser Rekursion die gleiche partielle Funktion zuordnet. Der folgende Satz gibt Bedingungen an, welche belegen, dass eine Rekursion nur von einer (totalen) Funktion erfüllt wird. Dabei spielt eine Terminierungsfunktion in einer Noethersch geordnete Menge wiederum die entscheidende Rolle. Um den Beweis zu vereinfachen, beschränken wir uns auf spezielle Rekursionen mit genau einem Terminierungsfall und genau einem Fall mit rekursiven Aufrufen, welche durch eine Bedingung unterschieden werden. Eine Erweiterung auf mehrere Terminierungsfälle und mehrere Fälle mit rekursiven Aufrufen ist nicht schwierig.

### 6.2.18 Satz: Lösung von Rekursionen

Es sei  $f : N \rightarrow P$  eine partielle Funktion, welche für alle  $x \in N$  die durch

$$f(x) = \begin{cases} E(f(K_1(x)), \dots, f(K_n(x))) & \text{falls } B(x) \\ F(x) & \text{falls } \neg B(x) \end{cases}$$

beschriebene Rekursion erfülle; dabei seien  $E : P^n \rightarrow P$  und  $F : N \rightarrow P$  Funktionen, alle  $K_i : N \rightarrow N$  ( $1 \leq i \leq n$ ) partielle Funktionen und  $B(x)$  eine überall auf  $N$  definierte Bedingung. Gibt es eine Funktion  $\delta : N \rightarrow M$  in einer Noethersch geordnete Menge  $(M, \sqsubseteq)$  so, dass für alle  $x \in N$  aus  $B(x)$  folgt

- (1)  $K_i(x)$  ist definiert für alle  $i \in \{1, \dots, n\}$ ,
- (2)  $\delta(K_i(x)) \sqsubset \delta(x)$  für alle  $i \in \{1, \dots, n\}$ ,

dann ist  $f(x)$  für alle  $x \in N$  definiert, also  $f$  eine Funktion.

**Beweis (durch Widerspruch):** Angenommen, es seien die Voraussetzungen wahr, aber es gebe ein  $x \in N$ , so dass  $f(x)$  nicht definiert ist. Wir betrachten die folgende Menge:

$$S := \{x \in N \mid f(x) \text{ ist nicht definiert}\}$$

Wegen  $S \neq \emptyset$  gilt  $\delta(S) \neq \emptyset$  und, weil  $(M, \sqsubseteq)$  Noethersch geordnet ist, existiert in  $\delta(S)$  ein minimales Element  $y_0 \in \delta(S)$ . Zu dem Element  $y_0$  gibt es ein Element  $x_0 \in S$  mit

$\delta(x_0) = y_0$ . Es ist  $f(x_0)$  nicht definiert. Die Totalität der Funktion  $F$  und die Rekursion zeigen nun  $B(x_0)$ , woraus mit Voraussetzung (1) folgt, dass die Aufrufe  $K_1(x_0)$  bis  $K_n(x_0)$  definiert sind. Weiterhin gilt für alle  $i \in \{1, \dots, n\}$ :

$$\begin{array}{lll} \text{Voraussetzung (2)} & \implies \delta(K_i(x_0)) \sqsubset y_0 & \text{da } B(x_0) \text{ und } \delta(x_0) = y_0 \\ & \implies \delta(K_i(x_0)) \notin \delta(S) & \text{da } y_0 \text{ minimal in } \delta(S) \\ & \implies K_i(x_0) \notin S & \\ & \iff f(K_i(x_0)) \text{ ist definiert} & \text{Definition } S \end{array}$$

Da  $E$  total ist, ist der Ausdruck  $E(f(K_1(x_0)), \dots, f(K_n(x_0)))$  somit definiert, und weil  $B(x_0)$  wahr ist, gilt aufgrund der Rekursion von  $f$  folglich die Gleichung

$$f(x_0) = E(f(K_1(x_0)), \dots, f(K_n(x_0))),$$

so dass auch der Aufruf  $f(x_0)$  definiert ist, im Widerspruch zu  $x_0 \in S$ .  $\square$

Durch eine sehr ähnliche Argumentation kann man zeigen, dass es unter den Voraussetzungen (1) und (2) höchstens eine Funktion  $f : N \rightarrow P$  gibt, welche die Rekursion von Satz 6.2.18 erfüllt. Wäre nämlich die Rekursion des Satzes durch zwei Funktionen  $f, g : N \rightarrow P$  mit  $f \neq g$  erfüllt, so ist die Teilmenge  $S := \{x \in N \mid f(x) \neq g(x)\}$  von  $N$  nicht leer. Also ist auch die Teilmenge  $\delta(S)$  von  $M$  nicht leer. Somit gibt es in  $\delta(S)$  ein minimales Element  $y_0 \in \delta(S)$ , denn  $(M, \sqsubseteq)$  ist eine Noethersch geordnete Menge. Zu  $y_0$  gibt es ein  $x_0 \in S$  mit  $\delta(x_0) = y_0$  und, analog zu dem Beweis von Satz 6.2.18, kann man den Widerspruch  $f(x_0) = g(x_0)$  herleiten.

Wenn wir die rekursive Funktion  $fib : \mathbb{N} \rightarrow \mathbb{N}$  aus Beispiel 6.2.13 zur Berechnung der Fibonacci-Zahlen in der schematischen Form von Satz 6.2.18 aufschreiben, dann erhalten wir für alle  $n \in \mathbb{N}$  die folgenden Spezifikation:

$$fib(n) = \begin{cases} fib(n-1) + fib(n-2) & \text{falls } n \geq 2 \\ 1 & \text{falls } n \leq 1 \end{cases}$$

Somit sind die zwei Funktionen  $E : \mathbb{N}^2 \rightarrow \mathbb{N}$  und  $F : \mathbb{N} \rightarrow \mathbb{N}$  für alle  $x, y \in \mathbb{N}$  durch  $E(x, y) = x + y$  und  $F(x) = 1$  festgelegt, die zwei partiellen Funktionen  $K_1 : \mathbb{N} \rightarrow \mathbb{N}$  und  $K_2 : \mathbb{N} \rightarrow \mathbb{N}$  durch  $K_1(x) = x - 1$  und  $K_2(x) = x - 2$ , sowie die überall auf  $\mathbb{N}$  definierte Bedingung  $B(x)$  durch  $x \geq 2$ . Um zu zeigen, dass  $fib(n)$  für alle  $n \in \mathbb{N}$  definiert ist, kann man die Noethersch geordnete Menge  $(\mathbb{N}, \leq)$  wählen, sowie  $\delta : \mathbb{N} \rightarrow \mathbb{N}$ , wobei  $\delta(x) = x$ , als Terminierungsfunktion. Dann sind nämlich  $K_1(x) = x - 1$  und  $K_2(x) = x - 2$  definiert, falls  $B(x)$  wahr ist, also  $x \geq 2$  gilt. Weiterhin gilt in diesem Fall die Abschätzung  $\delta(K_1(x)) = \delta(x - 1) = x - 1 < x = \delta(x)$  und auch die Abschätzung  $\delta(K_2(x)) = \delta(x - 2) = x - 2 < x = \delta(x)$ . Also gelten insgesamt die beiden Bedingungen (1) und (2) von Satz 6.2.18 und der Satz zeigt die Behauptung. Das eben gebrachte Beispiel zeigt, dass die Annahme von Satz 6.2.18, dass die Funktionen  $K_i$ ,  $1 \leq i \leq n$ , partiell sind, sehr natürlich ist. Durch die Bedingung  $B(x)$  wird normalerweise zugesichert, dass rekursive Aufrufe nur mit definierten Objekten erfolgen. Die Leserin oder der Leser übertrage zu Übungszwecken einige gängige Funktionen auf linearen Listen unter Verwendung der Operation des Linksanfügens und der (durch die Erweiterung auf  $M^*$ ) partiellen Operationen  $kopf : M^* \rightarrow M$  und  $rest : M^* \rightarrow M^*$  in die schematische Form von Satz 6.2.18 und beweise dann ihre Totalität mittels dieses Satzes.

## 6.3 Grundbegriffe gerichteter Graphen

Graphentheorie ist als Wissenschaft noch relativ jung, obwohl man ihre Wurzeln bis zum schon erwähnten schweizer Mathematiker Euler und seinem bekannten Königsberger Brückenproblem aus dem Jahr 1736 zurückdatieren kann. Die Bezeichnung „Graph“ scheint vom jüdisch-amerikanischen Mathematiker James Joseph Sylvester (1814-1897) zu stammen. Es gibt zwei Ausprägungen von Graphen, gerichtete Graphen und ungerichtete Graphen. Wir behandeln in diesem Abschnitt nur die erste Klasse. Sie steht in einer sehr engen Verbindung zu Relationen und das rechtfertigt die Zugehörigkeit zu dem derzeitigen Kapitel. Bildlich sind gerichtete Graphen nichts anderes als Zeichnungen in der Zeichenebene mit endlich vielen Knoten, mindestens einem, und sie verbindenden Pfeilen. Letztere besitzen eine durch die Pfeilspitze angegebene Richtung. Hier sind zwei Beispiele für solche gerichteten Graphen. Links sind  $a, b, c$  und  $d$  die Namen der vier Knoten, rechts sind es die natürlichen Zahlen von 1 bis 5.



Mathematisch betrachtet sind gerichtete Graphen Paare, bestehend aus einer Knotenmenge (in den obigen Zeichnungen  $\{a, b, c, d\}$  bzw.  $\{1, 2, 3, 4, 5\}$ ) und einer Menge von Pfeilen. Pfeile werden durch Knotenpaare dargestellt, etwa  $(a, b), (a, d), (b, c), (c, c), (d, b)$  und  $(d, c)$  im linken oberen Bild. Die Menge der Pfeile eines gerichteten Graphen ist also nichts anderes als eine Relation auf der Knotenmenge. Teil (1) der folgenden Definition ist eine unmittelbare Konsequenz dieser Beobachtung.

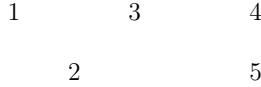
### 6.3.1 Definition: gerichteter Graph

- (1) Ein **gerichteter Graph** (wegen des englischen Worts „directed“ auch **Digraph** genannt)  $g = (V, P)$  ist ein Paar, bestehend aus einer **Knotenmenge**  $V$ , die endlich und nichtleer ist, und einer **Pfeilrelation**  $P \subseteq V \times V$ .
- (2) Ist das Paar  $(x, y)$  aus der Pfeilrelation  $P$ , so heißt es ein **Pfeil** mit **Anfangsknoten**  $x \in V$  und **Endknoten**  $y \in V$ .
- (3) Zum Knoten  $x \in V$  heißt  $nachf_g(x) := \{y \in V \mid x P y\}$  die **Menge der Nachfolger** von  $x$  und  $d_g^+(x) := |nachf_g(x)|$  der **Außengrad** von  $x$ . Analog definiert  $vorg_g(x) := \{y \in V \mid y P x\}$  die **Menge der Vorgänger** von  $x$  und  $d_g^-(x) := |vorg_g(x)|$  den **Innengrad** von  $x$ .  $\square$

In der Graphentheorie ist es üblich, nicht nur ein Paar  $(V, P)$  zu betrachten, sondern dieses gleichzeitig immer zu benennen. Typisch sind dabei Buchstaben wie „g“ oder „G“ und im Alphabet naheliegende. Statt Knoten sagt man manchmal auch „Ecke“ und statt Pfeil sagt man auch (gerichtete) „Kante“ oder (gerichteter) „Bogen“. Wir bleiben aber bei den Bezeichnungen Knoten und Pfeile. Auch werden wir uns bei der Angabe von konkreten gerichteten Graphen auf zeichnerische Darstellungen stützen, da diese viel leichter zu verstehen sind als die entsprechenden zwei Mengen von Knoten und Pfeilen. Nachfolgend betrachten wir nochmals zwei Beispiele für gerichtete Graphen.

### 6.3.2 Beispiele: gerichtete Graphen

Ein gerichteter Graph  $g = (V, P)$  mit  $P = \emptyset \subseteq V \times V$ , also mit leerer Pfeilrelation, heißt **leerer Graph**. Nachfolgend ist ein zeichnerisches Beispiel mit  $V := \{1, 2, 3, 4, 5\}$  als Knotenmenge angegeben.



Im Sinne der obigen Definition haben wir beim linken der zwei einführenden Bilder dieses Abschnitts ein Paar  $g = (V, P)$  vorliegen, mit  $V := \{a, b, c, d\}$  als Knotenmenge und  $P := \{(a, b), (a, d), (b, c), (c, c), (d, b), (d, c)\}$  als Pfeilrelation. Die Nachfolger- und Vorgängermengen und die zugehörigen Knotengrade sind in der folgenden Tabelle angegeben.

| Knoten $x$ | $nachf_g(x)$ | $d_g^+(x)$ | $vorg_g(x)$   | $d_g^-(x)$ |
|------------|--------------|------------|---------------|------------|
| $a$        | $\{b, d\}$   | 2          | $\emptyset$   | 0          |
| $b$        | $\{c\}$      | 1          | $\{a, d\}$    | 2          |
| $c$        | $\{c\}$      | 1          | $\{b, c, d\}$ | 3          |
| $d$        | $\{b, c\}$   | 2          | $\{a\}$       | 1          |

Der Nachfolgergrad entspricht also der Anzahl der Pfeile, die einen Knoten verlassen, und der Vorgängergrad entspricht der Anzahl der Pfeile, die in einen Knoten münden.  $\square$

Mit  $\sum_{x \in V} d_g^+(x)$  bezeichnet man die Summe der Außengrade eines gerichteten Graphen  $g = (V, P)$ . Wenn  $V = \{x_1, \dots, x_n\}$  gilt, so ist dies nur eine andere Schreibweise für die schon bekannte Schreibweise  $\sum_{i=1}^n d_g^+(x_i)$ . Analog ist  $\sum_{x \in V} d_g^-(x)$  als Schreibweise für  $\sum_{i=1}^n d_g^-(x_i)$  erklärt. Mit diesen Festlegungen gilt das nachfolgende Resultat.

### 6.3.3 Satz: Gradformeln

Für alle gerichteten Graphen  $g = (V, P)$  gilt

$$\sum_{x \in V} d_g^+(x) = |P| = \sum_{x \in V} d_g^-(x).$$

**Beweis:** Es sei  $V = \{x_1, \dots, x_n\}$  die Knotenmenge des vorgegebenen Graphen. Dann gilt

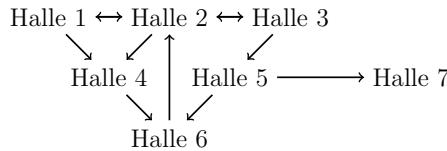
$$\begin{aligned} |P| &= \left| \bigcup_{i=1}^n \{(x_i, y) \mid y \in V \wedge x_i P y\} \right| && \text{disjunkte Zerlegung} \\ &= \sum_{i=1}^n |\{(x_i, y) \mid y \in nachf_g(x_i)\}| && \text{alle Mengen disjunkt} \\ &= \sum_{i=1}^n |\{x_i\} \times nachf_g(x_i)| \\ &= \sum_{i=1}^n |nachf_g(x_i)| && \text{Kardinalität Produkt} \\ &= \sum_{i=1}^n d_g^+(x_i) \end{aligned}$$

und analog dazu zeigt man auch die zweite Gleichung  $|P| = \sum_{i=1}^n d_g^-(x_i)$ .  $\square$

Wichtig bei gerichteten Graphen sind vor allem Fragen, welche die Erreichbarkeit betreffen. Wir wollen dies nachfolgend an einem Beispiel motivieren. Dieses zeigt auch, wie man praktische Problemstellungen mittels gerichteter Graphen modellieren kann. Dies macht Graphen insbesondere für Anwendungen bedeutsam, auch in der Informatik.

### 6.3.4 Beispiel: Graphen als Modelle

Der folgende gerichtete Graph beschreibt ein System von Fertigungshallen und gerichteten Transportbändern zwischen den Hallen. Ein Doppelpfeil deutet dabei an, dass ein Transport in beide Richtungen möglich ist. Oft werden Doppelpfeile auch als zwei einzelne Pfeile in entgegengesetzte Richtungen gezeichnet.



Aufgrund dieser Zeichnung kann man etwa Teile von Halle 1 zu allen anderen Hallen transportieren. Eine Möglichkeit zu Halle 3 zu kommen, ist, über Halle 2 zu transportieren. Dies ist aber nicht die einzige Möglichkeit. Es geht auch über Halle 4, dann Halle 6 und dann noch Halle 2. Von Halle 7 kommt man zu keiner anderen Halle und von Halle 6 kommt man z.B. auch wieder über Halle 2 und Halle 4 zu Halle 6 zurück.  $\square$

Man könnte solche Erreichbarkeiten in gerichteten Graphen beispielsweise auch durch Listen von Pfeilen beschreiben. Mathematisch sind Listen von Knoten jedoch einfacher handhabbar. Deshalb führt man Wege und Kreise wie nachfolgend gegeben als Knotenlisten ein. In Zeichnungen von gerichteten Graphen kennzeichnet man sie in der Regel jedoch durch das Hervorheben der entsprechenden Pfeile. Wir erinnern noch einmal an die beiden Listenoperationen *rest*, welche den Kopf einer nichtleeren Liste entfernt, und  $|\cdot|$ , welche die Listenlänge bestimmt.

### 6.3.5 Definition: Weg, Kreis, Erreichbarkeit, Kreisfreiheit

Es sei  $g = (V, P)$  ein gerichteter Graph.

- (1) Eine lineare Liste  $w \in V^+$  heißt ein **Weg** von  $w_1$  nach  $w_{|w|}$  in  $g$ , falls alle Knoten  $w_i, 1 \leq i \leq |w|$ , paarweise verschieden sind und für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq |w| - 1$  die Beziehung  $w_i P w_{i+1}$  gilt. Mit  $|w| - 1$  bezeichnet man die (**graphentheoretische Länge**) von  $w$ , d.h. die Anzahl der in  $w$  vorkommenden Pfeile.
- (2) Eine lineare Liste  $w \in V^+$  heißt ein **Kreis** in  $g$ , falls  $|w| \geq 2$  gilt (also mindestens ein Pfeil in  $w$  liegt), die Restliste  $rest(w)$  ein Weg (von  $w_2$  nach  $w_{|w|}$ ) ist,  $w_1 P w_2$  gilt (d.h. das Paar  $(w_1, w_2)$  ein Pfeil ist) und  $w_1 = w_{|w|}$  zutrifft. Mit  $|w| - 1$  bezeichnet man wiederum die (**graphentheoretische Länge**) von  $w$ .
- (3) Existiert ein Weg  $w \in V^+$  mit  $w_1 = x$  und  $w_{|w|} = y$ , so heißt der Knoten  $y \in V$  in  $g$  vom Knoten  $x \in V$  aus mittels des Weges  $w$  **erreichbar**.

(4) Gibt es in  $g$  keinen Kreis, so heißt  $g$  **kreisfrei**. □

Per Definition ist also jeder Knoten  $x$  von sich aus mittels des Weges ( $x$ ) erreichbar. Man beachte, dass es einen Weg mit mindestens zwei Knoten nur zwischen zwei verschiedenen Knoten geben kann.

Wenn aus dem Zusammenhang klar ist, welcher Graph  $g$  gemeint ist, und wenn der konkrete Weg  $w$  nicht relevant ist, so lässt man bei der Angabe der Beziehung „ist erreichbar“ sowohl  $g$  als auch  $w$  weg. Weil alle Knoten von Wegen in gerichteten Graphen paarweise verschieden sein müssen, gilt  $|w| \leq |V|$  für alle Wege  $w$  in  $g = (V, P)$ . Man spricht oft auch von **elementaren Wegen**. Bei Kreisen sind die Endknoten gleich, alle anderen Knoten sind ebenfalls paarweise verschieden. Das führt auch zur Sprechweise „**elementarer Kreis**“ für das, was wir in Punkt (2) von Definition 6.3.5 festgelegt haben. Im Hinblick auf das obige Beispiel mit den Hallen haben wir etwa: (Halle 1, Halle 2, Halle 3) ist ein Weg von Halle 1 zu Halle 3 der Länge 2, (Halle 1, Halle 4, Halle 6, Halle 2, Halle 3) ist ein Weg von Halle 1 zu Halle 3 der Länge 4 und (Halle 6, Halle 2, Halle 4, Halle 6) ist ein Kreis. Dieser letztgenannte Kreis ist beispielsweise verschieden vom Kreis (Halle 2, Halle 4, Halle 6, Halle 2), obwohl der eben aufgeführte Kreis in der Zeichnung unter der alleinigen Betrachtung der entsprechenden Pfeile gleich aussieht. Man beachte: Verschiedenheit von Wegen und Kreisen meint die Verschiedenheit als lineare Listen. Ein Problem entsteht oft bei der Angabe von Längen. Bei Wegen und Kreisen gibt es einen Längenbegriff im Sinne der linearen Listen und einen Längenbegriff im Sinne der Graphentheorie. Beide unterscheiden sich um Eins. Damit in Zukunft Verwechslungen vermieden werden, **werden wir ab jetzt bei Längenangaben konsequent immer die Länge im Sinne von linearen Listen verwenden**, also  $|w|$  schreiben. Das ist zwar aus graphentheoretischer Sicht etwas ungewöhnlich, aber besser vereinbar mit der bisherigen Behandlung von linearen Listen in diesem Text.

Die Erreichbarkeitsbeziehungen und das Vorhandensein bzw. Nichtvorhandensein von Kreisen in gerichteten Graphen kann durch eine bestimmte Konstruktion auf Relationen sehr elegant beschrieben werden. Dem Thema wollen wir uns nun zuwenden. Wir verlassen dazu kurzfristig die Welt der homogenen Relationen und starten mit der Definition einer neuen Operation auf beliebigen Relationen.

### 6.3.6 Definition: relationale Komposition

Zu zwei Relationen  $R \subseteq M \times N$  und  $S \subseteq N \times Q$  ist deren **Komposition** (auch Multiplikation oder Produkt genannt)  $RS \subseteq M \times Q$  definiert durch

$$RS := \{(x, z) \in M \times Q \mid \exists y \in N : x R y \wedge y S z\},$$

also für alle  $x \in M$  und  $z \in Q$  durch die Festlegung von  $x (RS) z$  genau dann, wenn ein  $y \in N$  mit  $x R y$  und  $y S z$  existiert. □

Sind  $R$  und  $S$  Funktionen, so entspricht die relationale Komposition  $RS$  genau der Funktionskomposition  $S \circ R$ . Im nachfolgenden Satz sind drei Grundtsachen der Komposition angegeben, die so einfach zu beweisen sind, dass wir auf die Beweise verzichten. Es sei jedoch der Leserin oder dem Leser empfohlen, sie zu Übungszwecken mittels logischer Transformationen im Sinne des zweiten Kapitels selbst durchzuführen.

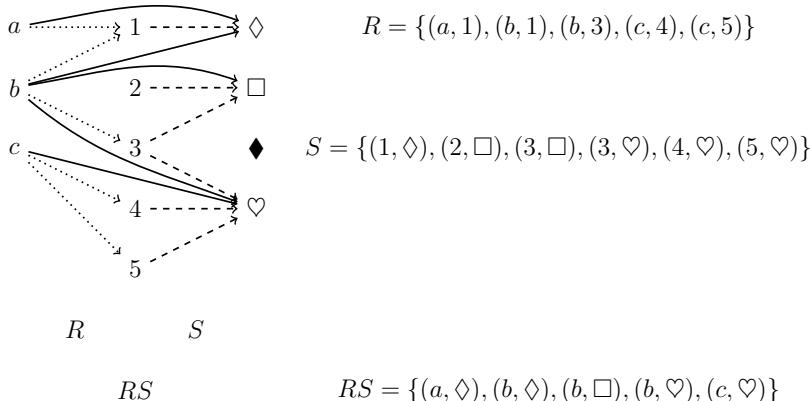
### 6.3.7 Satz: Grundeigenschaften der Komposition

- (1) Für alle Relationen  $R \subseteq M \times N$ ,  $S \subseteq N \times Q$  und  $T \subseteq Q \times Z$  gilt die Assoziativität  $R(ST) = (RS)T$  der Komposition.
- (2) Für alle Relationen  $R \subseteq M \times N$  gilt  $\mathbf{I}_M R = R$  (mit  $\mathbf{I}_M$  als identische Relation auf  $M$ ) und auch  $R\mathbf{I}_N = R$  (mit  $\mathbf{I}_N$  als identische Relation auf  $N$ ).  $\square$

Identische Relationen sind also links bzw. rechtsneutral hinsichtlich der Komposition. Sie werden in der Literatur in der Regel mit dem gleichen Buchstaben **I** bezeichnet. Der Index wird also weggelassen, da er aus dem Kontext rekonstruiert werden kann. Auch wir werden dies im Folgenden tun, da es sich bei den Anwendungen immer um die identische Relation auf der Knotenmenge eines vorgegebenen gerichteten Graphen handelt. Das folgende Beispiel verdeutlicht die Komposition von Relationen.

### 6.3.8 Beispiel: Komposition

Es seien drei Mengen  $M := \{a, b, c\}$ ,  $N := \{1, 2, 3, 4, 5\}$  und  $Q := \{\diamondsuit, \square, \blacklozenge, \heartsuit\}$  vorgegeben. In der nachfolgenden Zeichnung sind die bipartiten Pfeildiagramme für zwei Relationen  $R \subseteq M \times N$  und  $S \subseteq N \times Q$  und deren Komposition graphisch dargestellt.



Man sieht anhand dieser Zeichnung sofort, dass ein Pfeil in dem Produkt  $RS$  genau dann existiert, wenn dieser durch einen Zwischenpunkt und zwei Pfeile aus  $R$  und  $S$  beschrieben werden kann, die in dem Zwischenpunkt enden bzw. beginnen. Dies verdeutlicht noch einmal, dass im Fall von Funktionen die relationale Komposition genau der Funktionskomposition (mit vertauschten Argumenten) entspricht.  $\square$

Nach diesem Ausflug in die Welt der beliebigen Relationen kehren wir für den Rest des Abschnitts zu den homogenen Relationen und den gerichteten Graphen zurück. Ist  $R$  eine homogene Relation, so gibt es einen Pfeil in  $RR$  genau dann, wenn er bildlich als Folge von zwei Pfeilen aus  $R$  dargestellt werden kann, es gibt einen Pfeil in  $RRR$  genau dann, wenn er bildlich als Folge von drei Pfeilen in  $R$  dargestellt werden kann, und so weiter. Dies motiviert die folgende Definition von Potenzen homogener Relationen und, darauf aufbauend, von zwei sogenannten relationalen Hüllen.

### 6.3.9 Definition: transitive und reflexiv-transitive Hülle

Es sei  $R \subseteq M \times M$  eine homogene Relation auf der Menge  $M$ .

- (1) Die  $n$ -te **Potenz**  $R^n$  von  $R$  ist rekursiv definiert durch  $R^0 := \mathbf{I}$  und  $R^n := RR^{n-1}$  für alle  $n \in \mathbb{N} \setminus \{0\}$ .
- (2) Die Relation  $R^+ := \bigcup\{R^n \mid n \in \mathbb{N} \setminus \{0\}\}$  heißt die **transitive Hülle** von  $R$  und die Relation  $R^* := \bigcup\{R^n \mid n \in \mathbb{N}\}$  heißt die **reflexiv-transitive Hülle** von  $R$ .  $\square$

Die transitive Hülle von  $R$  ist die bezüglich der Inklusion kleinste transitive Relation, die  $R$  enthält, und die reflexiv-transitive Hülle von  $R$  ist die bezüglich der Inklusion kleinste reflexive und transitive Relation, die  $R$  enthält. Dies ist der Hintergrund für die Namensgebung, denn beide beschreiben eine sogenannte Hüllenbildung. In der Literatur schreibt man  $\bigcup_{n>0} R^n$  oder auch  $\bigcup_{n \geq 1} R^n$  statt der etwas schwerfälligen Notation  $\bigcup\{R^n \mid n \in \mathbb{N} \setminus \{0\}\}$ . Analog schreibt man normalerweise  $\bigcup_{n \geq 0} R^n$  statt  $\bigcup\{R^n \mid n \in \mathbb{N}\}$ . Auch wir verwenden aus Gründen der Lesbarkeit von nun an die einfacheren Schreibweisen, was zu  $R^+ = \bigcup_{n \geq 1} R^n$  und  $R^* = \bigcup_{n \geq 0} R^n$  führt. Wie der nächste Satz zeigt, sind die beiden Hüllen ineinander umrechenbar.

### 6.3.10 Satz: Zusammenhang zwischen den Hüllen

Für alle Relationen  $R \subseteq M \times M$  gelten die Gleichungen:  $R^* = \mathbf{I} \cup R^+$  und  $R^+ = RR^*$ .

**Beweis:** Die folgende Verifikation der ersten Gleichung verwendet die Definition von  $R^*$ , dann Teil (1) von Satz 1.2.7 und schließlich noch die Definition von  $R^+$  und von  $R^0$ :

$$R^* = \bigcup_{n \geq 0} R^n = (\bigcup_{n \geq 1} R^n) \cup R^0 = R^+ \cup \mathbf{I}.$$

Zum Beweis der zweiten Gleichung nehmen wir  $x, y \in M$  als beliebig gegeben an. Dann können wir wie folgt logisch umformen:

$$\begin{aligned} x(RR^*)y &\iff x(R(\bigcup_{n \geq 0} R^n))y && \text{Definition } R^* \\ &\iff \exists z \in M : xRz \wedge z(\bigcup_{n \geq 0} R^n)y && \text{Definition Komposition} \\ &\iff \exists z \in M : xRz \wedge \exists n \in \mathbb{N} : zR^n y && \text{Definition } \bigcup_{n \geq 0} R^n \\ &\iff \exists n \in \mathbb{N} : \exists z \in M : xRz \wedge zR^n y && \text{Logik} \\ &\iff \exists n \in \mathbb{N} : x(RR^n)y && \text{Definition Komposition} \\ &\iff \exists n \in \mathbb{N} : x(R^{n+1})y && \text{Definition Potenz} \\ &\iff \exists n \in \mathbb{N} \setminus \{0\} : xR^n y && \text{Indextransformation} \\ &\iff x(\bigcup_{n \geq 1} R^n)y && \text{Definition } \bigcup_{n \geq 1} R^n \\ &\iff xR^+y && \text{Definition } R^+ \end{aligned}$$

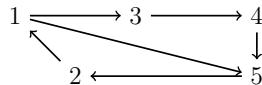
Die Definition der Mengengleichheit (Relationen sind ja spezielle Mengen) zeigt nun die Behauptung.  $\square$

Nach dieser Abschweifung in die Theorie der Relationen kehren wir wieder zum eigentlichen Thema zurück. Dabei verwenden wir wieder, wie anfangs eingeführt,  $P$  als Bezeichner für die Pfeilrelation. Bei der Definition des Begriffs „Weg“ hatten wir alle Knoten als paarweise verschieden gefordert. Diese Beschränkung lassen wir nun weg, weil es das Argumentieren mittels Hüllen wesentlich vereinfacht. Der folgende Begriff verallgemeinert Wege zu linearen Listen, in denen Knoten auch mehrfach vorkommen dürfen.

### 6.3.11 Definition: Pfad

Es sei  $g = (V, P)$  ein gerichteter Graph. Eine lineare Liste  $s \in V^+$  heißt ein **Pfad** von  $s_1$  nach  $s_{|s|}$ , falls für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq |s| - 1$  die Beziehung  $s_i P s_{i+1}$  gilt.  $\square$

Analog zu den Wegen heißt die Zahl  $|s| - 1$  die (graphentheoretische) **Länge des Pfads**. Wir werden, aus dem gleichen Grund wie schon bei den Wegen erklärt, diese graphentheoretische Längendefinition von Pfaden in Zukunft aber ebenfalls nicht verwenden. Wege sind offensichtlich Pfade, die Umkehrung gilt jedoch nicht, da in Pfaden Kreise als Teillisten auftreten können. Diese entstehen, wenn nicht alle Knoten paarweise verschieden sind. Wir machen den Unterschied noch an dem rechten der beiden einführenden Beispiele dieses Abschnitts deutlich. In dem folgenden gerichteten Graphen ist beispielsweise die lineare Liste  $(2, 1, 3, 4, 5)$  ein Weg vom Knoten 2 zum Knoten 5. Hingegen ist  $(2, 1, 3, 4, 5, 2, 1, 3, 4, 5)$  kein Weg vom Knoten 2 zum Knoten 5. Diese lineare Liste ist nur ein Pfad, da die Knoten 1, 2, 3, 4 und 5 mehrfach auftreten. Die Teilliste  $(1, 3, 4, 5, 2, 1)$  bildet etwa einen Kreis.



Einelementige Listen ( $x$ ) sind immer zugleich Wege und Pfade. Bezuglich der Erreichbarkeit in gerichteten Graphen macht das Vorhandensein von Kreisen in Paden keinen Unterschied zur Erreichbarkeit mittels Wegen, wie der folgende Satz zeigt. In seinem Beweis benutzen wir die aus Kapitel 3 bekannte Konkatenationsoperation auf linearen Listen.

### 6.3.12 Satz: Erreichbarkeit mittels Wegen und Pfaden

Es seien  $g = (V, P)$  ein gerichteter Graph und  $x, y \in V$  zwei Knoten. Dann sind die folgenden Aussagen äquivalent.

- (1) Es ist  $y$  von  $x$  aus in  $g$  erreichbar.
- (2) Es gibt in  $g$  einen Pfad von  $x$  nach  $y$ .

**Beweis:** Wir beweisen zuerst, dass die Aussage (2) aus (1) folgt. Ist der Knoten  $y$  vom Knoten  $x$  aus erreichbar, so gibt es per Definition einen Weg von  $x$  nach  $y$ . Dieser Weg ist insbesondere auch ein Pfad von  $x$  nach  $y$ . Somit gilt (2).

Nun kommen wir zur anderen Richtung und nehmen dazu an, dass (2) gilt. Gibt es einen Pfad von  $x$  nach  $y$ , so gibt es auch einen Pfad von  $x$  nach  $y$  mit kleinster Länge, denn die natürlichen Zahlen sind Noethersch geordnet. Es sei die Liste  $s \in V^+$  so ein kürzester Pfad. Wir zeigen nachfolgend, dass  $s$  dann auch ein Weg ist, womit auch (1) gezeigt ist. Dazu

führen wir einen Beweis durch Widerspruch. Angenommen, der Pfad  $s$  sei kein Weg. Dann gibt es in  $s$  zwei identische Knoten und somit hat  $s$  die Form  $s = a \& (z) \& b \& (z) \& c$ , mit  $a, b, c \in V^*$  und  $z \in V$ . Das Entfernen der Teilliste  $b \& (z)$  aus dem Pfad  $s$  führt offensichtlich immer noch zu einem Pfad von  $x$  nach  $y$ . Dieser Pfad  $a \& (z) \& c$  ist aber echt kürzer als  $s$ . Dies ist ein Widerspruch.  $\square$

Und hier ist nun die entscheidende Eigenschaft, welche die Existenz von Pfaden mit dem Enthaltensein in der reflexiv-transitiven Hülle verbindet. Die in ihm angegebene Beziehung zwischen  $P^n$  und  $|s|$  ist der Grund für die graphentheoretische Längendefinition von Wegen.

### 6.3.13 Satz: Pfade und Hüllen

Es sei  $g = (V, P)$  ein gerichteter Graph. Dann gilt für alle  $n \in \mathbb{N}$  und für alle Knoten  $x, y \in V$  die Beziehung  $x P^n y$  genau dann, wenn es einen Pfad  $s$  von  $x$  nach  $y$  mit  $|s| = n + 1$  (also  $n$  Pfeilen) gibt.

**Beweis (durch vollständige Induktion):** Das Prädikat  $A(n)$  besagt, dass für alle Knoten  $x, y \in V$  die zu zeigende Äquivalenz gilt.

Induktionsbeginn, Beweis von  $A(0)$ . Es sei  $n = 0$ . Weiterhin seien, zum Beweis von „ $\Rightarrow$ “, beliebige Knoten  $x, y \in V$  gegeben. Aus der Beziehung  $x P^0 y$  folgt dann  $x \mathbf{I} y$ , also auch  $x = y$ . Es ist aber  $s := (x)$  ein Pfad von  $x$  nach  $y$  mit der Länge  $|s| = 0 + 1$ . Gibt es, um die andere, noch verbleibende Richtung „ $\Leftarrow$ “ zu zeigen, einen Pfad  $s$  von  $x$  nach  $y$  mit  $|s| = 0 + 1 = 1$ , so muss  $s = (x) = (y)$  gelten und daraus folgt  $x = y$  aufgrund der Gleichheit von Listen.

Induktionsschluss von  $A(n)$  auf  $A(n + 1)$ : Es sei  $n \in \mathbb{N}$  und es gelte die Induktionshypothese  $A(n)$ . Wiederum seien  $x, y \in V$  beliebige Knoten. Wir teilen den Beweis in zwei Teilbeweise auf und verwenden dabei bekannte Operationen auf Listen.

Wir starten mit „ $\Rightarrow$ “. Es gelte also  $x P^{n+1} y$ . Wegen der Definition der relationalen Komposition gibt es dann ein  $z \in V$  mit  $x P z$  und  $z P^n y$ . Nach der Induktionshypothese  $A(n)$  existiert somit ein Pfad  $t$  von  $z$  nach  $y$  mit  $|t| = n + 1$ . Definiert man  $s := x : t$ , so ist, wie man sehr einfach verifiziert,  $s$  ein Pfad von  $x$  nach  $y$ . Seine Länge ist  $|s| = |x : t| = 1 + |t| = n + 2$ . Nun zeigen wir „ $\Leftarrow$ “. Dazu sei  $s = (s_1, \dots, s_{n+2}) \in V^{n+2}$  ein Pfad von  $x$  nach  $y$ . Dann gilt  $x P s_2$  und es ist auch  $\text{rest}(s)$  ein Pfad vom Knoten  $s_2$  nach  $y$  mit  $n + 1$  Knoten. Nach der Induktionshypothese  $A(n)$  gilt also  $s_2 P^n y$ . Die Definition der relationalen Komposition bringt nun  $x P^{n+1} y$ .  $\square$

Nun endlich können wir den Zusammenhang zwischen der Erreichbarkeit in gerichteten Graphen  $g = (V, P)$  und der reflexiv-transitiven Hülle  $P^*$  der entsprechenden Pfeilrelationen  $P$  herstellen, auf den wir die ganze Zeit hinarbeiteten.

### 6.3.14 Satz: Erreichbarkeit und Hüllen

Es seien  $g = (V, P)$  ein gerichteter Graph und  $x, y \in V$  zwei Knoten. Dann gilt  $x P^* y$  genau dann, wenn  $y$  von  $x$  aus erreichbar ist.

**Beweis:** Wir rechnen mittels der Definition von  $P^*$  und  $\bigcup_{n \geq 0} P^n$  wie folgt:

$$xP^*y \iff x\left(\bigcup_{n \geq 0} P^n\right)y \iff \exists n \in \mathbb{N} : xP^n y$$

Um den Beweis zu beenden, ist noch die folgende logische Äquivalenz nachzuweisen:

$$\exists n \in \mathbb{N} : xP^n y \iff y \text{ ist von } x \text{ aus erreichbar}$$

„ $\implies$ “: Es sei  $n \in \mathbb{N}$  so, dass  $xP^n y$  zutrifft. Dann gibt es einen Pfad  $s$  von  $x$  nach  $y$  (mit  $|s| = n + 1$ , was aber unwesentlich ist); siehe Satz 6.3.13. Aus Satz 6.3.12 folgt nun, dass  $y$  von  $x$  aus erreichbar ist.

„ $\impliedby$ “: Es sei  $y$  von  $x$  aus erreichbar. Nach Satz 6.3.12 gibt es dann einen Pfad  $s$  von  $x$  nach  $y$ . Wir setzen  $n := |s| - 1$ . Dann gibt es also ein  $n \in \mathbb{N}$  so, dass die folgende Aussage wahr ist: Es gibt einen Pfad von  $x$  nach  $y$  der Länge  $n + 1$ . Weil diese Aussage äquivalent zu  $xP^n y$  ist, siehe Satz 6.3.13, gibt es also ein  $n \in \mathbb{N}$  mit  $xP^n y$ .  $\square$

Mit Hilfe der Relation  $P^*$  kann man also alle Erreichbarkeiten von allen Knotenpaaren in einem gerichteten Graphen  $g = (V, P)$  testen. Nach Definition ist  $P^*$  eine unendliche Vereinigung von Potenzen von  $P$ . Algorithmisch kann man unendliche Vereinigungen nicht berechnen. Weil die Knotenmenge  $V$  endlich ist, ist dies aber auch gar nicht notwendig. Endlich viele Potenzen genügen schon, wie der folgende Satz zeigt.

### 6.3.15 Satz: Berechnung von Hüllen

Für alle gerichteten Graphen  $g = (V, P)$  gilt die Gleichung  $P^* = \bigcup_{n=0}^{|V|-1} P^n$ .

**Beweis:** Wegen  $\bigcup_{n=0}^{|V|-1} P^n \subseteq \bigcup_{n \geq 0} P^n = P^*$  ist für alle  $x, y \in V$  nur zu zeigen, dass aus  $xP^*y$  folgt  $x\left(\bigcup_{n=0}^{|V|-1} P^n\right)y$ . Gilt  $xP^*y$ , so ist  $y$  aufgrund von Satz 6.3.14 von  $x$  aus erreichbar. Per Definition gibt es also einen Weg  $w$  von  $x$  nach  $y$ . Dies impliziert  $xP^{|w|-1}y$  aufgrund von Satz 6.3.13, wobei  $1 \leq |w| \leq |V|$ . Also gibt es ein  $n \in \{0, \dots, |V| - 1\}$ , nämlich  $n := |w| - 1$ , mit  $xP^n y$ . Dies zeigt  $x\left(\bigcup_{n=0}^{|V|-1} P^n\right)y$ .  $\square$

Zum Testen der Kreisfreiheit von gerichteten Graphen  $g = (V, P)$  kann die transitive Hülle  $P^+$  herangezogen werden, welche ebenfalls aufgrund von  $P^+ = \bigcup_{n=1}^{|V|-1} P^n$  in endlich vielen Rechenschritten berechnet werden kann. Es gilt nämlich das folgende Resultat.

### 6.3.16 Satz: Testen auf das Vorhandensein von Kreisen

Es sei  $g = (V, P)$  ein gerichteter Graph. Dann sind die folgenden Aussagen äquivalent:

- (1) Der gerichtete Graph  $g$  enthält einen Kreis.
- (2) Es gibt einen Knoten  $x \in V$  mit  $xP^+x$ .

**Beweis:** Zum Beweis von „(1)  $\implies$  (2)“ sei  $w \in V^+$  ein Kreis in  $g$  mit  $w = (w_1, \dots, w_n)$ . Dann gilt  $w_1Pw_2$  und es ist  $(w_2, \dots, w_n)$  ein Weg von  $w_2$  nach  $w_n$ . Nach Satz 6.3.14 gilt also  $w_2P^*w_n$ . Die Definition der relationalen Komposition bringt  $w_1(PP^*)w_n$  und aus

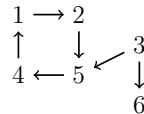
Satz 6.3.10 erhalten wir  $w_1 P^+ w_n$ . Aus  $w_1 = w_n$  folgt nun  $x P^+ x$ , wenn wir  $x := w_1$  setzen.

Die Implikation „(2)  $\implies$  (1)“ zeigt man wie folgt: Es sei  $x \in V$  mit  $x P^+ x$ . Nach Satz 6.3.10 gilt also  $x (PP^*) x$ . Folglich gibt es einen Knoten  $y \in V$  mit  $x Py$  und  $y P^* x$ . Mit Hilfe von Satz 6.3.14 bekommen wir die Existenz eines Weges  $w$  von  $y$  nach  $x$ . Offensichtlich ist dann die lineare Liste  $x : w$  ein Kreis in  $g$ .  $\square$

Für die folgenden Bemerkungen setzen wir voraus, dass der Leserin oder dem Leser der Begriff einer Matrix bekannt ist, sowie, wie man Matrizen multipliziert und addiert. Stellt man die Relation  $P$  eines gerichteten Graphen  $g = (V, P)$  durch eine Boolesche Matrix dar, also eine Matrix nur mit Einträgen 0 (für „falsch“) und 1 (für „wahr“), so entspricht die Komposition  $PP$  der Multiplikation von  $P$  mit sich selbst, wobei die Einträge wie bei Zahlen üblich multipliziert werden. Die Multiplikation entspricht nämlich bei der eben genannten Interpretation der Null und der Eins genau der Konjunktion. Die relationale Vereinigung bekommt man dadurch, indem man die Einträge der Matrizen mit einer Art von Addition verknüpft, welche der Disjunktion entspricht. Man addiert also 0 und 1 wie üblich mit der einen Ausnahme, dass  $1 + 1 = 1$  ergibt. Damit kann man sowohl die Relation  $P^+$  als auch die Relation  $P^*$  bestimmen. Diese Verfahren sind aber langsamer als die üblicherweise benutzten Algorithmen, welche man im Informatik-Studium später noch kennenlernen wird. Sie brauchen, in einer Angabe mit den Landau-Symbol des vorhergehenden Kapitels,  $\mathcal{O}(|V|^4)$  Boolesche Additionen und Multiplikationen, während bessere Verfahren schon mit  $\mathcal{O}(|V|^3)$  Booleschen Additionen und Multiplikationen auskommen (also „kubische Laufzeit besitzen“). In dem folgenden Beispiel demonstrieren wir die Vorgehensweise zur Berechnung von  $P^*$  und  $P^+$  in einer Matrizendarstellung an einer kleinen Matrix.

### 6.3.17 Beispiel: Erreichbarkeit und Kreise

Wir betrachten einen gerichteten Graphen  $g = (V, P)$  mit sechs Knoten. Diese seien die natürlichen Zahlen von 1 bis 6. Die zeichnerische Darstellung von  $g$  sieht wie folgt aus:



Dieser gerichtete Graph besitzt auch sechs Pfeile. Welcher Knoten mit welchen Knoten durch einen Pfeil verbunden ist, ergibt sich sofort aus der Zeichnung und auch aus der Booleschen Matrix zur Relation  $P$ , die nachfolgend angegeben ist. Im Prinzip ist die Matrix genau das, was wir früher als Kreuztabelle zu  $P$  bezeichnet haben.

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 1 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |

Weil die Gleichungen  $P^+ = P \cup P^2 \cup P^3 \cup P^4 \cup P^5$  und  $P^* = \mathbf{I} \cup P^+$  gelten, genügt es, die Potenzen  $P^2$  bis  $P^5$  der Relation (Matrix)  $P$  zu berechnen. Man bekommt hier als Matrizen die folgenden Resultate:

$$\begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & P^2 & & & & & \end{array} \quad \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & P^3 & & & & & \end{array} \quad \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & P^4 & & & & & \end{array} \quad \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 4 & 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 1 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & P^5 & & & & & \end{array}$$

Aus diesen Matrizen und der Einheitsmatrix (mit Einsen in der Diagonalen und sonst nur Nullen) berechnet man durch Matrix-Additionen die reflexiv-transitive Hülle  $P^*$  und die transitive Hülle  $P^+$  jeweils in einer Matrix-Darstellung wie folgt:

$$\begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 & 1 & 1 & 0 \\ 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 1 & 1 & 0 & 1 & 1 & 0 \\ 5 & 1 & 1 & 0 & 1 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline & P^* & & & & & \end{array} \quad \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & \mathbf{1} & 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & \mathbf{1} & 0 & 1 & 1 & 0 \\ 3 & 1 & 1 & 0 & 1 & 1 & 1 \\ 4 & 1 & 1 & 0 & \mathbf{1} & 1 & 0 \\ 5 & 1 & 1 & 0 & 1 & \mathbf{1} & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & P^+ & & & & & \end{array}$$

Aus der linken Matrix (der zu  $P^*$ ) ist durch die Einsen sofort erkennbar, welcher Knoten von welchem Knoten aus erreichbar ist. Man vergleiche die entsprechenden Einträge noch einmal mit der oben angegebenen zeichnerischen Darstellung des gerichteten Graphen. Anhand der Diagonale der rechten Matrix (der zu  $P^+$ ) bekommt man nicht nur, dass in  $g$  ein Kreis existiert. Darüber hinaus werden durch die Einsen auf ihr sogar genau diejenigen Knoten angegeben, die auf einem Kreis liegen. Es sind dies genau die Knoten 1, 2, 4 und 5. Diese Eigenschaft verifiziert man auch sofort anhand der obigen Zeichnung des Graphen.  $\square$

Wir hatten bei den gerichteten Graphen per Definition gefordert, dass die Knotenmengen immer endlich und auch nicht leer sind. Damit kann man Induktion über die Kardinalität der Knotenmenge durchführen. Wie das im Fall der vollständigen Induktion mit der Eins als Induktionsbeginn aussieht, ist nachfolgend angegeben. Der Induktionsbeginn ist dadurch bedingt, dass alle Knotenmengen nicht leer sein müssen. In analoger Weise kann man auch das Prinzip der Noetherschen Induktion auf gerichtete Graphen übertragen. Auch Induktion über die Anzahl der Pfeile ist möglich, wenn man die Anzahl der Knoten als fixiert annimmt. Darauf wollen wir aber nicht eingehen.

### 6.3.18 Satz: Induktion bei Graphen

Es sei  $A(g)$  eine Aussage, in der die Variable  $g$  für einen gerichteten Graphen steht. Weiterhin seien die folgenden Aussagen gültig:

- (1) Es gilt  $A(g)$  für alle gerichteten Graphen  $g$  mit einem Knoten.

- (2) Für alle  $n \in \mathbb{N}$  gilt: Ist  $A(h)$  für alle gerichteten Graphen  $h$  mit  $n$  Knoten wahr, so ist auch  $A(g)$  auch für alle gerichteten Graphen  $g$  mit  $n + 1$  Knoten wahr.

Dann gilt  $A(g)$  für alle gerichteten Graphen  $g$ . □

Die Aussage (1) dieses Satzes heißt wiederum Induktionsbeginn und die Aussage (2) nennt man ebenfalls Induktionsschluss, mit der Induktionshypothese, dass  $A(h)$  für alle gerichteten Graphen  $h$  mit  $n$  Knoten wahr ist. Ein Beweis des Satzes ist nicht notwendig, denn es handelt sich bei seiner Aussage um eine spezielle Instanz der vollständigen Induktion. Diese Instanz verwendet „für alle gerichteten Graphen  $g$  mit  $n$  Knoten gilt  $A(g)$ “ als Prädikat in  $n$ . Dass dieses Prädikat für alle  $n \in \mathbb{N}$  gilt, besagt genau, dass  $A(g)$  für alle gerichteten Graphen  $g$  gilt. Nachfolgend geben wir nun ein Beispiel für eine Anwendung von Satz 6.3.18 an.

### 6.3.19 Satz: Anwendung Grapheninduktion

Für alle gerichteten Graphen  $g = (V, P)$  gilt: Ist  $g$  kreisfrei, so existiert eine Funktion  $ts : V \rightarrow \{1, \dots, |V|\}$  mit der folgenden Eigenschaft:

$$\forall x, y \in V : x P y \Rightarrow ts(x) < ts(y)$$

**Beweis (durch Grapheninduktion):** Das Prädikat  $A(g)$ , welches wir verwenden, besagt gerade, dass eine Funktion  $ts : V \rightarrow \{1, \dots, |V|\}$  mit der geforderte Eigenschaft existiert, sofern  $g$  kreisfrei ist.

Zum Induktionsbeginn sei  $g = (V, P)$  ein beliebiger kreisfreier gerichteter Graph mit einem Knoten  $x$ . Dann erfüllt offensichtlich die Funktion

$$ts : V \rightarrow \{1\} \quad ts(x) = 1$$

die geforderte Eigenschaft, denn sowohl  $x P x$  (wegen der Kreisfreiheit) als auch die Ungleichung  $ts(x) < ts(x)$  sind falsch, was die geforderte Implikation zeigt. Also gilt  $A(g)$ .

Zum Induktionsschluss sei  $n \in \mathbb{N}$  und es existiere eine Funktion  $ts' : W \rightarrow \{1, \dots, n\}$  mit der geforderten Eigenschaft für alle kreisfreien gerichteten Graphen  $h = (W, Q)$  mit  $n$  Knoten, d.h. es gelte die Induktionshypothese. Wir haben zu zeigen, dass dann eine Funktion  $ts : V \rightarrow \{1, \dots, n+1\}$  mit der geforderten Eigenschaft für alle kreisfreien gerichteten Graphen  $g = (V, P)$  mit  $n+1$  Knoten existiert, da dies genau dem Beweis von  $A(g)$  für alle diese Graphen entspricht.

Es sei also  $g$  ein beliebiger solcher gerichteter Graph. Weil  $g$  kreisfrei und die Knotenmenge endlich ist, gibt es in  $g$  mindestens einen Knoten ohne Vorgänger. Es sei  $q \in V$  so ein Knoten. Wir definieren einen kreisfreien gerichteten Graphen  $h = (W, Q)$ , indem wir  $q$  und die ihn berührenden Pfeile aus  $g$  entfernen, also, indem wir  $W$  und  $Q$  wie nachfolgend angegeben festlegen<sup>9</sup>.

$$W := V \setminus \{q\} \quad Q := P \cap (W \times W)$$

---

<sup>9</sup>Die mengentheoretische Spezifikation von  $Q$  besagt genau, dass für alle  $x, y \in W$  die Beziehungen  $x Q y$  und  $x P y$  äquivalent sind. Dass  $Q$  eine Relation auf  $W$  ist, folgt aus der Graphendefinition und  $h = (W, Q)$ .

Aufgrund der Induktionshypothese existiert eine Funktion  $ts' : W \rightarrow \{1, \dots, n\}$  mit der geforderten Eigenschaft für den „Untergraphen“  $h$  von  $g$ . Mit Hilfe von  $ts'$  definieren wir nun die gewünschte Funktion für  $g$  wie folgt.

$$ts : V \rightarrow \{1, \dots, |V|\} \quad ts(x) = \begin{cases} 1 & \text{falls } x = q \\ ts'(x) + 1 & \text{falls } x \in W \end{cases}$$

Es bleibt für die Funktion  $ts$  noch die geforderte Eigenschaft zu zeigen. Dazu seien beliebige Knoten  $x, y \in V$  gegeben. Weiterhin sei  $x P y$  vorausgesetzt. Wir unterscheiden zwei Fälle.

- (a) Es gelte  $x = q$ . Hier folgt sofort  $y \neq q$  wegen  $x P y$  und der vorausgesetzten Kreisfreiheit von  $g$ . Also haben wir  $y \in W$ . Dies bringt

$$ts(x) = 1 < ts'(y) + 1 = ts(y).$$

- (b) Es gelte  $x \neq q$ . Dann gilt auch  $y \neq q$ . Wäre nämlich  $y = q$ , so folgt aus  $x P y$ , dass  $d_g^-(q) = d_g^-(y) \neq 0$ . Das ist ein Widerspruch zur Wahl von  $q$  als Knoten ohne Vorgänger. Also haben wir  $x, y \in W$  und dies zeigt

$$ts(x) = ts'(x) + 1 < ts'(y) + 1 = ts(y).$$

Damit ist der Beweis des Induktionsschlusses beendet und die Grapheninduktion zeigt die Behauptung.  $\square$

Die Funktion  $ts$  des Satzes 6.3.19 kann man so auffassen: Es werden die Knoten eines gegebenen gerichteten Graphen so mit Nummern versehen, dass die Nummerierung mit der Eins beginnt, lückenfrei ist und Pfeile nur zu echt größeren Nummern führen. Man sortiert also den Graphen topologisch im folgenden Sinne.

### 6.3.20 Definition: topologische Sortierung

Eine Funktion  $ts : V \rightarrow \{1, \dots, |V|\}$  heißt eine **topologische Sortierung** des gerichteten Graphen  $g = (V, P)$ , falls  $ts(x) < ts(y)$  für alle  $x, y \in V$  mit  $x P y$  gilt.  $\square$

Nach Satz 6.3.19 sind kreisfreie gerichtete Graphen topologisch sortierbar. Der Satz zeigt auch, wie man eine topologische Sortierung berechnen kann. Welche Funktion dabei berechnet wird, hängt von der Wahl von  $q$  ab. Das durch den Satz beschriebene Verfahren ist, wie man sagt, nichtdeterministisch. Von Satz 6.3.19 gilt auch die Umkehrung. Mit diesem Resultat beenden wir diesen Abschnitt.

### 6.3.21 Satz: topologische Sortierung impliziert Kreisfreiheit

Alle gerichteten Graphen  $g = (V, P)$ , die eine topologische Sortierung  $ts : V \rightarrow \{1, \dots, |V|\}$  besitzen, sind kreisfrei.

**Beweis (durch Widerspruch):** Angenommen, die Behauptung gelte nicht und es gibt somit einen gerichteten Graphen  $g = (V, P)$  mit einer topologischen Sortierung  $ts$ , der auch einen Kreis hat. Dieser Kreis sei die lineare Liste

$$(x_1, \dots, x_n),$$

mit  $n \geq 2$  Knoten. Dann gilt  $x_i P x_{i+1}$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq n - 1$ . Daraus bekommen wir  $ts(x_i) < ts(x_{i+1})$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq n - 1$ . Die Transitivität der Striktordnung impliziert  $ts(x_1) < ts(x_n)$ , also  $ts(x_1) < ts(x_1)$ , weil ja auch  $x_1 = x_n$  gilt. Das ist ein Widerspruch.  $\square$

Man kann die Bestimmung einer topologische Sortierung eines kreisfreien gerichteten Graphen  $g = (V, P)$  auch als eine Lösung des folgenden Problems interpretieren: Gesucht ist eine Partition von  $V$  in  $n$  Mengen und deren Anordnung in Form einer linearen Liste  $(T_1, \dots, T_n)$  so, dass Pfeile nur in echt rechtsstehende Mengen führen. Eine Variante des Problems ist dann dadurch gegeben, dass man nach einer solchen Liste minimaler Länge sucht. Darauf aufbauend ergeben sich für praktische Anwendungen interessante weitere Probleme. Eines davon ist etwa, dass man zusätzlich versucht, die kleinste Menge der Liste möglichst groß (im Sinne der Kardinalität) zu machen. Zur Lösung dieses Problems kennt man aber derzeit keinen effizienten Algorithmus.

## 6.4 Einige Bemerkungen zu mehrstelligen Relationen

Neben dem bisher behandelten Begriff einer Relation als Menge von Paaren gibt es noch den allgemeineren Begriff der mehrstelligen Relation. Diese stellen Mengen von  $n$ -Tupeln dar, also Teilmengen eines direkten Produkts  $\prod_{i=1}^n M_i$ , wobei normalerweise  $n > 1$  angenommen wird. Wie wir in Abschnitt 3.1 angemerkt haben, kann man  $n$ -Tupel  $(x_1, \dots, x_n)$  durch Paarbildungen modellieren, indem man künstlich klammert, beispielsweise in der Form  $(x_1, (x_2, (\dots, (x_{n-1}, x_n) \dots)))$ . Folglich sind  $n$ -stellige Relationen nichts anderes als spezielle Relationen im bisherigen Sinn. Aus praktischen Gründen verzichtet man aber auf die vielen Klammern und arbeitet mit Tupeln.

Ein Gebiet der Informatik, bei dem  $n$ -stellige Relationen eine überragende Rolle spielen, sind die Datenbanken. Bei dem relationalen Datenbankmodell, welches von dem englischen Informatiker Edgar Codd (1923-2003) eingeführt wurde, besteht eine Datenbank aus einer Menge von Tabellen und in jeder Tabelle stellt jede Zeile einen Datensatz dar. Alle Datensätze haben den gleichen Aufbau und werden durch die Angabe von sogenannten Attributen in der gleichen Weise interpretiert. Hier ist ein Beispiel:

| Vorname | Name        | Matrikelnummer | Studiengang | Nebenfach |
|---------|-------------|----------------|-------------|-----------|
| Anton   | Huber       | 405436         | inf         | math      |
| Josef   | Maier       | 307437         | inf         | phy       |
| Maria   | Engelbrecht | 407438         | inf         | math      |
| Egon    | Cordes      | 102430         | inf         | bio       |
| Bente   | Grohmann    | 102530         | inf         | bio       |

Formal sind solche Tabellen spezielle mathematische Objekte, nämlich Paare, bestehend aus einer mehrstelligen Relation und einer Funktion, welche den Komponenten der Tabelle (Relation) die entsprechenden Attribute zuordnet. In dem gerade gebrachten Beispiel ist die Relation fünfstellig und eine Teilmenge des direkten Produkts  $M^* \times M^* \times \mathbb{N} \times S \times S$ , mit den linearen Listen von  $M^*$  aufgefasst als Wörter und  $S = \{\text{math, inf, phys, bio, ...}\}$  als Menge der Studienfächer. Die Menge der Attribute und die Attributzuordnungs-Funktion

sind aus der Kopfzeile der Tabelle ersichtlich.

Die Manipulation und das Abfragen von Daten geschieht durch Operationen. So werden z.B. durch das Vereinigen von zwei Tabellen mit den gleichen Attributen die Datensätze unter Vermeidung von Duplikationen in eine neue Tabelle geschrieben. Die Differenz von zwei Tabellen mit gleichen Attributen filtert aus der ersten Tabelle diejenigen Datensätze heraus, die nicht in der zweiten Tabelle enthalten sind, und speichert sie in einer neuen Tabelle ab. Schließlich sei noch die Projektion genannt. Sie hat eine Menge von Attributen und eine Tabelle als Eingabe und liefert diejenigen Spalten der Tabelle in Form einer neuen Tabelle als Resultat, die zu den gegebenen Attributen gehören.

Insbesondere in der theoretischen Informatik sind spezielle dreistellige Relationen als Teilmengen von  $S \times A \times S$  von Bedeutung. Sie werden **Transitionssysteme** genannt und dazu verwendet, das Verhalten von zustandsbasierten Systemen zu modellieren und zu beschreiben. Dazu wird jedes Element von  $S$  als Zustand und jedes Element von  $A$  als elementare Aktion interpretiert. Transitionssysteme werden sehr oft durch einen Pfeil „ $\rightarrow$ “ bezeichnet und statt  $(s, a, t) \in \rightarrow$  schreibt man  $s \xrightarrow{a} t$ . Falls das Hinschreiben der Aktionen mehr Platz erfordert, dann sind auch andere Schreibweisen üblich, etwa  $a : s \vdash t$ .

So kann man etwa die Semantik von imperativen Programmiersprachen, also Sprachen, die auf Variablen, Anweisungen und einem Speichermodell aufbauen, formal mittels Transitionssystemen spezifizieren. Ist  $X = \{x_1, \dots, x_n\}$  die Menge der in einem imperativen Programm vorkommenden Variablen, so entspricht ein Zustand einem  $n$ -Tupel  $s = (s_1, \dots, s_n)$ , wobei  $s_i$  als derzeitiger Wert der Variablen  $x_i$  interpretiert wird. Die Semantik der Zuweisung wird dann beispielsweise wie folgt als Zustandsübergang spezifiziert:

$$x_i := E : s \vdash t,$$

mit  $t_j = s_j$  für alle  $j \neq i$  und  $t_i = \text{wert}(E, s)$ . Hier stellt  $\text{wert}(E, s)$  den Wert des Ausdrucks  $E$  im Zustand  $s$  dar. Wie sich der ergibt, muss natürlich auch durch Induktion nach dem Aufbau der Ausdrücke spezifiziert werden. Als ein zweites Beispiel geben wir noch die durch eine bedingte Anweisung bewirkten Zustandsübergänge an. Hier gilt

$$\text{if } B \text{ then } P \text{ else } Q : s \vdash t,$$

falls  $\text{wert}(B, s) = W$  und  $P : s \vdash t$ , und

$$\text{if } B \text{ then } P \text{ else } Q : s \vdash u,$$

falls  $\text{wert}(B, s) = F$  und  $Q : s \vdash u$ . All dies lernt man ganz genau etwa in einer entsprechenden Vorlesung aus dem Gebiet der theoretischen Informatik, beispielsweise in einer zur Semantik von Programmiersprachen.

## 6.5 Übungsaufgaben

### Aufgabe

Die Relation  $R \subseteq \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$  ist durch

$$X R Y : \iff \exists x \in \mathbb{N} : x \in X \wedge x \in Y$$

für alle  $X, Y \in \mathcal{P}(\mathbb{N})$  festgelegt. Beweisen oder widerlegen Sie die folgenden Aussagen:

- (1) Die Relation  $R$  ist reflexiv.
- (2) Die Relation  $R$  ist symmetrisch.
- (3) Die Relation  $R$  ist antisymmetrisch.
- (4) Die Relation  $R$  ist transitiv.

### Aufgabe

Es seien  $R$  und  $S$  Äquivalenzrelationen auf einer Menge  $M$ .

- (1) Zeigen Sie, dass auch der Durchschnitt  $R \cap S$  eine Äquivalenzrelation ist.
- (2) Geben Sie ein Beispiel dafür an, dass die Vereinigung  $R \cup S$  keine Äquivalenzrelation ist.

### Aufgabe

Geben Sie die durch die Partition  $\mathcal{M} := \{\{a\}, \{b, c\}, \{d\}\}$  der Menge  $M := \{a, b, c, d\}$  beschriebene Äquivalenzrelation  $\equiv$  auf  $M$

- (1) explizit an, d.h. durch die in Mengenklammern eingeschlossene Aufzählung ihrer Paare,
- (2) an in Form einer Kreuztabelle.

### Aufgabe

Wir betrachten die Menge  $M := \{0, 1, \dots, 10\}$ . Zeichnen Sie das Ordnungsdiagramm (Hasse-Diagramm) der geordneten Menge  $(M, |)$  und beantworten Sie mit dessen Hilfe für die Teilmenge  $X := \{2, 3, 4, 6, 8\}$  von  $M$  die folgenden Fragen:

- (1) Was sind die maximalen bzw. minimalen Elemente von  $X$ ?
- (2) Was sind die oberen bzw. unteren Schranken von  $X$ ?
- (3) Besitzt  $X$  ein größtes bzw. ein kleinstes Element?
- (4) Besitzt  $X$  eine kleinste obere Schranke bzw. eine größte untere Schranke?

### Aufgabe

Es sei  $(M, \leq)$  eine geordnete Menge. Beweisen Sie für alle  $x, y \in M$  die folgende logische Äquivalenz:

$$(a) \quad x = y \iff \forall z \in M : z \leq x \Leftrightarrow z \leq y$$

Wie lautet die Entsprechung von (a), wenn man die linke Seite zu  $x \leq y$  ändert (mit Beweis)?

### Aufgabe

Beweisen Sie, dass  $(\mathcal{P}(\mathbb{N}), \subseteq)$  nicht Noethersch geordnet ist.

### Aufgabe

Es sei  $M$  eine nichtleere Menge mit  $|M| \leq |\mathbb{N}|$ . Zeigen Sie, dass es auf  $M$  eine Ordnungsrelation  $\sqsubseteq$  gibt, so dass in der geordneten Menge  $(M, \sqsubseteq)$  jede nichtleere Teilmenge von  $M$  ein kleinstes Element besitzt.

### Aufgabe

Wir betrachten auf der Menge  $\mathbb{N} \times \mathbb{N}$  die Relation  $\sqsubseteq$ , welche für alle Paare  $(x, y) \in \mathbb{N} \times \mathbb{N}$  und  $(m, n) \in \mathbb{N} \times \mathbb{N}$  festgelegt ist durch  $(x, y) \sqsubseteq (m, n)$  genau dann, wenn  $x \leq m$  und  $y \leq n$ .

- (1) Beweisen Sie, dass  $(\mathbb{N} \times \mathbb{N}, \sqsubseteq)$  eine Noethersch geordnete Menge ist.
- (2) Die Funktion  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  erfülle für alle  $m, n \in \mathbb{N}$  die folgenden Gleichungen:

$$f(0, n) = n \quad f(m, 0) = m \quad f(m + 1, n + 1) = f(m, n)$$

Beweisen Sie durch Noethersche Induktion, dass  $f(m, n) = |m - n|$  für alle  $m, n \in \mathbb{N}$  gilt.

### Aufgabe

Es sei  $f : M \rightarrow M$  eine Funktion auf einer endlichen Menge  $M$ . Zeigen Sie mittels graphentheoretischer Argumentation die folgende Aussage:

$$f \text{ ist injektiv} \iff f \text{ ist bijektiv} \iff f \text{ ist surjektiv}$$

### Aufgabe

Wir betrachten zu  $m \in \mathbb{N}$  und der Menge  $M := \{x \in \mathbb{N} \mid 1 \leq x \leq m\}$  den gerichteten Graphen  $g_m = (V_m, P_m)$  mit der Knotenmenge  $V_m := \mathcal{P}(M)$  und der Pfeilrelation  $P_m \subseteq V \times V$ , welche für alle  $X, Y \in V$  definiert ist durch

$$X P_m Y : \iff X \subset Y \wedge \neg(\exists Z \in V : X \subset Z \wedge Z \subset Y).$$

- (1) Zeichnen Sie die gerichteten Graphen  $g_0$  bis  $g_3$ .
- (2) Beweisen Sie, dass es in  $g_m$  genau  $m!$  verschiedene Wege von  $\emptyset$  nach  $M$  gibt.

### Aufgabe

Gegeben sei ein gerichteter Graph  $g = (V, P)$ . Ein gerichteter Graph  $h = (V, Q)$  heißt eine transitive Reduktion von  $g$ , falls die Relation  $Q$  ein minimales Element der Menge

$$\{X \in \mathcal{P}(P) \mid X^* = P^*\}$$

in der geordneten Menge  $(\mathcal{P}(V \times V), \sqsubseteq)$  ist.

- (1) Beweisen Sie, dass jeder gerichtete Graph eine transitive Reduktion besitzt.
- (2) Zeigen Sie anhand eines Beispiels, dass ein gerichteter Graph mehr als eine transitive Reduktion besitzen kann und deren Pfeilrelationen sogar verschiedene Kardinalitäten haben können.

## 7 Elementare Kombinatorik und ungerichtete Graphen

Im letzten Abschnitt des vorhergehenden Kapitels wurden gerichtete Graphen behandelt. Dies sind im Prinzip nichts anderes als Relationen auf Knotenmengen, deshalb geschah die Zuordnung zum Kapitel über Relationen. Es gibt auch noch ungerichtete Graphen, bei denen die Verbindungen zwischen den Knoten keine Richtung besitzen, graphisch also keine Pfeile mit Spitzen an einem Ende darstellen. In diesem Kapitel behandeln wir nun die ungerichteten Graphen. Diese stehen oft in Verbindung mit Kombinatorik, also der Teildisziplin der Mathematik, die sich mit Aufzählungen von Möglichkeiten, Größen bestimmter endlicher Mengen usw. beschäftigt. Wir beginnen im ersten Abschnitt des Kapitels mit einigen elementaren Begriffen und Fragestellungen der Kombinatorik.

### 7.1 Fakultäten und Binomialkoeffizienten

Die Aufgabe der Kombinatorik ist, sehr abstrakt gesehen, oft die Bestimmung von Möglichkeiten von Aufzählungen und von Kardinalitäten von endlichen Mengen. Dies wird vielfach durch die **Kunst des geschickten Aufzählens und Einteilens** erreicht, beispielsweise durch eine Zerlegung in disjunkte Mengen, deren Größen man einfach berechnen kann, und das Herstellen von geeigneten Eins-zu-Eins-Beziehungen. Binomialkoeffizienten sind dabei ein häufig verwendetes Mittel. Wir definieren sie in diesem Abschnitt mittels Fakultäten und führen Letztere wie folgt ein.

#### 7.1.1 Definition: Fakultät

Zu  $n \in \mathbb{N}$  wird durch  $n! := \prod_{i=1}^n i$  die **Fakultät** von  $n$  definiert. □

Dabei bezeichnet, wie schon aus Abschnitt 3.1 bekannt,  $\prod_{i=1}^n i$  das Produkt  $1 \cdot 2 \cdot \dots \cdot n$  der Zahlen von 1 bis  $n$  im Fall  $n > 0$ . Als Erweiterung hiervon definiert man noch  $\prod_{i=1}^0 i := 1$ . Die rekursive Definition des Produktsymbols mit der Null als dem neuen Terminierungsfall (statt der Eins wie in Abschnitt 3.1) liefert sofort das erste Resultat dieses Kapitels.

#### 7.1.2 Satz: rekursive Beschreibung der Fakultät

Es gilt  $0! = 1$  und für alle  $n \in \mathbb{N} \setminus \{0\}$  gilt  $n! = n(n - 1)!$ .

**Beweis:** Indem die Definition der Fakultät zweimal verwendet wird, folgt

$$n! = \prod_{i=1}^n i = n \cdot \prod_{i=1}^{n-1} i = n(n - 1)!$$

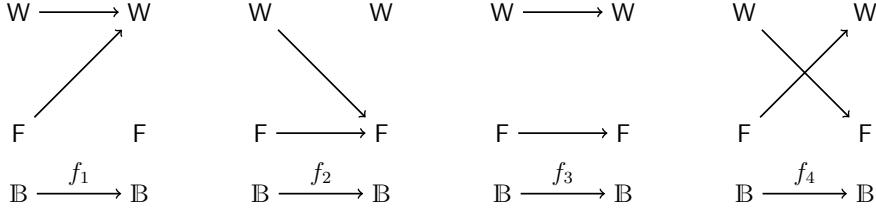
im Fall  $n \neq 0$ . Die Gleichung  $0! = 1$  folgt aus  $\prod_{i=1}^0 i = 1$ . □

Fakultäten treten insbesondere bei der Abzählung von speziellen Funktionen auf und damit in Situationen, wo man bei der Problemlösung auf diese stößt. Darauf werden wir später noch zurückkommen. Wir zeigen aber zuvor auf, wie man alle Funktionen auf endlichen Mengen aufzählt, d.h. formal die Größen von Mengen von Funktionen bestimmt. Dazu müssen wir, um einfach vorgehen zu können, zuerst Funktionenmengen in irgendeiner Art bezeichnen. In der Mathematik ist die folgende Beschreibung üblich; wir haben sie schon in den Beispielen 5.2.6 in Verbindung mit den konkreten Mengen  $\mathbb{N}$  und  $\{0, 1\}$  verwendet.

### 7.1.3 Definition: Funktionenmenge

Zu Mengen  $M$  und  $N$  bezeichnet  $N^M$  die Menge der Funktionen von  $M$  nach  $N$ .  $\square$

Beispielsweise ist  $\mathbb{B}^\mathbb{B}$  die Menge der Funktionen von  $\mathbb{B}$  nach  $\mathbb{B}$ . Davon gibt es genau vier Stück, nämlich  $f_1(x) = W$ ,  $f_2(x) = F$ ,  $f_3(x) = x$  und  $f_4(x) = \neg x$ . Hier sind die graphischen Darstellungen dieser Funktionen mittels bipartiter Pfeildiagramme:



Es gilt also  $|\mathbb{B}^\mathbb{B}| = 4 = |\mathbb{B}|^{|\mathbb{B}|}$ . Dieser Zusammenhang zur Potenzierung von Zahlen gilt sogar für beliebige endliche Mengen  $M$  und  $N$ , wie der folgende Satz zeigt. Die Endlichkeit braucht man hier wegen der Existenz der Kardinalitäten.

### 7.1.4 Satz: Kardinalität von Funktionenmengen

Für alle endlichen Mengen  $M$  und  $N$  gelten die folgenden Gleichungen:

$$|N^M| = |N|^{|M|} = |N^{|M|}|$$

**Beweis:** Wir zeigen zuerst  $|N^{|M|}| = |N|^{|M|}$ . Nach Definition ist  $N^{|M|}$  das  $|M|$ -fache direkte Produkt der Menge  $N$ . Aufgrund von Satz 3.1.3 erhalten wir im Fall  $|M| \geq 1$ , dass

$$\begin{aligned} |N^{|M|}| &= \left| \prod_{i=1}^{|M|} N \right| && \text{Definition Produkt} \\ &= \prod_{i=1}^{|M|} |N| && \text{Satz 3.1.3} \\ &= |N|^{|M|} && \text{Potenz von zwei Zahlen} \end{aligned}$$

gilt. Für  $|M| = 0$  bekommen wir  $|N^0| = |\{\emptyset\}| = 1$  nach der Definition von  $N^0$  und auch  $|N|^0 = 1$  nach einem bekannten Potenzgesetz. Dies zeigt insgesamt  $|N^{|M|}| = |N|^{|M|}$ .

Es bleibt noch  $|N^M| = |N^{|M|}|$  zu beweisen. Im Fall  $|M| = 0$ , d.h.  $M = \emptyset$ , gelten  $|N^\emptyset| = 1$  und  $|N^0| = 1$ . Man beachte, dass hierbei  $N^\emptyset$  eine Menge von Funktionen ist, mit der leeren Funktion  $\emptyset : \emptyset \rightarrow N$  als dem einzigen Element, und  $N^0$  eine Menge von 0-Tupeln ist, mit dem leeren Tupel  $\emptyset$  als dem einzigen Element.

Nun sei  $|M| = m$  und es gelte  $m \geq 1$  und  $M = \{a_1, \dots, a_m\}$ . Wir zeigen  $|N^M| = |N^{|M|}|$ , indem wir eine bijektive Funktion  $F$  von  $N^M$  nach  $N^{|M|} = N^m$  angeben. Diese und ihre Umkehrfunktion sehen wie folgt aus:

$$\begin{aligned} F : N^M &\rightarrow N^m & F(f) &= (f(a_1), \dots, f(a_m)) \\ G : N^m &\rightarrow N^M & G(s) &= \{(a_1, s_1), \dots, (a_m, s_m)\} \end{aligned}$$

Man beachte, dass die Relation  $\{(a_1, s_1), \dots, (a_m, s_m)\}$ , also  $G(s)$ , tatsächlich eine Funktion von  $M$  nach  $N$  ist. Es gelten die Gleichung  $G(F(f)) = f$  für alle  $f : M \rightarrow N$  und die Gleichung  $F(G(s)) = s$  für alle  $s \in N^m$ . Hier ist der Beweis der ersten Behauptung:

$$\begin{aligned} G(F(f)) &= G((f(a_1), \dots, f(a_m))) && \text{Definition } F \\ &= \{(a_1, f(a_1)), \dots, (a_m, f(a_m))\} && \text{Definition } G \\ &= f && \text{Gleichheit von Funktionen} \end{aligned}$$

Zum Beweis der zweiten Behauptung gehen wir wie folgt vor und beachten dabei, dass für alle  $i \in \{1, \dots, m\}$  die Anwendung der Funktion  $\{(a_1, s_1), \dots, (a_m, s_m)\}$  auf das Argument  $a_i$  per Definition das Resultat  $s_i$  liefert.

$$\begin{aligned} F(G(s)) &= F(\{(a_1, s_1), \dots, (a_m, s_m)\}) && \text{Definition } G \\ &= (s_1, \dots, s_m) && \text{Definition von } F \\ &= s \end{aligned}$$

Es sind also insgesamt  $F$  und  $G$  bijektiv, mit  $G$  als Umkehrfunktion  $F^{-1}$ .  $\square$

Gelten  $|M| = m$  und  $|N| = n$ , so kann man jede Funktion  $f$  von  $M$  nach  $N$  als genau ein  $m$ -Tupel auffassen. Dies besagt ja genau die Definition der Funktion  $F$  im letzten Beweis. Folglich gibt es genau  $n^m$  verschiedene **Tupel der Länge  $m$  über einer Menge mit  $n$  Elementen**. Über der Menge  $\{a, b, c\}$  kann man also genau  $3^3 = 27$  verschiedene Tupel der Länge 3 bilden.

Die **Menge der bijektiven Funktionen** von  $M$  nach  $N$  ist eine Teilmenge von  $N^M$ . Im Fall  $|M| \neq |N|$  ist diese Teilmenge bei endlichen Mengen immer leer. Deshalb kann man sich hier auf den Fall  $|M| = |N|$  beschränken. Nun ist unter dieser Voraussetzung die Anzahl der bijektiven Funktionen von der endlichen Menge  $M$  nach der endlichen Menge  $N$  gleich der von  $M$  nach  $M$ . Hintergrund ist der folgende einfach zu beweisende Sachverhalt, der sich aus der Bijektivität der Komposition von bijektiven Funktionen ergibt.

### 7.1.5 Satz: Kardinalitätsvergleich von Funktionenmengen

Sind  $f : M_1 \rightarrow M_2$  und  $g : N_1 \rightarrow N_2$  bijektive Funktionen, so ist auch

$$F : N_1^{M_1} \rightarrow N_2^{M_2} \quad F(h) = g \circ h \circ f^{-1}$$

eine bijektive Funktion, die bijektive Funktionen aus  $N_1^{M_1}$  auf bijektive Funktionen aus  $N_2^{M_2}$  abbildet.  $\square$

Man kann sich beim Aufzählen von bijektiven Funktionen somit auf die auf nur einer endlichen Menge beschränken. Weil im Fall  $M = \{a_1, \dots, a_m\}$  die Anzahl der bijektiven Funktionen auf  $M$  nach Satz 7.1.5 gleich der auf der speziellen gleichmächtigen Menge  $\{1, \dots, m\}$  ist, beschränkt man sich beim Aufzählen bijektiver Funktionen schließlich auf die Menge  $\{1, \dots, m\}$ , mit  $m \geq 0$ . Für  $m = 0$  gilt natürlich, wie auch schon erwähnt, die Gleichung  $\{1, \dots, m\} = \emptyset$ , und auf der leeren Menge gibt es genau eine bijektive Funktion, nämlich  $\emptyset : \emptyset \rightarrow \emptyset$ . Da man Funktionen  $f$  auf  $\{1, \dots, m\}$  als  $m$ -Tupel auffassen kann, trifft dies insbesondere auch für die bijektiven Funktionen zu. Diese entsprechen dann genau den nachfolgend definierten speziellen Tupeln.

### 7.1.6 Definition: Permutation

Ein  $n$ -Tupel  $s \in \{1, \dots, n\}^n$ , mit  $s = ()$  im Fall  $n = 0$ , heißt eine **Permutation** der Menge  $\{1, \dots, n\}$ , also der leeren Menge  $\emptyset$  im Fall  $n = 0$ , falls für alle  $i, j \in \mathbb{N}$  mit  $1 \leq i, j \leq n$  und  $i \neq j$  gilt  $s_i \neq s_j$ . Mit  $\mathcal{S}(n)$  ist die **Menge aller Permutationen** von  $\{1, \dots, n\}$  bezeichnet.  $\square$

Permutationen sind also  $n$ -Tupel über den natürlichen Zahlen, bei denen alle Komponenten paarweise verschieden sind. Im Fall der Tupellänge  $n = 0$  ist das leere Tupel  $() \in \emptyset^0$  offensichtlich eine Permutation der leeren Menge  $\emptyset$ , denn die Formeln  $1 \leq i \leq 0$  und  $1 \leq j \leq 0$  sind falsch. Also haben wir  $\mathcal{S}(0) = \{()\}$  und folglich  $|\mathcal{S}(0)| = |\{()\}| = 1 = 0!$ . Wir werden im Folgenden die Gleichheit  $\mathcal{S}(n) = n!$  für alle  $n \in \mathbb{N}$  beweisen. Dazu brauchen wir eine Hilfskonstruktion, die wir nachfolgend einführen. Sie basiert auf zwei partiellen Listenfunktionen  $bis : M^* \times \mathbb{N} \rightarrow M^*$  und  $nach : M^* \times \mathbb{N} \rightarrow M^*$ , die durch

$$\begin{array}{ll} bis(s, 0) &= () \\ nach(s, 0) &= s \end{array} \quad \begin{array}{ll} bis(a : s, n + 1) &= a : bis(s, n) \\ nach(a : s, n + 1) &= nach(s, n) \end{array}$$

für alle  $s \in M^*$ ,  $a \in M$  und  $n \in \mathbb{N}$  definiert sind. Es berechnet  $bis(s, n)$  die Anfangs-Teilliste von  $s$  der Länge  $n$  und  $nach(s, n)$  entfernt dieses Anfangsstück von  $s$ . Etwa gelten  $bis((3, 2, 1, 4, 1), 2) = (3, 2)$  und  $nach((3, 2, 1, 4, 1), 2) = (1, 4, 1)$ .

### 7.1.7 Definition: Einschieben in eine Permutation

Es seien  $n \in \mathbb{N}$  und  $s \in \mathcal{S}(n)$  gegeben. Wir definieren für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq n + 1$  eine lineare Liste  $s[i \leftarrow n + 1] \in \mathcal{S}(n + 1)$  durch die Festlegung

$$s[i \leftarrow n + 1] = bis(s, i - 1) \& (n + 1) \& nach(s, i - 1). \quad \square$$

Es entsteht also die Permutation  $s[i \leftarrow n + 1]$  der Zahlen von 1 bis  $n + 1$  aus der Permutation  $s$  der Zahlen von 1 bis  $n$  dadurch, dass die Zahl  $n + 1$  in  $s$  an der Position  $i$  eingeschoben wird. Für  $i = 1$  wird beispielsweise  $n + 1$  links an  $s$  angefügt und für  $i = n + 1$  wird  $n + 1$  rechts an  $s$  angefügt. Hier sind einige weitere Beispiele. Es sei  $(3, 1, 4, 2) \in \mathcal{S}(4)$ . Dann gelten die folgenden Gleichungen:

$$\begin{array}{ll} (3, 1, 4, 2)[1 \leftarrow 5] &= (5, 3, 1, 4, 2) & (3, 1, 4, 2)[2 \leftarrow 5] &= (3, 5, 1, 4, 2) \\ (3, 1, 4, 2)[3 \leftarrow 5] &= (3, 1, 5, 4, 2) & (3, 1, 4, 2)[4 \leftarrow 5] &= (3, 1, 4, 5, 2) \\ (3, 1, 4, 2)[5 \leftarrow 5] &= (3, 1, 4, 2, 5) \end{array}$$

Im Fall  $n = 0$  und  $() \in \mathcal{S}(0)$  ist nur  $i = 1$  möglich und es gilt dann  $()[1 \leftarrow 1] = (1) \in \mathcal{S}(1)$ .

Es ist natürlich  $s[i \leftarrow n + 1] \in \mathcal{S}(n + 1)$  zu verifizieren. Dass  $s[i \leftarrow n + 1]$  ein Tupel der Länge  $n + 1$  über  $\{1, \dots, n, n + 1\}$  ist, ist trivial; dass zusätzlich alle Elemente paarweise verschieden sind, folgt aus  $s \in \mathcal{S}(n)$  und  $n + 1 \notin \{1, \dots, n\}$ . Der nächste Satz zeigt, wie man  $\mathcal{S}(n + 1)$  mittels  $\mathcal{S}(n)$  berechnen kann. Diese Rekursion terminiert bei  $\mathcal{S}(0) = \{()\}$ .

### 7.1.8 Satz: Berechnung von Permutationsmengen

Für alle  $n \in \mathbb{N}$  gilt die folgende Gleichung:

$$\mathcal{S}(n + 1) = \bigcup_{i=1}^{n+1} \{s[i \leftarrow n + 1] \mid s \in \mathcal{S}(n)\}$$

**Beweis:** Wir starten mit der Inklusion „ $\subseteq$ “. Dazu gelte  $w \in \mathcal{S}(n+1)$  und  $w$  habe die Form  $w = (w_1, \dots, w_{n+1})$ , mit  $w_i \in \{1, \dots, n+1\}$  für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq n+1$ , also als die paarweise verschiedenen Komponenten. Dann gibt es einen Index  $i$  mit  $1 \leq i \leq n+1$  und  $w_i = n+1$ . Definiert man durch das Entfernen von  $w_i$  die Liste

$$s := bis(w, i-1) \& nach(w, i) = (w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_{n+1}),$$

so gilt  $s \in \mathcal{S}(n)$  und auch noch  $w = s[i \leftarrow n+1]$ . Dies zeigt

$$w \in \bigcup_{i=1}^{n+1} \{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\}.$$

Zum Beweis von „ $\supseteq$ “ gelte umgekehrt  $w \in \bigcup_{i=1}^{n+1} \{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\}$ . Dann existiert ein  $i \in \mathbb{N}$  mit  $1 \leq i \leq n+1$  und es gibt auch eine Liste  $s \in \mathcal{S}(n)$  mit  $w = s[i \leftarrow n+1]$ . Wegen  $s \in \mathcal{S}(n)$  gilt  $w \in \{1, \dots, n+1\}^{n+1}$  und aufgrund von  $n+1 \notin \{1, \dots, n\}$  folgt daraus mit Hilfe von  $s \in \mathcal{S}(n)$  sogar  $w \in \mathcal{S}(n+1)$ .  $\square$

Im folgenden Beispiel führen wir vor, wie man die Mengen  $\mathcal{S}(n)$  von Permutationen aufgrund von Satz 7.1.8 Schritt für Schritt aus  $\mathcal{S}(0)$  bestimmen kann.

### 7.1.9 Beispiel: Berechnung von Permutationsmengen

Wir wissen bereits, dass die Gleichung  $\mathcal{S}(0) = \{()\}$  gilt. Daraus folgt die Gleichheit von  $\mathcal{S}(1)$  und der Menge  $\{(1)\}$  wegen

$$\mathcal{S}(1) = \bigcup_{i=1}^1 \{s[i \leftarrow 1] \mid s \in \mathcal{S}(0)\} = \{()|1 \leftarrow 1\} = \{(1)\}.$$

Diese Gleichung verwenden wir nun, um wie folgt zu zeigen, dass  $\mathcal{S}(2)$  gleich der Menge  $\{(2, 1), (1, 2)\}$  von Permutationen ist:

$$\begin{aligned} \mathcal{S}(2) &= \bigcup_{i=1}^2 \{s[i \leftarrow 2] \mid s \in \mathcal{S}(1)\} \\ &= \{s[1 \leftarrow 2] \mid s \in \mathcal{S}(1)\} \cup \{s[2 \leftarrow 2] \mid s \in \mathcal{S}(1)\} \\ &= \{(2, 1)\} \cup \{(1, 2)\} \\ &= \{(2, 1), (1, 2)\} \end{aligned}$$

Aus  $\mathcal{S}(2) = \{(2, 1), (1, 2)\}$  können wir nun alle Elemente von  $\mathcal{S}(3)$  wie folgt berechnen:

$$\begin{aligned} \mathcal{S}(3) &= \bigcup_{i=1}^3 \{s[i \leftarrow 3] \mid s \in \mathcal{S}(2)\} \\ &= \{s[1 \leftarrow 3] \mid s \in \mathcal{S}(2)\} \cup \{s[2 \leftarrow 3] \mid s \in \mathcal{S}(2)\} \cup \{s[3 \leftarrow 3] \mid s \in \mathcal{S}(2)\} \\ &= \{(3, 2, 1), (3, 1, 2)\} \cup \{(2, 3, 1), (1, 3, 2)\} \cup \{(2, 1, 3), (1, 2, 3)\} \\ &= \{(3, 2, 1), (3, 1, 2), (2, 3, 1), (1, 3, 2), (2, 1, 3), (1, 2, 3)\} \end{aligned}$$

Man beachte das Bildungsgesetz  $|\mathcal{S}(0)| = 0!$ ,  $|\mathcal{S}(1)| = 1!$ ,  $|\mathcal{S}(2)| = 2!$  und  $|\mathcal{S}(3)| = 3!$  und unser Ziel ist zu zeigen, dass sich dieses auf alle natürlichen Zahlen verallgemeinert.  $\square$

Und hier ist nun das angekündigte Resultat über die Anzahl der Permutationen einer Menge  $\{1, \dots, n\}$ , woraus sich auch sofort die Anzahl der bijektiven Funktionen auf einer  $n$ -elementigen Menge ergibt.

### 7.1.10 Satz: Anzahl der bijektiven Funktionen

Für alle  $n \in \mathbb{N}$  gilt  $|\mathcal{S}(n)| = n!$  und damit ist die die Anzahl der bijektiven Funktionen  $f : M \rightarrow M$  auf der endlichen Menge  $M$  gleich  $|M|!$ .

**Beweis (durch vollständige Induktion):** Wir zeigen  $A(n)$  für alle  $n \in \mathbb{N}$ , mit  $A(n)$  festgelegt durch  $|\mathcal{S}(n)| = n!$ .

Induktionsbeginn: Es gilt  $A(0)$  wegen  $|\mathcal{S}(0)| = |\{\emptyset\}| = 1 = 0!$ .

Induktionsschluss: Nun sei  $n \in \mathbb{N}$  beliebig vorgegeben und es gelte die Aussage  $A(n)$ . Dann bekommen wir das gewünschte Resultat  $A(n+1)$  durch die folgende Rechnung:

$$\begin{aligned}
 |\mathcal{S}(n+1)| &= \left| \bigcup_{i=1}^{n+1} \{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\} \right| && \text{Satz 7.1.8} \\
 &= \sum_{i=1}^{n+1} |\{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\}| && \text{alle Mengen sind disjunkt} \\
 &= \sum_{i=1}^{n+1} |\mathcal{S}(n)| && \text{siehe unten} \\
 &= (n+1) \cdot |\mathcal{S}(n)| \\
 &= (n+1)n! && \text{Induktionshypothese } A(n) \\
 &= (n+1)! && \text{Satz 7.1.2}
 \end{aligned}$$

Dabei gilt  $|\{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\}| = |\mathcal{S}(n)|$ , weil genau jeder Permutation  $s[i \leftarrow n+1]$  in der Menge  $\{s[i \leftarrow n+1] \mid s \in \mathcal{S}(n)\}$  die Permutation  $s$  in  $\mathcal{S}(n)$  entspricht.  $\square$

Man benutzt oftmals die Notation  $\mathcal{S}(M)$  (oder auch  $\mathcal{S}_M$ ) für die Menge der bijektiven Funktionen auf der Menge  $M$ .

Wir demonstrieren nun eine Anwendung der bisherigen Resultate durch einige Schachprobleme. Solche Probleme wurden schon vor langer Zeit untersucht, nicht nur von Menschen mit einem Faible für das Schachspielen und Knobeln, sondern auch von Mathematikerinnen und Mathematikern. Unsere Probleme sind verwandt mit dem berühmten 8-Damen Problem, das der bayerische Schachmeister Max Bezzel (1824-1871) unter dem Pseudonym „Schachfreund“ im Jahr 1848 in der Berliner Schachzeitung stellte und mit dem sich auch Gauß beschäftigte. Das letztgenannte Problem fragt nach der Anzahl der Möglichkeiten, 8 Damen auf einem klassischen Schachbrett so zu platzieren, dass sie sich gegenseitig nicht bedrohen. Die Antwort ist 92. Diese Anzahl wurde im Jahr 1850 publiziert und im Jahr 1874 zeigte der englische Mathematiker und Astronom James W.L. Glaisher (1848-1928), dass es tatsächlich nicht mehr als 92 Möglichkeiten geben kann.

Die Schachprobleme des folgenden Beispiels 7.1.11 betreffen Türme statt Damen und beschränken sich nicht nur auf das Bedrohen. Ihre Lösungen gehen auf die russischen Mathematiker und Zwillingsbrüder Akita Yaglom (1921-2007) und Isaak Yaglom (1921-1988) zurück. Neben den Türmen haben die beiden auch die restlichen Offiziere des Schachspiels in der gleichen Weise behandelt.

### 7.1.11 Beispiel: Unabhängige und abdeckende Türme beim Schachspiel

Ein klassisches Schachbrett hat 8 Zeilen und 8 Spalten. Wir verallgemeinern dies nun zu einem  $n \times n$  Schachbrett mit  $n$  Zeilen und  $n$  Spalten. Darauf betrachten wir Türme, wobei die Zugregel wie beim klassischen Schachbrett festgelegt sei. Unsere erste Frage ist nun:

- (1) Was ist die maximale Anzahl von Türmen, die man auf ein  $n \times n$  Schachbrett stellen kann, ohne dass sie sich gegenseitig bedrohen (also unabhängig sind)?

Die Antwort ist  $n$ , denn es ist offensichtlich, dass  $n$  Türme auf einer der Diagonalen unabhängig sind und es mehr als  $n$  unabhängige Türme nicht geben kann. Interessant ist nun die aus dieser Antwort folgende nächste Frage:

- (2) Wie viele verschiedene Möglichkeiten gibt es, auf einem  $n \times n$  Schachbrett  $n$  unabhängige Türme zu platzieren?

Hier ist zur Beantwortung wesentlich, dass jede Platzierung von  $n$  unabhängigen Türmen genau einer bijektiven Funktion  $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  entspricht. Von der Platzierung zur Funktion kommt man, indem man  $f(i) = j$  definiert, wenn auf Zeile  $i$  des Bretts der Turm in Spalte  $j$  steht. Umgekehrt liefert jede bijektive Funktion eine Platzierung, indem man den Turm in Zeile  $i$  auf die Spalte  $f(i)$  stellt. Aus Satz 7.1.10 folgt also, dass es genau  $n!$  verschiedene Möglichkeiten gibt.

Dual zu Frage (1) nach der Unabhängigkeit von Schachfiguren ist die folgende Frage; die Eigenschaft, welche darin formuliert wird, heißt auch Dominanz.

- (3) Was ist die minimale Anzahl von Türmen, die man auf ein  $n \times n$  Schachbrett stellen muss, damit jedes leere Feld bedroht ist?

Einige relativ einfache Überlegungen zeigen, dass  $n$  auch die minimale Anzahl dominierender Türme ist. Mit  $n$  Türmen kann man nämlich alle Felder bedrohen. Stehen hingegen weniger als  $n$  Türme auf dem Brett, so sind mindestens eine Zeile und eine Spalte leer und ihr gemeinsames Feld wird damit nicht angegriffen. Wie sieht es nun mit der folgenden Frage aus?

- (4) Wie viele verschiedene Möglichkeiten gibt es, auf einem  $n \times n$  Schachbrett  $n$  dominierende Türme zu platzieren.

Zur Beantwortung verwenden wir wiederum Funktionenmengen. Damit  $n$  Türme dominierend sind, müssen sie entweder alle auf verschiedenen Zeilen oder alle auf verschiedenen Spalten stehen. Es sei  $T_z$  die Menge aller Stellungen der ersten Art und  $T_s$  die Menge aller Stellungen der zweiten Art. Dann gilt

$$|T_z \cup T_s| = |T_z| + |T_s| - |T_z \cap T_s| = n^n + n^n - n! = 2n^n - n!,$$

denn jede Stellung von  $T_z$  als auch von  $T_s$  entspricht genau einer Funktion von  $\{1, \dots, n\}$  nach  $\{1, \dots, n\}$  und jede Stellung, welche sowohl in  $T_z$  als auch in  $T_s$  enthalten ist, entspricht genau einer bijektiven Funktion von  $\{1, \dots, n\}$  nach  $\{1, \dots, n\}$ . Die Gleichung folgt also aus den Sätzen 7.1.4 und 7.1.10.  $\square$

Wir kommen nun zu den Binomialkoeffizienten. Es sind mehrere Möglichkeiten gegeben, diese zu definieren. Am einfachsten erklärt man sie mit der Hilfe von Fakultäten. Dies sieht dann wie folgt aus:

### 7.1.12 Definition: Binomialkoeffizient

Für alle  $n, k \in \mathbb{N}$  definieren wir

$$\binom{n}{k} := \begin{cases} \frac{n!}{k!(n-k)!} & \text{falls } n \geq k \\ 0 & \text{falls } n < k \end{cases}$$

und nennen den Ausdruck  $\binom{n}{k}$  den **Binomialkoeffizienten** von  $n$  und  $k$ . □

Gesprochen wird  $\binom{n}{k}$  als „ $n$  über  $k$ “. Wegen  $0! = 1$  folgt aus Definition 7.1.12 sofort

$$(1) \quad \binom{n}{n} = \frac{n!}{n!(n-n)!} = 1$$

und auch

$$(2) \quad \binom{n}{0} = \frac{n!}{0!(n-0)!} = 1$$

für alle  $n \in \mathbb{N}$ . Weiterhin gilt für alle  $n \in \mathbb{N}$  auch

$$(3) \quad \binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n(n-1)!}{(n-1)!} = n$$

falls  $n \geq 1$ . Gleichung (3) gilt sogar auch für  $n = 0$ , da  $\binom{0}{1} = 0$  nach Definition 7.1.12 gilt. Der folgende Satz zeigt, wie man Binomialkoeffizienten rekursiv berechnen kann. Das Resultat geht auf den französischen Philosophen, Literaten und Mathematiker Blaise Pascal (1623-1662) zurück, der Namensgeber für eine früher an Hochschulen sehr viel verwendete Programmiersprache ist. In der Mathematik gilt Pascal, zusammen mit Pierre de Fermat (vor 1610-1665), einem französischen Juristen und Mathematiker, als Begründer der Wahrscheinlichkeitsrechnung.

### 7.1.13 Satz (B. Pascal)

Für alle  $n, k \in \mathbb{N}$  mit  $1 \leq k \leq n$  gilt die folgende Gleichung:

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

**Beweis:** Wir beginnen die Rechnung mit der komplizierten Seite.

$$\begin{aligned} \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-1)!(n-k)}{k!(n-k)!} + \frac{(n-1)!k}{k!(n-k)!} \quad \text{Satz 7.1.2} \\ &= \frac{(n-1)!(n-k) + (n-1)!k}{k!(n-k)!} \\ &= \frac{(n-1)!(n-k+k)}{k!(n-k)!} \\ &= \frac{(n-1)!n}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \quad \text{Satz 7.1.2} \\ &= \binom{n}{k} \end{aligned}$$

Die Idee hinter der vorangehenden Rechnung ist, auf den gemeinsamen Nenner  $k!(n-k)!$  zuzusteuern. Dazu wird die Gleichung

$$(n-1) - (k-1) = n - k - 1 + 1 = n - k$$

in ihrem ersten Schritt verwendet. □

Wir werden auf das durch diesen Satz gegebene Berechnungsschema der Binomialkoeffizienten später noch zurückkommen und auch zeigen, wie man damit für kleine Werte von  $\binom{n}{k}$ , d.h. also auch für kleine Werte von  $n$  und  $k$ , die Rechnung graphisch durchführen kann. Doch zuerst studieren wir noch einen anderen sehr wichtigen Zusammenhang, der bei kombinatorischen Anwendungen oft verwendet werden kann.

Für endliche Mengen  $M$  wissen wir, dass  $|\mathcal{P}(M)| = 2^{|M|}$  gilt. Was nun auch interessant ist, ist zu klären, wie sich diese  $2^{|M|}$  Teilmengen von  $M$  nach ihren Größen aufteilen. Teilmengen von  $M$  der Kardinalität 0 gibt es genau eine, nämlich die leere Menge. Es gibt auch genau eine Teilmenge von  $M$  der Kardinalität  $|M|$ , nämlich  $M$  selbst. Teilmengen der Kardinalität 1 gibt es  $|M|$  Stück, nämlich die Mengen  $\{a\}$  mit  $a \in M$ . Wie sieht es aber allgemein aus? Zur Klärung dieser Frage betrachten wir wiederum den Spezialfall  $\{1, \dots, n\}$ , mit  $n \in \mathbb{N}$ , denn die Anzahl der  $k$ -elementigen Teilmengen von  $\{1, \dots, n\}$  ist offensichtlich gleich der Anzahl der  $k$ -elementigen Teilmengen einer beliebigen Menge der Form  $\{a_1, \dots, a_n\}$ .

### 7.1.14 Definition: Menge der $k$ -Teilmengen

Für alle  $n \in \mathbb{N}$  und  $k \in \mathbb{N}$  mit der Eigenschaft  $k \leq n$  definieren wir die **Menge der  $k$ -Teilmengen** von  $\{1, \dots, n\}$  wie folgt:

$$\mathcal{P}_k(n) := \{X \in \mathcal{P}(\{1, \dots, n\}) \mid |X| = k\}$$

Für  $n = 0$  ist dabei, wie üblich, die Gleichheit  $\{1, \dots, n\} = \emptyset$  unterstellt. □

Damit gilt insbesondere die Gleichung

$$\mathcal{P}_0(0) = \{X \in \mathcal{P}(\emptyset) \mid |X| = 0\} = \{X \in \{\emptyset\} \mid |X| = 0\} = \{\emptyset\}$$

und diese impliziert  $|\mathcal{P}_0(0)| = 1$ . Die Mengen  $\mathcal{P}_k(n)$  kann man rekursiv berechnen, so wie auch die Potenzmengen. Allerdings sieht die Rekursion anders aus. Wie, das zeigt das nächste Resultat.

### 7.1.15 Satz: Rekursion für Mengen von $k$ -Teilmengen

Für alle  $n, k \in \mathbb{N}$  mit  $n \geq k \geq 1$  gilt

$$\mathcal{P}_k(n) = \mathcal{P}_k(n-1) \cup \{X \cup \{n\} \mid X \in \mathcal{P}_{k-1}(n-1)\}.$$

**Beweis:** Zum Beweis von „ $\subseteq$ “ sei  $Y \in \mathcal{P}_k(n)$  beliebig vorgegeben, also  $Y \in \mathcal{P}(\{1, \dots, n\})$  mit  $|Y| = k$ . Nach Satz 1.3.3 gibt es zwei Fälle.

- (a) Es gelte  $Y \in \mathcal{P}(\{1, \dots, n-1\})$ . Wegen der Eigenschaft  $|Y| = k$  gilt dann insgesamt  $Y \in \mathcal{P}_k(n-1)$ .

- (b) Es existiert  $X \in \mathcal{P}(\{1, \dots, n-1\})$  mit  $Y = X \cup \{n\}$ . Weil damit  $|X| = k-1$  zutrifft, bekommen wir  $X \in \mathcal{P}_{k-1}(n-1)$  und folglich auch

$$Y \in \{X \cup \{n\} \mid X \in \mathcal{P}_{k-1}(n-1)\}.$$

Beide Fälle zusammen zeigen  $Y \in \mathcal{P}_k(n-1) \cup \{X \cup \{n\} \mid X \in \mathcal{P}_{k-1}(n-1)\}$ .

Nun zeigen wir „ $\supseteq$ “ und nehmen an, es sei  $Y$  aus der rechten Seite der Gleichung. Auch hier gibt es zwei Fälle.

- (a) Es sei  $Y \in \mathcal{P}_k(n-1)$ . Dann gelten  $Y \subseteq \{1, \dots, n-1\} \subseteq \{1, \dots, n\}$  und  $|Y| = k$ . Also haben wir  $Y \in \mathcal{P}_k(n)$ .
- (b) Es gibt  $X \in \mathcal{P}_{k-1}(n-1)$  mit  $Y = X \cup \{n\}$ . Dann folgt daraus  $X \subseteq \{1, \dots, n-1\}$ , also erhalten wir die Inklusion

$$Y = X \cup \{n\} \subseteq \{1, \dots, n-1\} \cup \{n\} = \{1, \dots, n\}.$$

Weiterhin gilt  $|X| = k-1$  und daraus bekommen wir die Gleichung

$$|Y| = |X \cup \{n\}| = |X| + 1 = k-1 + 1 = k.$$

Dies zusammen bringt ebenfalls  $Y \in \mathcal{P}_k(n)$ .  $\square$

Nach diesen Vorbereitungen können wir nun den folgenden Satz zeigen. Er gibt in seinem zweiten Teil an, wie sich mit Hilfe von Binomialkoeffizienten die Aufteilung aller Teilmengen einer beliebigen endlichen Menge nach ihren Kardinalitäten bestimmen lässt. Der erste Teil behandelt den entscheidenden Spezialfall. Dass aus ihm das allgemeine Resultat folgt, wurde schon früher bemerkt.

### 7.1.16 Satz: Anzahl der $k$ -Teilmengen

Es gilt  $|\mathcal{P}_k(n)| = \binom{n}{k}$  für alle  $n, k \in \mathbb{N}$  mit  $n \geq k$ . Insbesondere gibt es also in jeder endlichen Menge  $M$  genau  $\binom{|M|}{k}$   $k$ -elementige Teilmengen.

**Beweis (durch vollständige Induktion):** Wir definieren  $A(n)$  als

$$\forall k \in \mathbb{N} : n \geq k \Rightarrow |\mathcal{P}_k(n)| = \binom{n}{k}.$$

Beim Induktionsbeginn, dem Beweis von  $A(0)$ , sei  $k \in \mathbb{N}$  mit  $0 \geq k$  gegeben. Dann gilt  $k = 0$  und daraus folgt die Gleichung

$$\mathcal{P}_0(0) = |\{\emptyset\}| = 1 = \binom{0}{0}.$$

Zum Induktionsschluss gelte die Aussage  $A(n)$  für eine beliebig vorgegebene natürliche Zahl  $n$ , also  $|\mathcal{P}_k(n)| = \binom{n}{k}$  für alle  $k \in \mathbb{N}$  mit  $n \geq k$ . Nun sei eine natürliche Zahl  $k$  mit  $n+1 \geq k$  beliebig gewählt. Dann gibt es zwei Fälle.

(a) Es gelte  $k \neq 0$ . Hier können wir wie folgt rechnen, was die Behauptung zeigt:

$$\begin{aligned}
|\mathcal{P}_k(n+1)| &= |\mathcal{P}_k(n) \cup \{X \cup \{n+1\} \mid X \in \mathcal{P}_{k-1}(n)\}| && \text{Satz 7.1.15} \\
&= |\mathcal{P}_k(n)| + |\{X \cup \{n+1\} \mid X \in \mathcal{P}_{k-1}(n)\}| && \text{beide Mengen disjunkt} \\
&= |\mathcal{P}_k(n)| + |\mathcal{P}_{k-1}(n)| && \text{siehe unten} \\
&= \binom{n}{k} + \binom{n}{k-1} && \text{Induktionshypothese } A(n) \\
&= \binom{n+1}{k} && \text{Satz 7.1.13}
\end{aligned}$$

Dabei gilt die Gleichung  $|\{X \cup \{n+1\} \mid X \in \mathcal{P}_{k-1}(n)\}| = |\mathcal{P}_{k-1}(n)|$ , weil jedes Element  $X \cup \{n+1\}$  der ersten Mengen genau dem Element  $X$  der zweiten Menge entspricht, also eine Eins-zu-Eins-Beziehung vorliegt.

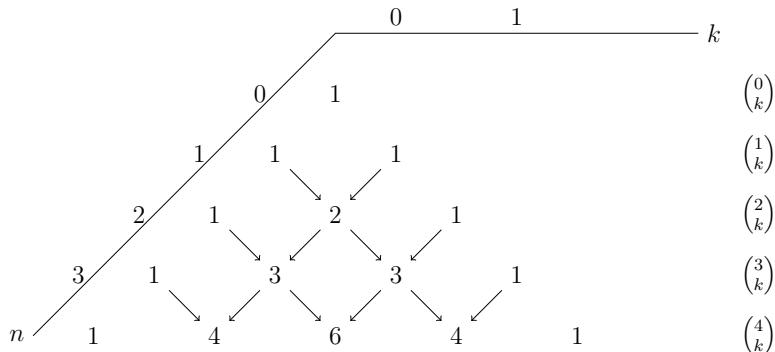
(b) Es gelte  $k = 0$ . In diesem Fall schließen wir auf die Gleichung

$$|\mathcal{P}_0(n+1)| = |\{\emptyset\}| = 1 = \binom{n+1}{0}$$

und dies beendet den Induktionsschritt.  $\square$

Die Aussage des eben bewiesenen Satzes gilt auch im Fall  $k > |M|$ . Dies folgt aus der Gleichung  $|\{X \in \mathcal{P}(M) \mid |X| = k\}| = |\emptyset| = 0$  für diesen Fall und der Festlegung  $\binom{n}{k} = 0$  falls  $k > n$ .

Nach Satz 7.1.13 kann man die Binomialkoeffizienten rekursiv berechnen. Bei kleinen Zahlen macht man dies per Hand in der graphischen Form eines **Pascalschen Dreiecks**. In dem folgenden Bild ist so ein Dreieck bis zur Tiefe 4 dargestellt. Die waagrechten Zeilen entsprechen den  $\binom{n}{k}$ -Werten zu einem festen  $n$  und die schrägen Spalten entsprechen den  $\binom{n}{k}$ -Werten zu einem festen  $k$ . Anfangs werden die Werte der beiden Schenkel des Pascalschen Dreiecks mit Einsen besetzt. Die inneren Zahlen des Dreiecks ergeben sich dann zeilenweise von oben nach unten durch Additionen, die im Bild durch Pfeile angedeutet sind. Formal wird bei jeder Addition Satz 7.1.13 angewendet.

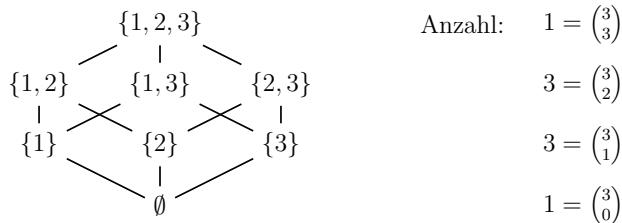


Alle Binomialkoeffizienten, die nicht Teil des Pascalschen Dreiecks sind, sind per Definition Null. Sie sind in der Zeichnung nicht mit aufgeführt. Bei Verwendung eines Computer-Programms berechnet man den Wert von  $\binom{n}{k}$ , indem man anschaulich im Dreieck zeilenweise von oben nach unten vorgeht. Dabei nimmt die Anzahl der Elemente ungleich 0 von Zeile zu Zeile um 1 zu. Der Start erfolgt mit der obersten Zeile bis zum Element  $k$ , also mit  $(1, 0, 0, \dots, 0)$ , und man muss genau so viele Zeilen berechnen, bis man bei der Zahl  $n$  angelangt ist. In einer imperativen Programmiersprache kommt man bei dieser Vorgehensweise mit einem Feld der Länge  $k + 1$  aus.

Wir wollen auch die Anzahl der Teilmengen einer vorgegebenen Größe in einer Menge an einem konkreten kleinen Beispiel demonstrieren.

### 7.1.17 Beispiel: $k$ -Teilmengen und Binomialkoeffizienten

Wir betrachten die Menge  $M := \{1, 2, 3\}$ . In dem folgenden Bild ist das Hasse-Diagramm der inklusions-geordneten Potenzmenge von  $M$  angegeben. Jede waagrechte Schicht enthält dabei die Mengen einer bestimmten Kardinalität, angefangen bei 0 unten und endend mit 3 oben. Die Anzahl der Mengen einer Schicht ergibt sich aus dem entsprechenden Binomialkoeffizienten. Alle diese Zahlen sind auch in der Zeichnung mit angegeben.



Aus diesem Bild erkennt man auch eine Symmetrie, die allgemein durch die Gleichung  $\binom{n}{k} = \binom{n}{n-k}$  für alle  $n, k \in \mathbb{N}$  mit  $n \geq k$  beschrieben ist. Die Beziehung zwischen den Binomialkoeffizienten und den Mengen einer bestimmten Kardinalität einerseits und der Kardinalität der Potenzmenge und einer Zweierpotenz andererseits impliziert die Gleichung  $\sum_{k=0}^n \binom{n}{k} = 2^n$  für alle  $n \in \mathbb{N}$ , was auch aus der obigen Zeichnung ersichtlich ist.  $\square$

Aus der höheren Schule kennt man die binomische Formel

$$(a + b)^2 = a^2 + 2ab + b^2 = 1 \cdot a^2 + 2 \cdot ab + 1 \cdot b^2.$$

Multipliziert man den Ausdruck  $(a + b)^3$  vollständig aus, so folgt

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = 1 \cdot a^3 + 3 \cdot a^2b + 3 \cdot ab^2 + 1 \cdot b^3.$$

Natürlich gelten auch  $(a + b)^0 = 1$  und  $(a + b)^1 = a + b = 1 \cdot a + 1 \cdot b$ . Aus diesen einfachen Rechnungen bekommen wir, wie nachstehend angezeigt, genau den Anfang des Pascalschen Dreiecks bis zu  $n = 3$ .

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & 1 & 1 & \\ & & & & 1 & 2 & 1 \\ & & & & 1 & 3 & 3 & 1 \end{array}$$

Die eben angezeigte Beziehung zwischen den Einträgen des Pascalschen Dreiecks und den Potenzen  $(a+b)^n$  einer Summe  $a+b$  gilt auch allgemein für die Koeffizienten vor den Gliedern  $a^i b^j$  bei der vollständig ausmultiplizierten Potenz. Dieses Resultat ist als binomischer Lehrsatz bekannt. In den obigen Gleichungen sind ganz rechts jeweils die Potenzen von  $a$  absteigend und die von  $b$  aufsteigend sortiert. Bei der nachfolgend angegebenen üblichen Formulierung des Lehrsatzes ist genau umgekehrt sortiert.

### 7.1.18 Satz: Binomischer Lehrsatz

Für alle  $n \in \mathbb{N}$  und alle  $a, b \in \mathbb{R}$  gilt

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} = \binom{n}{0} b^n + \binom{n}{1} a b^{n-1} + \dots + \binom{n}{n-1} a^{n-1} b^1 + \binom{n}{n} a^n.$$

**Beweis (durch vollständige Induktion):** Es stehe  $A(n)$  für die behauptete Gleichung (deren zweite Form mit den Punkten nur dem besseren Verstehen dient).

Der Induktionsbeginn ist  $A(0)$ . Hier gilt (unter der Verwendung von  $0^0 = 1$ )

$$(a+b)^0 = 1 = \binom{0}{0} a^0 b^0 = \sum_{k=0}^0 \binom{0}{k} a^k b^{0-k}.$$

Zum Induktionsschluss von  $A(n)$  nach  $A(n+1)$  gelte die Gleichung wie in der Formulierung des Satzes angegeben. Dann können wir wie folgt rechnen:

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b) \left( \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \right) \\ &= \left( \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} \right) + \left( \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \right) \\ &= \left( \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} \right) + \left( \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \right) \\ &= \binom{n}{n} a^{n+1} b^0 + \left( \sum_{k=1}^n \binom{n}{k-1} a^k b^{n+1-k} \right) + \left( \sum_{k=1}^n \binom{n}{k} a^k b^{n+1-k} \right) + \binom{n}{0} a^0 b^{n+1} \\ &= a^{n+1} + \left( \sum_{k=1}^n \left( \binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \right) + b^{n+1} \\ &= a^{n+1} + \left( \sum_{k=1}^n \binom{n+1}{k} a^k b^{n+1-k} \right) + b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} \end{aligned}$$

Dabei verwenden wir im zweiten Schritt die Induktionshypothese  $A(n)$ . In den nächsten beiden Schritten multiplizieren wir aus und transformieren in der linken Summe den Index. Dann spalten wir Summenglieder ab, damit die Indexbereiche beider Summensymbole identisch werden. Der sechste Schritt besteht in einer Vereinfachung. Deren Resultat kann

mit Satz 7.1.13 behandelt werden. Im letzten Schritt verwenden wir schließlich noch die Gleichungen  $\binom{n+1}{0}a^0b^{n+1-0} = b^{n+1}$  und  $\binom{n+1}{n+1}a^{n+1}b^{n+1-(n+1)} = a^{n+1}$ .  $\square$

Die spezielle Wahl von  $a = b = 1$  im binomischen Lehrsatz zeigt für alle  $n \in \mathbb{N}$  sofort die folgende Gleichheit, welche wir schon früher erwähnt haben:

$$2^n = (1+1)^n = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^n \binom{n}{k}$$

Im Fall von  $a = 1$  und  $b = -1$  bekommen wir den binomischen Lehrsatz in der Form

$$0 = (1-1)^n = \sum_{k=0}^n (-1)^k \binom{n}{k}.$$

Allerdings ist hier  $n \geq 1$  vorauszusetzen, denn es gilt im Fall  $n = 0$  die Gleichung  $\sum_{k=0}^0 (-1)^0 \binom{0}{k} = \binom{0}{0} = 1$ , was  $\sum_{k=0}^0 (-1)^0 \binom{0}{k} \neq 0$  nach sich zieht. Will man auf diese Einschränkung verzichten, so hat man in der Aussage 0 durch  $0^n$  zu ersetzen.

## 7.2 Grundbegriffe ungerichteter Graphen

In Abschnitt 6.3 werden gerichtete Graphen als Paare  $g = (V, P)$  definiert, wobei die Pfeilmenge  $P$  von  $g$  eine Relation auf der endlichen Knotenmenge  $V$  von  $g$  ist. Damit ist ein (gerichteter) Pfeil mathematisch ein Paar  $(x, y)$  von Knoten. Zeichnerisch werden Pfeile durch eine  $x$  und  $y$  verbindende Linie mit einer Pfeilspitze bei  $y$  dargestellt. Diese gibt die Richtung an.

Graphen sind ein wertvolles Mittel bei der Modellierung praktischer Probleme. Nun gibt es hier oft Situationen, wo die Verbindungen zwischen den Objekten, die den Knoten entsprechen, ungerichtet sind. Beispielsweise ist dies bei Straßenverbindungen so, falls keine Einbahnstraßen vorliegen, oder bei Brettspielen wie Schach, wo man Züge zwischen Stellungen auch in umgekehrter Richtung ausführen kann, oder bei allen Beziehungen, welche durch symmetrische Relationen beschrieben werden. Man zeichnet hier in der Regel eine Beziehung zwischen zwei Objekten in der Form einer sie verbindenden Linie ohne eine Pfeilspitze und spricht dann von einer (ungerichteten) **Kante** zwischen den Objekten. Wenn eine Richtungsangabe ohne Bedeutung ist, so spielen in sehr vielen Fällen Beziehungen keine Rolle, die in der zeichnerischen Darstellung Schlingen an nur einem Objekt entsprechen. Man kann Kanten also mathematisch durch zweielementige Mengen von Objekten modellieren. Dies erlaubt, ungerichtete Graphen wie folgt formal zu definieren.

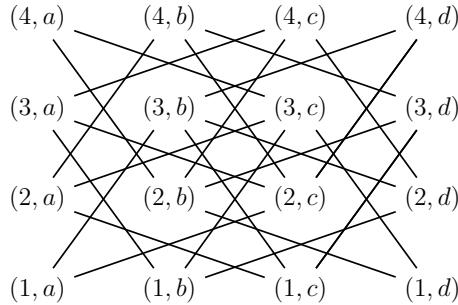
### 7.2.1 Definition: ungerichteter Graph

Ein **ungerichteter Graph**  $g = (V, K)$  ist ein Paar, bestehend aus einer endlichen und nichtleeren Menge  $V$  von **Knoten** und einer Menge  $K$  von **Kanten**. Dabei ist jedes Element der **Kantenmenge**  $K$  eine zweielementige Teilmenge der **Knotenmenge**  $V$ .  $\square$

Insbesondere gelten also für alle ungerichteten Graphen  $g = (V, K)$  die Inklusion  $K \subseteq \mathcal{P}(V)$  und die Ungleichung  $|K| \leq \frac{1}{2}|V|(|V|-1)$ . Nachfolgend geben wir, schon in der oben besprochenen graphischen Darstellung mit Linien ohne Pfeilspitzen zwischen den Knoten als Kanten, ein Beispiel für einen ungerichteten Graphen an. Dabei beziehen wir uns auf das Brettspiel Schach und betrachten dessen Brett in einer verkleinerten Variante.

### 7.2.2 Beispiel: ungerichteter Graph

Modelliert man ein  $4 \times 4$  Schachbrett und alle möglichen Züge eines Springers auf ihm graphentheoretisch, so führt dies zu dem folgenden ungerichteten Graphen:



Die Knotenmenge  $V$  des durch diese Zeichnung dargestellten ungerichteten Graphen ist das direkte Produkt der Zeilenmenge  $\{1, 2, 3, 4\}$  und der Spaltenmenge  $\{a, b, c, d\}$  des Schachbretts und modelliert die 16 Felder von  $(1, a)$  bis  $(4, d)$ . Ein Paar  $(i, u), (j, v)$  von Feldern bildet eine Kante genau dann, wenn ein Springer auf einem der Felder gemäß der Springer-Zugregel „ein Feld waagrecht und zwei Felder senkrecht oder zwei Felder waagrecht und ein Feld senkrecht“ das andere Feld bedroht.  $\square$

In der folgenden Definition führen wir, analog zu den gerichteten Graphen, einige wichtige Sprechweisen und Begriffe für ungerichtete Graphen ein.

### 7.2.3 Definition: Nachbarschaft, Endknoten, Knotengrad

Es sei  $g = (V, K)$  ein ungerichteter Graph. Gilt für  $x, y \in V$ , dass  $\{x, y\} \in K$ , so heißen die Knoten  $x$  und  $y$  **benachbart** und die **Endknoten** der Kante  $\{x, y\}$ . Es definiert weiterhin  $nachb_g(x) := \{y \in V \mid \{x, y\} \in K\}$  die **Nachbarschaftsmenge** des Knoten  $x \in V$  und ihre Kardinalität  $d_g(x) := |nachb_g(x)|$  den **Knotengrad** von  $x$ .  $\square$

Im folgenden Satz sind die wichtigsten Eigenschaften bezüglich der Knotengrade zusammengestellt. Der erste Teil entspricht genau den Gradformeln bei den gerichteten Graphen. Wie bei diesen, so wird auch in Satz 7.2.4 durch  $\sum_{x \in V} d_g(x)$  die Summe aller Knotengrade festgelegt. Weiterhin bezeichnen wir im Beweis von Teil (2) mit  $\sum_{x \in X} d_g(x)$  die Summe aller Knotengrade der Knoten der Teilmenge  $X$  von  $V$ .

### 7.2.4 Satz: Eigenschaften der Knotengrade

Für alle ungerichteten Graphen  $g = (V, K)$  gelten die folgenden Eigenschaften:

- (1)  $\sum_{x \in V} d_g(x) = 2|K|$ .
- (2) Die Anzahl der Knoten ungeraden Grades ist gerade.
- (3) Gilt  $|V| > 1$ , so gibt es  $x, y \in V$  mit  $x \neq y$  und  $d_g(x) = d_g(y)$ .

**Beweis:** (1) Diesen Teil kann man vollkommen analog zur Gradformel beweisen. Es sei dies der Leserin oder dem Leser zur Übung empfohlen.

(2) Wir betrachten die folgenden zwei Teilmengen  $U$  und  $G$  von  $V$ , deren Durchschnitt leer ist und deren Vereinigung gerade  $V$  ergibt:

$$U := \{x \in V \mid d_g(x) \text{ ungerade}\} \quad G := \{x \in V \mid d_g(x) \text{ gerade}\}$$

Nun führen wir einen Widerspruchsbeweis und nehmen an, dass  $|U|$  eine ungerade Zahl sei. Dann ist auch  $\sum_{x \in U} d_g(x)$  als Summe einer ungeraden Anzahl von ungeraden Zahlen ungerade. Aufgrund von (1) gilt weiterhin die folgende Gleichung:

$$2|K| = \sum_{x \in V} d_g(x) = \sum_{x \in U} d_g(x) + \sum_{x \in G} d_g(x)$$

Damit hat auch  $\sum_{x \in G} d_g(x)$  ungerade zu sein. Dies ist aber ein Widerspruch, denn die Summe einer beliebigen Anzahl von geraden Zahlen ist gerade.

(3) Auch hier führen wir einen Widerspruchsbeweis und nehmen an, dass für alle  $x, y \in V$  mit  $x \neq y$  gilt  $d_g(x) \neq d_g(y)$ , also alle Knotengrade verschieden sind. Weil ein Knoten höchstens mit allen anderen Knoten benachbart sein kann, gilt die folgende Abschätzung für alle  $x \in V$ :

$$0 \leq d_g(x) \leq |V| - 1$$

In Kombination mit der Annahme folgt daraus, dass es einen Knoten  $x_0 \in V$  mit  $d_g(x_0) = 0$  gibt, und auch einen Knoten  $x_1 \in V$  mit  $d_g(x_1) = |V| - 1$ . Wegen  $|V| > 1$  gilt  $d_g(x_1) > 0$  und dies impliziert  $x_0 \neq x_1$ . Aufgrund von  $d_g(x_0) = 0$  ist  $x_0$  mit keinem Knoten benachbart. Aus  $d_g(x_1) = |V| - 1$  folgt, dass jeder Knoten  $x \in V \setminus \{x_1\}$  mit  $x_1$  benachbart ist, also auch  $x_0$ . Dies ist ein Widerspruch.  $\square$

Die Teile (2) und (3) von Satz 7.2.4 kann man anschaulich wie folgt beschreiben: Bei einer Party begrüßen sich alle Gäste anfangs per Handschlag. Dann ist die Zahl der Gäste, die einer ungeraden Zahl von Personen die Hände schütteln, gerade. Weiterhin gibt es mindestens zwei Gäste, welche gleich oft begrüßt werden. Wegen dieser Interpretation wird Satz 7.2.4 auch als **Handschatglemma** bezeichnet.

Die beiden Begriffe „Weg“ und „Kreis“ werden für ungerichtete Graphen  $g = (V, K)$  fast analog zu den selben Begriffen bei den gerichteten Graphen als lineare Listen von Knoten definiert. Man hat die entsprechenden Definitionen nur wie folgt an den neuen Fall der ungerichteten Verbindungen zwischen den Knoten anzupassen.

- (1) Definition eines **Wegs**  $w \in V^+$  in  $g = (V, K)$ : Ersetze in Definition 6.3.5 in Punkt (1) die Beziehungen  $w_i P w_{i+1}$  durch  $\{w_i, w_{i+1}\} \in K$ .
- (2) Definition eines **Kreises**  $w \in V^+$  in  $g = (V, K)$ : Ersetze in Definition 6.3.5 in Punkt (2) ebenfalls die Beziehungen  $w_i P w_{i+1}$  durch  $\{w_i, w_{i+1}\} \in K$  und noch  $|w| \geq 2$  durch  $|w| \geq 4$ .

Ein Kreis  $(x, x)$  ist im Gegensatz zum gerichteten Fall nicht möglich, da  $\{x\}$  keine Kante ist. Auch lineare Listen mit 3 Knoten dürfen nun keine Kreise mehr sein, da sonst jeder

ungerichtete Graph  $g = (V, K)$  mit mindestens einer Kante  $\{x, y\}$  einen Kreis hätte, nämlich die Liste  $(x, y, x)$ . Zur besseren Unterscheidung vom gerichteten Fall werden Wege in ungerichteten Graphen manchmal auch als **Züge** bezeichnet und Kreise als **Zyklen**. **Erreichbarkeit** von  $y \in V$  aus  $x \in V$  heißt bei ungerichteten Graphen  $g = (V, K)$  ebenfalls, dass es einen Weg von  $x$  nach  $y$  gibt. Damit wird durch alle Erreichbarkeitsbeziehungen eine Relation  $E$  auf der Knotenmenge  $V$  definiert, also durch

$$x E y : \iff \text{Es gibt einen Weg von } x \text{ nach } y$$

für alle  $x, y \in V$ . Wie bei den gerichteten Graphen ist  $E$  reflexiv und transitiv. Nun ist  $E$  aber sogar noch symmetrisch, also insgesamt eine Äquivalenzrelation. Die Äquivalenzklassen von  $E$  heißen die **Zusammenhangskomponenten** von  $g = (V, K)$ . Es ergibt hingegen wenig Sinn, auch bei ungerichteten Graphen durch eine naive Änderung von  $s_i P s_{i+1}$  in  $\{s_i, s_{i+1}\} \in K$  einen zu „Pfad“ analogen Begriff zu definieren, da dieser in den zeichnerischen Darstellungen zu Liniengebilden „mit Stacheln“ führt, die nur wenig mit dem zu tun haben, was man sich intuitiv unter einem Weg mit eventuell vorkommenden Kreisen vorstellt. Natürlich kann man auch Pfade so definieren, dass sie die Intuition treffen, indem man beispielsweise auch Kanten in die Listen mit aufnimmt. **Kreisfreiheit** heißt schließlich auch bei ungerichteten Graphen, dass es keinen Kreis gibt.

### 7.2.5 Beispiele: Wege, Kreise und Zusammenhangskomponenten

In dem ungerichteten Springergraphen von Beispiel 7.2.2 ist die lineare Liste

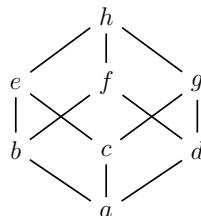
$$((1, a), (2, c), (3, a), (4, c))$$

ein Weg vom Knoten / Feld  $(1, a)$  zum Knoten / Feld  $(4, c)$ . Es gibt in dem angegebenen ungerichteten Graphen auch einige Kreise, etwa die lineare Liste

$$((2, a), (4, b), (3, d), (1, c), (2, a)).$$

Jedoch gibt es keinen Kreis, der alle Knoten „durchläuft“, also, mit Ausnahme des Anfangs und des Endes, jeden Knoten genau einmal beinhaltet. Solche speziellen Kreise werden in diesem Zusammenhang auch „geschlossene Springerzüge“ genannt. Für größere Schachbretter existieren geschlossene Springerzüge, beispielsweise auch für das klassische Schachbrett mit 8 Zeilen und 8 Spalten.

Betrachten wir hingegen das Ordnungsdiagramm der Potenzmenge  $\mathcal{P}(\{1, 2, 3\})$  als einen ungerichteten Graphen und benennen dabei die 8 Mengen in die Buchstaben  $a$  bis  $h$  um, so bekommen wir die folgende graphische Darstellung:



Auch dieser ungerichtete Graph hat Kreise; beispielsweise ist die lineare Liste

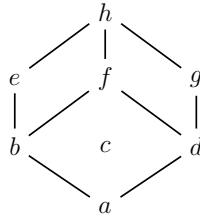
$$(b, e, h, f, b)$$

ein Kreis mit 4 Kanten, nämlich  $\{b, e\}$ ,  $\{e, h\}$ ,  $\{h, f\}$  und  $\{f, b\}$ , und die lineare Liste

$$(b, e, h, g, d, a, b)$$

ist ein Kreis mit 6 Kanten, nämlich  $\{b, e\}$ ,  $\{e, h\}$ ,  $\{h, g\}$ ,  $\{g, d\}$ ,  $\{d, a\}$  und  $\{a, b\}$ .

Nun ändern wir den eben betrachteten ungerichteten Graphen wie nachfolgend angegeben etwas ab, indem wir 3 Kanten entfernen:



Dadurch zerfällt der ungerichtete Graph in zwei Zusammenhangskomponenten, nämlich  $\{a, b, d, e, f, g, h\}$  und  $\{c\}$ .  $\square$

In der Einleitung zu diesem Abschnitt haben wir bemerkt, dass ungerichtete Graphen oft in Verbindung mit Problemen aus der Kombinatorik vorkommen. Nachfolgend geben wir nun einige Beispiele dazu an. In den entsprechenden Beweisen werden wir immer wieder Eins-zu-Eins-Beziehungen zwischen endlichen Mengen verwenden und, dass diese die Gleichheiten der Kardinalitäten implizieren. Dabei verzichten wir aber auf die formalen Bijektivitätsbeweise, da diese in allen Fällen einfach zu erbringen sind und diese Zwischenbeweise auch dazu führen können, dass die grundlegende Beweisidee der Reduktion auf bekannte Kardinalitäten nicht klar erkannt wird. Wir starten mit dem Zählen von Wegen in Gittergraphen. Diese speziellen Graphen sind wie folgt definiert.

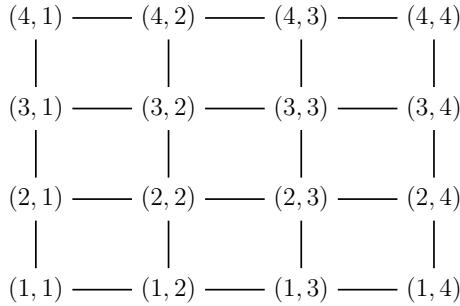
### 7.2.6 Definition: Gittergraph

Mittels  $X := \{1, \dots, m\}$  und  $Y := \{1, \dots, n\}$  ist der Gittergraph  $M_{m,n} = (V, K)$  mit  $m > 0$  vertikalen und  $n > 0$  horizontalen Schichten definiert durch  $V := X \times Y$  und

$$\{(x, y), (u, v)\} \in K \iff |x - u| + |y - v| = 1$$

für alle Knotenpaare  $(x, y) \in V$  und  $(u, v) \in V$ .  $\square$

Diese spezielle Art von Graphen kommt vielfach in der Praxis vor. Gittergraphen werden beispielsweise bei der Layout-Synthese elektronischer Schaltungen verwendet. Ein weiteres Anwendungsgebiet ist das sogenannte orthogonale Zeichnen von Graphen mit Hilfe von speziellen Algorithmen. In dem folgenden Bild ist der Gittergraph mit 4 vertikalen und 4 horizontalen Schichten zeichnerisch dargestellt. Anhand dieser Zeichnung erkennt man sofort den Bezug zum Namen.



In einem Gittergraphen besteht ein **kürzester Weg** zwischen zwei Knoten  $(x, y)$  und  $(u, v)$  aus  $|u - x|$  senkrechten Kanten und  $|v - y|$  waagrechten Kanten; er hat also als lineare Liste die Länge  $|u - x| + |v - y| + 1$ . Der nächste Satz gibt an, wie viele solcher Wege es gibt.

### 7.2.7 Satz: kürzeste Wege in Gittergraphen

Es seien  $(x, y)$  und  $(u, v)$  Knoten im Gittergraphen  $M_{m,n} = (V, K)$ . Dann gibt es genau

$$\binom{|u - x| + |v - y|}{|u - x|}$$

kürzeste Wege von  $(x, y)$  nach  $(u, v)$ .

**Beweis:** Es bezeichne  $W$  die Menge aller kürzesten Wege von  $(x, y)$  nach  $(u, v)$ . Weiterhin sei  $k$  als ihre Kantenanzahl definiert, also als

$$k := |u - x| + |v - y|.$$

Da, wie oben bemerkt, jeder Weg aus  $W$  aus  $|u - x|$  senkrechten Kanten und  $|v - y|$  waagrechten Kanten besteht, gibt es eine Eins-zu-Eins-Beziehung zwischen der Menge  $W$  und der Menge  $T$  der Tupel aus  $\{0, 1\}^k$ , in denen genau  $|u - x|$  Komponenten den Wert 1 und  $|v - y|$  Komponenten den Wert 0 besitzen. Die entsprechende bijektive Funktion ordnet einem kürzesten Weg  $((x_1, y_1), \dots, (x_{k+1}, y_{k+1})) \in W$  von links nach rechts die Richtungen seiner Kanten zu, wobei 1 „senkrecht“ und 0 „waagrecht“ heißt. Das Resultat-Tupel  $(s_1, \dots, s_k) \in T$  ist also komponentenweise durch

$$s_i = \begin{cases} 1 & \text{falls } |y_i - y_{i+1}| = 0 \\ 0 & \text{falls } |x_i - x_{i+1}| = 0 \end{cases}$$

festgelegt, für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$ . Es gibt aber auch eine Eins-zu-Eins-Beziehung zwischen der Menge  $T$  und der Menge  $\mathcal{M} := \{X \in \mathcal{P}(\{1, \dots, k\}) \mid |X| = |u - x|\}$ , nämlich die bijektive Abbildung des  $k$ -Tupels  $(s_1, \dots, s_k) \in T$  auf die Menge

$$\{i \in \{1, \dots, k\} \mid s_i = 1\}$$

aus  $\mathcal{M}$ . Aufgrund von Satz 7.1.16 gilt  $|\mathcal{M}| = \binom{k}{|u-x|}$  und folglich auch  $|W| = \binom{k}{|u-x|}$ . Die Festlegung von  $k$  zeigt nun die Behauptung.  $\square$

Zu Demonstrationszwecken betrachten wir noch einmal den oben gezeichneten Gittergraphen. Für das Paar  $(3, 1)$  und  $(2, 3)$  bekommen wir  $k = |2 - 3| + |3 - 1| = 3$  und  $|2 - 3| = 1$  und somit  $\binom{3}{1} = 3$  Wege mit 4 Knoten vom  $(3, 1)$  nach  $(2, 3)$ . Diese sind:

$$((3, 1), (3, 2), (3, 3), (2, 3)) \quad ((3, 1), (3, 2), (2, 2), (2, 3)) \quad ((3, 1), (2, 1), (2, 2), (2, 3))$$

Im Fall des Paares  $(3, 1)$  und  $(1, 3)$  erhalten wir  $k = |1 - 3| + |3 - 1| = 4$  und  $|1 - 3| = 2$ , was zu  $\binom{4}{2} = 6$  Wegen mit 5 Knoten vom  $(3, 1)$  nach  $(1, 3)$  führt. Es ist nicht schwierig, alle 6 Wege durch eine systematische Suche zu bestimmen.

Bei ungerichteten Graphen  $g = (V, K)$  bestimmt die Anzahl der Knoten die Maximalzahl der möglichen Kanten. Weil Kanten zweielementige Teilmengen von  $V$  sind, besitzt  $g = (V, K)$  maximal  $\binom{|V|}{2}$  Kanten. Ungerichtete Graphen mit  $\binom{|V|}{2} = \frac{1}{2}|V|(|V| - 1)$  Kanten erhalten einen speziellen Namen.

### 7.2.8 Definition: vollständiger Graph

Ein ungerichteter Graph  $g = (V, K)$  heißt **vollständig**, falls  $|K| = \frac{1}{2}|V|(|V| - 1)$  gilt.  $\square$

Es ist  $g = (V, K)$  also genau dann vollständig, falls je zwei verschiedene Knoten benachbart sind. Für so einen speziellen Graphen und Knoten  $x, y \in V$  mit  $x \neq y$  ist damit die lineare Liste  $(x, y)$  der eindeutig gegebene kürzeste Weg von  $x$  nach  $y$ . Weil damit kürzeste Wege ziemlich uninteressant sind, bietet es sich an, längste Wege zu betrachten. Alle längsten Wege von  $x$  nach  $y$  haben offensichtlich die Listenlänge  $|V|$ . Wie viele es davon genau gibt, das besagt das nächste Resultat.

### 7.2.9 Satz: längste Wege in vollständigen Graphen

Es sei  $g = (V, K)$  ein vollständiger ungerichteter Graph mit  $|V| \geq 2$ . Dann gibt es zu allen Knoten  $x, y \in V$  mit  $x \neq y$  genau  $(|V| - 2)!$  längste Wege von  $x$  nach  $y$ .

**Beweis:** Falls  $|V| = 2$  zutrifft, dann gibt es genau einen längsten Weg von  $x$  nach  $y$ , nämlich  $(x, y)$ . In diesem Fall gilt aber auch  $(|V| - 2)! = 0! = 1$ .

Im Fall  $|V| > 2$  betrachten wir die nichtleere Teilmenge  $X := V \setminus \{x, y\}$  der Knotenmenge  $V$  und erhalten  $|X| = |V| - 2$ . Da  $g$  nach Voraussetzung vollständig ist, definiert jede bijektive Funktion  $f : \{1, \dots, |X|\} \rightarrow X$  mittels

$$w := (x, f(1), \dots, f(|X|), y)$$

eindeutig einen längsten Weg  $w$  von  $x$  nach  $y$ . Umgekehrt liefert (weil alle Knoten paarweise verschieden sind) jeder längste Weg  $(w_1, \dots, w_{|V|})$  von  $x$  nach  $y$  durch die nachfolgende Festlegung auch eindeutig eine bijektive Funktion von  $\{1, \dots, |X|\}$  nach  $X$ :

$$f : \{1, \dots, |X|\} \rightarrow X \quad f(i) = w_{i+1}$$

Wegen dieser Eins-zu-Eins-Beziehung zwischen der Menge der längsten Wege von  $x$  nach  $y$  und der Menge der bijektiven Funktionen von  $\{1, \dots, |X|\}$  nach  $X$  und der Gleichmäßigkeit der letzten Menge und der Menge  $S(|X|)$  von Permutationen zeigt Satz 7.1.10 in

Verbindung mit  $|X| = |V| - 2$  die Behauptung.  $\square$

Es bietet sich nun an, Satz 7.2.9 auf alle Wege zu erweitern. Das Abzählen aller Wege von einem Knoten zu einem anderen Knoten geschieht dann günstigerweise mit Hilfe der Weglängen. Um den Beweis des entsprechenden Satzes zu vereinfachen, lagern wir einen Teil in das nachfolgende Lemma aus.

### 7.2.10 Lemma

Es sei  $g = (V, K)$  ein vollständiger ungerichteter Graph mit  $|V| \geq 2$  und es seien  $x, y \in V$  verschiedene Knoten. Dann gibt es zu allen  $k \in \mathbb{N}$  mit  $1 \leq k \leq |V| - 1$  genau

$$(k-1)! \binom{|V|-2}{k-1}$$

Wege  $w$  von  $x$  nach  $y$  mit  $|w| = k+1$  (also mit  $k$  Kanten).

**Beweis:** Zur Vereinfachung seien  $n := |V|$  und  $X := V \setminus \{x, y\}$  definiert. Weiterhin bezeichne  $W_{k+1}$  die Menge der Wege von  $x$  nach  $y$  der Länge  $k+1$  (also mit  $k$  Kanten) und  $\mathcal{P}_{k-1}(X)$  die Menge der Teilmengen von  $X$  der Kardinalität  $k-1$ . Dann gilt

$$W_{k+1} = \bigcup \{W_{k+1}(Y) \mid Y \in \mathcal{P}_{k-1}(X)\},$$

mit  $W_{k+1}(Y) := \{w \in W_{k+1} \mid w_2, \dots, w_k \in Y\}$  als die Menge der Wege von  $x$  nach  $y$  der Länge  $k+1$  mit inneren Knoten aus  $Y$ . Da alle Mengen der Mengenvereinigung paarweise disjunkt sind, erhalten wir

$$|W_{k+1}| = |\bigcup \{W_{k+1}(Y) \mid Y \in \mathcal{P}_{k-1}(X)\}| = \sum_{Y \in \mathcal{P}_{k-1}(X)} |W_{k+1}(Y)|,$$

wobei die Summe alle Werte  $|W_{k+1}(Y)|$  addiert. Analog zum Beweis von Satz 7.2.9 kann man  $|W_{k+1}(Y)| = |Y|!$  für alle  $Y \in \mathcal{P}_{k-1}(Y)$  zeigen, denn aufgrund der Vollständigkeit des Graphen  $g$  entspricht jede der  $|Y|!$  Anordnungen von  $Y$  als lineare Liste aus  $X^{k-1}$  genau einem Weg aus  $W_{k+1}(Y)$ . Dies bringt, zusammen mit  $|X| = n - 2$ ,  $|Y| = k - 1$  für alle  $Y \in \mathcal{P}_{k-1}(X)$  und Satz 7.1.16 die Gleichung

$$|W_{k+1}| = |\mathcal{P}_{k-1}(X)| (k-1)! = \binom{|X|}{k-1} (k-1)! = \binom{n-2}{k-1} (k-1)!$$

und  $n = |V|$  impliziert die Behauptung.  $\square$

Und hier ist der Satz über die Anzahl aller Wege von einem Knoten zu einem anderen Knoten in einem vollständigen ungerichteten Graphen, an dem wir interessiert sind.

### 7.2.11 Satz: alle Wege in vollständigen Graphen

Wiederum seien  $g$ ,  $x$  und  $y$  wie in Lemma 7.2.10 vorausgesetzt. Dann ist die Anzahl der Wege von  $x$  nach  $y$  durch den folgenden Ausdruck gegeben:

$$\sum_{k=2}^{|V|} \frac{(|V|-2)!}{(|V|-k)!}$$

**Beweis:** Wenn wir zur Abkürzung wiederum  $n := |V|$  definieren, so gilt für alle  $k \in \mathbb{N}$  mit  $1 \leq k \leq n - 1$  die folgende Gleichung:

$$(k-1)! \binom{n-2}{k-1} = \frac{(k-1)!(n-2)!}{(k-1)!(n-2-(k-1))!} = \frac{(n-2)!}{(n-k-1)!} = \frac{(n-2)!}{(n-(k+1))!}$$

Nun sei  $W$  die Menge der Wege von  $x$  nach  $y$  und zu  $k \in \mathbb{N}$  mit  $1 \leq k \leq n - 1$  sei, wie im Lemma,  $W_{k+1}$  die Menge der Wege von  $x$  nach  $y$  mit  $k$  Kanten. Dann erhalten wir unter Verwendung der paarweisen Disjunktheit dieser Mengen, von Lemma 7.2.10, der obigen Rechnung und einer abschließenden Indextransformation die Gleichung

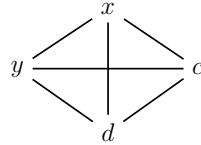
$$|W| = \left| \bigcup_{k=1}^{n-1} W_{k+1} \right| = \sum_{k=1}^{n-1} |W_{k+1}| = \sum_{k=1}^{n-1} (k-1)! \binom{n-2}{k-1} = \sum_{k=1}^{n-1} \frac{(n-2)!}{(n-(k+1))!} = \sum_{k=2}^n \frac{(n-2)!}{(n-k)!}$$

und mit  $n = |V|$  folgt aus ihr die behauptete Aussage.  $\square$

Die vorhergehenden Resultate bestimmen die Anzahlen der betrachteten Wege in den entsprechenden Graphen jeweils nur zwischen zwei vorgegebenen verschiedenen Knoten  $x$  und  $y$ . Unter Betrachtung von Mengen von Paaren können auch allgemeinere Aufgaben gelöst werden, etwa die Bestimmung der Anzahl der kürzesten Wege in einem Gittergraphen  $M_{m,n}$ , die im Knoten  $(1, 1)$  (der Ecke links unten) starten und in irgendeinem Knoten  $(m, k)$ , mit  $1 \leq k \leq n$ , enden (also in der obersten horizontalen Schicht). Nachfolgend demonstrieren wir die Vorgehensweise in den Beweisen von Lemma 7.2.10 und Satz 7.2.11 mittels eines kleinen Beispielgraphen.

### 7.2.12 Beispiel: alle Wege in vollständigen Graphen

Wir betrachten den in dem folgenden Bild gegebenen vollständigen ungerichteten Graphen  $g = (V, K)$  mit 4 Knoten und darin zuerst alle Wege von  $x$  nach  $y$ .



Aufgrund der Rechnung  $\sum_{k=2}^{|V|} \frac{(|V|-2)!}{(|V|-k)!} = \sum_{k=2}^4 \frac{(2)!}{(4-k)!} = 2!(\frac{1}{2!} + \frac{1}{1!} + \frac{1}{0!}) = 2(\frac{1}{2} + 1 + 1) = 5$  müssen genau 5 Wege von  $x$  nach  $y$  existieren. Zu ihrer Bestimmung nach dem Vorgehen in den obigen zwei Beweisen setzen wir  $X := \{c, d\}$  und verwenden auch die restlichen dort eingeführten Bezeichnungen. Dann können wir wie folgt rechnen: Für  $k = 1$  haben wir  $\mathcal{P}_0(X) = \emptyset$  und dies liefert

$$W_2 = W_2(\emptyset) = \{(x, y)\}.$$

Gilt  $k = 2$ , so bekommen wir  $\mathcal{P}_1(X) = \{\{c\}, \{d\}\}$  und dies impliziert

$$W_3 = W_3(\{c\}) \cup W_3(\{d\}) = \{(x, c, y)\} \cup \{(x, d, y)\} = \{(x, c, y), (x, d, y)\}.$$

Es bleibt noch der Fall  $k = 3$  mit  $\mathcal{P}_2(X) = \{\{c, d\}\}$ . Dieser Fall bringt

$$W_4 = W_4(\{c, d\}) = \{(x, c, d, y), (x, d, c, y)\}$$

als die  $(|V| - 2)! = (4 - 2)! = 2$  längsten Wege von  $x$  nach  $y$  (siehe auch Satz 7.2.9). Insgesamt erhalten wir also die in der Menge

$$W = W_2 \cup W_3 \cup W_4 = \{(x, y), (x, c, y), (x, d, y), (x, c, d, y), (x, d, c, y)\}$$

aufgeführten 5 Wege von  $x$  nach  $y$ . Analog gibt es 5 Wege von  $x$  nach  $c$  und 5 Wege von  $x$  nach  $d$ , also, wegen des noch nicht betrachteten Wegs  $(x)$ , insgesamt 16 Wege, die in  $x$  beginnen. Gleiches gilt für die restlichen drei Knoten, so dass der Graph  $g$  insgesamt 64 Wege enthält.  $\square$

Bei Graphen kann man die Aufwandsfunktion eines Algorithmus manchmal dadurch verfeinern, dass man nicht nur die Anzahl  $n$  der Knoten als Eingabegröße nimmt, sondern auch noch die Anzahl der Kanten (bzw. Pfeile im gerichteten Fall) mit betrachtet. So kann es dann etwa vorkommen, dass ein Algorithmus  $\mathcal{A}_1$  eine Aufwandsfunktion aus der Funktionenmenge  $\mathcal{O}(n \cdot \text{kanz}(n))$  besitzt, mit  $\text{kanz}(n)$  als die Anzahl der Kanten in Abhängigkeit von der Knotenzahl  $n$ . Für die Kantenanzahlfunktion  $\text{kanz} : \mathbb{N} \rightarrow \mathbb{N}$  gilt  $\text{kanz}(n) \leq \frac{n(n-1)}{2}$  für alle  $n \in \mathbb{N} \setminus \{0\}$ , also  $\text{kanz}(n) \in \mathcal{O}(n^2)$ . Damit besitzt  $\mathcal{A}_1$  eine kubische Laufzeit in der Anzahl der Knoten, also eine aus  $\mathcal{O}(n^3)$ . Hat ein anderer Algorithmus  $\mathcal{A}_2$  hingegen z.B. eine Aufwandsfunktion aus  $\mathcal{O}(n + \text{kanz}(n))$ , so ist er von quadratischer Laufzeit, also seine Aufwandsfunktion aus  $\mathcal{O}(n^2)$ . Kann die Aufwandsfunktion eines graphentheoretischen Algorithmus also in Abhängigkeit von  $n$  und  $\text{kanz}(n)$  angegeben werden, so sind insbesondere solche Graphen als Eingaben interessant, bei denen die Eigenschaft  $\text{kanz}(n) \in \mathcal{O}(n)$  gilt. Für diese liegt die Aufwandsfunktion von  $\mathcal{A}_1$  nämlich in  $\mathcal{O}(n^2)$  und die von  $\mathcal{A}_2$  sogar in  $\mathcal{O}(n)$  (lineare Laufzeit).

## 7.3 Dünne ungerichtete Graphen

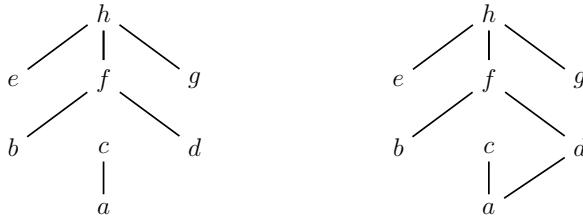
Motiviert durch die Schlussbemerkungen des letzten Abschnitts geben wir in diesem Abschnitt Klassen von ungerichteten Graphen an, bei denen  $\text{kanz}(n) \in \mathcal{O}(n)$  beweisbar ist. Da solche Graphen, im Hinblick auf die Maximalzahl der möglichen Kanten, nur wenige Kanten besitzen, nennt man sie auch dünn. Die behandelten Klassen sind nicht künstlich, sondern kommen in zahlreichen praktischen Anwendungen von Graphen vor. Wir starten mit den Wäldern und Bäumen. Zur Definition der zweiten Graphenklaasse brauchen wir den schon früher eingeführten Begriff einer Zusammenhangskomponente. Nach der Einführung von Wegen und Kreisen haben wir eine Zusammenhangskomponente festgelegt als eine Äquivalenzklasse derjenigen Äquivalenzrelation auf der Knotenmenge des zugrundeliegenden ungerichteten Graphen, welche genau die Paare in Beziehung setzt, zwischen denen ein Weg existiert.

### 7.3.1 Definition: Wald und Baum

Ein ungerichteter Graph  $g = (V, K)$  heißt ein **Wald**, falls es in ihm keinen Kreis gibt, und ein **Baum**, falls er zusätzlich genau eine Zusammenhangskomponente besitzt.  $\square$

Wälder sind also genau die kreisfreien ungerichteten Graphen und Bäume sind also genau die kreisfreien ungerichteten Graphen, welche, wie man sagt, auch noch **zusammenhängend** sind. Die folgenden Bilder zeigen links einen Wald mit den zwei Zusammenhangskomponenten  $\{a, c\}$  und  $\{b, d, e, f, g, h\}$  und rechts einen Baum. Die beiden ungerichteten

Graphen basieren auf der gleichen 8-elementigen Knotenmenge  $V := \{a, b, c, d, e, f, g, h\}$ . Der Wald besitzt 6 Kanten und der Baum hat 7 Kanten.



Aufgrund des rechten Bildes wird deutlich, warum man für ungerichtete Graphen mit solchen bildlichen Darstellungen den Begriff Baum gewählt hat. Betrachtet man im linken Bild jede der zwei Zusammenhangskomponenten als eigenen ungerichteten Graphen, so erhält man zwei Bäume. Ein Wald besteht also aus Bäumen, genau wie in der Wirklichkeit. Man beachte, dass der Baumbegriff dieses Abschnitts, der klassische Baumbegriff der Graphentheorie, sehr verschieden ist vom Baumbegriff von Abschnitt 3.3.

Mit Hilfe der Anzahl der Zusammenhangskomponenten kann man die Anzahl der Kanten eines Waldes genau angeben. Es gilt hier das folgende Resultat, welches man schon aus den obigen Bildern erahnen konnte. Unter Verwendung der oben eingeführten Kantenanzahlfunktion  $\text{kanz}$  zeigt es für Wälder (und damit auch Bäume) mit  $n$  Knoten die beabsichtigte Eigenschaft  $\text{kanz}(n) \in \mathcal{O}(n)$ .

### 7.3.2 Satz: Kantenzahl in Wäldern

Für alle ungerichteten Graphen  $g = (V, K)$  gelten die folgenden Eigenschaften:

- (1) Ist  $g$  ein Baum, so gilt  $|K| = |V| - 1$ .
- (2) Ist  $g$  ein Wald mit  $k$  Zusammenhangskomponenten, so gilt  $|K| = |V| - k$ .

**Beweis:** (1) Wir verwenden das Prinzip der Grapheninduktion von Abschnitt 6.3, welches auch für ungerichtete Graphen gilt, und zeigen  $A(g)$  für alle ungerichteten Graphen  $g = (V, K)$ , wobei die Aussage  $A(g)$  gerade der Behauptung (1) entspricht,

Induktionsbeginn: Es sei  $g = (V, K)$  ein ungerichteter Graph mit  $|V| = 1$ . Ist  $g$  ein Baum, so impliziert die Kreisfreiheit  $K = \emptyset$ , also  $|K| = 0$ , was  $|K| = |V| - 1$  bringt. Also gilt  $A(g)$ .

Induktionsschluss: Nun sei  $n \in \mathbb{N}$  mit  $n \geq 1$  gegeben und es gelte die Induktionshypothese  $A(h)$  für alle ungerichteten Graphen  $h$  mit  $n$  Knoten. Es sei  $g = (V, K)$  ein ungerichteter Graph mit  $|V| = n + 1$ . Zum Nachweis von  $A(g)$  setzen wir  $g$  als Baum voraus. Zuerst wählen wir in  $g$  einen Knoten  $x$ , in dem ein längster Weg beginnt. Dann gilt  $d_g(x) = 1$ , denn  $d_g(x) \neq 0$  folgt aus dem Zusammenhang von  $g$  und die Maximalität der Weglänge zusammen mit der Kreisfreiheit von  $g$  verhindert  $d_g(x) > 1$ . Es sei nun  $y \in V$  der einzige Nachbar von  $x$ . Wenn wir  $x$  aus  $V$  und  $\{x, y\}$  aus  $K$  entfernen, so erhalten wir wieder einen ungerichteten Graphen

$$h = (V \setminus \{x\}, K \setminus \{\{x, y\}\})$$

mit  $|V \setminus \{x\}| = |V| - 1 = n$ , von dem man sehr einfach zeigen kann, dass er ein Baum ist. Aufgrund der Induktionshypothese  $A(h)$  gilt  $|K \setminus \{\{x, y\}\}| = |V \setminus \{x\}| - 1$  und dies bringt

$$|K| = |K \setminus \{\{x, y\}\}| + 1 = |V \setminus \{x\}| - 1 + 1 = |V \setminus \{x\}| = |V| - 1.$$

Damit ist der Nachweis von  $A(g)$  beendet.

(2) Wir nehmen an, dass  $Z_1, \dots, Z_k$  die  $k$  Zusammenhangskomponenten von  $g$  seien. Für alle  $i \in \mathbb{N}$  mit  $1 \leq i \leq k$  betrachten wir die Menge

$$K_i := \{\{x, y\} \mid \{x, y\} \in K \wedge x \in K_i \wedge y \in K_i\},$$

also die Menge der Kanten von  $g$ , deren Endknoten in  $K_i$  enthalten sind, sowie die ungerichteten Graphen  $g_i = (Z_i, K_i)$ . Alle diese Graphen  $g_i$  sind Bäume, denn die Kreisfreiheit von  $g$  vererbt sich auf  $g_i$  und der Zusammenhang von  $g_i$  ergibt sich aus der Definition der Zusammenhangskomponenten mittels der Erreichbarkeits-Äquivalenzrelation. Weil die Menge  $\{Z_1, \dots, Z_k\}$  eine Partition von  $V$  darstellt, bildet die Menge  $\{K_1, \dots, K_k\}$  eine Partition von  $K$ . Dies impliziert die Gleichung

$$|K| = \left| \bigcup_{i=1}^k K_i \right| = \sum_{i=1}^k |K_i| = \sum_{i=1}^k (|Z_i| - 1) = \left| \bigcup_{i=1}^k Z_i \right| - k = |V| - k$$

mit Hilfe der Aussage (1), also die Behauptung.  $\square$

Aussage (1) dieses Satzes erlaubt es, mittels einiger Zusatzüberlegungen Bäume auf eine andere Weise durch Kantenzahlen zu charakterisieren. Wie dies geht, wird nun gezeigt.

### 7.3.3 Satz: Kantenzahl zur Charakterisierung von Bäumen

Ein ungerichteter und zusammenhängender Graph  $g = (V, K)$  ist genau dann ein Baum, wenn  $|K| = |V| - 1$  gilt.

**Beweis:** Die Richtung „ $\implies$ “ wurde im letzten Satz gezeigt.

Zum Beweis von „ $\impliedby$ “ ist nur die Kreisfreiheit nachzuweisen, da der Zusammenhang von  $g$  nach der Voraussetzung gegeben ist. Wir nehmen zu einem Widerspruchsbeweis an, dass  $g$  einen Kreis besitze. Wenn wir  $X$  als die Menge der Knoten des Kreises definieren, so gibt es in  $g$  mindestens die  $|X|$  Kanten des Kreises. Aufgrund des Zusammenhangs von  $g$  ist von jedem Knoten  $y \in V \setminus X$  ein Knoten aus  $X$  erreichbar. Ist  $w^{(y)} \in V^+$  ein entsprechender mit  $y$  beginnender Weg mit kürzester Länge, so gilt

$$|\{\{w_1^{(y)}, w_2^{(y)}\} \mid y \in V \setminus X\}| = |V \setminus X| = |V| - |X|,$$

denn alle Kanten, mit denen die Wege  $w^{(y)} = (w_1^{(y)}, w_2^{(y)}, \dots, w_{|w^{(y)}|}^{(y)})$  beginnen, sind paarweise verschieden. Sie sind auch keine Kanten des Kreises. Also gibt es in  $g$  mindestens  $|X| + |V| - |X| = |V|$  Kanten. Das widerspricht der Voraussetzung  $|K| = |V| - 1$ .  $\square$

In Bäumen kann man besonders einfach Wege zählen. Das Analogon von Satz 7.2.11 sieht hier wie folgt aus:

### 7.3.4 Satz: alle Wege in Bäumen

Es seien  $g = (V, K)$  ein Baum mit  $|V| \geq 2$  und  $x, y \in V$  verschiedene Knoten. Dann gibt es genau einen Weg von  $x$  nach  $y$ .

**Beweis:** Wegen des Zusammenhangs von  $g$  gibt es mindestens einen Weg von  $x$  nach  $y$ . Durch einen Widerspruchsbeweis zeigen wir nachfolgend noch, dass es auch höchstens einen Weg von  $x$  nach  $y$  gibt.

Angenommen, es seien  $v = (v_1, \dots, v_m)$  und  $w = (w_1, \dots, w_n)$  zwei verschiedene Wege von  $x$  nach  $y$ . Dann gibt es einen Index  $i \in \mathbb{N}$  mit  $1 \leq i < \min\{m, n\}$ , so dass  $v$  und  $w$  sich nach ihm erstmals aufteilen. Es gilt also  $v_1 = w_1, v_2 = w_2$  usw. bis  $v_i = w_i$  und dann  $v_{i+1} \neq w_{i+1}$ . Weiterhin gibt es Indizes  $j, k \in \mathbb{N}$  mit  $i < j \leq m$  und  $i < k \leq n$ , so dass  $v$  und  $w$  sich nach dem Aufteilen bei ihnen erstmals wieder treffen. Es gilt also  $v_j = w_k$  und die Knoten  $v_{i+1}, \dots, v_{j-1}, w_{i+1}, \dots, w_{k-1}$  sind paarweise verschieden. Offensichtlich bildet dann die durch die Konkatenation von  $(v_i, \dots, v_j)$  mit der Revertierung von  $(w_i, \dots, w_{k-1})$  entstehende lineare Liste

$$(v_i, v_{i+1}, \dots, v_j, w_{k-1}, w_{k-2}, \dots, w_i)$$

einen Kreis in  $g$  und das widerspricht der Baumeigenschaft.  $\square$

Den nun folgenden Überlegungen, die zur letzten Graphenklasse dieses Abschnitts mit der schönen Eigenschaft  $\text{kanz}(n) \in \mathcal{O}(n)$  führen, liegt die Eulersche Polyederformel zugrunde. Ein **Polyeder** ist eine Teilmenge des Euklidschen Raums  $\mathbb{R}^3$ , welche ausschließlich von ebenen Flächen begrenzt wird. Von der höheren Schule her kennt man sicher das Prisma, die Pyramide, die Rechtecksäule, den Würfel als deren Spezialfall und das Tetraeder. Die letzten beiden Polyeder sind sogenannte **Platonische Körper**, benannt nach dem griechischen Philosophen Platon (ca. 428–347 v. Chr.). Allen diesen Gebilden ist gemeinsam, dass sie die **Eulersche Polyederformel**

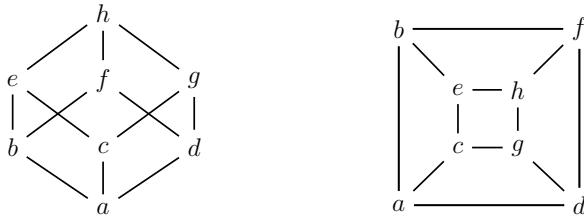
$$e + f = k + 2$$

erfüllen, mit  $e$  als die Anzahl der Ecken,  $f$  als die Anzahl der Flächen und  $k$  als die Anzahl der Kanten. Im Fall des Prismas gibt es etwa 6 Ecken, 5 Flächen und 9 Kanten und bei der Pyramide gibt es 5 Ecken, 5 Flächen und 8 Kanten. Wenn man sich die Kanten eines Polyeders als ein Netz von Gummibändern vorstellt und dieses an den Ecken einer ausgewählten Fläche weit genug auseinanderzieht, so kann man das Netz so in die Ebene projizieren, dass sich die den Gummibändern (Kanten) entsprechenden Geradenstücke, oder **Strecken**, nur an den Endpunkten treffen. Das entstehende Bild kann man als die Zeichnung eines ungerichteten Graphen auffassen.

### 7.3.5 Beispiel: Projektion des Würfels

In den Beispielen 7.2.5 haben wir das Ordnungsdiagramm der Potenzmenge  $\mathcal{P}(\{1, 2, 3\})$  als ungerichteten Graphen mit den Knoten als den Buchstaben von  $a$  bis  $h$  angegeben. Das entsprechende Bild kann man sich als Zeichnung eines Würfels denken, dessen Ecken ebenfalls mit  $a$  bis  $h$  bezeichnet sind. Zieht man diese Zeichnung an der Fläche mit den

Eckpunkten  $a, b, f$  und  $d$  auseinander, so bekommt man das rechte der folgenden zwei Bilder. Das linke der Bilder zeigt zum Vergleich noch einmal die Originalzeichnung.



In der rechten Zeichnung wird die ursprüngliche Würfelfläche mit den Eckpunkten  $a, b, f$  und  $d$ , also die, an der auseinandergenommen wird, zur unbeschränkten Außenfläche. Die restlichen fünf Flächen des Würfels der linken Zeichnung entsprechen genau den durch die Strecken der rechten Zeichnung eingerahmten fünf Gebieten (es sind sogenannte **Polygone**) in der Ebene. Weil die Außenfläche mitgezählt wird, bleibt die Eulersche Polyederformel gültig.  $\square$

Treffen sich in einer Zeichnung eines ungerichteten Graphen die den Kanten entsprechenden Strecken nur an den Endpunkten, so spricht man von einer planaren Zeichnung. Formal kann man planare Graphzeichnungen wie nachfolgend angegeben definieren. In Definition 7.3.6 bezeichnen griechische Buchstaben Punkte in der Euklidischen Ebene  $\mathbb{R}^2$  und  $\overline{\alpha\beta}$  ist die Strecke mit den Endpunkten  $\alpha, \beta \in \mathbb{R}^2$ . Wir haben bereits in Abschnitt 3.1 bemerkt, dass Geraden formal Teilmengen von  $\mathbb{R}^2$  sind. Jedoch verzichten wir auf eine präzise Beschreibung von Strecken als Teilmengen von  $\mathbb{R}^2$  mittels der kartesischen Koordinaten ihrer Endpunkte, weil es für das Folgende nicht wesentlich ist. Das durch die höhere Schule gegebene intuitive Verständnis genügt hier vollkommen.

### 7.3.6 Definition: planare linealische Graphzeichnung

Eine **planare linealische Graphzeichnung** ist ein Paar  $z = (P, \mathcal{S})$ . Dabei ist  $P$  eine endliche Teilmenge von  $\mathbb{R}^2$  und  $\mathcal{S}$  eine Teilmenge von  $\{\overline{\alpha\beta} \mid \alpha, \beta \in P \wedge \alpha \neq \beta\}$ . Weiterhin wird für alle Strecken  $\overline{\alpha\beta}, \overline{\rho\lambda} \in \mathcal{S}$  mit  $\overline{\alpha\beta} \neq \overline{\rho\lambda}$  gefordert, dass

$$\overline{\alpha\beta} \cap \overline{\rho\lambda} \subseteq \{\alpha, \beta, \rho, \lambda\}$$

gilt. Ein durch einen Streckenzug beschränktes Gebiet der Ebene heißt eine **Innenfläche** von  $z$ . Die **Außenfläche** von  $z$  ist definiert als  $\mathbb{R}^2 \setminus (\mathcal{I} \cup \mathcal{U}\mathcal{S})$ , wobei  $\mathcal{I}$  die Vereinigung aller Innenflächen ist.  $\square$

Die Forderung  $\overline{\alpha\beta} \cap \overline{\rho\lambda} \subseteq \{\alpha, \beta, \rho, \lambda\}$  in dieser Definition besagt gerade, dass sich die beiden Strecken  $\overline{\alpha\beta}$  und  $\overline{\rho\lambda}$  nur in den Endpunkten schneiden. Gilt die Gleichung  $\overline{\alpha\beta} \cap \overline{\rho\lambda} = \emptyset$ , so schneiden sich die beiden Strecken nicht. Trifft hingegen  $\overline{\alpha\beta} \cap \overline{\rho\lambda} \neq \emptyset$  zu, so gibt es genau einen Punkt  $\gamma \in \mathbb{R}^2$ , in dem sie sich schneiden, der also  $\overline{\alpha\beta} \cap \overline{\rho\lambda} = \{\gamma\}$  erfüllt. Die Forderung erzwingt nun  $\gamma = \alpha$  oder  $\gamma = \beta$  oder  $\gamma = \rho$  oder  $\gamma = \lambda$ . Mit Hilfe von planaren linealischen Graphzeichnungen können wir nun planare ungerichtete Graphen wie folgt formal definieren:

### 7.3.7 Definition: planarer Graph

Ein ungerichteter Graph  $g = (V, K)$  heißt **planar** (oder auch **plättbar**), falls es eine planare linealische Graphzeichnung  $z = (P, \mathcal{S})$  und eine bijektive Funktion  $\Phi : V \rightarrow P$  so gibt, dass die Gleichung

$$\mathcal{S} = \{\overline{\Phi(x)\Phi(y)} \mid \{x, y\} \in K\}$$

gilt. Man nennt  $z$  dann eine planare linealische Graphzeichnung von  $g$  und  $\Phi$  die **Einbettungsfunktion**.  $\square$

Weil die Einbettungsfunktion bijektiv ist, gilt in dieser Definition  $|V| = |P|$ . Daraus kann man sofort folgern, dass auch  $|K| = |\mathcal{S}|$  gilt, denn  $\Phi$  induziert die bijektive Funktion  $\Psi : K \rightarrow \mathcal{S}$  mit der Spezifikation  $\Psi(\{x, y\}) = \overline{\Phi(x)\Phi(y)}$ . Wir formulieren diese Eigenschaften explizit als Lemma, da sie nachfolgend noch mehrmals verwendet werden.

### 7.3.8 Lemma

Ist  $z = (P, \mathcal{S})$  eine planare linealische Graphzeichnung des planaren ungerichteten Graphen  $g = (V, K)$ , so gelten  $|V| = |P|$  und  $|K| = |\mathcal{S}|$ .  $\square$

Die Definition 7.3.7 besagt anschaulich, dass man  $g = (V, P)$  in der Ebene so zeichnen kann, dass die Kanten zu Strecken zwischen den Knoten entsprechenden Punkten werden und sich Kanten nicht kreuzen. Durch die bijektive Einbettungsfunktion  $\Phi$  wird jedem Knoten von  $g$  genau ein Punkt in der Ebene zugeordnet und die der Kante  $\{x, y\}$  von  $g$  entsprechende Strecke verbindet die Punkte  $\Phi(x)$  und  $\Phi(y)$ .

### 7.3.9 Beispiele: planare ungerichtete Graphen

Offensichtlich sind alle Gittergraphen  $M_{m,n}$  planar. Die Einbettungsfunktion  $\Phi$  von Definition 7.3.7 ist hier durch

$$\Phi : \{1, \dots, m\} \times \{1, \dots, n\} \rightarrow \mathbb{R}^2 \quad \Phi(x, y) = (x, y)$$

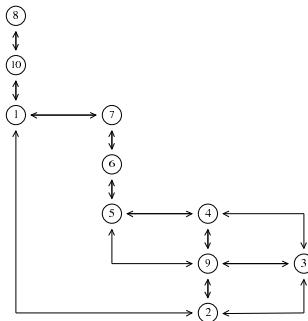
gegeben. Auch Bäume und Wälder sind planar. Die Einbettungsfunktion  $\Phi$  ergibt sich hierbei durch die Zuordnung der Knoten zu den kartesischen Koordinaten der Punkte der Ebene (Zeichenfläche), welche sie darstellen. Wenn man etwa in den beiden Zeichnungen nach Definition 7.3.1 jeweils  $\Phi(a) = (0, 0)$  festlegt, so kann man die restlichen Funktionswerte durch Messungen bestimmen. Auch die vollständigen ungerichteten Graphen mit weniger als 4 Knoten sind planar. Ab 5 und mehr Knoten sind sie hingegen nicht mehr planar.  $\square$

An dieser Stelle ist noch eine Bemerkung angebracht. Normalerweise werden planare Graphzeichnungen so definiert, dass den Kanten sogenannte **Jordan-Kurven** (benannt nach Camille Jordan (1838-1922), einem französischen Mathematiker) zwischen den ihnen zugeordneten Punkten entsprechen, also, anschaulich gesprochen, Linien, die auch gekrümmt sein dürfen, aber sich nicht selbst schneiden. Man kann zeigen, dass jede planare Graphzeichnung mit Jordan-Kurven durch das geeignete Verschieben der Punkte in der Ebene in eine planare linealische Graphzeichnung transformiert werden kann. Wir haben uns für den zweiten Ansatz entschieden, weil Strecken von der höheren Schule

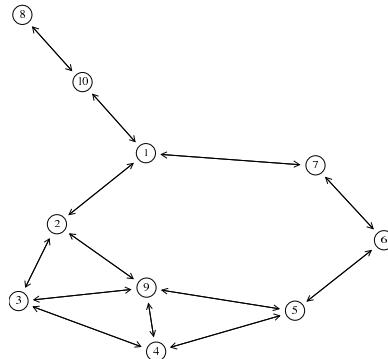
her bekannt sind, Jordan-Kurven hingegen nicht. Letztere lernt man in einem Lehrbuch über Analysis oder Topologie kennen. Es gibt effiziente Verfahren, die Planarität zu testen und dann gegebenenfalls eine planare Graphzeichnung zu erstellen. Implementierte Algorithmen zeichnen Kanten oft als Strecken oder Aneinanderreihungen von Strecken. Auch spezielle Kurven sind gebräuchlich, etwa Kreisbögen oder die besonders eleganten **Bezier-Kurven**, benannt nach dem französischen Ingenieur Pierre Bezier (1910-1999).

### 7.3.10 Beispiele: automatisches Zeichnen planarer Graphen

Um zu demonstrieren, wie Bilder aussehen, die von implementierten Algorithmen zum „schönen“ Zeichnen von (auch) planaren Graphen erzeugt werden, geben wir nachfolgend zwei Beispiele an. Das erste Bild zeigt einen gezeichneten Graphen, wobei die Kanten durch Aneinanderreihungen von Strecken dargestellt werden. Dem Algorithmus liegt der Ansatz zugrunde, die Zeichnung auf einem Gitter in der Ebene durchzuführen und dabei die benötigte Fläche zu minimieren.



Und hier ist eine Zeichnung des gleichen Graphen mit Strecken als Kanten:



Beim zweiten Zeichenalgorithmus wird ein physikalisches Modell verwendet. Die Knoten des gegebenen Graphen werden als Körper (etwa Planeten) im Raum mit einer gewissen Anziehungskraft aufgefasst und die Kanten dazwischen als dehbare Federn. Der Graph wird dann so gezeichnet, dass sich das gesamte System in einem physikalischen Gleichgewicht befindet. Beide Algorithmen sind Teil des Computersystems RELVIEW, das an der Christian-Albrechts-Universität zu Kiel entwickelt wurde. Dieses behandelt hauptsächlich

gerichtete Graphen. Kanten von ungerichteten Graphen werden in RELVIEW mit Pfeilspitzen an beiden Enden dargestellt.  $\square$

Bei planaren ungerichteten Graphen und deren Zeichnungen sieht die Eulersche Polyederformel wie in dem nachfolgenden Satz angegeben aus.

### 7.3.11 Satz: Eulersche Polyederformel für Graphzeichnungen

Für alle planaren linealischen Graphzeichnungen  $z = (P, \mathcal{S})$  von zusammenhängenden planaren ungerichteten Graphen  $g = (V, K)$ , mit  $f$  als die Zahl aller Flächen von  $z$ , gilt die Gleichung  $|P| + f = |\mathcal{S}| + 2$ .

**Beweis (durch Widerspruch):** Angenommen, es gäbe eine planare linealische Graphzeichnung eines zusammenhängenden planaren ungerichteten Graphen  $g = (V, K)$ , für den die behauptete Gleichung nicht gilt. Dann wählen wir unter allen diesen Graphzeichnungen eine mit einer möglichst kleinen Anzahl von Strecken aus. Diese sei  $z_0 = (P_0, \mathcal{S}_0)$  und  $f_0$  sei die Anzahl ihrer Flächen.

Es kann  $g$  kein Baum sein. Wäre  $g$  ein Baum, so gilt aufgrund von Aussage (1) von Satz 7.3.2 und Lemma 7.3.8 die Gleichung

$$|\mathcal{S}_0| = |K| = |V| - 1 = |P_0| - 1.$$

Auch gibt es dann in der Graphzeichnung  $z_0$  offensichtlich keine Innenfläche, was  $f_0 = 1$  impliziert. Insgesamt bekommen wir also

$$|P_0| + f_0 = |P_0| + 1 = |\mathcal{S}_0| + 1 + 1 = |\mathcal{S}_0| + 2.$$

Damit gilt die behauptete Gleichung, im Widerspruch zur Annahme über  $z_0$ .

Da  $g$  zusammenhängt und kein Baum ist, gibt es in ihm einen Kreis. Als eine Konsequenz existiert in  $z_0$  mindestens eine Innenfläche. Wir wählen eine Strecke  $\overline{\alpha\beta}$  aus ihrer Begrenzung und entfernen sie aus der Streckenmenge  $\mathcal{S}_0$ . Das Resultat  $z_0^* = (P_0, \mathcal{S}_0 \setminus \{\overline{\alpha\beta}\})$  ist immer noch eine planare linealische Graphzeichnung eines zusammenhängenden planaren ungerichteten Graphen. Da sie echt weniger Strecken als  $z_0$  hat und angenommen ist, dass  $z_0$  eine planare linealische Graphzeichnung mit kleinster Streckenzahl ist, in der die zu beweisende Gleichung nicht gilt, gilt diese in  $z_0^*$ . Mit  $f_0^*$  als die Anzahl der Flächen von  $z_0^*$  erhalten wir somit die Gleichung

$$|P_0| + f_0^* = |\mathcal{S}_0 \setminus \{\overline{\alpha\beta}\}| + 2 = |\mathcal{S}_0| + 1.$$

Weil wir aber genau eine Strecke aus der Begrenzung einer Innenfläche von  $z_0$  entfernt haben, hat  $z_0^*$  genau eine Fläche weniger als  $z_0$ , was  $f_0^* = f_0 - 1$  bringt. Wenn wir dies in die obige Gleichung einsetzen, so erhalten wir  $|P_0| + f_0 - 1 = |\mathcal{S}_0| + 1$ , also  $|P_0| + f_0 = |\mathcal{S}_0| + 2$ . Das widerspricht der Annahme, dass in  $z_0$  die behauptete Gleichung nicht gilt.  $\square$

In diesem Satz kann auf den Zusammenhang des gezeichneten planaren ungerichteten Graphen nicht verzichtet werden. Beispielsweise gilt er nicht für planare linealische Graphzeichnungen von Wäldern mit mehr als einer Zusammenhangskomponente. Wenn man den

Beweis von Satz 7.3.11 mit den früheren Beweisen von Induktionsprinzipien vergleicht, so stellt man eine große Ähnlichkeit beim Vorgehen fest. Und in der Tat kann man den Satz auch durch eine Induktion nach der Kardinalität von  $\mathcal{S}$  beweisen, also nach der Anzahl der Strecken der Graphzeichnungen bzw. der Kanten der gezeichneten Graphen.

Und nun beweisen wir mit Hilfe von Satz 7.3.11, also der Eulerschen Polyederformel für Graphzeichnungen, unser beabsichtigtes Resultat. Dabei setzen wir den Zusammenhang des zugrundeliegenden Graphen voraus, um Satz 7.3.11 unmittelbar anwenden zu können. Mit der Methode des Beweises von Teil (2) von Satz 7.3.2 kann man aus dem folgenden Satz 7.3.12 recht schnell als Verallgemeinerung die Ungleichung  $|K| \leq 3|V| - 6k$  beweisen, wenn  $g = (V, K)$  planar ist und  $k$  Zusammenhangskomponenten besitzt.

### 7.3.12 Satz: maximale Kantenzahl bei planaren Graphen

Für alle planaren zusammenhängenden ungerichteten Graphen  $g = (V, K)$  mit  $|V| \geq 3$  gilt  $|K| \leq 3|V| - 6$ .

**Beweis:** Es sei  $z = (P, \mathcal{S})$  eine planare linealische Graphzeichnung von  $g$ . Wegen Lemma 7.3.8 genügt es, die Abschätzung  $|\mathcal{S}| \leq 3|P| - 6$  zu beweisen. Dazu setzen wir  $f$  als die Anzahl der Flächen von  $z$  voraus. Weiterhin bezeichne  $f_i$  die Anzahl der Flächen von  $z$ , die von genau  $i$  Strecken begrenzt werden, mit einer entsprechenden Interpretation des Begriffs „Begrenzung“ im Fall der Außenfläche und einer Innenfläche „mit Stacheln“. Jede Strecke, die auf beiden Seiten nur die gleiche Fläche berührt, wird in ihrer Begrenzung doppelt gezählt<sup>10</sup>.

Aufgrund der gerade getroffenen Festlegung und weil  $g$  zusammenhängend ist, wird jede Fläche von  $z$  von mindestens 3 Strecken begrenzt. Daraus folgt

$$f = f_3 + f_4 + \dots + f_n,$$

mit  $n \geq 3$  als der Maximalzahl von Strecken aus  $\mathcal{S}$ , die eine Fläche der Graphzeichnung  $z$  begrenzen. Wenn wir die Strecken von  $z$  hinsichtlich der Zahl  $i$  der Flächen zählen, die sie begrenzen, so erhalten wir die doppelte Anzahl der Strecken als

$$2|\mathcal{S}| = 3f_3 + 4f_4 + \dots + nf_n.$$

Zu jeder der  $f_i$  Flächen, die von genau  $i$  Strecken begrenzt werden, gehören nämlich genau  $i$  Strecken. Weil aber jede Strecke zwischen genau 2 Flächen von  $z$  liegt (im entarteten Fall sind beide gleich der Außenfläche oder einer Innenfläche mit Stacheln), wird sie damit

---

<sup>10</sup> Im Beispiel der Zeichnung des Baums nach der Definition 7.3.1 wird somit jede Kante/Strecke des rechten Bilds doppelt gezählt und es gelten  $f_{14} = 1$  und  $f_i = 0$  für alle  $i \neq 14$ . Wären noch zwei Kanten zwischen  $c$  und  $b$  und zwischen  $b$  und  $e$  vorhanden, so ist der entsprechende ungerichtete Graph immer noch planar. Nun gelten aber  $f_4 = f_5 = f_9 = 1$  und  $f_i = 0$  für alle anderen  $i$ . Die Außenfläche wird nun von 9 Strecken begrenzt. Dabei wird die Strecke zwischen  $g$  und  $h$  doppelt gezählt. Fügt man in den Baum hingegen nur die Kante zwischen  $a$  und  $b$  ein, so entsteht eine Innenfläche mit einem Stachel, da die beiden Seiten der Kante zwischen  $a$  und  $c$  die gleiche Fläche berühren. Für dieses Beispiel gelten  $f_6 = f_{10} = 1$  und  $f_i = 0$  für alle anderen  $i$ . Bei der Bestimmung von  $f_6$  wird die Strecke zwischen  $a$  und  $c$  doppelt gezählt und bei der Bestimmung von  $f_{10}$  werden die Strecken zwischen  $e$  und  $h$ ,  $f$  und  $h$  und  $g$  und  $h$  doppelt gezählt.

in der Summation  $3f_3 + 4f_4 + \dots + nf_n$  zweimal gezählt. Eine Kombination der eben hergeleiteten Gleichungen bringt

$$3f = 3(f_3 + f_4 + \dots + f_n) = 3f_3 + 3f_4 + \dots + 3f_n \leq 3f_3 + 4f_4 + \dots + nf_n = 2|\mathcal{S}|.$$

Nun verwenden wir die Eulersche Polyederformel für planare linealische Graphzeichnungen in der umgestellten Form  $|\mathcal{S}| = |P| + f - 2$ . Mit Hilfe der eben bewiesenen Abschätzung  $f \leq \frac{2|\mathcal{S}|}{3}$  erhalten wir daraus die Eigenschaft

$$|\mathcal{S}| \leq |P| + \frac{2|\mathcal{S}|}{3} - 2.$$

Eine zweimalige Umstellung dieser Formel bringt zuerst  $\frac{1}{3}|\mathcal{S}| \leq |P| - 2$  und dann die Behauptung  $|\mathcal{S}| \leq 3|P| - 6$ .  $\square$

Auf die Voraussetzung  $|V| \geq 3$  (bzw., dass im nicht zusammenhängenden Fall jede Zusammenhangskomponente mindestens drei Knoten besitzt) kann nicht verzichtet werden. Ein planarer zusammenhängender ungerichteter Graph mit 2 Knoten hat genau eine Kante. Für den Ausdruck  $3|V| - 6$  ergibt sich hier hingegen der Wert 0. Auch die spezielle Behandlung der Begrenzung der Außenfläche und aller Begrenzungen von Innenflächen mit Stacheln beim Zählen von Strecken im Beweis ist notwendig. Weiterhin ist die bewiesene Abschätzung, wie man im Jargon sagt, **scharf**, da es zusammenhängende planare ungerichtete Graphen mit  $3|V| - 6$  Kanten gibt. Ein Beispiel ist der vollständige ungerichtete Graph mit 4 Knoten. Aus dem Satz folgt auch sofort, dass alle vollständigen ungerichteten Graphen mit mehr als 4 Knoten nicht planar sind. Für alle natürlichen Zahlen  $n$  mit  $n > 4$  gilt nämlich die Ungleichung  $3n - 6 < \frac{n(n-1)}{2}$ , was eine einfache Diskussion der Funktion  $f : \mathbb{R} \rightarrow \mathbb{R}$ , definiert durch  $f(x) = \frac{x(x-1)}{2} - 3x + 6$ , zeigt.

Planare ungerichtete Graphen treten oft auf, wenn man Verbindungsnetze mittels Graphen modelliert. Beispielsweise führt eine Modellierung des deutschen Autobahnnetzes zu solch einem Graphen, wenn man die Autobahndreiecke und -kreuze als Knoten auffasst und die sie verbindenden Autobahnteilstücke als Kanten. Auch Eisenbahnnetze und Wasserstraßennetze führen beispielsweise zu planaren ungerichteten Graphen. Bei allen diesen Modellierungen ist natürlich vereinfachend unterstellt, dass keine nicht höhengleichen Kreuzungen vorliegen. Solche gibt es aber sogar bei Wasserstraßen, etwa das Wasserstraßenkreuz bei Minden. Hier wird der Mittellandkanal in einer Trogbrücke über die Weser geführt.

Aufgrund von Satz 7.3.12 sollte man bei der algorithmischen Lösung von Problemen auf solchen Netzen mittels Graphen unbedingt versuchen, den Aufwand auch asymptotisch in der Kantenanzahl abzuschätzen. Dann ist diese  $\mathcal{O}$ -Abschätzung nämlich gleich der  $\mathcal{O}$ -Abschätzung in der Knotenzahl und man bekommt so in der Regel bessere Abschätzungen als durch einen Ansatz, der von  $\text{kanz}(n) \in \mathcal{O}(n^2)$  ausgeht.

## 7.4 Einige Variationen des Graphenbegriffs

In Kapitel 6 und in diesem Kapitel haben wir die einfachsten Typen von gerichteten und ungerichteten Graphen eingeführt. Graphen sind sehr allgemeine mathematische Strukturen und sehr gut zum Beschreiben, Visualisieren und Modellieren geeignet. Sie werden

deshalb in den vielfältigsten Anwendungen eingesetzt, sowohl in der Theorie als auch in der Praxis. Für viele Anwendungen sind die bisher beschriebenen Graphen aber zu einschränkend. Deshalb wurden Erweiterungen und Variationen entwickelt, die den jeweiligen Problemstellungen besser genügen. Auf einige dieser Erweiterungen wollen wir nachfolgend knapp eingehen.

Eine erste Erweiterung der derzeitigen Typen  $g = (V, P)$  mit  $P \subseteq V \times V$  (gerichteter Graph) bzw.  $g = (V, K)$  mit  $K \subseteq \{\{x, y\} \mid x, y \in V \wedge x \neq y\}$  (ungerichteter Graph) ist, dass man sie um Funktionen anreichert, die den Knoten bzw. den Pfeilen/Kanten gewisse Werte zuordnen. Werden den Pfeilen von gerichteten Graphen Zahlen zugeordnet, so dient dies oft dazu, bei der Modellierung von Straßennetzen die Längen der einzelnen Straßen anzugeben, woraus sich dann die Längen von Verbindungen bestimmen lassen, die aus mehreren Straßen bestehen. Formal sieht dies wie folgt aus: Ist  $g = (V, P, \delta)$  ein gerichteter Graph mit einer Funktion  $\delta : P \rightarrow \mathbb{R}_{>0}$ , die jedem Pfeil  $(x, y) \in P$  seine Länge  $\delta(x, y)$  zuordnet, so ist in diesem Zusammenhang die Länge eines Wegs  $w = (w_1, \dots, w_n)$  definiert durch die Summe seiner Pfeillängen, also durch

$$\text{länge}(w) = \delta(w_1, w_2) + \dots + \delta(w_{n-1}, w_n).$$

Eine Grundaufgabe ist dann, zu gegebenen zwei Knoten  $x, y \in V$  die Länge eines kürzesten Wegs vom  $x$  nach  $y$  zu bestimmen, sofern überhaupt ein Weg von  $x$  nach  $y$  existiert. Bezeichnet  $W(x, y) \subseteq \mathcal{P}(V^+)$  die Menge aller Wege von  $x$  nach  $y$  in  $g$ , so entspricht diese Aufgabe der algorithmischen Realisierung einer Funktion  $\text{minlänge} : V \times V \rightarrow \mathbb{R} \cup \{\infty\}$  mit der folgenden Definition:

$$\text{minlänge}(x, y) = \begin{cases} \min\{\text{länge}(w) \mid w \in W(x, y)\} & \text{falls } W(x, y) \neq \emptyset \\ \infty & \text{sonst} \end{cases}$$

In dieser Definition zeigt das Symbol „ $\infty$ “ an, dass es keinen Weg von  $x$  nach  $y$  gibt. Die Interpretation mit unendlich ist typisch für fast alle Ansätze, das Kürzeste-Wege-Problem zu lösen. Algorithmen zu diesem Problem lernt man beispielsweise in einer Vorlesung über kombinatorische Optimierung kennen.

Zuordnungen von Aktionen an die Pfeile von gerichteten Graphen kann man beispielsweise dazu verwenden, Transitionssysteme darzustellen. Ein mit  $a$  markierter Pfeil von  $x$  nach  $y$  entspricht dann der Beziehung  $x \xrightarrow{a} y$ . Zuordnungen von Zahlen an die Knoten sind schließlich typisch für Anwendungen in der Elektrotechnik, wenn man durch Graphen elektrische Leitungsnetze oder Schaltungen modelliert. Die Zahlen entsprechen dann in der Regel den Spannungen an den Knotenpunkten.

Bei den bisher behandelten Typen von Graphen sind Pfeile und Kanten immer mittels Knoten beschrieben, entweder als Paare  $(x, y)$  oder als zweielementige Mengen  $\{x, y\}$ . Folglich ist es nicht möglich, dass es zwischen zwei Knoten mehrere parallele Pfeile und Kanten gibt. Eine erste Möglichkeit, parallele Pfeile und Kanten einzuführen, ist, sie mittels verschiedener Marken zu benennen. Häufig wird auch die Möglichkeit gewählt, Pfeilen und Kanten durch entsprechende Mengen eine eigene Identität zu geben. Gerichtete Graphen werden bei so einem Ansatz dann definiert als Quadrupel  $g = (V, P, \alpha, \omega)$ . Dabei ist  $V$  die endliche und nichtleere Menge von Knoten und  $P$  die endliche Menge von Pfeilen.

Weiterhin sind  $\alpha, \omega : P \rightarrow V$  zwei Funktionen, die allen Pfeilen  $p \in P$  den Anfangsknoten  $\alpha(p) \in V$  und den Endknoten  $\omega(p) \in V$  zuordnen. Ungerichtete Graphen werden bei diesem Ansatz zu Tripeln  $g = (V, K, \iota)$ . Wieder ist  $V$  die endliche und nichtleere Menge von Knoten und  $K$  die endliche Menge von Kanten. Die Funktion  $\iota : K \rightarrow \mathcal{P}(V)$  ordnet jeder Kante die Menge der Knoten zu, welche die Kante berühren (mit ihr inzidieren). Damit ergibt sich  $|\iota(k)| = 2$  für alle  $k \in K$  als zusätzliche Bedingung.

Es wird der Leserin oder dem Leser empfohlen, zu Übungszwecken einige der graphentheoretischen Begriffe der letzten zwei Kapitel von den gerichteten Graphen  $g = (V, P)$  bzw. den ungerichteten Graphen  $g = (V, K)$  auf die Varianten  $g = (V, P, \alpha, \omega)$  bzw.  $g = (V, K, \iota)$  zu übertragen.

Ersetzt man bei den ungerichteten Graphen des Typs  $g = (V, K, \iota)$  die Einschränkung  $|\iota(k)| = 2$  durch  $\iota(k) \neq \emptyset$  für alle  $k \in K$ , so nennt man die Resultate Hypergraphen und die Elemente von  $K$  Hyperkanten. Hyperkanten können mehr als einen Knoten berühren. In zeichnerischen Darstellungen werden sie oft als „Segel“ gezeichnet, welche zwischen den Knoten aufgespannt sind. Die Einschränkung  $\iota(k) \neq \emptyset$  besagt, dass es keine „frei schwebenden“ Segel gibt. Hypergraphen kann man auch dadurch definieren, dass man in der Festlegung von den ungerichteten Graphen  $g = (V, K)$  nur fordert, dass jedes Element von  $K$  eine nichtleere Teilmenge von  $V$  ist. In dieser Auffassung von  $K$  als eine Teilmenge von  $\mathcal{P}(V)$  sind Venn-Diagramme oft ein geeignetes Mittel zur Visualisierung von Hypergraphen. Eine weitere Definitionsart ist  $g = (V, K, R)$ , mit  $V$  als endliche und nichtleere Menge von Knoten,  $K$  als endliche Menge von Hyperkanten und  $R \subseteq K \times V$  als totale Relation, die beschreibt, welche Hyperkante welche Knoten berührt. Hypergraphen werden etwa bei der Lösung von Zuordnungsproblemen verwendet. Ein Beispiel hierzu ist das Aufstellen von Stundenplänen.

Hypergraphen sind ungerichtet. Eine den Hypergraphen entsprechende Erweiterung der gerichteten Graphen auf gerichtete Hypergraphen wird bisher in der Literatur fast gar nicht diskutiert.

## 7.5 Übungsaufgaben

### Aufgabe

Beantworten Sie die folgenden Fragen (mit jeweiliger Begründung).

- (1) An einer Party nehmen 21 Personen teil, wobei anfangs jede Person alle anderen Teilnehmer per Handschlag begrüßt. Wie oft werden dabei insgesamt Hände gedrückt?
- (2) Auf wie viele Arten können sich 5 Personen auf 5 Stühle setzen?
- (3) Wie viele Wörter der Länge 3 kann man aus den 26 lateinischen Kleinbuchstaben  $a, \dots, z$  bilden, in denen der Buchstabe  $a$  genau einmal vorkommt?

### Aufgabe

Zu  $s \in M^*$  und  $x \in M$  bezeichne  $|s|_x$  die Anzahl der Vorkommen von  $x$  in  $s$ , beispielsweise  $|(a, b, a, c)|_a = 2$ .

- (1) Geben Sie eine formale Definition der Notation  $|s|_x$  über den Aufbau der linearen Listen mittels () und der Linksanfügeoperation an.
- (2) Zeigen Sie für alle  $n, k \in \mathbb{N}$ , dass  $|\{s \in \{0,1\}^* \mid |s| = n \wedge |s|_1 = k\}| = \binom{n}{k}$ .

### Aufgabe

Beweisen Sie für alle  $n, k \in \mathbb{N}$  mit  $k \leq n$  die folgende Gleichung:

$$\sum_{i=0}^n \binom{i}{k} = \binom{n+1}{k+1}$$

Was besagt diese Gleichung für das Pascalsche Dreieck?

### Aufgabe

Wir erweitern das klassische Schachbrett zu einem  $m \times m$  Schachbrett mit  $m > 0$  Zeilen und Spalten und den  $m^2$  Feldern  $(1, 1)$  bis  $(m, m)$  von links unten bis rechts oben. Auf solch einem  $m \times m$  Schachbrett habe eine Spielfigur genau die folgenden zwei Zugmöglichkeiten:

- (1) Ein Schritt horizontal nach rechts.
- (2) Ein Schritt vertikal nach oben.

Wie viele Möglichkeiten gibt es, die Spielfigur vom Feld  $(1, 1)$  links unten zum Feld  $(m, m)$  rechts oben zu bewegen?

### Aufgabe

Beantworten Sie die folgenden zwei Fragen zu Läuferstellungen auf einem Schachbrett jeweils durch eine mathematische Begründung:

- (1) Was ist die maximale Anzahl von Läufern, die man auf einem  $m \times m$  Schachbrett so platzieren kann, dass sie sich gegenseitig nicht bedrohen?
- (2) Wie viele Möglichkeiten gibt es, eine maximale Anzahl von Läufern auf einem  $m \times m$  Schachbrett so platzieren, dass sie sich gegenseitig nicht bedrohen?

Hinweis: Beweisen Sie zur Beantwortung der zweiten Frage, dass bei einer maximalen Anzahl von Läufern alle auf einem Randfeld platziert werden müssen.

### Aufgabe

Wie viele gerichtete Graphen  $g = (V, P)$  bzw. ungerichtete Graphen  $g = (V, K)$  mit Knotenmenge  $V$  gibt es (mit Begründungen)?

### Aufgabe

Es sei  $V$  eine endliche und nichtleere Menge. Zeigen Sie, dass es genau so viele ungerichtete Graphen  $g = (V, K)$  wie gerichtete Graphen  $g = (V, P)$  gibt, bei denen die Relation  $P$  der Pfeile symmetrisch und irreflexiv ist.

### Aufgabe

Zu einer natürlichen Zahl  $n \neq 0$  ist der Hyperwürfel  $Q_n = (V_n, K_n)$  definiert als derjenige ungerichtete Graph, dessen Knotenmenge  $V_n$  gleich  $\{0, 1\}^n$  ist und dessen Kantenmenge  $K_n$  aus allen Mengen  $\{s, t\}$  besteht, so dass sich die  $n$ -Tupel  $s$  und  $t$  in genau einer Komponente unterscheiden.

- (1) Spezifizieren Sie durch eine Formel, dass sich  $s, t \in \{0, 1\}^n$  in genau einer Komponente unterscheiden.
- (2) Zeichnen Sie die Hyperwürfel  $Q_1, Q_2$  und  $Q_3$  und bestimmen Sie anhand der Zeichnungen für alle Knoten der Hyperwürfel  $Q_1, Q_2$  und  $Q_3$  die Knotengrade und die Nachbarnmengen.

### Aufgabe

Gegeben sei eine natürliche Zahl  $n \neq 0$ . Wie viele Knoten bzw. Kanten besitzt der Hyperwürfel  $Q_n = (V_n, K_n)$  (mit Begründung)?

### Aufgabe

Es sei  $g = (V, K)$  ein ungerichteter Graph. Eine nichtleere Teilmenge  $C$  von  $V$  heißt eine Clique, falls für alle  $x, y \in C$  gilt:  $x = y$  oder  $\{x, y\} \in K$ .

- (1) Zeigen Sie, dass alle einelementigen Teilmengen von  $V$  Cliques sind.
- (2) Wie viele Cliques  $C$  mit  $|C| = 2$  besitzt der ungerichtete Graph  $g$ , wenn er ein Baum ist (mit Begründung)?

### Aufgabe

Es sei  $g = (V, K)$  ein Baum mit  $|V| > 1$ . Zeigen Sie, dass es mindestens zwei Knoten  $x, y \in V$  mit  $x \neq y$ ,  $d_g(x) = 1$  und  $d_g(y) = 1$  gibt.

### Aufgabe

Zwei ungerichtete Graphen  $g_1 = (V_1, K_1)$  und  $g_2 = (V_2, K_2)$  werden isomorph genannt, falls es eine bijektive Funktion  $\Phi : V_1 \rightarrow V_2$  gibt, so dass

$$\{x, y\} \in K_1 \iff \{\Phi(x), \Phi(y)\} \in K_2$$

für alle  $x, y \in V_1$  gilt.

- (1) Es sei  $V := \{a, b, c, d\}$ . Welche der ungerichteten Graphen  
 $g_1 = (V, \{\{a, b\}, \{d, b\}\}) \quad g_2 = (V, \{\{a, c\}, \{c, d\}\}) \quad g_3 = (V, \{\{a, c\}, \{b, d\}\})$   
sind isomorph bzw. nicht isomorph (mit Begründung)?
- (2) Stellen Sie eine Verbindung her zwischen der Isomorphie ungerichteter Graphen, dem Begriff „planar“ und den planaren linealischen Graphzeichnungen.
- (3) Beweisen Sie: Durch die Relation „sind isomorph“ wird zu jeder endlichen und nichtleeren Menge  $V$  eine Äquivalenzrelation auf der Menge aller ungerichteten Graphen mit  $V$  als Knotenmenge definiert.

# 8 Grundbegriffe algebraischer Strukturen

Große Teile der Mathematik und der theoretischen Informatik untersuchen mathematische Strukturen und wenden solche zur Lösung von Problemen an. Sehr allgemein betrachtet besteht eine mathematische Struktur aus einer Liste von nichtleeren Mengen, genannt Trägermengen, von Elementen aus den Trägermengen, genannt Konstanten, und von mengentheoretischen Konstruktionen über den Trägermengen. Bisher kennen wir etwa geordnete Mengen, gerichtete Graphen und ungerichtete Graphen als mathematische Strukturen. In den ersten beiden Fällen gibt es genau eine Trägermenge, keine Konstanten und genau eine mengentheoretische Konstruktion, welche jeweils eine Relation über der Trägermenge ist. Beim dritten Fall gibt es ebenfalls genau eine Trägermenge und keine Konstanten. Die einzige mengentheoretische Konstruktion ist nun jedoch eine spezielle Teilmenge der Potenzmenge der Trägermenge. In diesem Kapitel behandeln wir fast nur algebraische Strukturen. Dies heißt konkret, dass die mengentheoretischen Konstruktionen Funktionen über den Trägermengen sind. Wir beschränken uns weiterhin größtenteils auf den Fall einer einzigen Trägermenge. Solche Strukturen werden auch homogen genannt. Alle speziell behandelten homogenen algebraischen Strukturen stammen aus der klassischen Algebra. Auf allgemeinere mathematische Strukturen gehen wir im letzten Abschnitt des Kapitels noch kurz ein. Wir hoffen, dass die Leserin oder der Leser durch den gewählten allgemeinen Ansatz dieses Kapitels gut auf die Verwendung allgemeiner mathematischer Strukturen vorbereitet wird.

## 8.1 Homogene algebraische Strukturen

Wenn wir die oben gegebene informelle Beschreibung einer homogenen algebraischen Struktur in eine formale Definition fassen, so erhalten wir die folgende Festlegung.

### 8.1.1 Definition: homogene algebraische Struktur

Eine **homogene algebraische Struktur** ist ein Tupel  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  mit  $m \geq 0$  und  $n \geq 1$ . Dabei ist  $M$  eine nichtleere Menge, genannt **Trägermenge**, alle  $c_i$  sind (gewisse ausgezeichnete) Elemente aus  $M$ , genannt die **Konstanten**, und alle  $f_i$  sind (irgendwelche)  $s_i$ -stellige Funktionen  $f_i : M \rightarrow M$  im Fall  $s_i = 1$  und  $f_i : M^{s_i} \rightarrow M$  im Fall  $s_i > 1$ , genannt die (inneren) **Operationen**. Die lineare Liste  $(0, \dots, 0, s_1, \dots, s_n)$  mit  $m$  Nullen heißt der **Typ** oder die **Signatur**.  $\square$

Man beachte, dass laut dieser Definition bei homogenen algebraischen Strukturen die Konstanten fehlen dürfen, jedoch mindestens eine Operation vorhanden sein muss. Beispielsweise bildet das Paar  $(\mathbb{N}, +)$  eine homogene algebraische Struktur des Typs (2), das 5-Tupel  $(\mathbb{N}, 0, 1, +, \cdot)$  bildet eine homogene algebraische Struktur des Typs (0, 0, 2, 2) und das Tripel  $(M^*, (), \&)$  bildet eine homogene algebraische Struktur des Typs (0, 2). Nachfolgend sprechen wir vereinfachend nur noch von algebraischen Strukturen. Die Operationen, die vorkommen werden, sind 1- oder 2-stellig. Im zweiten Fall verwenden wir immer eine Infix-Notation und sprechen manchmal auch von einer **Verknüpfung**.

Wir haben in Definition 8.1.1 der Übersichtlichkeit halber gefordert, dass in der Tupelaufschreibung einer homogenen algebraischen Struktur erst die Trägermenge kommt, dann

die Konstanten kommen und am Ende die Operationen stehen. In der Praxis macht man sich von dieser Forderung oft frei und vermischt die Aufzählung der Konstanten und Operationen nach der Trägermenge. Dann ist etwa  $(\mathbb{N}, 0, +, 1, \cdot)$  eine homogene algebraische Struktur des Typs  $(0, 2, 0, 2)$ . Wir bleiben aber im Rest des Kapitels bei der Aufzählung gemäß Definition 8.1.1.

Algebraische Strukturen unterscheiden sich zuerst durch ihren Typ. Wesentlich wichtiger ist aber ihre Unterscheidung durch die Eigenschaften, welche für die Konstanten und Operationen gefordert werden, also ihre Axiome. Werden Konstanten, Operationen und Axiome nach und nach hinzugenommen, so entsteht eine gewisse Hierarchie von immer feineren Strukturen. Am Anfang der Hierarchie, die wir nachfolgend aufbauen, stehen die Monoide, welche wie folgt festgelegt sind.

### 8.1.2 Definition: Monoid

Eine algebraische Struktur  $(M, e, \cdot)$  des Typs  $(0, 2)$  heißt ein **Monoid**, falls für alle  $x, y, z \in M$  die folgenden Monoid-Axiome gelten:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad e \cdot x = x \quad x \cdot e = x$$

Gilt zusätzlich noch für alle  $x, y \in M$  die Gleichung  $x \cdot y = y \cdot x$ , so heißt  $(M, e, \cdot)$  ein **kommutatives Monoid**.  $\square$

Die erste und die letzte Gleichung dieser Definition kennen wir schon von den Mengen und der Logik her als Assoziativ- bzw. Kommutativgesetz. Das Element  $e$  heißt **neutral** hinsichtlich der Operation „·“, wobei die zweite Gleichung die **Linksneutralität** und die dritte Gleichung die **Rechtsneutralität** spezifiziert. Aufgrund der Assoziativität der 2-stelligen Operation können wir auf die Klammerung verzichten. Wie schon früher werden wir auch in den Rechnungen dieses Kapitels bei assoziativen Operationen die Klammern fast immer weglassen und auch Anwendungen des Assoziativgesetzes nicht gesondert erwähnen.

Beispiele für zahlartige kommutative Monoide sind  $(\mathbb{N}, 0, +)$ ,  $(\mathbb{N}, 1, \cdot)$  und  $(\mathbb{Z}, 0, +)$ . Jede Menge  $M$  führt zu den kommutativen Monoiden  $(\mathcal{P}(M), \emptyset, \cup)$  und  $(\mathcal{P}(M), M, \cap)$  und zu den Monoiden  $(M^*, (), \&)$  der linearen Listen und  $(\mathcal{S}(M), id_M, \circ)$  der bijektiven Funktionen. Die letzten beiden Monoide sind im Allgemeinen nicht kommutativ, wie man sehr leicht durch die Angabe entsprechender Gegenbeispiele belegt. Bei Monoiden kann man eine Potenzierung analog zu den Zahlen wie folgt festlegen.

### 8.1.3 Definition: Potenzierung

In einem Monoid  $(M, e, \cdot)$  definiert man die  $n$ -te **Potenz**  $x^n$  von  $x \in M$  durch  $x^0 := e$  und  $x^{n+1} = x \cdot x^n$  für alle  $n \in \mathbb{N}$ .  $\square$

So entspricht in  $(\mathbb{N}, 0, +)$  die Potenz  $x^n$  beispielsweise der  $n$ -fachen Addition von  $x$  mit sich selbst, also dem Produkt  $xn$ , in  $(\mathbb{N}, 1, \cdot)$  ist  $x^n$  die übliche Potenzierung und in  $(\mathcal{P}(M), \emptyset, \cup)$  gelten  $X^0 = \emptyset$  und  $X^n = X$  für alle  $n > 0$ . Durch vollständige Induktion kann man leicht die üblichen Potenzgesetze auch für Monoide zeigen. Wir empfehlen der Leserin oder dem Leser, den nachfolgenden Satz zu Übungszwecken zu beweisen.

### 8.1.4 Satz: Potenzgesetze

Ist  $(M, e, \cdot)$  ein Monoid, so gelten für alle  $x \in M$  und  $m, n \in \mathbb{N}$  die Gleichungen  $x^{m+n} = x^m \cdot x^n$  und  $x^{mn} = (x^m)^n$  und, falls  $(M, e, \cdot)$  kommutativ ist, weiterhin  $(x \cdot y)^m = x^m \cdot y^m$ .  $\square$

Was die zwei Monoide  $(\mathbb{Z}, 0, +)$  und  $(\mathcal{S}(M), id_M, \circ)$  von all den anderen oben angeführten Monoiden wesentlich unterscheidet, ist, dass eine Gleichung der Form  $x + y = z$  bzw. der Form  $f \circ g = h$  nach allen Objekten umgestellt werden kann. Sind beispielsweise ganze Zahlen  $x$  und  $z$  gegeben, so bekommt man die ganze Zahl  $y$  durch  $y = -x + z$  und sind beispielsweise bijektive Funktionen  $g : M \rightarrow M$  und  $h : M \rightarrow M$  gegeben, so bekommt man die bijektive Funktion  $f : M \rightarrow M$  durch  $f = h \circ g^{-1}$ . Es gibt also jeweils eine entsprechende 1-stellige Operation, welche die entsprechenden Umstellungen erlaubt. Ihre Existenz macht aus Monoiden Gruppen im folgenden Sinn:

### 8.1.5 Definition: Gruppe

Eine algebraische Struktur  $(G, e, \cdot, inv)$  des Typs  $(0, 2, 1)$  heißt eine **Gruppe**, falls für alle  $x, y, z \in G$  die folgenden Gruppen-Axiome gelten:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad e \cdot x = x \quad inv(x) \cdot x = e$$

Gilt wiederum die Gleichung  $x \cdot y = y \cdot x$  für alle  $x, y \in G$ , so heißt  $(G, e, \cdot, inv)$  eine **kommutative Gruppe**.  $\square$

Kommulative Gruppen werden auch Abelsche Gruppen genannt, nach dem norwegischen Mathematiker Nils Henrik Abel (1802-1829). Kleine Gruppen stellt man in der Regel durch Gruppentafeln dar, die aufzeigen, was das Resultat  $x \cdot y$  für jedes Paar  $(x, y) \in G^2$  ist.

### 8.1.6 Beispiel: Kleinsche Vierergruppe

Wir betrachten die Menge  $V_4 := \{e, a, b, c\}$ , das spezielle Element  $e$  aus  $V_4$  und die zwei Operationen  $\cdot : V_4^2 \rightarrow V_4$  und  $inv : V_4 \rightarrow V_4$ , welche durch die folgende Tafel bzw. den folgenden Vektor vollständig spezifiziert sind:

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $inv(\cdot)$ |
|---------|-----|-----|-----|-----|--------------|
| $e$     | $e$ | $a$ | $b$ | $c$ | $e$          |
| $a$     | $a$ | $e$ | $c$ | $b$ | $a$          |
| $b$     | $b$ | $c$ | $e$ | $a$ | $b$          |
| $c$     | $c$ | $b$ | $a$ | $e$ | $c$          |

Durch eine Überprüfung aller 27 Tripel aus  $V_4^3$  kann man leicht die Assoziativität der Gruppen-Operation „·“ nachrechnen. Die zweite Zeile und die zweite Spalte der Tafel zeigen, dass  $e$  das neutrale Element ist. Aus der Diagonale der Tafel folgt nochmals  $inv(x) = x$  für alle  $x \in \{e, a, b, c\}$ . Weil eine Spiegelung der Tafel an der Hauptdiagonale die Tafel in sich überführt, ist die Gruppe  $(V_4, e, \cdot, inv)$  sogar kommutativ. Sie wird nach dem deutschen Mathematiker Felix Klein (1849-1925) Kleinsche Vierergruppe genannt.  $\square$

Es fällt auf, dass im Vergleich zu Definition 8.1.2 in Definition 8.1.5 die Gleichung der Rechtsneutralität von  $e$  fehlt. Weiterhin hätte man zusätzlich zur Forderung  $inv(x) \cdot x = e$

für alle  $x \in G$ , welche in der üblichen Terminologie besagt, dass  $\text{inv}(x)$  ein **linksinverses Element** zu  $x$  ist, auch noch die Forderung  $x \cdot \text{inv}(x) = e$  für alle  $x \in G$  erwartet, welche besagt, dass  $\text{inv}(x)$  auch ein **rechtsinverses Element** zu  $x$  ist. Beides ist nicht notwendig, da es aus den Gruppen-Axiomen von Definition 8.1.5 bewiesen werden kann, wie das folgende Lemma zeigt.

### 8.1.7 Lemma

In jeder Gruppe  $(G, e, \cdot, \text{inv})$  gelten für alle  $x \in G$  die folgenden Formeln:

$$x \cdot x = x \Rightarrow x = e \quad x \cdot e = x \quad x \cdot \text{inv}(x) = e$$

**Beweis:** Zum Beweis der Implikation gelte die Voraussetzung  $x \cdot x = x$ . Dann folgt daraus

$$x = e \cdot x = \text{inv}(x) \cdot x \cdot x = \text{inv}(x) \cdot x = e$$

aufgrund der Linksneutralität von  $e$ , der Voraussetzung und der Forderung, dass  $\text{inv}(x)$  ein linksinverses Element zu  $x$  ist.

Nun beweisen wir zuerst die rechte Gleichung für ein beliebiges  $x \in G$ . Dazu starten wir mit der Rechnung

$$(x \cdot \text{inv}(x)) \cdot (x \cdot \text{inv}(x)) = x \cdot (\text{inv}(x) \cdot x) \cdot \text{inv}(x) = x \cdot e \cdot \text{inv}(x) = x \cdot \text{inv}(x),$$

wobei wir wieder nur die Linksneutralität von  $e$  und die Forderung verwenden, dass  $\text{inv}(x)$  ein linksinverses Element zu  $x$  ist. Aufgrund der anfangs bewiesenen Implikation erhalten wir  $x \cdot \text{inv}(x) = e$ .

Zum Beweis der linken Gleichung sei  $x \in G$  angenommen. Dann bekommen wir

$$x \cdot e = x \cdot \text{inv}(x) \cdot x = e \cdot x = x,$$

indem wir zuerst verwenden, dass  $\text{inv}(x)$  ein linksinverses Element zu  $x$  ist, dann die schon bewiesene rechte Gleichung und schließlich noch die Linksneutralität von  $e$ .  $\square$

Wir haben bei der Definition eines Monoids und einer Gruppe das (links)neutrale Element und die Funktion der Linksinversenbildung jeweils in den Typ mit aufgenommen. In der Regel werden Monoide und Gruppen in Mathematik-Lehrbüchern aber anders definiert, nämlich als algebraische Strukturen  $(M, \cdot)$  bzw.  $(G, \cdot)$  des Typs (2). Neben der Assoziativität der Gruppen-Operation „ $\cdot$ “ wird bei diesem Ansatz bei Monoiden die Existenz eines Elements  $e \in M$  mit der folgenden Eigenschaft gefordert:

$$\forall x \in M : e \cdot x = x \wedge x \cdot e = x$$

Bei Gruppen wird ebenfalls die Existenz eines Elements  $e \in G$  gefordert, nun aber mit der folgenden komplizierteren Eigenschaft:

$$(\forall x \in G : e \cdot x = x) \wedge (\forall x \in G : \exists y \in G : y \cdot x = e)$$

Der traditionellen Auffassung einer Gruppe als algebraische Struktur  $(G, \cdot)$  liegt unter anderem zugrunde, die geforderten Eigenschaften möglichst klein zu halten und auch, dass

man aus der Tafel von „·“ sowohl  $e$  als auch die Operation  $\text{inv}$  bekommen kann.

Offensichtlich gelten für Monoide und Gruppen nach unserer Definition die obigen Formeln. Bei den Gruppen der traditionellen Auffassung kann man umgekehrt zeigen, dass das im rechten Teil der Formel als existierend geforderte  $y$  eindeutig ist. Somit definiert bei der traditionellen Auffassung die Zuordnung von  $x$  zu dem einzigen Element  $y$  mit  $y \cdot x = e$  die Operation  $\text{inv}$  in unserem Sinne. Der Vorteil unseres Ansatzes ist, dass die Gruppen-Axiome als Gleichungen sehr einfach sind. Das erleichtert sowohl das Verstehen als auch das Rechnen. Weiterhin sind sehr allgemeine Resultate aus der sogenannten universellen Algebra anwendbar, die Aussagen über **gleichungsdefinierte algebraische Strukturen** machen. Bei diesen haben alle Axiome die Form  $A_1(x_1, \dots, x_n) = A_2(x_1, \dots, x_n)$  und es wird gefordert, dass sie für alle Elemente  $x_1, \dots, x_n$  der Trägermenge gelten. Gleichungsdefinierte algebraische Strukturen kommen oft in der Informatik zum Einsatz, insbesondere wenn man Datenstrukturen algebraisch spezifiziert. Wir können dieses Thema auch im letzten Abschnitt des Kapitels leider nicht sehr vertiefen.

Um einen kleinen Eindruck davon zu geben, wie man in der universellen Algebra argumentiert, zeigen wir nachfolgend, dass die Gruppen der traditionellen Auffassung nicht gleichungsdefinierbar sind. Weil uns die Mittel aus der formalen mathematischen Logik fehlen, können wir den Beweis leider nicht in der Formalität angeben, wie es mit diesen Mitteln möglich wäre.

### 8.1.8 Satz: Gruppen der traditionellen Auffassung nicht gleichungsdefinierbar

Es gibt keine Menge  $\mathcal{G}$  von Gleichungen der Art

$$A_1(x_1, \dots, x_n) = A_2(x_1, \dots, x_n),$$

wobei die Ausdrücke  $A_1(x_1, \dots, x_n)$  und  $A_2(x_1, \dots, x_n)$  der Gleichungen nur aufgebaut sind unter Verwendung von Variablen und einem 2-stelligen Operationssymbol „·“ in Infix-Schreibweise, so dass für alle algebraischen Strukturen  $(G, \cdot)$  des Typs (2) die folgenden zwei Eigenschaften äquivalent sind:

- (1) Es ist  $(G, \cdot)$  eine Gruppe der traditionellen Auffassung.
- (2) Für alle Gleichungen  $A_1(x_1, \dots, x_n) = A_2(x_1, \dots, x_n)$  aus  $\mathcal{G}$  und alle  $a_1, \dots, a_n \in G$  gilt  $A_1(a_1, \dots, a_n) = A_2(a_1, \dots, a_n)$ .

**Beweis (durch Widerspruch):** Angenommen, es gäbe eine Menge  $\mathcal{G}$  mit den geforderten Eigenschaften. Weil  $(\mathbb{Q} \setminus \{0\}, \cdot)$  eine Gruppe der traditionellen Auffassung ist, gilt, wegen der angenommen Äquivalenz von (1) und (2) (wir folgern von (1) auf (2)) die Formel

$$\forall a_1, \dots, a_n \in \mathbb{Q} \setminus \{0\} : A_1(a_1, \dots, a_n) = A_2(a_1, \dots, a_n)$$

für alle Gleichungen  $A_1(x_1, \dots, x_n) = A_2(x_1, \dots, x_n)$  aus  $\mathcal{G}$ . Daraus folgt, dass auch die Formel

$$\forall a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\} : A_1(a_1, \dots, a_n) = A_2(a_1, \dots, a_n)$$

für alle Gleichungen  $A_1(x_1, \dots, x_n) = A_2(x_1, \dots, x_n)$  aus  $\mathcal{G}$  gilt. Nun wenden wir wieder die Äquivalenz von (1) und (2) an, folgern nun aber von (2) nach (1). Also bekommen wir,

dass  $(\mathbb{Z} \setminus \{0\}, \cdot)$  eine Gruppe der traditionellen Auffassung ist. Das ist aber offensichtlich falsch. Somit ist der Widerspruchsbeweis beendet.  $\square$

Man kann also bei einer traditionellen Auffassung der Gruppen als algebraische Strukturen  $(G, \cdot)$  des Typs (2) die Forderung nach der Existenz des Elements  $e$  mit der obigen Eigenschaft nicht durch eine Menge von Gleichungen ausdrücken.

Nach dieser kleinen Abschweifung kehren wir wieder zu den Gruppen  $(G, e, \cdot, \text{inv})$  in unserem Sinne zurück. Nachfolgend zeigen wir, dass bei Gruppen die linksneutralen und die linksinversen Elemente eindeutig bestimmt sind und mit dem Element  $e$  bzw. den Resultaten von  $\text{inv}$  zusammenfallen.

### 8.1.9 Satz: Eindeutigkeit neutraler und inverser Elemente

In jeder Gruppe  $(G, e, \cdot, \text{inv})$  gelten für alle  $x, y \in G$  die folgenden Formeln:

$$(\forall z \in G : x \cdot z = z) \Rightarrow x = e \quad x \cdot y = e \Rightarrow x = \text{inv}(y)$$

**Beweis:** Die Gültigkeit der linken Implikation folgt aus der folgenden logischen Implikation. Deren erster Schritt besteht aus einer Spezialisierung und der zweite Schritt verwendet die oben bewiesene Rechtsneutralität von  $e$ .

$$\forall z \in G : x \cdot z = z \implies x \cdot e = e \iff x = e$$

Zum Beweis der rechten Implikation gelte ihre Voraussetzung  $x \cdot y = e$ . Dann folgt

$$x = x \cdot e = x \cdot y \cdot \text{inv}(y) = e \cdot \text{inv}(y) = \text{inv}(y),$$

wobei  $x \cdot y = e$  im dritten Schritt der Rechnung Verwendung findet. Daneben werden noch die Neutralität von  $e$  im ersten und vierten Schritt benutzt und in Schritt 2, dass  $\text{inv}(y)$  rechtsinvers zu  $y$  ist.  $\square$

Nach Lemma 8.1.7 ist das links neutrale Element  $e$  auch rechtsneutral und jedes linksinversible Element  $\text{inv}(x)$  von  $x$  ist auch rechtsinvers bezüglich  $x$ . Somit gibt es als unmittelbare Konsequenz dieses Satzes und des Lemmas in Gruppen insgesamt nur ein neutrales Element  $e$  mit  $x \cdot e = e \cdot x = x$  für alle  $x$  und zu jedem Element  $x$  gibt es genau ein inverses Element  $\text{inv}(x)$  mit  $\text{inv}(x) \cdot x = x \cdot \text{inv}(x) = e$ .

Die Komposition  $f \circ g$  von bijektiven Funktionen  $f$  und  $g$  ist wiederum bijektiv und die Umkehrfunktion der Komposition ergibt sich durch  $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ . Weiterhin gilt bei bijektiven Funktionen auch  $(f^{-1})^{-1} = f$ . Schließlich ist die identische Funktion ihre eigene Umkehrfunktion. Der folgende Satz zeigt, dass diese drei Resultate nicht nur für die speziellen Gruppen  $(\mathcal{S}(M), \text{id}_M, \circ)$  gelten, sondern für alle Gruppen.

### 8.1.10 Satz: Rechenregeln

In jeder Gruppe  $(G, e, \cdot, \text{inv})$  gelten für alle  $x, y \in G$  die folgenden Gleichungen:

$$\text{inv}(x \cdot y) = \text{inv}(y) \cdot \text{inv}(x) \quad \text{inv}(\text{inv}(x)) = x \quad \text{inv}(e) = e$$

**Beweis:** Wir starten mit der folgenden Rechnung:

$$(\text{inv}(y) \cdot \text{inv}(x)) \cdot (x \cdot y) = \text{inv}(y) \cdot (\text{inv}(x) \cdot x) \cdot y = \text{inv}(y) \cdot e \cdot y = \text{inv}(y) \cdot y = e$$

Damit ist  $\text{inv}(y) \cdot \text{inv}(x)$  linksinvers zu  $x \cdot y$ . Die Eindeutigkeit der linksinversen Elemente zeigt nun die erste Gleichung. Auf eine sehr ähnliche Weise kann man auch die restlichen zwei Gleichungen zeigen.  $\square$

Bevor wir zur dritten algebraischen Struktur unserer Hierarchie kommen, wollen wir einige gängige Schreib- und Sprechweisen einführen, die in der Literatur üblich sind und nachfolgend auch von uns verwendet werden.

### 8.1.11 Schreib- und Sprechweisen

Wird die 2-stellige Operation einer Gruppe, wie auch bei uns in Definition 8.1.5, mit dem Multiplikationssymbol „ $\cdot$ “ bezeichnet, so schreibt man abkürzend  $xy$  statt  $x \cdot y$ . Auch bezeichnet man dann das neutrale Element mit 1 und das zu  $x$  inverse Element mit  $x^{-1}$ . Die dadurch entstehende algebraische Struktur  $(G, 1, \cdot, -1)$  nennt man **multiplikative Gruppe** mit Einselement 1. Bei kommutativen Gruppen verwendet man hingegen das Additionssymbol „ $+$ “ für die 2-stellige Operation, das Symbol 0 für das neutrale Element, oft Nullelement genannt, und  $-x$  als Schreibweise für das zu  $x$  inverse Element. Das führt zu  $(G, 0, +, -)$  als **additive Gruppe**. Bei einer solchen Schreibweise notiert man auch die Potenzierung anders, nämlich als  $xn$ . Damit werden die Gleichungen von Satz 8.1.4 zu  $x(m + n) = xm + xn$ ,  $x(mn) = (xm)n$  und  $(x + y)m = xm + ym$ .  $\square$

Man beachte, dass in der eben gebrachten Gleichung  $x(m + n) = xm + xn$  das linke Additionssymbol die Addition auf der Menge  $\mathbb{N}$  bezeichnet und das rechte Additionssymbol die 2-stellige Gruppenoperation von  $(G, 0, +, -)$  ist. Solche Überladungen von Symbolen sind in der Mathematik leider sehr häufig und für einen Anfänger manchmal nur schwer zu verstehen.

Ringe entstehen aus additiven Gruppen. Die Trägermenge wird dabei nicht verändert. Es wird jedoch zusätzlich noch durch eine weitere Konstante und eine weitere 2-stellige Operation eine Monoid-Struktur auf ihr definiert. Die Verbindung zwischen den beiden algebraischen Strukturen geschieht durch die Distributivgesetze, wie wir sie von den Zahlen, Mengen und der Logik her schon kennen.

### 8.1.12 Definition: Ring

Ein **Ring** ist eine algebraische Struktur  $(R, 0, 1, +, \cdot, -)$  des Typs  $(0, 0, 2, 2, 1)$  mit den folgenden Eigenschaften:

- (1) Es ist  $(R, 0, +, -)$  eine kommutative Gruppe.
- (2) Es ist  $(R, 1, \cdot)$  ein Monoid.
- (3) Für alle  $x, y, z \in R$  gelten die Distributivgesetze  $x(y + z) = xy + xz$  und  $(y + z)x = yx + zx$ .

Ist  $(R, 1, \cdot)$  ein kommutatives Monoid, so nennt man  $(R, 0, 1, +, \cdot, -)$  einen **kommutativen Ring**.  $\square$

Die durch die Punkte (1) und (2) geforderten Axiome sind Gleichungen. Somit sind Ringe ebenfalls gleichungsdefinierte algebraische Strukturen. Wir haben im Ring-Axiom (3) schon die abkürzende Schreibweise der multiplikativen Gruppen verwendet und auch die von der Schule bekannte Vorrangregel „Punkt vor Strich“ um Klammern zu sparen. In der Literatur werden Ringe sehr oft auch in einer schwächeren Form als bei uns eingeführt, nämlich als Tupel  $(R, 0, +, \cdot, -)$ , bei denen statt (2) nur die Assoziativität der Operation „ $\cdot$ “ gefordert wird. Die Ringe von Definition 8.1.12 nennt man bei diesem Ansatz Ringe mit Einselement. Wie bei den Gruppen gibt es auch bei Ringen die traditionelle Auffassung, in der nur das Tupel  $(R, +, \cdot)$  betrachtet wird und die Axiome komplizierter sind. Die Ringe der traditionellen Auffassung sind wiederum nicht gleichungsdefinierbar.

Wenn wir mit  $G$  die Menge der geraden ganzen Zahlen bezeichnen, so bildet das Tupel  $(G, 0, +, -)$  eine kommutative Gruppe und die Multiplikation ist auf der Menge  $G$  assoziativ. Trotzdem bekommen wir keinen Ring, da ein Einselement fehlt. In der oben erwähnten schwächeren Form als Tupel ohne ein Einselement ist  $(G, 0, +, \cdot, -)$  hingegen ein Ring.

Beispiele für zahlartige Ringe sind  $(\mathbb{Z}, 0, 1, +, \cdot, -)$ ,  $(\mathbb{Q}, 0, 1, +, \cdot, -)$  und  $(\mathbb{R}, 0, 1, +, \cdot, -)$ . Hier ist ein weiteres Beispiel, welches nichts mit Zahlen zu tun hat.

### 8.1.13 Beispiel: Mengenring

Ist  $M$  eine Menge, so ist  $(\mathcal{P}(M), \emptyset, \cap)$  ein kommutatives Monoid. Man kann auf die Potenzmenge  $\mathcal{P}(M)$  sogar die Struktur einer kommutativen Gruppe aufprägen, indem man  $M$  als das neutrale Element wählt, die 2-stellige Operation definiert durch

$$\oplus : \mathcal{P}(M)^2 \rightarrow \mathcal{P}(M) \quad X \oplus Y = (X \setminus Y) \cup (Y \setminus X)$$

(genannt **symmetrische Differenz**) und als Inversenbildung die Komplementoperation  $X \mapsto \overline{X}$  nimmt. Es erfordert etwas Aufwand, zu zeigen, dass das Distributivgesetz

$$X \cap (Y \oplus Z) = (X \cap Y) \oplus (X \cap Z)$$

(eines genügt ja) für alle Mengen  $X, Y, Z \in \mathcal{P}(M)$  gilt. Insgesamt erhält man damit den kommutativen Ring  $(\mathcal{P}(M), \emptyset, M, \oplus, \cap, \overline{\phantom{x}})$ .  $\square$

Bezüglich der additiven Teilstruktur eines Ringes gelten alle aus den Axiomen einer kommutativen Gruppe herleitbaren Aussagen. Der folgende Satz zeigt einige weitere grundlegende Rechenregeln für Ringe auf.

### 8.1.14 Satz: Rechenregeln

In einem Ring  $(R, 0, 1, +, \cdot, -)$  gelten für alle  $x, y \in R$  die folgenden Gleichungen:

$$0x = x0 = 0 \quad (-x)y = -(xy) = x(-y) \quad (-x)(-y) = xy$$

**Beweis:** Zum Beweis des linken Teils der ersten Gleichungen rechnen wir unter Verwendung eines Distributivgesetzes wie folgt:

$$0x = (0 + 0)x = 0x + 0x$$

Die Implikation von Lemma 8.1.7 zeigt, dass  $0x$  das neutrale Element der additiven Gruppe  $(R, 0, +, -)$  ist, was  $0x = 0$  heißt. Analog zeigt man den rechten Teil.

Wir zeigen wiederum nur den linken Teil der zweiten Gleichungen. Wegen der Eindeutigkeit der inversen Elemente genügt es,  $(-x)y$  als linksinverses Element von  $xy$  in der additiven Gruppe  $(R, 0, +, -)$  nachzuweisen. Hier ist die entsprechende Rechnung, wobei wir wieder ein Distributivgesetz verwenden:

$$(-x)y + xy = ((-x) + x)y = 0y = 0$$

Die dritte Gleichung bekommt man durch

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$$

unter Verwendung der zweiten Gleichungen und von Satz 8.1.10 für die additive Gruppe  $(R, 0, +, -)$  im letzten Schritt.  $\square$

Alle einelementigen Mengen  $\{a\}$  führen in einer offensichtlichen Weise zu einer kommutativen Gruppe  $(\{a\}, a, +, -)$  und daraus bekommt man auch sofort einen kommutativen Ring  $(\{a\}, a, a, +, +, -)$ . Diese Gruppen und Ringe werden **trivial** genannt. Aus den linken Gleichungen von Satz 8.1.14 erhält man unmittelbar, dass in allen nicht trivialen Ringen  $(R, 0, 1, +, \cdot, -)$  die Eigenschaft  $0 \neq 1$  gilt.

In Ringen  $(R, 0, 1, +, \cdot, -)$  kann man auch **subtrahieren**, wenn man  $x - y$  als Abkürzung für  $x + (-y)$  definiert. Es gelten dann alle von den ganzen Zahlen her bekannten Gesetze, etwa  $x(y - z) = xy - xz$ . Weiterhin kann man in offensichtlicher Weise die 2-stellige Addition zur Addition  $\sum_{i=1}^n x_i$  der Ringelemente  $x_1, \dots, x_n$  erweitern, indem man definiert  $\sum_{i=1}^0 x_i = 0$  und  $\sum_{i=1}^{n+1} x_i = x_{n+1} + \sum_{i=1}^n x_i$ . Dann verallgemeinern sich die Distributivgesetze (3) von Definition 8.1.12 zu  $x \sum_{i=1}^n y_i = \sum_{i=1}^n xy_i$  und  $(\sum_{i=1}^n y_i)x = \sum_{i=1}^n y_i x$ .

In allen Mengenringen  $(\mathcal{P}(M), \emptyset, M, \oplus, \cap, \neg)$  gilt  $X \cap X = X$  für alle  $X \in \mathcal{P}(M)$ . Ringe  $(R, 0, 1, +, \cdot, -)$ , in denen die Gleichung  $xx = x$  für alle  $x \in R$  gilt, nennt man Boolesche Ringe. Sie stellen ein algebraisches Modell der Aussagenlogik mit den drei Junktoren  $\vee$ ,  $\wedge$  und  $\neg$  dar, indem man 1 als Aussage **wahr** und 0 als Aussage **falsch** interpretiert, die drei logischen Junktoren mittels der drei neuen Ring-Operationen

$$x \vee y := x + y - xy \quad x \wedge y := xy \quad \neg x := 1 - x$$

modelliert und die logische Äquivalenz von aussagenlogischen Formeln als Gleichheit von Ringelementen interpretiert. Mit diesen Entsprechungen kann man alle logischen Äquivalenzen der Aussagenlogik mit Formeln über den drei genannten Junktoren beweisen<sup>11</sup>.

---

<sup>11</sup>Will man die gesamte Aussagenlogik behandeln, so muss man die restlichen Junktoren  $\Rightarrow$  und  $\Leftrightarrow$  mittels der Junktoren  $\vee$ ,  $\wedge$  und  $\neg$  ausdrücken.

Beispielsweise entspricht die logische Äquivalenz  $A \iff \neg\neg A$  der Gleichheit  $x = \neg\neg x$  in  $R$  und diese folgt aus

$$\neg\neg x = 1 - (1 - x) = 1 - 1 + x = x.$$

Wir geben noch ein weiteres Beispiel an. Die der logischen Äquivalenz  $\neg(A \vee B) \iff \neg A \wedge \neg B$  entsprechende Gleichheit in  $R$  ist  $\neg(x \vee y) = \neg x \wedge \neg y$  und diese zeigt man durch

$$\neg(x \vee y) = 1 - (x + y - xy) = 1 - x - y + xy = (1 - x)(1 - y) = \neg x \wedge \neg y.$$

Die schwierigste Aufgabe bei dieser Modellierung der Aussagenlogik ist der Beweis der Kommutativität der Disjunktion. Nachfolgend zeigen wir das entsprechende Resultat. Man beachte, wie wichtig bei den einzelnen Aussagen die Quantifizierung der entsprechenden Variablen ist.

### 8.1.15 Satz: Boolesche Ringe sind kommutativ

Gilt in einem Ring  $(R, 0, 1, +, \cdot, -)$  für alle  $x \in R$  die Gleichung  $xx = x$ , so ist der Ring kommutativ.

**Beweis:** Wegen der Voraussetzung erhalten wir

$$x + y = (x + y)(x + y) = xx + xy + yx + yy = x + xy + yx + y$$

für alle Elemente  $x, y \in R$ . Diese Eigenschaft bringt durch Subtraktion von  $x + y$  auf beiden Seiten, dass  $0 = xy + yx$  für alle Elemente  $x, y \in R$  gilt. Da die eben bewiesene Gleichung für alle Ringelemente gilt, können wir insbesondere für  $x$  und  $y$  das gleiche Element wählen und erhalten, dass  $0 = zz + zz$ , also, wegen der Voraussetzung,  $0 = z + z$  für alle Elemente  $z \in R$  gilt.

Nach diesen Vorbereitungen beweisen wir nun die Kommutativität. Dazu seien  $x, y \in R$  beliebig vorgegeben. Wegen der letzten vorbereitenden Gleichung bekommen wir  $0 = xy + xy$ , indem wir  $xy$  für  $z$  nehmen. Auf Grund der vorletzten vorbereitenden Gleichung wissen wir aber auch, dass  $0 = xy + yx$  gilt. Also haben wir insgesamt  $xy + xy = xy + yx$ , woraus durch Subtraktion von  $xy$  auf beiden Seiten  $xy = yx$  folgt.  $\square$

Wir wollen das Thema Ringe an dieser Stelle noch nicht vertiefen, sondern wenden uns nun der letzten algebraischen Struktur unserer Hierarchie zu.

### 8.1.16 Definition: Körper

Ein Ring  $(K, 0, 1, +, \cdot, -)$  heißt ein **Körper**, wenn er kommutativ ist,  $0 \neq 1$  gilt und die Formel

$$x \neq 0 \Rightarrow \exists y \in K : yx = 1$$

für alle  $x \in K$  gilt.  $\square$

Im Vergleich zu den bisherigen Definitionen von Monoiden, Gruppen und Ringen fällt bei dieser Definition ein Stilbruch auf. Zuerst haben wir eine Ungleichung als Axiom gefordert. Weiterhin haben wir ein noch komplizierteres Axiom eingeführt, nämlich eine Implikation mit einer Ungleichung als linker und einer Existenzquantifizierung als rechter

Seite. Schließlich haben wir auch noch, im Gegensatz zu den Gruppen, im zweiten Axiom das linksinverse Element  $y$  zu  $x$  bezüglich der Multiplikation nicht durch eine Operation spezifiziert, sondern durch eine Existenzquantifizierung. Körper sind somit algebraische Strukturen, die nicht gleichungsdefiniert sind. Damit sind die oben erwähnten Resultate der universellen Algebra nicht anwendbar.

Nach dem folgenden Satz gibt es zu  $x \neq 0$  nur ein linksinverses Element und aufgrund der Kommutativität von „.“ ist dieses auch rechtsinvers.

### 8.1.17 Satz: Eindeutigkeit der linksinversen Elemente

Es seien  $(K, 0, 1, +, \cdot, -)$  ein Körper und  $x \in K$  mit  $x \neq 0$ . Dann gilt für alle  $y_1, y_2 \in K$  mit  $y_1x = 1$  und  $y_2x = 1$ , dass  $y_1 = y_2$ .

**Beweis:** Wir bekommen das Resultat durch

$$y_1 = y_1 1 = y_1 y_2 x = y_2 y_1 x = y_2 1 = y_2,$$

wobei wir im zweiten und im vierten Schritt die Annahmen  $y_2x = 1$  und  $y_1x = 1$  verwenden und im dritten Schritt die Kommutativität von „.“.  $\square$

Wenn man also mit  $x^{-1}$  das zu  $x \neq 0$  eindeutig existierende linksinverse Element bezüglich „.“ bezeichnet, diese Operation (unter Beibehaltung des Symbols) auf die (wegen  $0 \neq 1$  nichtleere) Menge  $K \setminus \{0\}$  einschränkt, so erhält man eine kommutative multiplikative Gruppe  $(K \setminus \{0\}, 1, \cdot, -1)$ . Für diese gelten alle bewiesenen Gruppeneigenschaften. Jedoch kann man die Operation  $-1 : K \setminus \{0\} \rightarrow K \setminus \{0\}$  nicht in das Tupel  $(K, 0, 1, +, \cdot, -)$  mit aufnehmen, da, laut Definition 8.1.1, bei algebraischen Strukturen nur Operationen zugelassen sind, die die Trägermenge oder eine Potenz von ihr als Quelle und die Trägermenge als Ziel besitzen.

Von den oben aufgeführten zahlartigen Ringen ist  $(\mathbb{Z}, 0, 1, +, \cdot, -)$  kein Körper. Hingegen ist sowohl der Ring  $(\mathbb{Q}, 0, 1, +, \cdot, -)$  als auch der Ring  $(\mathbb{R}, 0, 1, +, \cdot, -)$  ein Körper. In beiden Fällen ist das zu einem Element  $x \neq 0$  existierende inverse Element durch  $x^{-1} := \frac{1}{x}$  gegeben. Als Verallgemeinerung hiervon bekommt man  $\frac{x}{y} := xy^{-1}$  als Definition der **Division** in Körpern, wobei, wie bei den Zahlen,  $y \neq 0$  vorausgesetzt ist. Es sollte an dieser Stelle auch noch angemerkt werden, dass, wie im Fall der Ringe, in vielen Lehrbüchern auch Körper als Tupel  $(K, +, \cdot)$  eingeführt werden, mit einer entsprechenden Abänderung unserer Axiome.

Ein Vorteil der algebraischen Strukturen ist der Leserin oder dem Leser sicher schon jetzt aufgefallen: Durch sie werden die grundlegendsten Eigenschaften von Operationen zu Axiomen erhoben und daraus entsprechende weitere Eigenschaften hergeleitet. Aufgrund dieser Abstraktion kann man sehr viele Beweise sparen, die bei konkreten Mengen und konkreten Operationen immer wieder gleich ablaufen würden. Man hat nur zu zeigen, dass die Axiome der algebraischen Struktur erfüllt sind, die man für die konkrete Problemstellung als angemessen ansieht. Dann kann man alles verwenden, was jemals über diese gezeigt wurde. Weil beispielsweise die ganzen Zahlen eine Gruppe bilden, kann man für sie alles verwenden, was jemals über Gruppen bewiesen wurde.

## 8.2 Strukterhaltende Funktionen

Algebraische Strukturen dienen in der Mathematik und der Informatik häufig auch dazu, gewisse Beziehungen zwischen Mengen und gewissen dazugehörigen Funktionen herzustellen. Eine erste Frage, die sich immer wieder stellt, ist die, festzustellen, ob zwei Strukturen eigentlich gleich sind, obwohl sie aufgrund ihrer Definitionen bzw. den textuellen Aufschreibungen verschieden aussehen. Der entscheidende Begriff hier ist die Verträglichkeit von Funktionen mit Paaren von Funktionen. Nachfolgend wollen wir dies anhand eines Beispiels motivieren.

### 8.2.1 Beispiel: Motivation von Verträglichkeit

Wir betrachten nachfolgend links noch einmal die Verknüpfungstafel der Kleinschen Vierergruppe, wie sie in Beispiel 8.1.6 eingeführt wird. Rechts daneben ist diese Verknüpfungstafel noch einmal angegeben. Im Vergleich zur linken Tafel sind jedoch die Elemente  $e, a, b$  und  $c$  in  $0, 1, 2$  und  $3$  umbenannt und es wird statt der multiplikativen die additive Schreibweise für Gruppen verwendet.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $+$ | $0$ | $1$ | $2$ | $3$ |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $e$     | $e$ | $a$ | $b$ | $c$ | $0$ | $0$ | $1$ | $2$ | $3$ |
| $a$     | $a$ | $e$ | $c$ | $b$ | $1$ | $1$ | $0$ | $3$ | $2$ |
| $b$     | $b$ | $c$ | $e$ | $a$ | $2$ | $2$ | $3$ | $0$ | $1$ |
| $c$     | $c$ | $b$ | $a$ | $e$ | $3$ | $3$ | $2$ | $1$ | $0$ |

Es sei  $(G, 0, +, -)$  die durch die rechte Verknüpfungstafel beschriebene Gruppe. Dann ist sie zwar formal verschieden von der Kleinschen Vierergruppe  $(V_4, e, \cdot, \text{inv})$ , denn schon die Trägermengen sind verschieden, aber eigentlich kann man sie doch als gleich zu ihr auffassen. Es werden ja nur Objekte umbenannt.

Die Umbenennung der Elemente der Trägermengen kann man durch eine bijektive Funktion  $\Phi : V_4 \rightarrow G$  beschreiben, die wie folgt abbildet:

$$\Phi(e) = 0 \quad \Phi(a) = 1 \quad \Phi(b) = 2 \quad \Phi(c) = 3$$

Dass sich die Einträge der zwei Tafeln genau entsprechen, kann man wie folgt beschreiben: Für alle  $x, y, z \in V_4$  ist  $z$  das Resultat der Operation „ $\cdot$ “ mit den Argumenten  $x$  und  $y$  genau dann, wenn  $\Phi(z)$  das Resultat der korrespondierenden Operation  $+$  mit den Argumenten  $\Phi(x)$  und  $\Phi(y)$  ist. Formalisiert sieht dies wie folgt aus:

$$\forall x, y, z \in V_4 : z = x \cdot y \Leftrightarrow \Phi(z) = \Phi(x) + \Phi(y)$$

Es ist eine relativ einfache Übung zu zeigen, dass diese Formel logisch äquivalent ist zu der nachfolgend angegebenen:

$$\forall x, y \in V_4 : \Phi(x \cdot y) = \Phi(x) + \Phi(y)$$

Dass sich die Einträge der Verknüpfungstafeln genau entsprechen, kann man also auch wie folgt beschreiben: Es ist egal, ob man zuerst in der ersten Gruppe zwei Elemente verknüpft und dann das Resultat in die zweite Gruppe abbildet, oder man zuerst beide Elemente in

die zweite Gruppe abbildet und dann deren Resultate dort verknüpft.  $\square$

Die eben durch zwei Gruppen motivierte Eigenschaft zur Beschreibung der genauen Entsprechung der Einträge in Verknüpfungstafeln von Operationen von algebraischen Strukturen kann man wie folgt verallgemeinern.

### 8.2.2 Definition: verträgliche Funktionen

Eine Funktion  $\Phi : M \rightarrow N$  heißt mit den Funktionen  $f : M^k \rightarrow M$  und  $g : N^k \rightarrow N$  gleicher Stelligkeit **verträglich**, falls die Gleichung  $\Phi(f(x_1, \dots, x_k)) = g(\Phi(x_1), \dots, \Phi(x_k))$  für alle  $x_1, \dots, x_k \in M$  gilt.  $\square$

Damit sind wir nun in der Lage, formal festlegen zu können, wann man zwei algebraische Strukturen gleichen Typs (diese Voraussetzung ist offensichtlich) als gleich auffassen kann, obwohl sie eventuell völlig verschieden definiert oder textuell aufgeschrieben sind. Zur Verträglichkeit der abbildenden Funktion mit allen Paaren von korrespondierenden Operationen kommt nur noch hinzu, dass auch die korrespondierenden Konstanten entsprechend in Verbindung gesetzt werden.

### 8.2.3 Definition: Strukturisomorphismus

Es seien  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und  $(N, d_1, \dots, d_m, g_1, \dots, g_n)$  algebraische Strukturen des gleichen Typs. Eine Funktion  $\Phi : M \rightarrow N$  heißt ein **Strukturisomorphismus**, falls die folgenden Eigenschaften gelten:

- (1)  $\Phi$  ist bijektiv.
- (2) Für alle  $i \in \{1, \dots, m\}$  gilt  $\Phi(c_i) = d_i$ .
- (3) Für alle  $i \in \{1, \dots, n\}$  ist  $\Phi$  mit  $f_i$  und  $g_i$  verträglich.

Existiert ein Strukturisomorphismus zwischen algebraischen Strukturen, so nennt man diese **isomorph** oder **strukturgleich**.  $\square$

Neben der Strukturisomorphie gibt es noch einige Variationen dieses Begriffs, wobei aber fast immer nur die Forderung (1) verändert wird. Nachfolgend sind die drei wichtigsten Variationen angegeben.

### 8.2.4 Definition: Strukturhomomorphismus

Wird in Definition 8.2.3 auf die Forderung (1) verzichtet, so nennt man  $\Phi$  einen **Strukturhomomorphismus**. Wird sie ersetzt durch „ $\Phi$  ist injektiv“ (bzw. „ $\Phi$  ist surjektiv“), so heißt  $\Phi$  ein **Strukturmonomorphismus** (bzw. ein **Strukturepimorphismus**).  $\square$

Alle diese speziellen Funktionen nennt man zusammenfassend auch **Strukturmorphismen** oder **strukturerhaltend**. Im Rest dieses Abschnitts spezialisieren wir diese nun wieder auf die algebraischen Strukturen der Hierarchie des letzten Abschnitts. Wir führen dies nur für Gruppen und Ringe durch und beschränken uns dabei zusätzlich noch auf die Homomorphismen und die Isomorphismen. Der Leserin oder dem Leser ist sicher aufgefallen, dass Strukturmorphismen sich nur auf den Typ von algebraischen Strukturen beziehen,

nicht aber auf die für sie geforderten Axiome. Damit brauchen wir Körpermorphismen, wie wir sehen werden, nicht eigens zu behandeln. Auf die Betrachtung von Monoidmorphismen verzichten wir, da sie für den weiteren Text unwesentlich sind.

In der Literatur werden Gruppen- und Ringmorphismen in der Regel nicht so definiert, wie es die Definitionen 8.2.3 und 8.2.4 eigentlich nahelegen. Dies liegt an der speziellen Form der Axiome dieser beiden algebraischen Strukturen. Mit ihrer Hilfe kann man nämlich einige der allgemeinen Forderungen für Strukturmorphismen aus anderen beweisen. Der Vorteil der üblichen Definitionen ist, dass beim Nachweis der Strukturhomomorphe-  
schaft weniger zu zeigen ist. Wir haben wiederum den Ansatz der strukturerhaltenden Funktionen bei beliebigen algebraischen Strukturen als Ausgangspunkt gewählt, damit es der Leserin oder dem Leser später leichter fällt, sich in die Strukturerhaltung von noch allgemeineren Strukturen (wie beispielsweise denen, die im letzten Abschnitt des Kapitels erwähnt werden) einzuarbeiten.

Weil nachfolgend mehrere Gruppen im Zusammenhang betrachtet werden, verwenden wir wieder die ursprüngliche Notation  $(G, e, \cdot, \text{inv})$ . Sie erlaubt es nämlich in einfacher Weise, die Gruppen durch Indizes zu unterscheiden. Hier ist die übliche Definition der Gruppenhomomorphismen und -isomorphismen.

### 8.2.5 Definition: Gruppenhomomorphismus

Es seien  $(G_1, e_1, \cdot_1, \text{inv}_1)$  und  $(G_2, e_2, \cdot_2, \text{inv}_2)$  Gruppen. Eine Funktion  $\Phi : G_1 \rightarrow G_2$  heißt ein **Gruppenhomomorphismus**, falls sie mit „ $\cdot_1$ “ und „ $\cdot_2$ “ verträglich ist. Ein **Gruppenisomorphismus** ist ein bijektiver Gruppenhomomorphismus.  $\square$

Gruppen nennt man wiederum isomorph, wenn es einen Gruppenisomorphismus zwischen ihnen gibt. Aufgrund von Eigenschaft (3) des folgenden Satzes ist dabei die Richtung der Funktion belanglos.

### 8.2.6 Satz: Eigenschaften von Gruppenhomomorphismen

- (1) Die Komposition von Gruppenhomomorphismen ist ein Gruppenhomomorphismus.
- (2) Die Komposition von Gruppenisomorphismen ist ein Gruppenisomorphismus.
- (3) Die Umkehrfunktion eines Gruppenisomorphismus ist ein Gruppenisomorphismus.

**Beweis:** (1) Es seien  $\Phi : G_1 \rightarrow G_2$  und  $\Psi : G_2 \rightarrow G_3$  zwei Gruppenhomomorphismen und „ $\cdot_1$ “, „ $\cdot_2$ “ und „ $\cdot_3$ “ die 2-stelligen Operationen. Weiterhin seien  $x, y \in G_1$ . Dann folgt der Beweis aus der Rechnung

$$\Psi(\Phi(x \cdot_1 y)) = \Psi(\Phi(x) \cdot_2 \Phi(y)) = \Psi(\Phi(x)) \cdot_3 \Psi(\Phi(y)),$$

in der die Gruppenhomomorphe-eigenschaft für  $\Phi$  und  $\Psi$  verwendet wird, und der Definition der Funktionskomposition.

- (2) Dies folgt aus (1) und der Tatsache, dass die Komposition von bijektiven Funktionen bijektiv ist.

(3) Es seien  $\Phi : G_1 \rightarrow G_2$  ein Gruppenisomorphismus und „ $\cdot_1$ “ und „ $\cdot_2$ “ die 2-stelligen Operationen. Es ist nur die Homomorphismuseigenschaft von  $\Phi^{-1}$  zu verifizieren. Dazu seien  $x, y \in G_2$  beliebig vorgegeben. Aufgrund der Surjektivität von  $\Phi$  gibt es dann  $a, b \in G_1$  mit  $\Phi(a) = x$  und  $\Phi(b) = y$ . Dies bringt

$$\Phi^{-1}(x \cdot_2 y) = \Phi^{-1}(\Phi(a) \cdot_2 \Phi(b)) = \Phi^{-1}(\Phi(a \cdot_1 b)) = a \cdot_1 b = \Phi^{-1}(x) \cdot_1 \Phi^{-1}(y),$$

weil  $\Phi(a) = x$  impliziert  $\Phi^{-1}(x) = a$  und  $\Phi(b) = y$  impliziert  $\Phi^{-1}(y) = b$  und  $\Phi$  ein Gruppenhomomorphismus ist.  $\square$

Im einleitenden Beispiel dieses Abschnitts haben wir schon einen konkreten Gruppenhomomorphismus angegeben, der sogar ein Gruppenisomorphismus ist. Nachfolgend geben wir nun einige weitere Beispiele für Gruppenhomomorphismen und -isomorphismen an.

### 8.2.7 Beispiele: Gruppenhomomorphismen und -isomorphismen

Zu jedem Paar  $(G_1, e_1, \cdot_1, \text{inv}_1)$  und  $(G_2, e_2, \cdot_2, \text{inv}_2)$  von Gruppen ist die konstantwertige Funktion  $\Phi : G_1 \rightarrow G_2$  mit  $\Phi(x) = e_2$  ein Gruppenhomomorphismus. Eine konstantwertige Funktion  $\Psi : G_1 \rightarrow G_2$  mit  $\Psi(x) = c$  und  $c \neq e_2$  kann kein Gruppenhomomorphismus sein. Dies ist eine unmittelbare Konsequenz des nächsten Satzes 8.2.8, wo wir zeigen, dass ein Gruppenhomomorphismus ein Strukturhomomorphismus ist.

Für alle Gruppen  $(G, e, \cdot, \text{inv})$  ist die identische Funktion  $\text{id}_G : G \rightarrow G$  ein Gruppenisomorphismus von  $(G, e, \cdot, \text{inv})$  nach  $(G, e, \cdot, \text{inv})$ .

Die Funktion  $f : \mathbb{Z} \rightarrow \mathbb{Q}$  mit  $f(x) = -x$  ist ein Gruppenhomomorphismus von  $(\mathbb{Z}, 0, +, -)$  nach  $(\mathbb{Q}, 0, +, -)$ . Sie ist kein Gruppenisomorphismus, da sie nicht surjektiv ist. Schränkt man ihr Ziel auf  $\mathbb{Z}$  ein, betrachtet also  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  mit  $f(x) = -x$ , so bekommt man sogar einen Gruppenisomorphismus von  $(\mathbb{Z}, 0, +, -)$  nach  $(\mathbb{Z}, 0, +, -)$ .  $\square$

Wir zeigen nun das schon angekündigte Resultat, dass Gruppenhomomorphismen in der Tat Strukturhomomorphismen im Sinne der allgemeinen Theorie der algebraischen Strukturen sind.

### 8.2.8 Satz: Gruppenhomomorphismen sind Strukturhomomorphismen

Es seien  $(G_1, e_1, \cdot_1, \text{inv}_1)$  und  $(G_2, e_2, \cdot_2, \text{inv}_2)$  Gruppen und  $\Phi : G_1 \rightarrow G_2$  eine Funktion. Dann sind die beiden folgenden Aussagen äquivalent:

- (1)  $\Phi$  ist ein Gruppenhomomorphismus,
- (2) Es gilt  $\Phi(e_1) = e_2$  und  $\Phi$  ist verträglich mit „ $\cdot_1$ “ und „ $\cdot_2$ “ und auch mit  $\text{inv}_1$  und  $\text{inv}_2$ .

**Beweis:** Richtung (1)  $\implies$  (2): Es gilt

$$\Phi(e_1) \cdot_2 \Phi(e_1) = \Phi(e_1 \cdot_1 e_1) = \Phi(e_1)$$

wegen der Homomorphismuseigenschaft. Wendet man nun Lemma 8.1.7 mit der Gruppe  $(G_2, e_2, \cdot_2, \text{inv}_2)$  an, so folgt  $\Phi(e_1) = e_2$ . Als Gruppenhomomorphismus ist  $\Phi$  verträglich

mit „ $\cdot_1$ “ und „ $\cdot_2$ “. Schließlich gilt noch für alle  $x \in G_1$  aufgrund der Homomorphismuseigenschaft und  $\Phi(e_1) = e_2$ , dass

$$\Phi(x) \cdot_2 \Phi(\text{inv}_1(x)) = \Phi(x \cdot_1 \text{inv}_1(x)) = \Phi(e_1) = e_2.$$

Die Eindeutigkeit der inversen Elemente bringt also  $\text{inv}_2(\Phi(x)) = \Phi(\text{inv}_1(x))$ . Damit ist  $\Phi$  auch verträglich mit  $\text{inv}_1$  und  $\text{inv}_2$ .

Die Richtung (2)  $\implies$  (1) ist trivial.  $\square$

Nach den Gruppenhomomorphismen wenden wir uns nun den Ringhomomorphismen zu. Hier ist die klassische Definition.

### 8.2.9 Definition: Ringhomomorphismus

Es seien  $(R_1, 0_1, 1_1, +_1, \cdot_1, -_1)$  und  $(R_2, 0_2, 1_2, +_2, \cdot_2, -_2)$  Ringe. Eine Funktion  $\Phi : R_1 \rightarrow R_2$  heißt ein **Ringhomomorphismus**, falls  $\Phi(1_1) = 1_2$  gilt und  $\Phi$  mit  $+_1$  und  $+_2$  und auch mit „ $\cdot_1$ “ und „ $\cdot_2$ “ verträglich ist. Ein **Ringisomorphismus** ist ein bijektiver **Ringhomomorphismus**.  $\square$

Auch Ringe nennt man isomorph, wenn es einen Ringisomorphismus zwischen ihnen gibt. Es fällt sofort auf, dass, im Vergleich zu den Homomorphismen bei den Gruppen, bei Ringhomomorphismen gefordert werden muss, dass die Gleichung  $\Phi(1_1) = 1_2$  gilt. Ohne diese Forderung wäre etwa, nichttriviale Ringe vorausgesetzt, die konstantwertige Funktion  $\Phi : R_1 \rightarrow R_2$  mit  $\Phi(x) = 0_2$  ein Ringhomomorphismus, was aber dem allgemeinen Konzept der Strukturerhaltung von Definition 8.2.4 widerspricht. Der für Gruppenhomomorphismen bewiesene Satz 8.2.6 überträgt sich unmittelbar auf Ringhomomorphismen. Dies zu beweisen sei der Leserin oder dem Leser zur Übung überlassen. Wir geben nur den entsprechenden Satz nachfolgend an.

### 8.2.10 Satz: Eigenschaften von Ringhomomorphismen

- (1) Die Komposition von Ringhomomorphismen ist ein Ringhomomorphismus.
- (2) Die Komposition von Ringisomorphismen ist ein Ringisomorphismus.
- (3) Die Umkehrfunktion eines Ringisomorphismen ist ein Ringisomorphismus.  $\square$

Eine Verallgemeinerung der Sätze 8.2.6 und 8.2.10 auf beliebige Strukturhomomorphismen und -isomorphismen sei der Leserin oder dem Leser ebenfalls zu Übungszwecken empfohlen. Nachfolgend geben wir einige einfache Beispiele für Ringhomomorphismen und -isomorphismen an.

### 8.2.11 Beispiele: Ringhomomorphismen und -isomorphismen

Auch bei allen Ringen  $(R, 0, 1, +, \cdot, -)$  ist die identische Funktion  $\text{id}_R : R \rightarrow R$  ein Ringisomorphismus.

Die Einbettungen von  $\mathbb{Z}$  in  $\mathbb{Q}$  und von  $\mathbb{Q}$  in  $\mathbb{R}$  mittels  $f : \mathbb{Z} \rightarrow \mathbb{Q}$ , wobei  $f(x) = x$ ,

und  $g : \mathbb{Q} \rightarrow \mathbb{R}$ , wobei  $g(x) = x$ , sind beides Ringhomomorphismen von  $(\mathbb{Z}, 0, 1, +, \cdot, -)$  nach  $(\mathbb{Q}, 0, 1, +, \cdot, -)$  bzw. von  $(\mathbb{Q}, 0, 1, +, \cdot, -)$  nach  $(\mathbb{R}, 0, 1, +, \cdot, -)$ . Sie sind jedoch keine Ringisomorphismen, da sie nicht surjektiv sind. Die Funktion  $g \circ f : \mathbb{Z} \rightarrow \mathbb{R}$  ist ein Ringhomomorphismus von  $(\mathbb{Z}, 0, 1, +, \cdot, -)$  nach  $(\mathbb{R}, 0, 1, +, \cdot, -)$ .  $\square$

Und hier ist nun auch noch die Übertragung von Satz 8.2.8 auf die Ringhomomorphismen, womit auch diese Funktionen in den allgemeinen Rahmen am Beginn des Kapitels eingebettet werden.

### 8.2.12 Satz: Ringhomomorphismen sind Strukturhomomorphismen

Es seien  $(R_1, 0_1, 1_1, +_1, \cdot_1, -_1)$  und  $(R_2, 0_2, 1_2, +_2, \cdot_2, -_2)$  Ringe und  $\Phi : R_1 \rightarrow R_2$  eine Funktion. Dann sind die beiden folgenden Aussagen äquivalent:

- (1)  $\Phi$  ist ein Ringhomomorphismus,
- (2) Es gelten  $\Phi(0_1) = 0_2$ ,  $\Phi(1_1) = \Phi(1_2)$  und  $\Phi$  ist verträglich mit „ $+_1$ “ und „ $+_2$ “, mit „ $\cdot_1$ “ und „ $\cdot_2$ “ und auch mit „ $-_1$ “ und „ $-_2$ “.

**Beweis:** Richtung (1)  $\implies$  (2): Nach Definition ist  $\Phi$  mit „ $+_1$ “ und „ $+_2$ “ und auch mit „ $\cdot_1$ “ und „ $\cdot_2$ “ verträglich. Wegen der ersten Verträglichkeit ist  $\Phi$  ein Gruppenhomomorphismus von  $(R_1, 0_1, +_1, -_1)$  nach  $(R_2, 0_2, +_2, -_2)$ . Damit gilt  $\Phi(0_1) = 0_2$  und es ist  $\Phi$  auch verträglich mit „ $-_1$ “ und „ $-_2$ “. Die Gleichung  $\Phi(1_1) = 1_2$  ist schließlich noch ein Teil der Forderungen an einen Ringhomomorphismus,

Die Richtung (2)  $\implies$  (1) ist wiederum trivial.  $\square$

Wir haben am Anfang dieses Abschnitts bemerkt, dass wir Körpermorphismen nicht eigens behandeln müssen. Dies wollen wir nun nachfolgend erklären. Es seien  $(K_1, 0_1, 1_1, +_1, \cdot_1, -_1)$  und  $(K_2, 0_2, 1_2, +_2, \cdot_2, -_2)$  Körper und  $\Phi : K_1 \rightarrow K_2$  ein Ringhomomorphismus. Weiterhin seien  $(K_1 \setminus \{0_1\}, 1_1, \cdot_1, \text{inv}_1)$  und  $(K_2 \setminus \{0_2\}, 1_2, \cdot_2, \text{inv}_2)$  die dadurch gegebenen kommutativen multiplikativen Gruppen<sup>12</sup> in dem Sinne, wie nach Satz 8.1.17 eingeführt. Weil die Einschränkung von  $\Phi$  auf  $K_1 \setminus \{0_1\}$  als Quelle und  $K_2 \setminus \{0_2\}$  als Ziel offensichtlich ein Gruppenhomomorphismus zwischen diesen Gruppen ist, gilt

$$\Phi(\text{inv}_1(x)) = \text{inv}_2(\Phi(x))$$

für alle  $x \in K_1 \setminus \{0_1\}$ . Die Einschränkung von  $\Phi$  ist also mit den multiplikativen Inversenbildungen verträglich. Im Fall von Körpern nennt man Ringmorphismen **Körpermorphisten** und zwei Körper  $(K_1, 0_1, 1_1, +_1, \cdot_1, -_1)$  und  $(K_2, 0_2, 1_2, +_2, \cdot_2, -_2)$  heißen isomorph, falls ein Körperisomorphismus  $\Phi : K_1 \rightarrow K_2$  existiert.

In den gängigen Algebra-Lehrbüchern werden die behandelten algebraischen Strukturen zu Abkürzungszwecken oft nur durch ihre Trägermengen bezeichnet. Damit ist jedoch bei manchen Variationen der behandelten Strukturen nicht sofort klar ersichtlich, was nun genau die Typen der neuen Strukturen sind und was für die entsprechenden Homomorphismen gefordert wird. Die Kenntnis der Typen und die sich daraus ergebenden

---

<sup>12</sup>Wir verwenden hier wieder die ursprüngliche Notation *inv* für die Inversenbildung, um diese in beiden Gruppen durch Indizes unterscheiden zu können.

Homomorphismus-Forderungen sind jedoch wesentlich, wie das folgende Beispiel demonstriert.

### 8.2.13 Beispiel: Strukturen und Homomorphismen

Es sei  $(R, 0, 1, +, \cdot, -)$  ein Ring und es bezeichne  $\mathfrak{R}$  die Menge der Ringhomomorphismen auf ihm. Dann bekommt man ein 6-Tupel  $(\mathfrak{R}, O, I, \oplus, \odot, \ominus)$ , indem man die Funktionen  $O : R \rightarrow R$  und  $I : R \rightarrow R$  definiert durch

$$O(x) = 0 \quad I(x) = 1$$

und die drei Operationen  $\oplus : \mathfrak{R}^2 \rightarrow \mathfrak{R}$ ,  $\odot : \mathfrak{R}^2 \rightarrow \mathfrak{R}$  und  $\ominus : \mathfrak{R} \rightarrow \mathfrak{R}$  auf den Ringhomomorphismen definiert durch

$$(f \oplus g)(x) = f(x) + g(x) \quad (f \odot g)(x) = f(x) \cdot g(x) \quad (\ominus f)(x) = -f(x)$$

für alle Funktionen  $f, g \in \mathfrak{R}$  und alle Elemente  $x \in R$ . Es sind „ $\oplus$ “ und „ $\odot$ “ assoziative Operationen und „ $\oplus$ “ ist auch kommutativ. Weiterhin gelten die Eigenschaften

$$O \oplus f = f \quad (\ominus f) \oplus f = O \quad 1 \odot f = f \quad f \odot 1 = f$$

für alle  $f \in \mathfrak{R}$ , sowie auch die beiden Distributivgesetze

$$f \odot (g \oplus h) = f \odot g \oplus f \odot h \quad (f \oplus g) \odot h = f \odot h \oplus g \odot h$$

für alle  $f, g, h \in \mathfrak{R}$ . All dies kann man mit Hilfe der Definition der Gleichheit von Funktionen relativ elementar beweisen. Wir behandeln als Beispiel ein Distributivgesetz. Es seien  $f, g, h \in \mathfrak{R}$ . Dann gilt für alle  $x \in R$ , wenn wir die Vorrangregel „Punkt vor Strich“ auch für „ $\odot$ “ und „ $\oplus$ “ verwenden,

$$\begin{aligned} (f \odot (g \oplus h))(x) &= f(x) \cdot (g \oplus h)(x) && \text{Definition } \odot \\ &= f(x) \cdot (g(x) + h(x)) && \text{Definition } \oplus \\ &= f(x) \cdot g(x) + f(x) \cdot h(x) && f(x), g(x), h(x) \in R \\ &= (f \odot g)(x) + (f \odot h)(x) && \text{Definition } \odot \\ &= (f \odot g \oplus f \odot h)(x) && \text{Definition } \oplus \end{aligned}$$

und dies ist genau  $f \odot (g \oplus h) = f \odot g \oplus f \odot h$  nach der Definition der Gleichheit von Funktionen.

Jedoch bildet  $(\mathfrak{R}, O, I, \oplus, \odot, \ominus)$  keinen Ring, denn die Funktionen  $O$  und  $I$  sind keine Ringhomomorphismen im Sinne von Definition 8.2.9. Hätten wir die im letzten Abschnitt erwähnte schwächere Form von Ringen als Tupel  $(R, 0, +, \cdot, -)$  und den entsprechenden schwächeren Ringhomomorphismus-Begriff ohne die Forderung  $\Phi(1_1) = 1_2$  verwendet, so wäre das Tupel  $(\mathfrak{R}, O, \oplus, \odot, \ominus)$  in der Tat ein Ring. Es würde auch einen Ring bilden, wenn wir bei einer Definition von Ringen das Einselement nicht explizit in den Typ mit aufgenommen hätten, sondern es nur implizit in der Form einer Existenzquantifizierung „es gibt ein Element  $1 \in R$  mit  $1x = x$  und  $x1 = x$ “ gefordert hätten. Auch auf diese Weise werden Ringe mit Einselement in der Literatur behandelt. Dies zieht den schwächeren Ringhomomorphismus-Begriff nach sich.  $\square$

## 8.3 Unterstrukturen

Es gibt einige Möglichkeiten, aus algebraischen Strukturen neue zu gewinnen. Eine sehr wichtige Möglichkeit ist die Bildung von sogenannten Unterstrukturen. Man betrachtet dazu eine Teilmenge der Trägermenge, die alle Konstanten enthält, und schränkt die Operationen der gegebenen algebraischen Struktur auf diese Teilmenge ein. Damit durch die Einschränkungen die Totalität der Operationen (im Sinne ihrer Definition als Relationen) erhalten bleibt, also wiederum Funktionen auf einer Menge entstehen, muss die in der nachfolgenden Definition eingeführte Abgeschlossenheit der Teilmenge unter allen Operationen gelten.

### 8.3.1 Definition: abgeschlossene Teilmenge

Es sei  $f : M^k \rightarrow M$  eine Funktion. Eine Teilmenge  $N$  von  $M$  heißt **abgeschlossen** unter  $f$ , falls für alle  $x_1, \dots, x_k \in N$  gilt  $f(x_1, \dots, x_k) \in N$ .  $\square$

Neben der Abgeschlossenheit von Teilmengen hinsichtlich der Operationen gilt es, wie schon erwähnt, die Konstanten zu beachten. Schließlich muss die ausgewählte Teilmenge nicht leer sein, denn sie soll ja als Trägermenge der neuen algebraischen Struktur dienen. Dies führt zur folgenden Festlegung.

### 8.3.2 Definition: Unterstruktur

Es sei  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  eine algebraische Struktur. Eine nichtleere Teilmenge  $N$  von  $M$  heißt **Unterstruktur**, falls  $c_1, \dots, c_m \in N$  gilt und  $N$  abgeschlossen unter allen Operationen  $f_1, \dots, f_n$  ist.  $\square$

Damit sind Unterstrukturen formal nur nichtleere Teilmengen  $N$ , also keine Tupel mit zusätzlichen Konstanten und Operationen. Erst durch die Hinzunahme der Konstanten der Originalstruktur und der Einschränkungen der Operationen der Originalstruktur auf  $N$  bekommt man wieder eine algebraische Struktur des gleichen Typs. Wenn man, wie früher bei den Körpern, die eingeschränkten Operationen mit dem gleichen Symbol bezeichnet, dann liefert die algebraische Struktur  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  die algebraische Struktur  $(N, c_1, \dots, c_m, f_1, \dots, f_n)$  des gleichen Typs.

### 8.3.3 Festlegung: Einschränkungen von Operationen

Zur Vereinfachung bezeichnen wir im Fall von algebraischen Strukturen zu einer nichtleeren Teilmenge  $N$  der Trägermenge die Einschränkungen der Operationen auf  $N$  mit den gleichen Symbolen wie die Originaloperationen.  $\square$

Es ist im Allgemeinen nicht sichergestellt, dass die Axiome der algebraischen Struktur  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  auch in der durch die Einschränkung der Operationen auf  $N \subseteq M$  entstehenden algebraischen Struktur  $(N, c_1, \dots, c_m, f_1, \dots, f_n)$  gelten. Bei gleichungsdefinierten algebraischen Strukturen ist dem jedoch so. Dieses ist eines der früher angesprochenen allgemeinen Resultate aus der universellen Algebra, welches wir aber hier in seiner Allgemeinheit nicht beweisen können (da uns die Mittel der formalen mathematischen Logik fehlen). Aufgrund dieses Resultats werden wir, wenn wir nachfolgend

Untergruppen und Unterringe als Teilmengen definieren, wieder Gruppen und Ringe erhalten. In diesen beiden konkreten Fällen ist, wie übrigens im Fall aller konkret gegebenen gleichungsdefinierten algebraischen Strukturen, das Nachrechnen der Axiome jedoch sehr einfach. Dies liegt daran, dass für die durch die Einschränkung der Operation  $f_i : M^{s_i} \rightarrow M$  auf  $N$  entstehende (nun, zu Argumentationszwecken letztmals anders bezeichnete) Operation  $g_i : N^{s_i} \rightarrow N$  und alle  $x_1, \dots, x_{s_i} \in N$  die Gleichheit  $f_i(x_1, \dots, x_{s_i}) = g_i(x_1, \dots, x_{s_i})$  gilt.

Wie bei den Strukturmorphismen weichen auch die klassischen Definitionen von Untergruppen und Unterringen von dem ab, was Definition 8.3.2 allgemein fordert. Der Grund ist wiederum, dass die spezielle Form der Axiome bei Gruppen und Ringen es erlaubt, einige Forderungen aus anderen zu beweisen. Untergruppen werden unter Verwendung der multiplikativen Schreibweise und Unterdrückung des Multiplikationssymbols in Ausdrücken üblicherweise wie folgt definiert:

### 8.3.4 Definition: Untergruppe

Ist  $(G, 1, \cdot, {}^{-1})$  eine Gruppe und ist  $N \subseteq G$  nichtleer, so heißt  $N$  eine **Untergruppe**, falls für alle  $x, y \in N$  gilt  $xy^{-1} \in N$ .  $\square$

Dass dadurch Unterstrukturen im allgemeinen Sinne von Definition 8.3.2 festgelegt werden, ist das erste Resultat dieses Abschnitts.

### 8.3.5 Satz: Untergruppen sind Unterstrukturen

Es seien  $(G, 1, \cdot, {}^{-1})$  eine Gruppe und  $N \subseteq G$  nichtleer. Dann sind die beiden folgenden Aussagen äquivalent:

- (1)  $N$  ist eine Untergruppe von  $(G, 1, \cdot, {}^{-1})$ .
- (2) Es gilt  $1 \in N$  und  $N$  ist abgeschlossen unter den Operationen „ $\cdot$ “ und „ ${}^{-1}$ “.

**Beweis:** Zum Beweis der Richtung (1)  $\implies$  (2) wählen wir  $x \in N$  beliebig. Dann gilt  $1 = xx^{-1} \in N$ . Dies wenden wir nun an, um die Abgeschlossenheit von  $N$  unter „ ${}^{-1}$ “ zu zeigen. Es sei wiederum  $x \in N$  beliebig. Wegen  $1 \in N$  gilt dann auch  $x^{-1} = 1x^{-1} \in N$ . Es bleibt noch die Abgeschlossenheit von  $N$  unter der Multiplikation „ $\cdot$ “ zu verifizieren. Dazu seien  $x, y \in N$ . Wir haben eben gezeigt, dass dann auch  $y^{-1} \in N$  gilt und dies bringt  $xy = x(y^{-1})^{-1} \in N$  aufgrund von Satz 8.1.10.

Um (2)  $\implies$  (1) zu beweisen, seien  $x, y \in N$  beliebig vorgegeben. Dann gilt  $y^{-1} \in N$  wegen der Abgeschlossenheit von  $N$  unter  ${}^{-1}$  und das bringt  $xy^{-1} \in N$  wegen der Abgeschlossenheit von  $N$  unter „ $\cdot$ “.  $\square$

Wenn  $N$  eine Untergruppe von  $(G, 1, \cdot, {}^{-1})$  ist, so ist auch  $(N, 1, \cdot, {}^{-1})$  eine Gruppe, denn Gruppen sind gleichungsdefiniert. Man nennt  $(N, 1, \cdot, {}^{-1})$  auch die von  $N$  induzierte Gruppe. Nach dieser Rechtfertigung der einfacheren klassischen Definition einer Untergruppe im Hinblick auf den allgemeinen Ansatz von Definition 8.3.2 geben wir nachfolgend einige Beispiele für Untergruppen an.

### 8.3.6 Beispiele: Untergruppen

In jeder Gruppe  $(G, 1, \cdot, -^{-1})$  gibt es mindestens die beiden speziellen Untergruppen  $\{1\}$  und  $G$ .

Es ist  $\mathbb{Z}$  eine Untergruppe sowohl der Gruppe  $(\mathbb{Q}, 0, +, -)$  als auch der Gruppe  $(\mathbb{R}, 0, +, -)$ . Hingegen ist  $\mathbb{N}$  keine Untergruppe von  $(\mathbb{Z}, 0, +, -)$ , denn die natürlichen Zahlen sind nicht abgeschlossen bezüglich der einstelligen Negation. Wenn man nämlich die Negationsoperation  $- : \mathbb{Z} \rightarrow \mathbb{Z}$  auf die Teilmenge  $\mathbb{N}$  einschränkt, so wird aus ihr die Relation  $R := \{(0, 0)\}$  auf  $\mathbb{N}$ . Folglich ist das Tupel  $(\mathbb{N}, 0, +, R)$  keine Gruppe, denn es ist laut Definition 8.1.1 ja nicht einmal mehr eine algebraische Struktur.

Die Kleinsche Vierergruppe  $(V_4, e, \cdot, \text{inv})$  von Beispiel 8.1.6 besitzt, wie man leicht anhand der Verknüpfungstafel verifiziert, genau 5 Untergruppen, nämlich die Teilmengen  $\{e\}$ ,  $\{e, a\}$ ,  $\{e, b\}$ ,  $\{e, c\}$  und  $V_4$ . Dass die restlichen 11 Teilmengen von  $V_4$  keine Untergruppen sind, erkennt man daran, dass sie immer aus der Menge  $\{a, b, c\}$  genau zwei Elemente enthalten. Deren Verknüpfung liefert laut Tafel aber genau das fehlende dritte Element.  $\square$

Untergruppen sind Mengen und damit kann man sie insbesondere vereinigen und Durchschnitte bilden. Vereinigungen von Untergruppen sind im Normalfall keine Untergruppen. Man belegt dies recht schnell durch Beispiele. Durchschnitte von Untergruppen sind hingegen wieder Untergruppen. Wie der folgende Satz zeigt, gilt dies sogar für beliebige Durchschnitte. Wegen des Universums  $G$ , in dem ja alle Untergruppen einer Gruppe  $(G, 1, \cdot, -^{-1})$  enthalten sind, dürfen wir in diesem Zusammenhang (man vergleiche mit Abschnitt 2.4) die Eigenschaft  $\bigcap \emptyset = G$  annehmen. Das korrespondiert mit der Tatsache, dass die Trägermenge  $G$  eine Untergruppe der Gruppe  $(G, 1, \cdot, -^{-1})$  ist.

### 8.3.7 Satz: Durchschnitt von Untergruppen

Es seien  $(G, 1, \cdot, -^{-1})$  eine Gruppe und  $\mathcal{G} \subseteq \mathcal{P}(G)$  eine Menge von Untergruppen. Dann ist auch  $\bigcap \mathcal{G}$  eine Untergruppe.

**Beweis:** Offensichtlich gilt  $1 \in \bigcap \mathcal{G}$ , also  $\bigcap \mathcal{G} \neq \emptyset$ . Es gilt weiterhin für alle  $x, y$ , dass

$$x, y \in \bigcap \mathcal{G} \iff \forall X \in \mathcal{G} : x \in X \wedge y \in X \implies \forall X \in \mathcal{G} : xy^{-1} \in X \iff xy^{-1} \in \bigcap \mathcal{G}$$

aufgrund der Definition von  $\bigcap \mathcal{G}$  und der Untergruppeneigenschaft.  $\square$

Da  $\bigcap \mathcal{G}$  auch eine Untergruppe ist, ist diese Menge hinsichtlich der Inklusionsordnung das kleinste Element der Menge aller Untergruppen von  $(G, 1, \cdot, -^{-1})$ . Nach den Untergruppen wenden wir uns nun den Unterringen zu. Wir beginnen wiederum mit der Definition, wie sie üblicherweise gebracht wird.

### 8.3.8 Definition: Unterring

Ist  $(R, 0, 1, +, \cdot, -)$  ein Ring und ist  $N \subseteq R$  nicht leer, so heißt  $N$  ein **Unterring**, falls  $N$  eine Untergruppe von  $(R, 0, +, -)$  bildet, die Eigenschaft  $1 \in N$  gilt und  $N$  abgeschlossen

unter der Operation „·“ ist. □

Natürlich ist auch diese Definition mit dem allgemeinen Ansatz verträglich, d.h. Unterringe sind Unterstrukturen im generellen Sinne der algebraischen Strukturen. Wir geben den entsprechenden Satz ohne Beweis an, da dieser sehr ähnlich zum Beweis von Satz 8.3.5 geführt werden kann.

### 8.3.9 Satz: Unterringe sind Unterstrukturen

Es seien  $(R, 0, 1, +, \cdot, -)$  ein Ring und  $N \subseteq R$  nichtleer. Dann sind die beiden folgenden Aussagen äquivalent:

- (1)  $N$  ist ein Unterring von  $(R, 0, 1, +, \cdot, -)$ .
- (2) Es gelten  $0 \in N$  und  $1 \in N$  und  $N$  ist abgeschlossen unter den Operationen „+“, „·“ und „-“. □

Wiederum nennt man den Ring  $(N, 0, 1, +, \cdot, -)$  den durch den Unterring  $N$  induzierten Ring. Und hier sind nun einige Beispiele für Unterringe.

### 8.3.10 Beispiele: Unterringe

Wie bei den Gruppen, so gibt es auch bei allen Ringen  $(R, 0, 1, +, \cdot, -)$  die zwei speziellen Unterringe  $\{0, 1\}$  (die mindestens vorausgesetzten Konstanten) und  $R$  (die gesamte Trägermenge).

Beispiele für zahlartige Unterringe sind die folgenden: Es ist die Menge  $\mathbb{Z}$  ein Unterring des Rings  $(\mathbb{Q}, 0, 1, +, \cdot, -)$  und die Menge  $\mathbb{Q}$  ein Unterring von  $(\mathbb{R}, 0, 1, +, \cdot, -)$ . Hingegen bildet die Menge  $\mathbb{G}$  der geraden ganzen Zahlen keinen Unterring von  $(\mathbb{Z}, 0, 1, +, \cdot, -)$ . Es gilt nämlich die Eigenschaft  $1 \in \mathbb{G}$  nicht und damit bekommt man keinen Ring, ja nicht einmal eine algebraische Struktur, wenn man  $\mathbb{G}$  mit den Konstanten der Originalstruktur und der Einschränkung deren Operationen auf  $\mathbb{G}$  zu einem Tupel  $(\mathbb{G}, 0, 1, +, \cdot, -)$  zusammenfasst.

Nun sei  $N$  ein Unterring des Körpers  $(K, 0, 1, +, \cdot, -)$ . Dann ist  $(N, 0, 1, +, \cdot, -)$  ein Ring, denn Ringe sind gleichungsdefiniert. Es ist  $(N, 0, 1, +, \cdot, -)$  aber im Allgemeinen kein Körper. Diese algebraische Struktur wird erst zu einem Körper, wenn  $N$  abgeschlossen unter der multiplikativen Inversenbildung ist, also zusätzlich noch zu allen Elementen  $x \in N$  mit  $x \neq 0$  und den eindeutig bestimmten Elementen  $y \in K$  mit  $yx = 1$  gilt  $y \in N$ . Man nennt  $N$  in so einem Fall einen **Unterkörper** des Körpers  $(K, 0, 1, +, \cdot, -)$ . Etwa ist die Menge  $\mathbb{Q}$  ein Unterkörper des Körpers  $(\mathbb{R}, 0, 1, +, \cdot, -)$  der reellen Zahlen, denn  $\mathbb{Q}$  ist ein Unterring des Rings  $(\mathbb{R}, 0, 1, +, \cdot, -)$  und für alle  $x \in \mathbb{Q}$  mit  $x \neq 0$  gilt  $\frac{1}{x} \in \mathbb{Q}$ . Hingegen ist offensichtlich der Unterring  $\mathbb{Z}$  des Rings  $(\mathbb{R}, 0, 1, +, \cdot, -)$  kein Unterkörper des Körpers der reellen Zahlen. □

Der Beweis des Satzes, dass der Durchschnitt von Untergruppen wieder eine Gruppe ist, kann in vollkommen analoger Weise auch für Ringe geführt werden. Damit erhalten wir das folgende Resultat, auf dessen Beweis wir verzichten.

### 8.3.11 Satz: Durchschnitt von Unterringen

Es seien  $(R, 0, 1, +, \cdot, -)$  ein Ring und  $\mathcal{R} \subseteq \mathcal{P}(R)$  eine Menge von Unterringen. Dann ist auch  $\bigcap \mathcal{R}$  ein Unterring.  $\square$

Wiederum ist  $\bigcap \mathcal{R}$  der kleinste Unterring hinsichtlich der Inklusionsordnung. Die beiden Sätze 8.3.7 und 8.3.11 haben dazu geführt, sich mit der Erzeugung von Gruppen und Ringen zu beschäftigen. Konkret geht es hier um die Frage, ob schon eine Teilmenge der Trägermenge ausreicht, alle Elemente der Trägermenge zu beschreiben. Wir greifen zum Abschluss des Abschnitts diese Fragen nur für Gruppen auf und betrachten hier auch nur den einfachsten Fall, dass eine einelementige Teilmenge der Trägermenge schon ausreicht, alle Elemente zu beschreiben. Für solche Gruppen werden wir Resultate zeigen, deren Beweise Schlussweisen verwenden, wie sie typisch für Gruppentheorie sind. Hier ist zuerst die Definition der von uns behandelten Gruppenklasse.

### 8.3.12 Definition: zyklische Gruppe

Es sei  $(G, 1, \cdot, ^{-1})$  eine Gruppe und  $\mathcal{U}_G$  die Menge ihrer Untergruppen.

- (1) Zu  $x \in G$  nennt man  $\langle x \rangle := \bigcap \{N \in \mathcal{U}_G \mid x \in N\}$  die von  $x$  **erzeugte Untergruppe**.
- (2) Gibt es ein Element  $x \in G$  mit  $\langle x \rangle = G$ , so heißt die Gruppe  $(G, 1, \cdot, ^{-1})$  **zyklisch** und  $x$  ein **erzeugendes Element**.  $\square$

Beispielsweise ist die Gruppe  $(\mathbb{Z}, 0, +, -)$  zyklisch. Ein erzeugendes Element ist etwa 1. Dass  $\langle 1 \rangle = \mathbb{Z}$  gilt, folgt aus dem nachfolgenden Resultat, indem man die additive Schreibweise  $xn$  für die Potenzierung verwendet. Das Resultat zeigt allgemein, wie man zyklische Gruppen durch Potenzen darstellen kann.

### 8.3.13 Satz: Beschreibung zyklischer Gruppen

Es seien  $(G, 1, \cdot, ^{-1})$  eine zyklische Gruppe und  $x \in G$  ein erzeugendes Element. Definiert man zu  $n \in \mathbb{N}$  die negative Potenz  $x^{-n}$  durch  $x^{-n} := (x^{-1})^n$ , so gilt  $G = \{x^n \mid n \in \mathbb{Z}\}$ .

**Beweis:** Wir haben  $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$  zu beweisen, denn daraus folgt mit der Voraussetzung  $\langle x \rangle = G$  die Behauptung.

Zum Beweis der Inklusion  $\langle x \rangle \subseteq \{x^n \mid n \in \mathbb{Z}\}$  starten wir mit der Eigenschaft, dass die Menge  $\{x^n \mid n \in \mathbb{Z}\}$  eine Untergruppe ist, die  $x$  enthält. Dies ist eine unmittelbare Konsequenz der Potenzierung und ihrer Gesetze. Weil aber  $\langle x \rangle$  nach Definition die kleinste Untergruppe im Inklusionssinne ist, die  $x$  enthält, folgt  $\langle x \rangle \subseteq \{x^n \mid n \in \mathbb{Z}\}$ .

Zum Beweis der verbleibenden Inklusion  $\{x^n \mid n \in \mathbb{Z}\} \subseteq \langle x \rangle$  beweisen wir zuerst durch eine vollständige Induktion, dass  $x^n \in \langle x \rangle$  für alle  $n \in \mathbb{N}$  gilt.

- (a) Den Induktionsbeginn zeigt  $x^0 = 1 \in \langle x \rangle$  unter Verwendung der Untergruppeneigenschaft von  $\langle x \rangle$ .
- (b) Zum Induktionsschluss sei  $n \in \mathbb{N}$  beliebig vorgegeben. Aus der Induktionshypothese  $x^n \in \langle x \rangle$  und der Eigenschaft  $x \in \langle x \rangle$  bekommen wir dann  $xx^n \in \langle x \rangle$ , wiederum

aufgrund der Untergruppeneigenschaft von  $\langle x \rangle$ . Die Definition der Potenzierung bringt nun  $x^{n+1} \in \langle x \rangle$ .

Es bleibt noch die Eigenschaft  $x^{-n} \in \langle x \rangle$  für alle  $n \in \mathbb{N}$  zu beweisen. Dazu verwenden wir zuerst  $x^{-n} = (x^n)^{-1}$ . Nach dem obigen Beweis gilt  $x^n \in \langle x \rangle$  und die Untergruppeneigenschaft von  $\langle x \rangle$  bringt  $(x^n)^{-1} \in \langle x \rangle$ .  $\square$

Gilt die Gleichung  $\langle x \rangle = G$ , so haben alle Elemente  $y, z \in G$  die Form  $y = x^m$  und  $z = x^n$ , mit natürlichen Zahlen  $m, n \in \mathbb{N}$ . Aufgrund von Eigenschaften der Potenzierung erhalten wir somit  $yz = x^m x^n = x^{m+n} = x^{n+m} = x^n x^m = zy$  und dies bringt das folgende Resultat.

### 8.3.14 Korollar

Alle zyklischen Gruppen sind kommutativ.  $\square$

Ist  $\Phi : G_1 \rightarrow G_2$  ein Gruppenhomomorphismus, so gilt, wie man leicht zeigt, für alle  $x \in G_1$  und  $n \in \mathbb{Z}$  die Gleichung  $\Phi(x^n) = \Phi(x)^n$ . Falls  $G_1$  die Trägermenge einer zyklischen Gruppe mit dem erzeugenden Element  $x$  ist, dann bestimmt der Wert  $\Phi(x)$  eindeutig die Werte  $\Phi(y)$  für alle  $y \in G_1$ . Insbesondere gilt  $\Phi = \Psi$  für alle Gruppenhomomorphismen  $\Psi : G_1 \rightarrow G_2$  mit  $\Phi(x) = \Psi(x)$ .

Als letztes Resultat dieses Abschnitts beweisen wir noch den folgenden Satz, der zeigt, dass sich das Zyklischsein auf die Untergruppen vererbt. Da insbesondere  $(\mathbb{Z}, 0, +, -)$  eine zyklische Gruppe ist, sind alle Untergruppen der additiven Gruppe der ganzen Zahlen zyklisch.

### 8.3.15 Satz: Untergruppen zyklischer Gruppen sind zyklisch

Ist  $N$  eine Untergruppe einer zyklischen Gruppe  $(G, 1, \cdot, -1)$ , so ist auch  $(N, 1, \cdot, -1)$  eine zyklische Gruppe.

**Beweis:** Im ersten Fall sei  $N$  gleich der Untergruppe  $\{1\}$ . Dann ist  $(N, 1, \cdot, -1)$  offensichtlich eine zyklische Gruppe.

Nun gelte  $\{1\} \subset N$ . Nach Voraussetzung und wegen  $1^n = 1$  für alle  $n \in \mathbb{Z}$  gibt es ein Element  $x \in G \setminus \{1\}$  mit  $G = \langle x \rangle$ . Wegen Satz 8.3.13 ist jedes Element von  $N$  eine (positive oder negative) Potenz  $x^k$  von  $x$ . Wir betrachten nun die folgende Menge:

$$X := \{n \in \mathbb{N} \mid n \neq 0 \wedge x^n \in N\}$$

Dann gilt  $X \neq \emptyset$ . Wegen  $\{1\} \subset N$  gibt es nämlich ein Element  $y \in N$  mit  $y \neq 1$  und  $y = x^k$  für ein  $k \in \mathbb{Z} \setminus \{0\}$ . Gilt  $k \in \mathbb{N} \setminus \{0\}$ , so impliziert dies  $k \in X$ . Trifft hingegen  $k \notin \mathbb{N}$  zu, so bekommen wir  $-k \in X$  aufgrund von  $y^{-1} \in N$  und

$$y^{-1} = (x^k)^{-1} = x^{-k}.$$

Nun sei  $n_0$  das kleinste Element von  $X$ . Wir zeigen nachfolgend, dass  $N = \langle x^{n_0} \rangle$  gilt, womit der Satz bewiesen ist.

Die Inklusion  $\langle x^{n_0} \rangle \subseteq N$  gilt wegen  $x^{n_0} \in N$  und der Eigenschaft, dass  $\langle x^{n_0} \rangle$  die kleinste Untergruppe im Inklusionssinne mit dieser Eigenschaft ist.

Zum Beweis der verbleibenden Inklusion  $N \subseteq \langle x^{n_0} \rangle$  sei  $x^k$  als ein beliebiges Element von  $N$  vorgegeben. Eine ganzzahlige Division mit Rest ergibt  $k = qn_0 + r$ , mit  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}$  so, dass  $r < n_0$ . Dies bringt

$$x^r = x^{k-qn_0} = x^k x^{-qn_0} = x^k (x^{n_0})^{-1} = x^k ((x^{n_0})^q)^{-1}.$$

Nach Voraussetzung gelten  $x^k \in N$  und  $x^{n_0} \in N$ . Die Untergruppeneigenschaft zeigt die folgende Implikation:

$$x^{n_0} \in N \implies (x^{n_0})^q \in N \implies ((x^{n_0})^q)^{-1} \in N \implies x^k ((x^{n_0})^q)^{-1} \in N$$

Folglich gilt  $x^r \in N$  und die Minimalität von  $n_0$  in der Menge  $X$  impliziert  $r = 0$ . Dies bringt nun  $x^k = x^{qn_0} = (x^{n_0})^q$ , was  $x^k \in \langle x^{n_0} \rangle$  zeigt.  $\square$

Somit sind insbesondere alle Untergruppen der zyklischen Gruppe  $(\mathbb{Z}, 0, +, -)$  der ganzen Zahlen zyklisch.

## 8.4 Produkt- und Quotientenstrukturen

Neben der Bildung von Unterstrukturen gibt es noch einige weitere Möglichkeiten, aus vorgegebenen algebraischen Strukturen neue algebraische Strukturen des gleichen Typs zu erzeugen. In diesem Abschnitt behandeln wir Produkt- und Quotientenbildungen. Im ersten Fall, mit dem wir die Diskussion beginnen, wird die Trägermenge der neuen Struktur als das direkte Produkt der Trägermengen der gegebenen Strukturen festgelegt und die neuen Konstanten und Operationen werden durch Tupelbildungen definiert. Nachfolgend betrachten wir der Einfachheit halber nur den Fall von binären direkten Produkten, also zwei algebraischen Strukturen. In der nächsten Definition wird die allgemeine Konstruktion angegeben.

### 8.4.1 Definition: Produktstruktur

Es seien algebraische Strukturen  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und  $(N, d_1, \dots, d_m, g_1, \dots, g_n)$  des gleichen Typs gegeben. Dann ist ihr **Produkt** definiert als

$$(M \times N, (c_1, d_1), \dots, (c_m, d_m), [f_1, g_1], \dots, [f_n, g_n]),$$

wobei für alle  $i \in \{1, \dots, n\}$  die Operation  $[f_i, g_i] : M \times N \rightarrow M \times N$ , das **Tupeling** von  $f_i$  und  $g_i$ , festgelegt ist durch  $[f_i, g_i](x, y) = (f_i(x), g_i(y))$ .  $\square$

Sind die algebraischen Strukturen  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und  $(N, d_1, \dots, d_m, g_1, \dots, g_n)$  durch die gleichen Axiome definiert und sind diese nur Gleichungen, so gelten die Axiome auch für das Produkt. Nachfolgend beweisen wir diesen wichtigen allgemeinen Satz der universellen Algebra für den Spezialfall der Gruppen. Wir verwenden dabei wieder die ursprüngliche Notation  $(G, e, \cdot, \text{inv})$ , um in einfacher Weise die Gruppen durch Indizes unterscheiden zu können.

### 8.4.2 Satz: Produktgruppe

Sind  $(G_1, e_1, \cdot_1, \text{inv}_1)$  und  $(G_2, e_2, \cdot_2, \text{inv}_2)$  Gruppen, so ist auch ihr Produkt eine Gruppe.

**Beweis:** Wir bezeichnen  $[\cdot_1, \cdot_2]$  mit dem Symbol „ $\cdot$ “ und verwenden die letzte Operation auch in Infix-Schreibweise. Dann folgt die Assoziativität aus

$$\begin{aligned} (x, y) \cdot ((u, v) \cdot (w, z)) &= (x, y) \cdot (u \cdot_1 w, v \cdot_2 z) \\ &= (x \cdot_1 (u \cdot_1 w), y \cdot_2 (v \cdot_2 z)) \\ &= ((x \cdot_1 u) \cdot_1 w, (y \cdot_2 v) \cdot_2 z) \\ &= (x \cdot_1 u, y \cdot_2 v) \cdot (w, z) \\ &= ((x, y) \cdot (u, v)) \cdot (w, z) \end{aligned}$$

für alle  $(x, y), (u, v), (w, z) \in G_1 \times G_2$ . Die Linksneutralität von  $(e_1, e_2)$  zeigt

$$(e_1, e_2) \cdot (x, y) = (e_1 \cdot_1 x, e_2 \cdot_2 y) = (x, y)$$

für alle  $(x, y) \in G_1 \times G_2$ . Wenn wir die Operation  $[\text{inv}_1, \text{inv}_2]$  mit dem Symbol  $\text{inv}$  bezeichnen, dann gilt die Gleichheit

$$\text{inv}(x, y) \cdot (x, y) = (\text{inv}_1(x), \text{inv}_2(y)) \cdot (x, y) = (\text{inv}_1(x) \cdot_1 x, \text{inv}_2(y) \cdot_2 y) = (e_1, e_2)$$

für alle  $(x, y) \in G_1 \times G_2$ , was schließlich auch noch die Linksinversedegenschaft zeigt.  $\square$

Es ist klar, wie man diesen Beweis auf beliebige gleichungsdefinierte algebraische Strukturen übertragen kann. Man wendet die Operationen der Produktstruktur von außen nach innen komponentenweise solange an, bis sie alle durch die der gegebenen algebraischen Strukturen ersetzt sind. Dann wendet man auf jene die Gleichung an, die man für die Produktstruktur zeigen will. Schließlich ersetzt man die Operationen der vorgegebenen algebraischen Strukturen von innen nach außen komponentenweise solange, bis nur noch Operationen der Produktstruktur übrig bleiben. Dieses Verfahren zeigt bei Ringen das folgende Resultat:

### 8.4.3 Satz: Produktring

Sind  $(R_1, 0_1, 1_1, +_1, \cdot_1, -_1)$  und  $(R_2, 0_2, 1_2, +_2, \cdot_2, -_2)$  Ringe, so ist auch ihr Produkt ein Ring.  $\square$

In dem folgenden Beispiel zeigen wir, wie man einen Produktring konstruiert.

### 8.4.4 Beispiel: Produktring

Wir betrachten die Menge  $R := \{0, 1\}$  und den Ring  $(R, 0, 1, +, \cdot, -)$ , wobei die 2-stelligen Operationen durch die folgenden Verknüpfungstafeln definiert sind:

| $+$ | 0 | 1 |
|-----|---|---|
| 0   | 0 | 1 |
| 1   | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---------|---|---|
| 0       | 0 | 0 |
| 1       | 0 | 1 |

Aus der linken Tafel bekommt man sofort  $-0 = 0$  und  $-1 = 1$ . Nun bestimmen wir das Produkt von  $(R, 0, 1, +, \cdot, -)$  mit sich selbst. Wenn wir die Tupelinge  $[+, +]$  und  $[\cdot, \cdot]$  mit den Symbolen „ $\oplus$ “ und „ $\odot$ “ bezeichnen und Paare  $(x, y)$  in der Form  $xy$  notieren, dann bekommen wir für „ $\oplus$ “ und „ $\odot$ “ die folgenden Verknüpfungstafeln:

| $\oplus$ | 00 | 01 | 10 | 11 | $\odot$ | 00 | 01 | 10 | 11 |
|----------|----|----|----|----|---------|----|----|----|----|
| 00       | 00 | 01 | 10 | 11 | 00      | 00 | 00 | 00 | 00 |
| 01       | 01 | 00 | 11 | 10 | 01      | 00 | 01 | 00 | 01 |
| 10       | 10 | 11 | 00 | 01 | 10      | 00 | 00 | 10 | 10 |
| 11       | 11 | 10 | 01 | 00 | 11      | 00 | 01 | 10 | 11 |

Die linke Verknüpfungstafel zeigt, dass 00 das neutrale Element bezüglich  $\oplus$  ist, und dass die Operation der Inversenbildung der identischen Funktion auf der Menge  $\{00, 01, 10, 11\}$  entspricht. Weiterhin kann man dieser Tafel durch einen Vergleich mit der Gruppentafel von Beispiel 8.1.6 entnehmen, dass die additive Gruppe des Produktrings isomorph zur Kleinschen Vierergruppe ist. Die rechte Verknüpfungstafel zeigt, dass 11 das Einselement des Produktrings ist.  $\square$

Körper sind nicht gleichungsdefiniert und deshalb ist das obige Verfahren auch nicht anwendbar, um zu zeigen, dass das Produkt von Körpern ein Körper ist. Und tatsächlich gibt es Körper, deren Produkt nur ein Ring ist. Dies trifft sogar immer zu. Nachfolgend geben wir dazu zwei spezielle Beispiele an, die man leicht verallgemeinern kann.

#### 8.4.5 Beispiele: Produkte von Körpern

Der Ring  $(R, 0, 1, +, \cdot, -)$  von Beispiel 8.4.4 ist ein Körper, denn das einzige Element 1 ungleich 0 hat sich selbst als multiplikatives inverses Element. Jedoch ist der Produktring von  $(R, 0, 1, +, \cdot, -)$  mit sich selbst kein Körper. Die beiden Elemente 01 und 10 besitzen jeweils kein multiplikatives inverses Element.

Wir betrachten nun den Körper  $(\mathbb{R}, 0, 1, +, \cdot, -)$  der reellen Zahlen. Bildet man das Produkt mit ihm selbst, so ist  $(0, 0) \in \mathbb{R}^2$  das Nullelement und  $(1, 1) \in \mathbb{R}^2$  das Einselement in diesem Produkt, einem Produktring. Nun sei  $x \in \mathbb{R}$  mit  $x \neq 0$  beliebig vorgegeben. Dann gilt  $(0, x) \neq (0, 0)$ . Es gibt zu  $(0, x) \in \mathbb{R}^2$  aber kein linksinverses Element bezüglich der Multiplikation im Produktring. Gäbe es so ein Element, etwa  $(y, z) \in \mathbb{R}^2$ , so muss die Gleichung  $(y, z) \cdot (0, x) = (1, 1)$  gelten. Wegen

$$(y, z) \cdot (0, x) = (y0, zx) = (0, zx) \neq (1, 1)$$

ist dies aber nicht möglich.  $\square$

Mit den obigen Beispielen kann man auch schön demonstrieren, welchen Wert die sehr weitreichenden und allgemeinen Aussagen der universellen Algebra haben können. Beispielsweise folgt aus der Aussage, dass die Produkte von gleichungsdefinierten algebraischen Strukturen wieder die Axiome der Strukturen erfüllen, aus denen sie konstruiert werden, dass es nicht möglich ist, die zwei Körper-Axiome  $0 \neq 1$  und  $\forall x \in K : x \neq 0 \Rightarrow \exists y \in K : xy = 1$  durch logisch äquivalente allquantifizierte Gleichungen zu ersetzen. Wäre dies möglich, so

wären Körper gleichungsdefiniert, also Produkte von Körpern wieder Körper. Das widerspricht aber den obigen Beispielen.

Nach den Produktstrukturen wenden wir uns nun den Quotientenstrukturen zu. Diese beruhen auf speziellen Äquivalenzrelationen. Im folgenden Beispiel motivieren wir die entscheidende Eigenschaft.

#### 8.4.6 Beispiel: Motivation von Vertreterunabhängigkeit

Wir betrachten eine algebraische Struktur  $(M, \cdot)$  des Typs (2). Deren Trägermenge sei gegeben durch die vierelementige Menge  $M := \{e, a, b, c\}$  und deren Operation  $\cdot : M^2 \rightarrow M$  sei spezifiziert durch die nachstehend links angegebene Verknüpfungstafel. Rechts von der Verknüpfungstafel ist eine Äquivalenzrelation  $\equiv$  auf der Menge  $M$  mittels einer Kreuztabelle definiert, woran man sofort die Äquivalenzklassen erkennt.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $\equiv$ | $e$ | $a$ | $b$ | $c$ |
|---------|-----|-----|-----|-----|----------|-----|-----|-----|-----|
| $e$     | $e$ | $a$ | $b$ | $c$ | $e$      | X   | X   |     |     |
| $a$     | $a$ | $a$ | $a$ | $a$ | $a$      | X   | X   |     |     |
| $b$     | $b$ | $b$ | $b$ | $b$ | $b$      |     |     | X   | X   |
| $c$     | $c$ | $c$ | $c$ | $c$ | $c$      |     |     | X   | X   |

Aufgrund der Kreuztabelle gilt  $M/\equiv = \{\{e, a\}, \{b, c\}\}$ . Wir wollen nun aus der algebraischen Struktur  $(M, \cdot)$  eine algebraische Struktur  $(M/\equiv, \circ)$  des gleichen Typs (2) gewinnen. Dazu haben wir eine Operation  $\circ : (M/\equiv)^2 \rightarrow M/\equiv$  anzugeben. Sinnvoll scheint es zu sein, diese für alle Äquivalenzklassen wie folgt zu definieren:

$$[x]_{\equiv} \circ [y]_{\equiv} = [x \cdot y]_{\equiv}$$

Das führt jedoch zu Schwierigkeiten. Wir bekommen nämlich einerseits aufgrund dieser Festlegung und der Verknüpfungstafel das folgende Resultat:

$$[e]_{\equiv} \circ [b]_{\equiv} = [e \cdot b]_{\equiv} = [b]_{\equiv}$$

Andererseits könnten wir aber auch wie nachstehend angegeben mit dem anderen Vertreter  $a$  der Äquivalenzklasse  $[e]_{\equiv}$  rechnen:

$$[a]_{\equiv} \circ [b]_{\equiv} = [a \cdot b]_{\equiv} = [a]_{\equiv}.$$

Damit hängt das Resultat der Operation  $\circ$  vom gewählten Vertreter der Äquivalenzklasse ab. Wählt man  $e$ , so wird das Paar  $(\{e, a\}, \{b, c\})$  mit  $\{b, c\}$  in Beziehung gesetzt, wählt man  $a$ , so wird es hingegen mit  $\{e, a\}$  in Beziehung gesetzt. Die obige Festlegung von  $\circ$  ist also nicht sinnvoll, denn die Eindeutigkeitseigenschaft von Funktionen ist nicht erfüllt. Man sagt auch, dass die Operation nicht **wohldefiniert** ist.  $\square$

Bei dem im Beispiel gewählten Ansatz ist unbedingt notwendig, dass die Definition der Operation auf den Äquivalenzklassen unabhängig von der Wahl der Klassenvertreter ist. Es handelt sich also wieder um eine Verträglichkeit, nun aber zwischen einer Funktion und einer Relation.

#### 8.4.7 Definition: Verträglichkeit

Eine Relation  $R$  auf  $M$  heißt mit einer Funktion  $f : M^k \rightarrow M$  **verträglich**, falls die logische Implikation

$$x_1 R y_1 \wedge \dots \wedge x_k R y_k \implies f(x_1, \dots, x_k) R f(y_1, \dots, y_k)$$

für alle Tupel  $(x_1, \dots, x_k)$  und  $(y_1, \dots, y_k)$  aus  $M^k$  gilt.  $\square$

Im Fall einer Äquivalenzrelation besagt diese Definition, dass äquivalente Argumente von  $f$  zu äquivalenten Resultaten führen. Und dies ist genau das, was man zur Wohldefiniertheit benötigt. Deshalb definiert man:

#### 8.4.8 Definition: Kongruenz

Gegeben seien eine algebraische Struktur  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und eine Äquivalenzrelation  $\equiv$  auf  $M$ . Dann heißt  $\equiv$  eine **Kongruenz**, falls sie mit allen Operationen  $f_1, \dots, f_n$  verträglich ist.  $\square$

Definiert man nun zur algebraischen Struktur  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und einer Kongruenz  $\equiv$  auf  $M$  zu jeder  $s_i$ -stetigen Operation  $f_i$  die Operation

$$\tilde{f}_i : (M/\equiv)^{s_i} \rightarrow M/\equiv \quad \tilde{f}_i([x_1]_\equiv, \dots, [x_{s_i}]_\equiv) = [f_i(x_1, \dots, x_{s_i})]_\equiv,$$

so ist diese tatsächlich auch wohldefiniert. Es gilt nämlich für alle Tupel  $(x_1, \dots, x_{s_i})$  und  $(y_1, \dots, y_{s_i})$  mit  $([x_1]_\equiv, \dots, [x_{s_i}]_\equiv) = ([y_1]_\equiv, \dots, [y_{s_i}]_\equiv)$  die folgende Gleichheit:

$$\tilde{f}_i([x_1]_\equiv, \dots, [x_{s_i}]_\equiv) = [f_i(x_1, \dots, x_{s_i})]_\equiv = [f_i(y_1, \dots, y_{s_i})]_\equiv = \tilde{f}_i([y_1]_\equiv, \dots, [y_{s_i}]_\equiv)$$

Diese Rechnung verwendet im ersten Schritt die Definition von  $\tilde{f}_i$ . Dann kommt die vorausgesetzte Gleichheit  $([x_1]_\equiv, \dots, [x_{s_i}]_\equiv) = ([y_1]_\equiv, \dots, [y_{s_i}]_\equiv)$  zur Anwendung. Sie zeigt nämlich die Gültigkeit von  $x_1 \equiv y_1 \wedge \dots \wedge x_{s_i} \equiv y_{s_i}$ . Daraus folgt  $f_i(x_1, \dots, x_{s_i}) \equiv f_i(y_1, \dots, y_{s_i})$  aufgrund der Kongruenzeigenschaft und dies zeigt, dass der zweite Schritt korrekt ist. Im dritten Schritt wird nochmals die Definition von  $\tilde{f}_i$  verwendet. Insgesamt rechtfertigt das eben Gebrachte die folgende Festlegung von Quotientenstrukturen.

#### 8.4.9 Definition: Quotientenstruktur

Es seien eine algebraische Struktur  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  und eine Kongruenz  $\equiv$  auf  $M$  gegeben. Dann ist die **Quotientenstruktur modulo  $\equiv$**  definiert als

$$(M/\equiv, [c_1]_\equiv, \dots, [c_m]_\equiv, \tilde{f}_1, \dots, \tilde{f}_n),$$

wobei für alle  $i \in \{1, \dots, n\}$  die Operation  $\tilde{f}_i : (M/\equiv)^{s_i} \rightarrow M/\equiv$  festgelegt ist durch die Gleichung  $\tilde{f}_i([x_1]_\equiv, \dots, [x_{s_i}]_\equiv) = [f_i(x_1, \dots, x_{s_i})]_\equiv$ .  $\square$

Statt Quotientenstruktur wird auch der Name **Faktorstruktur** verwendet. Ein allgemeines Resultat der universellen Algebra besagt, dass bei gleichungsdefinierten algebraischen Strukturen die Axiome auch für die Quotientenstruktur gelten. Nachfolgend beweisen wir dies wiederum nur für den Spezialfall der Gruppen.

### 8.4.10 Satz: Quotientengruppe

Sind  $(G, 1, \cdot, -^{-1})$  eine Gruppe und  $\equiv$  eine Kongruenz auf  $G$ , so ist die Quotientenstruktur modulo  $\equiv$  ebenfalls eine Gruppe.

**Beweis:** Es bezeichne „ $\circ$ “ die zu der Operation „ $\cdot$ “ korrespondierende Operation auf der Menge der Äquivalenzklassen (also „tilde  $\cdot$ “, in Infix-Schreibweise angewendet) und, analog dazu,  $inv$  die zu der Operation „ $-^{-1}$ “ korrespondierende Operation (also „tilde  $-^{-1}$ “). Dann zeigt

$$\begin{aligned} [x]_{\equiv} \circ ([y]_{\equiv} \circ [z]_{\equiv}) &= [x]_{\equiv} \circ [y \cdot z]_{\equiv} \\ &= [x \cdot (y \cdot z)]_{\equiv} \\ &= [(x \cdot y) \cdot z]_{\equiv} \\ &= [x \cdot y]_{\equiv} \circ [z]_{\equiv} \\ &= ([x]_{\equiv} \circ [y]_{\equiv}) \circ [z]_{\equiv} \end{aligned}$$

für alle Äquivalenzklassen  $[x]_{\equiv}, [y]_{\equiv}, [z]_{\equiv} \in M/\equiv$  das Assoziativgesetz. Auf die vollkommen gleiche Weise kann man auch die restlichen zwei Gruppen-Axiome beweisen. Für alle Äquivalenzklassen  $[x]_{\equiv} \in M/\equiv$  gilt

$$[1]_{\equiv} \circ [x]_{\equiv} = [1x]_{\equiv} = [x]_{\equiv}.$$

Das ist die Linksneutralität von  $[1]_{\equiv}$ . Weiterhin haben wir für alle  $[x]_{\equiv} \in M/\equiv$ , dass

$$inv([x]_{\equiv}) \circ [x]_{\equiv} = [x^{-1}]_{\equiv} \circ [x]_{\equiv} = [x^{-1} \cdot x]_{\equiv} = [1]_{\equiv}$$

gilt. Folglich liefert die Operation  $inv$  das linksinverse Element.  $\square$

Das Vorgehen bei diesem Beweis ist im Prinzip gleich dem Vorgehen beim Beweis von Satz 8.4.2. Damit ist auch offensichtlich, wie man ihn auf beliebige gleichungsdefinierte algebraische Strukturen übertragen kann. Im Fall der Ringe erhalten wir dann das folgende Resultat:

### 8.4.11 Satz: Quotientenring

Sind  $(R, 0, 1, +, \cdot, -)$  ein Ring und  $\equiv$  eine Kongruenz auf  $R$ , so ist die Quotientenstruktur modulo  $\equiv$  auch ein Ring.  $\square$

Wir wollen nun noch eine sehr wichtige Klasse von Quotientenringen studieren, die ursprünglich aus der Zahlentheorie stammen, mittlerweile aber auch sehr viele Anwendungen in der Informatik besitzen, beispielsweise bei der sogenannten Streuspeicherung von Daten (Stichwort: Hash-Funktionen) oder dem Verschlüsseln von Information. Diese Quotientenringe basieren auf den in Abschnitt 6.1 eingeführten Modulo-Relationen  $\equiv_m$  auf den ganzen Zahlen. Wir haben in Satz 6.1.10 bewiesen, dass alle Relationen  $\equiv_m$  Äquivalenzrelationen sind. Auch haben wir in Abschnitt 6.1 schon angemerkt, dass man beim Vorliegen von  $x \equiv_m y$  auch sagt, dass  $x$  kongruent zu  $y$  modulo  $m$  ist. Dieser Sprechweise liegt der folgende Satz zugrunde, der besagt, dass  $\equiv_m$  für alle  $m \in \mathbb{Z}$  eine Kongruenzrelation bezüglich des Rings der ganzen Zahlen ist. Wir verwenden in seinem Beweis die folgende Beschreibung der Modulo-Relation (siehe Abschnitt 6.1): Es gilt  $x \equiv_m y$  genau dann, wenn ein  $k \in \mathbb{Z}$  existiert mit  $x = y + mk$ .

### 8.4.12 Satz: Modulo-Relation ist eine Kongruenz

Für alle  $m \in \mathbb{Z}$  und alle  $x, y, u, v \in \mathbb{Z}$  gelten die folgenden Eigenschaften:

- (1) Aus  $x \equiv_m y$  und  $u \equiv_m v$  folgt  $x + u \equiv_m y + v$ .
- (2) Aus  $x \equiv_m y$  und  $u \equiv_m v$  folgt  $xu \equiv_m yv$ .

**Beweis:** (1) Aus  $x \equiv_m y$  und  $u \equiv_m v$  folgt, dass es  $k_1, k_2 \in \mathbb{Z}$  gibt mit  $x = y + mk_1$  und  $u = v + mk_2$ . Nun berechnen wir

$$x + u = y + mk_1 + v + mk_2 = y + v + m(k_1 + k_2)$$

und dies bringt  $x + u \equiv_m y + v$ .

(2) Aus  $x \equiv_m y$  und  $u \equiv_m v$  folgt wiederum, dass es  $k_1, k_2 \in \mathbb{Z}$  gibt mit  $x = y + mk_1$  und  $u = v + mk_2$ . Hinsichtlich der Multiplikation gehen wir wie folgt vor:

$$xu = (y + mk_1)(v + mk_2) = yv + ymk_2 + mk_1v + m^2k_1k_2 = yv + m(yk_2 + k_1v + mk_1k_2)$$

Diese Gleichheit impliziert  $xu \equiv_m yv$ . □

Jede Relation  $\equiv_m$  führt also zu einem Quotientenring  $(\mathbb{Z}/\equiv_m, [0]_{\equiv_m}, [1]_{\equiv_m}, \oplus, \odot, \ominus)$  des Rings  $(\mathbb{Z}, 0, 1, +, \cdot, -)$ , wobei wir die Symbole „ $\oplus$ “, „ $\odot$ “ und „ $\ominus$ “ statt den Tilde-Schreibweisen von Definition 8.4.9 verwendet haben. In der gängigen Literatur wird normalerweise die Zahl  $m$  immer als positiv gewählt. Weiterhin wird auch statt  $\mathbb{Z}/\equiv_m$  die Bezeichnung  $\mathbb{Z}_m$  verwendet. Dabei werden als Elemente dieser Menge bei der Darstellung des Rings aus Gründen der Lesbarkeit oft nicht die  $m$  Äquivalenzklassen  $[0]_{\equiv_m}, \dots, [m-1]_{\equiv_m}$  genommen, sondern nur ihre Vertreter  $0, \dots, m-1$ . Teilweise schreibt man auch  $\overline{0}, \dots, \overline{m-1}$  und meint damit doch die Äquivalenzklassen. Schließlich werden statt der Operationssymbole „ $\oplus$ “, „ $\odot$ “ und „ $\ominus$ “, wie bei den ganzen Zahlen, nur „ $+$ “, „ $\cdot$ “ und „ $-$ “ genommen. Der dadurch entstehende Ring  $(\mathbb{Z}_m, 0, 1, +, \cdot, -)$  bzw.  $(\mathbb{Z}_m, \overline{0}, \overline{1}, +, \cdot, -)$  heißt der **Quotientenring (oder Restklassenring) der ganzen Zahlen modulo  $m$** . Zur Verdeutlichung geben wir nachfolgend drei Beispiele an.

### 8.4.13 Beispiele: Quotientenringe der ganzen Zahlen

Der Ring von Beispiel 8.4.4 mit  $\{0, 1\}$  als Trägermenge und den folgenden Verknüpfungstafeln ist genau der Ring  $(\mathbb{Z}_2, 0, 1, +, \cdot, -)$ .

| + | 0 | 1 | · | 0 | 1 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 |

Wenn man den Quotientenring modulo 2 im ursprünglichen Sinne der Definition einer Quotientenstruktur auffasst, also als Menge  $\mathbb{Z}_2$  die Menge der Äquivalenzklassen  $\{[0]_{\equiv_2}, [1]_{\equiv_2}\}$  bzw.  $\{\overline{0}, \overline{1}\}$  nimmt, dann ist der Ring von Beispiel 8.4.4 natürlich nur isomorph zum Quotientenring modulo 2. Diese Bemerkung trifft auch auf die folgenden Beispiele zu. Die beiden Verknüpfungstafeln zur Addition und Multiplikation des Rings  $(\mathbb{Z}_3, 0, 1, +, \cdot, -)$  sehen wie folgt aus:

| $+$ | 0 | 1 | 2 |  | $\cdot$ | 0 | 1 | 2 |  |
|-----|---|---|---|--|---------|---|---|---|--|
| 0   | 0 | 1 | 2 |  | 0       | 0 | 0 | 0 |  |
| 1   | 1 | 2 | 0 |  | 1       | 0 | 1 | 2 |  |
| 2   | 2 | 0 | 1 |  | 2       | 0 | 2 | 1 |  |

Und nachfolgend sind noch die beiden entsprechenden Operationen des Rings  $(\mathbb{Z}_4, 0, 1, +, \cdot, -)$  in der Form von Verknüpfungstafeln angegeben:

| $+$ | 0 | 1 | 2 | 3 |  | $\cdot$ | 0 | 1 | 2 | 3 |  |
|-----|---|---|---|---|--|---------|---|---|---|---|--|
| 0   | 0 | 1 | 2 | 3 |  | 0       | 0 | 0 | 0 | 0 |  |
| 1   | 1 | 2 | 3 | 0 |  | 1       | 0 | 1 | 2 | 3 |  |
| 2   | 2 | 3 | 0 | 1 |  | 2       | 0 | 2 | 0 | 2 |  |
| 3   | 3 | 0 | 1 | 2 |  | 3       | 0 | 3 | 2 | 1 |  |

Es fällt auf, dass sowohl der Ring  $(\mathbb{Z}_2, 0, 1, +, \cdot, -)$  als auch der Ring  $(\mathbb{Z}_3, 0, 1, +, \cdot, -)$  ein Körper ist. Hingegen ist der Ring  $(\mathbb{Z}_4, 0, 1, +, \cdot, -)$  kein Körper.  $\square$

Würden wir die beiden Verknüpfungstafeln für die Quotientenringe der ganzen Zahlen modulo  $m$  auch für weitere ganze Zahlen  $5, 6, 7, 8, 9, \dots$  aufstellen, so würden wir für die Zahlen  $5, 7, 11, \dots$ , also für die Primzahlen, jeweils Körper erhalten. Dies ist ein bekanntes Resultat der Algebra, welches wir zum Abschluss dieses Abschnitts noch beweisen wollen. Wir benötigen zum Beweis von Satz 8.4.15 eine Hilfseigenschaft, die in der Literatur als Lemma von Bezout bekannt ist, benannt nach dem französischen Mathematiker Etienne Bezout (1730-1783).

#### 8.4.14 Lemma (E. Bezout)

Es seien  $x, m \in \mathbb{Z}$  und  $\text{ggT}(x, m)$  ihr (nichtnegativer) größter gemeinsamer Teiler. Gilt  $x \neq 0$  oder  $m \neq 0$ , so gibt es  $y, k \in \mathbb{Z}$  mit  $xy + mk = \text{ggT}(x, m)$ .

**Beweis:** Wir erweitern die Teilbarkeitsrelation in einer offensichtlichen Weise von  $\mathbb{N}$  nach  $\mathbb{Z}$ , indem wir für alle  $a, b \in \mathbb{Z}$  festlegen:

$$a | b : \iff \exists c \in \mathbb{Z} : ac = b$$

Dadurch ist es möglich, durch  $\text{ggT}(a, b) := \max\{c \in \mathbb{N} \mid c | a \wedge c | b\}$  den nichtnegativen größten gemeinsamen Teiler festzulegen. Die relationale Struktur  $(\mathbb{Z}, |)$  ist keine Ordnung. Hingegen ist  $(\mathbb{N}, |)$  eine Ordnung. In ihr ist 1 das kleinste Element von  $\mathbb{N}$  und für alle  $a, b \in \mathbb{N}$  ist  $\text{ggT}(a, b)$  das Infimum von  $\{a, b\}$ .

Nun betrachten wir zu den gegebenen Zahlen  $x, m \in \mathbb{Z}$  die Menge  $X$  von ganzen Zahlen, die genau alle möglichen Linearkombinationen von  $x$  und  $m$  enthält, definieren also

$$X := \{xa + mb \mid a, b \in \mathbb{Z}\}.$$

Wegen  $x \neq 0$  oder  $m \neq 0$  gibt es in  $X$  sicherlich positive ganze Zahlen. Es sei  $d$  die kleinste positive ganze Zahl in  $X$  bezüglich der Ordnung  $\leq$  und es seien  $y, k \in \mathbb{Z}$  so, dass  $d = xy + mk$  gilt. Einfach zu verifizieren ist, dass  $\text{ggT}(x, m) | x$  und  $\text{ggT}(x, m) | m$  implizieren  $\text{ggT}(x, m) | (xy + mk)$ , also  $\text{ggT}(x, m) | d$  gilt. Wir zeigen nachfolgend, dass

sogar  $d = \text{ggT}(x, m)$  zutrifft, womit das Lemma bewiesen ist. Dabei betrachten wir zwei Fälle.

Zuerst gelte  $d = 1$ . Aus  $\text{ggT}(x, m) \mid d$  folgt dann die Gleichung  $\text{ggT}(x, m) = d$ , denn als kleinstes Element von  $\mathbb{N}$  in  $(\mathbb{N}, \mid)$  ist  $d$  auch minimal in  $\mathbb{N}$  hinsichtlich  $(\mathbb{N}, \mid)$ .

Nun gelte  $d > 1$ . In diesem Fall führen wir eine ganzzahlige Division mit Rest durch und erhalten  $x = qd + r$ , mit  $q, r \in \mathbb{Z}$  so, dass  $0 \leq r < d$ . Wir berechnen zuerst

$$x = qd + r = q(xy + mk) + r$$

und durch eine Umstellung nach  $r$  erhalten wir daraus

$$r = x - q(xy + mk) = x - qxy - qmk = x(1 - qy) + m(-qk).$$

Folglich ist  $r$  eine nichtnegative Linearkombination von  $x$  und  $m$ . Aufgrund von  $r < d$  und weil  $d$  die kleinste positive Linearkombination von  $x$  und  $m$  ist, erhalten wir  $r = 0$ , was  $d \mid x$  zeigt. Analog beweist man  $d \mid m$ . Diese zwei Eigenschaften bringen nun  $d \mid \text{ggT}(x, m)$  und mit der schon gezeigten Eigenschaft  $\text{ggT}(x, m) \mid d$  und der Antisymmetrie der Teilbarkeitsrelation auf  $\mathbb{N}$  folgt  $d = \text{ggT}(x, m)$ .  $\square$

Man kann die Zahlen  $y$  und  $k$  dieses Lemmas effizient durch eine Verallgemeinerung des Euklidschen Algorithmus berechnen. Und hier ist nun das angekündigte Resultat. Zu seinem Beweis ist es vorteilhaft, die ursprüngliche Definition einer Quotientenstruktur mit der Menge der Äquivalenzklassen als Trägermenge zu verwenden.

#### 8.4.15 Satz: Quotientenringe modulo Primzahlen

Es sei  $m \in \mathbb{N}$  eine Primzahl. Dann ist der Quotientenring  $(\mathbb{Z}_m, [0]_{\equiv_m}, [1]_{\equiv_m}, +, \cdot, -)$  ein Körper.

**Beweis:** Die Ringeigenschaft wurde schon bewiesen. Für alle  $[x]_{\equiv_m}, [y]_{\equiv_m} \in \mathbb{Z}_m$  gilt

$$[x]_{\equiv_m} \cdot [y]_{\equiv_m} = [xy]_{\equiv_m} = [yx]_{\equiv_m} = [y]_{\equiv_m} \cdot [x]_{\equiv_m}$$

und folglich ist der Ring kommutativ. Die Eigenschaft  $[0]_{\equiv_m} \neq [1]_{\equiv_m}$  gilt trivialerweise. Zum Beweis des letzten Körper-Axioms sei  $[x]_{\equiv_m} \in \mathbb{Z}_m \setminus \{[0]_{\equiv_m}\}$  beliebig vorgegeben. Da  $m$  positiv ist, dürfen wir für den Vertreter  $x$  die Eigenschaft  $0 < x < m$  annehmen. Es sind  $x$  und  $m$  teilerfremd, denn  $m$  ist eine Primzahl. Nun können wir wie folgt logisch umformen:

$$\begin{aligned} \exists y \in \mathbb{Z} : [y]_{\equiv_m} \cdot [x]_{\equiv_m} = [1]_{\equiv_m} &\iff \exists y \in \mathbb{Z} : [yx]_{\equiv_m} = [1]_{\equiv_m} \\ &\iff \exists y \in \mathbb{Z} : yx \equiv_m 1 \\ &\iff \exists y \in \mathbb{Z} : \exists k \in \mathbb{Z} : yx - 1 = mk && \text{Abschnitt 6.1} \\ &\iff \exists y, k \in \mathbb{Z} : xy + mk = 1 \\ &\iff \exists y, k \in \mathbb{Z} : xy + mk = \text{ggT}(x, m) && x, m \text{ teilerfr.} \end{aligned}$$

Nach dem Lemma von Bezout (wegen  $m \neq 0$  anwendbar!) ist die letzte Formel dieser Rechnung wahr. Also trifft dies auch für die erste Formel zu.  $\square$

## 8.5 Der Körper der komplexen Zahlen

Wir haben bisher die Zahlenmengen  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  in dem intuitiven Sinne verwendet, wie sie von der höheren Schule her bekannt sind. Auch sind wir auf die algebraischen Strukturen eingegangen, welche sie mit den fundamentalen Konstanten und Operationen (den sogenannten Grundrechenarten) bilden. Die wesentliche Eigenschaft von Körpern ist, dass die Grundrechenarten unbeschränkt ausführbar sind und alle von den Zahlen her bekannten Gesetze gelten. In diesem Abschnitt führen wir nun als Erweiterung der reellen Zahlen die komplexen Zahlen als Körper ein. Die Motivation für diese Erweiterung geht bis in das 16. Jahrhundert zurück, als der italienische Mathematiker Gerolamo Cardano (1501-1576) bemerkte, dass gewisse quadratische Gleichungen lösbar wären, wenn Wurzelausdrücke  $\sqrt{-a}$  mit negativen Radikanden  $-a$  einen Sinn ergeben würden. Wegen  $\sqrt{-a} = \sqrt{-1}\sqrt{a}$  kann man sich dabei auf den negativen Radikanden  $-1$  beschränken, also auf eine Lösung der Gleichung  $x^2 = -1$  in den reellen Zahlen.

Die gängige Konstruktion der komplexen Zahlen erfolgt über Paare reeller Zahlen. Bei diesem Vorgehen können wir aber zunächst nur komponentenweise addieren, da, wie wir schon in Abschnitt 8.4 angemerkt haben, das Produkt des Körpers der reellen Zahlen mit sich selbst im Sinne der allgemeinen Definition 8.4.1 zu keinem Körper führt. Wir halten nachfolgend fest, was wir bisher wissen.

### 8.5.1 Definition und Satz: additive Gruppe der komplexe Zahlen

Es seien definiert

- (1) die Menge  $\mathbb{C}$  durch  $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ ,
- (2) die Konstante  $0_{\mathbb{C}}$  durch  $0_{\mathbb{C}} := (0, 0)$ ,
- (3) die Operation  $\oplus : \mathbb{C}^2 \rightarrow \mathbb{C}$  durch  $(x, y) \oplus (u, v) = (x + u, y + v)$  und
- (4) die Operation  $\ominus : \mathbb{C} \rightarrow \mathbb{C}$  durch  $\ominus(x, y) = (-x, -y)$ .

Dann bildet das Tupel  $(\mathbb{C}, 0_{\mathbb{C}}, \oplus, \ominus)$  eine (additive) kommutative Gruppe. Jedes Element aus  $\mathbb{C}$  heißt eine **komplexe Zahl**.  $\square$

Nun haben wir eine von der komponentenweisen Multiplikation auf  $\mathbb{R} \times \mathbb{R}$  verschiedene 2-stellige Multiplikationsoperation „ $\odot$ “ auf der Menge  $\mathbb{C}$  anzugeben und auch eine weitere Konstante  $1_{\mathbb{C}}$ , so dass durch deren Hinzunahme zur additiven Gruppe  $(\mathbb{C}, 0_{\mathbb{C}}, \oplus, \ominus)$  der komplexen Zahlen ein Körper entsteht. Die folgende Definition gibt die entsprechenden Festlegungen an.

### 8.5.2 Definition: Multiplikation und Einselement

Die Operation  $\odot : \mathbb{C}^2 \rightarrow \mathbb{C}$  ist definiert durch  $(x, y) \odot (u, v) = (xu - yv, xv + yu)$  und die Konstante  $1_{\mathbb{C}}$  ist definiert durch  $1_{\mathbb{C}} := (1, 0)$ .  $\square$

Auch bei den komplexen Zahlen verwenden wir die Vorrangregel „Punkt vor Strich“. Die folgenden zwei Eigenschaften der Multiplikation im Hinblick auf die spezielle komplexe Zahl  $(0, 1)$  werden uns am Ende des Abschnitts noch einmal begegnen, wenn wir auf die

sogenannte algebraische Darstellung von komplexen Zahlen eingehen. Wir verzichten auf die einfachen Beweise.

### 8.5.3 Lemma

- (1) Es gilt  $(0, 1) \odot (0, 1) = (-1, 0)$ .
- (2) Für alle  $(x, y) \in \mathbb{C}$  gilt  $(x, y) = (x, 0) \oplus (0, 1) \odot (0, y)$ .  $\square$

Nach der Definition einer Multiplikation und eines Einselementes sind wir nun in der Lage, die beabsichtigte Körpereigenschaft der komplexen Zahlen zu beweisen. Wir teilen dies auf und beginnen mit dem Beweis der Ringeigenschaft.

### 8.5.4 Satz: Ring der komplexen Zahlen

Das Tupel  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$  bildet einen kommutativen Ring.

**Beweis:** Die Multiplikation „ $\odot$ “ ist assoziativ, weil für alle  $(x, y), (u, v), (r, s) \in \mathbb{C}$  aufgrund ihrer Definition die nachfolgende Eigenschaft gilt:

$$\begin{aligned}
 (x, y) \odot ((u, v) \odot (r, s)) &= (x, y) \odot (ur - vs, us + vr) \\
 &= (x(ur - vs) - y(us + vr), x(us + vr) + y(ur - vs)) \\
 &= (xur - xvs - yus - yvr, xus + xvr + yur - yvs) \\
 &= (xur - yvr - xvs - yus, xus - yvs + xvr + yur) \\
 &= ((xu - yv)r - (xv + yu)s, (xu - yv)s + (xv + yu)r) \\
 &= (xu - yv, xv + yu) \odot (r, s) \\
 &= ((x, y) \odot (u, v)) \odot (r, s)
 \end{aligned}$$

Die Multiplikation ist auch eine kommutative Operation. Um dies zu beweisen, rechnen wir für alle  $(x, y), (u, v) \in \mathbb{C}$  wie folgt:

$$(x, y) \odot (u, v) = (xu - yv, xv + yu) = (ux - vy, uy + vx) = (u, v) \odot (x, y)$$

Es ist die komplexe Zahl  $1_{\mathbb{C}}$  neutral bezüglich der Multiplikation, weil

$$1_{\mathbb{C}} \odot (u, v) = (1, 0) \odot (u, v) = (1u - 0v, 1v + 0u) = (u, v)$$

für alle  $(u, v) \in \mathbb{C}$  gilt und diese Linksneutralität von  $1_{\mathbb{C}}$  aufgrund der Kommutativität der Multiplikation auch die Rechtsneutralität impliziert.

Weil wir für alle  $(x, y), (u, v), (r, s) \in \mathbb{C}$  haben, dass

$$\begin{aligned}
 (x, y) \odot ((u, v) \oplus (r, s)) &= (x, y) \odot (u + r, v + s) \\
 &= (x(u + r) - y(v + s), x(v + s) + y(u + r)) \\
 &= (xu + xr - yv - ys, xv + xs + yu + yr) \\
 &= (xu - yv + xr - ys, xv + yu + xs + yr) \\
 &= (xu - yv, xv + yu) \oplus (xr - ys, xs + yr) \\
 &= (x, y) \odot (u, v) \oplus (x, y) \odot (r, s),
 \end{aligned}$$

gilt das erste Distributivgesetz. Das zweite Distributivgesetz ist wiederum eine Folge der Kommutativität der Multiplikation.  $\square$

Im nächsten Satz geben wir an, wie bei komplexen Zahlen die inversen Elemente hinsichtlich der Multiplikation aussehen. Damit erhalten wir auch das insgesamt beabsichtigte Resultat, die Körpereigenschaft der komplexen Zahlen.

### 8.5.5 Satz: Körper der komplexen Zahlen

Im Ring  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$  der komplexen Zahlen ist zu jedem Paar  $(x, y) \in \mathbb{C} \setminus \{0_{\mathbb{C}}\}$  durch die Festlegung des Paares

$$\left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right)$$

ein linksinverses Element hinsichtlich der Multiplikation gegeben. Der Ring bildet also einen Körper.

**Beweis:** Die folgende Rechnung zeigt die behauptete Eigenschaft:

$$(x, y) \odot \left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) = \left( \frac{x^2}{x^2 + y^2} + \frac{y^2}{x^2 + y^2}, \frac{-xy}{x^2 + y^2} + \frac{yx}{x^2 + y^2} \right) = (1, 0) = 1_{\mathbb{C}}$$

Man beachte, dass die Voraussetzung  $(x, y) \neq 0_{\mathbb{C}}$  wegen des Nenners des linksinversen Elements notwendig ist.  $\square$

Wir haben in Abschnitt 8.1  $x - y := x + (-y)$  als Definition der Subtraktion in Ringen und  $\frac{x}{y} := xy^{-1}$  als Definition der Division in Körpern eingeführt. Damit ist durch eine Spezialisierung die komplexe Zahl

$$(x, y) \ominus (u, v) := (x, y) \oplus (\ominus(u, v)) = (x - u, y - v)$$

als die Differenz der komplexen Zahlen  $(x, y), (u, v) \in \mathbb{C}$  gegeben und durch

$$\frac{(x, y)}{(u, v)} := (x, y) \odot \left( \frac{u}{u^2 + v^2}, \frac{-v}{u^2 + v^2} \right) = \left( \frac{xu + yv}{u^2 + v^2}, \frac{-xv + yu}{u^2 + v^2} \right)$$

ihre Division. Es gelten auch hier die üblichen Gesetze. Wir führen nun vier neue Begriffe auf den komplexen Zahlen ein, wobei die ersten drei in einer Auffassung von Funktionen reellwertige Resultate liefern.

### 8.5.6 Definition: weitere Funktionen

Zu einer komplexen Zahl  $(x, y) \in \mathbb{C}$  heißt  $x \in \mathbb{R}$  der **Realteil**,  $y \in \mathbb{R}$  der **Imaginärteil**,  $\sqrt{x^2 + y^2} \in \mathbb{R}$  der **Betrag** und  $(x, -y) \in \mathbb{C}$  die **konjugiert-komplexe Zahl**.  $\square$

Benennt man im Kontext komplexer Zahlen das Paar  $(x, y)$  mit einer Variablen, in der Literatur wird in der Regel der Buchstabe  $z$  für komplexe Zahlen verwendet, so schreibt man oft auch  $Re(z)$  für den Realteil von  $z$ ,  $Im(z)$  für den Imaginärteil von  $z$  und  $\|z\|$  für den Betrag von  $z$ . (Statt  $\|z\|$  wird auch  $|z|$  verwendet.) Dies definiert drei Funktionen  $Re$ ,

$\text{Im}$  und  $\|\cdot\|$  von  $\mathbb{C}$  nach  $\mathbb{R}$ . Die konjugiert-komplexe Zahl von  $z$  bezeichnet man oft mit  $\bar{z}$  und damit wird die Konjugation eine bijektive Funktion  $\bar{\cdot}$  von  $\mathbb{C}$  nach  $\mathbb{C}$ , die offensichtlich ihre eigene Umkehrfunktion ist.

Jedes Element  $(x, y)$  des direkten Produkts  $\mathbb{R} \times \mathbb{R}$  entspricht genau einem Punkt in der Euklidischen Ebene oder genau einem Pfeil (Vektor) vom Nullpunkt  $(0, 0)$  des kartesischen Koordinatensystems zu  $(x, y)$ . In so einer Deutung von komplexen Zahlen – man nennt sie die **Gaußsche Zahlenebene**, obwohl die Vorgehensweise schon vor Gauß vom norwegisch-dänischen Mathematiker und Vermesser Caspar Wessel (1745-1818) verwendet wurde – kann man alle bisher gebrachten Begriffe geometrisch veranschaulichen. Sehr einfach sind die geometrischen Veranschaulichungen von Real- und Imaginärteil, Betrag und Konjugation:

- (1) Den Realteil von  $(x, y)$  bekommt man durch eine Projektion von  $(x, y)$  auf die Abszisse und den Imaginärteil liefert eine Projektion auf die Ordinate.
- (2) Der Betrag von  $(x, y)$  ergibt sich nach dem Satz von Pythagoras als die Länge der Strecke von  $(0, 0)$  nach  $(x, y)$ .
- (3) Die zu  $(x, y)$  konjugiert-komplexe Zahl erhält man durch eine Spiegelung des Punktes  $(x, y)$  an der Abszisse.

Auch die Addition von zwei komplexen Zahlen ist geometrisch noch sehr einfach zu beschreiben:

- (4) Bei der Addition erhält man das Resultat  $(x, y) \oplus (u, v)$  dadurch, indem man den Pfeil zu  $(u, v)$  parallel solange verschiebt, bis er in  $(x, y)$  beginnt. Er endet dann genau in  $(x, y) \oplus (u, v)$ .

Es handelt sich bei der Addition also im Prinzip um eine Vektoraddition im Vektorraum  $\mathbb{R}^2$ , die manche Leserin oder mancher Leser schon von der höheren Schule her kennt. Die geometrische Beschreibung der Multiplikation von zwei komplexen Zahlen ist hingegen etwas komplizierter. Hier ist es sinnvoll, Paare reeller Zahlen statt durch kartesische Koordinaten durch die schon in Beispiel 3.1.5 besprochenen Polarkoordinaten („Länge“, „Winkel“) darzustellen. Mit deren Hilfe kann man die Multiplikation geometrisch wie folgt beschreiben:

- (5) Haben die Paare  $(x, y)$  und  $(u, v)$  die Polarkoordinaten  $(a, \varphi)$  und  $(b, \psi)$ , so ist die Polarkoordinatendarstellung von  $(x, y) \odot (u, v)$  durch  $(ab, \varphi + \psi)$  gegeben, also dadurch, dass man die Längen multipliziert und die Winkel addiert.

Wenn wir Winkel in der Euklidischen Ebene im Bogenmaß angeben, dann haben beispielsweise die zwei komplexen Zahlen  $(1, 1)$  und  $(0, 2)$  die Polarkoordinatendarstellungen  $(\sqrt{2}, \frac{\pi}{4})$  bzw.  $(2, \frac{\pi}{2})$ . Also bekommen wir aufgrund der obigen geometrischen Deutung (5) das Paar  $(2\sqrt{2}, \frac{3\pi}{4})$  als Polarkoordinaten des Produkts  $(1, 1) \odot (0, 2)$ . Die kartesischen Koordinaten von  $(2\sqrt{2}, \frac{3\pi}{4})$  berechnen sich zu  $(-2, 2)$  und in der Tat gilt die Gleichung  $(1, 1) \odot (0, 2) = (-2, 2)$ , wie man leicht nachrechnet. Aufgrund der eben gebrachten geometrischen Veranschaulichung der komplexen Zahlen und ihrer Operationen mittels der

Gaußschen Zahlenebene sind auch die in den nachfolgenden drei Sätzen aufgeführten Resultate intuitiv einsichtig. Wir werden sie trotzdem formal beweisen. Der folgende Satz stellt diejenigen Resultate vor, die man durch die Strukturerhaltung von Funktionen ausdrücken kann. Der bisher noch nicht verwendete Begriff eines Monoidhomomorphismus in Teil (2) ergibt sich dabei direkt aus der allgemeinen Definition eines Strukturhomomorphismus.

### 8.5.7 Satz: Strukturerhaltung

- (1) Die Funktionen  $Re : \mathbb{C} \rightarrow \mathbb{R}$  und  $Im : \mathbb{C} \rightarrow \mathbb{R}$  sind Gruppenhomomorphismen von  $(\mathbb{C}, 0_{\mathbb{C}}, \oplus, \ominus)$  nach  $(\mathbb{R}, 0, +, -)$ .
- (2) Die Funktion  $\|\cdot\| : \mathbb{C} \rightarrow \mathbb{R}$  ist ein Monoidhomomorphismus von  $(\mathbb{C}, 1_{\mathbb{C}}, \odot)$  nach  $(\mathbb{R}, 1, \cdot)$ .
- (3) Die Funktion  $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}$  ist ein Körperisomorphismus von  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$  nach sich selbst.

**Beweis:** (1) Es gilt die Gleichung

$$Re(0_{\mathbb{C}}) = Re(0, 0) = 0.$$

Die Verträglichkeit der Funktion  $Re$  mit den Operationen  $\oplus$  und  $+$  folgt aus der Tatsache, dass für alle  $(x, y), (u, v) \in \mathbb{C}$  die folgende Gleichheit gilt:

$$Re((x, y) \oplus (u, v)) = Re(x + u, y + v) = x + u = Re(x, y) + Re(uv)$$

Die Beweise zu  $Im$  verlaufen vollkommen analog.

(2) Das (rein technische) Nachrechnen der entsprechenden zwei Eigenschaften sei der Lesein oder dem Leser als Übungsaufgabe gegeben.

(3) Die Bijektivität der Konjugierungs-Funktion wurde schon erwähnt und in der Tat folgt sie aus  $\overline{(x, y)} = \overline{(x, -y)} = (x, -y) = (x, y)$  für alle  $(x, y) \in \mathbb{C}$ . Zum Beweis der Strukturverträglichkeit seien  $(x, y), (u, v) \in \mathbb{C}$  gegeben. Dann gilt die Gleichheit

$$\begin{aligned} \overline{(x, y) \oplus (u, v)} &= \overline{(x + u, y + v)} \\ &= (x + u, -y - v) \\ &= (x, -y) \oplus (u, -v) \\ &= \overline{(x, y) \oplus (u, v)} \end{aligned}$$

und auch die Gleichheit

$$\begin{aligned} \overline{(x, y) \odot (u, v)} &= \overline{(xu - yv, xv + yu)} \\ &= (xu - yv, -xv - yu) \\ &= (x, -y) \odot (u, -v) \\ &= \overline{(x, y) \odot (u, v)}, \end{aligned}$$

was die Verträglichkeit der Konjugation sowohl mit der Addition als auch mit der Multiplikation zeigt. Wegen der Gleichheit

$$\overline{1_{\mathbb{C}}} = \overline{(1, 0)} = (1, -0) = 1_{\mathbb{C}}$$

ist die Konjugation insgesamt ein Ringhomomorphismus, also auch ein Körperhomomorphismus.  $\square$

Zum Angeben und Beweisen der bisherigen Resultate verwendeten wir immer die Definition von komplexen Zahlen als Paare von reellen Zahlen. Bei der Formulierung der Resultate des nachfolgenden Satzes machen wir uns nun erstmals von der Paardarstellung komplexer Zahlen frei und verwenden stattdessen die Buchstaben  $z_1$  und  $z_2$  für sie. Die Tatsache, dass diese Buchstaben Paare von reellen Zahlen bezeichnen, wird erst im Beweis des Satzes verwendet.

### 8.5.8 Satz: Rechenregeln

Für alle  $z_1, z_2 \in \mathbb{C}$  gelten die folgenden Eigenschaften:

- (1)  $Im(z_1 \odot \bar{z}_1) = Im(\bar{z}_1 \odot z_1) = 0$
- (2)  $Re(z_1 \odot \bar{z}_1) = Re(\bar{z}_1 \odot z_1) = \|z_1\|^2$
- (3)  $Re(z_1 \odot \bar{z}_2) = Re(z_2 \odot \bar{z}_1)$  und  $Im(z_1 \odot \bar{z}_2) = Im(z_2 \odot \bar{z}_1)$ .
- (4)  $Re(z_1) \leq \|z_1\|$  und  $Im(z_1) \leq \|z_1\|$ .

**Beweis:** Es gelte  $z_1 = (x, y)$ . Dann haben wir

$$z_1 \odot \bar{z}_1 = (x, y) \odot (x, -y) = (x^2 + y^2, -xy + yx) = (\|z_1\|^2, 0),$$

woraus die Gleichungen  $Im(z_1 \odot \bar{z}_1) = 0$  und  $Re(z_1 \odot \bar{z}_1) = \|z_1\|^2$  folgen. Analog kann man die Gleichung  $Im(\bar{z}_1 \odot z_1) = 0$  und  $Re(\bar{z}_1 \odot z_1) = \|z_1\|^2$  verifizieren. Ein Beweis von (3) setzt zusätzlich  $z_2 = (u, v)$  voraus. Dann gilt

$$Re(z_1 \odot \bar{z}_2) = Re((x, y) \odot (u, -v)) = xu + yv = Re((u, v) \odot (x, -y)) = Re(z_2 \odot \bar{z}_1)$$

und analog zeigt man  $Im(z_1 \odot \bar{z}_2) = Im(z_2 \odot \bar{z}_1)$ . Die trivialen Beweise der Ungleichungen von (4) lassen wir weg.  $\square$

Auch bei der Formulierung des letzten der oben angekündigten Resultate machen wir uns von der Paardarstellung komplexer Zahlen frei – nun sogar im Beweis. Der verwendete Name „Dreiecksungleichung“ für die Aussage wird klar, wenn man die Addition und den Betrag im Rahmen eines durch Pfeile gebildeten Dreiecks in der Gaußschen Zahlenebene geometrisch deutet. Dann werden die komplexen Zahlen  $\|z_1 \oplus z_2\|$ ,  $\|z_1\|$  und  $\|z_2\|$  zu den drei Seiten eines Dreiecks und die erste Seite ist kürzer als die Summe der beiden anderen Seiten.

### 8.5.9 Satz: Dreiecksungleichung

Für alle komplexen Zahlen  $z_1, z_2 \in \mathbb{C}$  gilt die folgende Eigenschaft:

$$\|z_1 \oplus z_2\| \leq \|z_1\| + \|z_2\|.$$

**Beweis:** Wir starten mit dem Quadrat der linken Seite der Ungleichung und rechnen wie nachstehend angegeben:

$$\begin{aligned}
\|z_1 \oplus z_2\|^2 &= \operatorname{Re}((z_1 \oplus z_2) \odot \overline{z_1 \oplus z_2}) && \text{Satz 8.5.8 (2)} \\
&= \operatorname{Re}((z_1 \oplus z_2) \odot (\overline{z_1} \oplus \overline{z_2})) && \text{Satz 8.5.7 (3)} \\
&= \operatorname{Re}(z_1 \odot \overline{z_1} \oplus z_1 \odot \overline{z_2} \oplus z_2 \odot \overline{z_1} \oplus z_2 \odot \overline{z_2}) && \text{Satz 8.5.4} \\
&= \operatorname{Re}(z_1 \odot \overline{z_1}) + \operatorname{Re}(z_1 \odot \overline{z_2}) + \operatorname{Re}(z_2 \odot \overline{z_1}) + \operatorname{Re}(z_2 \odot \overline{z_2}) && \text{Satz 8.5.7 (1)} \\
&= \|z_1\|^2 + \operatorname{Re}(z_1 \odot \overline{z_2}) + \operatorname{Re}(z_2 \odot \overline{z_1}) + \|z_2\|^2 && \text{Satz 8.5.8 (2)} \\
&= \|z_1\|^2 + 2\operatorname{Re}(z_1 \odot \overline{z_2}) + \|z_2\|^2 && \text{Satz 8.5.8 (3)} \\
&\leq \|z_1\|^2 + 2\|z_1 \odot \overline{z_2}\| + \|z_2\|^2 && \text{Satz 8.5.8 (4)} \\
&= \|z_1\|^2 + 2\|z_1\|\|\overline{z_2}\| + \|z_2\|^2 && \text{Satz 8.5.7 (2)} \\
&= \|z_1\|^2 + 2\|z_1\|\|z_2\| + \|z_2\|^2 \\
&= (\|z_1\| + \|z_2\|)^2
\end{aligned}$$

Die Monotonie der Wurzelfunktion impliziert nun  $\|z_1 \oplus z_2\| \leq \|z_1\| + \|z_2\|$ , also die Behauptung.  $\square$

Weil komplexe Zahlen formal Paare von reellen Zahlen sind, ist  $\mathbb{R}$  formal keine Teilmenge von  $\mathbb{C}$  im Sinne der Mengenlehre. Man kann aber die reellen Zahlen  $\mathbb{R}$  durchaus als eine Teilmenge von  $\mathbb{C}$  auffassen, indem man jede reelle Zahl  $x$  mit der komplexen Zahl  $(x, 0)$  identifiziert. Dies entspricht in der geometrischen Deutung der Tatsache, dass man die Abszisse als Teil der Euklidschen Ebene betrachtet. Wie der folgende Satz zeigt, bilden die komplexen Zahlen der speziellen Bauart  $(x, 0)$  einen Unterkörper von  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$ , der, versehen mit den Einschränkungen der Operationen des Oberkörpers, als Körper isomorph zum Körper der reellen Zahlen ist.

### 8.5.10 Satz: Einbettung der reellen Zahlen

Die Teilmenge  $\mathbb{C}_R := \mathbb{R} \times \{0\}$  von  $\mathbb{C}$  ist ein Unterkörper von  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$  und die Funktion  $\Phi : \mathbb{R} \rightarrow \mathbb{C}_R$  mit  $\Phi(x) = (x, 0)$  ist ein Körperisomorphismus von  $(\mathbb{R}, 0, 1, +, \cdot, -)$  nach  $(\mathbb{C}_R, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$ .

**Beweis:** Es seien  $(x, 0), (u, 0) \in \mathbb{C}_R$  gegeben. Dann gilt

$$(x, 0) \oplus (\ominus(u, 0)) = (x - u, 0) \in \mathbb{C}_R,$$

womit diese Menge eine Untergruppe der Gruppe  $(\mathbb{C}, 0_{\mathbb{C}}, \oplus, \ominus)$  ist. Sie ist auch ein Unterring des Rings  $(\mathbb{C}, 0_{\mathbb{C}}, 1_{\mathbb{C}}, \oplus, \odot, \ominus)$  aufgrund der folgenden zwei Eigenschaften:

$$1_{\mathbb{C}} = (1, 0) \in \mathbb{C}_R \quad (x, 0) \odot (u, 0) = (xu, 0) \in \mathbb{C}_R$$

Schließlich gilt im Fall  $(x, 0) \neq 0_{\mathbb{C}}$  für das linksinverse Element noch

$$\left( \frac{x}{x^2 + 0^2}, \frac{-0}{x^2 + 0^2} \right) = \left( \frac{1}{x}, 0 \right) \in \mathbb{C}_R.$$

Damit sind alle Eigenschaften eines Unterkörpers verifiziert.

Ein Beweis der Bijektivität der Funktion  $\Phi$  ist trivial. Wegen  $\Phi(1) = (1, 0) = 1_{\mathbb{C}}$  und

$$\Phi(r + s) = (r + s, 0) = (r, 0) \oplus (s, 0) = \Phi(r) \oplus \Phi(s)$$

und auch

$$\Phi(rs) = (rs, 0) = (r, 0) \odot (s, 0) = \Phi(r)\Phi(s)$$

für alle  $r, s \in \mathbb{R}$  ist  $\Phi$  ein Ringisomorphismus von  $(\mathbb{R}, 0, 1, +, \cdot, -)$  nach  $(\mathbb{C}_R, 0_C, 1_C, \oplus, \odot, \ominus)$  und Ringisomorphismen sind im Fall von Körpern Körperisomorphismen.  $\square$

Wenn man also in  $\mathbb{C}$  die Menge  $\mathbb{C}_R$  durch die Menge  $\mathbb{R}$  ersetzt, die so entstehende neue Menge wieder in  $\mathbb{C}$  umbenenn und schließlich noch die Operationen „ $\oplus$ “, „ $\odot$ “ und „ $\ominus$ “ an die neue Menge unter Abänderung ihrer Namen zu „ $+$ “, „ $\cdot$ “ und „ $-$ “ anpasst, so gilt die beabsichtigte Inklusion  $\mathbb{R} \subseteq \mathbb{C}$  und es ist weiterhin  $(\mathbb{R}, 0, 1, +, \cdot, -)$  ein Unterkörper von  $(\mathbb{C}, 0, 1, +, \cdot, -)$ . Wie bei den reellen Zahlen drückt man auch nun die Multiplikation in  $\mathbb{C}$  durch das Hintereinanderschreiben der Argumente aus.

In diesem Zusammenhang wird nun auch Lemma 8.5.3 wichtig. Bezeichnet man die dort behandelte spezielle komplexe Zahl  $(0, 1)$  mit dem Symbol  $i$ , so besagt das Lemma, dass in dem Körper  $(\mathbb{C}, 0, 1, +, \cdot, -)$  die Gleichung  $i^2 = -1$  gilt und weiterhin jede komplexe Zahl  $z$  in der Form  $z = Re(z) + iIm(z)$  geschrieben werden kann, oder auch in der Form  $z = x + iy$ , mit den Zusatzeigenschaften  $x = Re(z)$  und  $y = Im(z)$ . Man nennt dies die **algebraische Darstellung von komplexen Zahlen** und  $i$  die **imaginäre Einheit**. Es ergibt sich daraus  $\bar{z} = x - iy$  als konjugiert-komplexe Zahl. Ein gewisser Vorteil der algebraischen Darstellung ist, dass man damit wie in den reellen Zahlen rechnen kann. Die einzige zusätzliche Eigenschaft ist  $i^2 = -1$ . Nachfolgend geben wir ein Beispiel für das Rechnen mit algebraischen Darstellungen an.

### 8.5.11 Beispiel: Dualität

Es seien  $z_1 = x + iy$  und  $z_2 = u + iv$  komplexe Zahlen in der algebraischen Darstellung. Dann gilt

$$z_1 \odot \overline{z_2} = (x + iy)(u - iv) = xu + yv + i(yu - xv).$$

Weiterhin gilt

$$z_2 \odot \overline{z_1} = (u + iv)(x - iy) = ux + vy + i(vx - uy).$$

Eine Konjugation der zweiten Gleichheit bringt

$$\overline{z_2 \odot z_1} = ux + vy - i(vx - uy) = xu + yv + i(yu - xv) = z_1 \odot \overline{z_2}.$$

Man nennt diese Eigenschaft auch Dualität.  $\square$

Eine Warnung ist am Schluss noch angebracht. Die algebraische Darstellung von komplexen Zahlen verleitet Anfänger leicht dazu, die Ordnungsrelation auf den reellen Zahlen und ihre Eigenschaften leichtfertigerweise auch für die komplexen Zahlen zu verwenden, also etwa  $1 + i2 \leq 1 + i3$  zu rechnen. Dies ist nicht erlaubt! Der Grund hierfür ist, dass die dadurch implizit verwendete komponentenweise Ordnung auf Paaren reeller Zahlen nicht mit den Körperoperationen der komplexen Zahlen im Sinn von Definition 8.4.7 verträglich ist. Rechnungen mit komplexen Zahlen, bei denen die Ordnung auf den reellen Zahlen verwendet wird, obwohl die Zahlen nicht reell sind, führen deshalb zu irregulären Ergebnissen. Die Ordnungsbeziehung  $z_1 \leq z_2$  darf nur verwendet werden, wenn die Imaginärteile von  $z_1$  und  $z_2$  gleich Null sind.

## 8.6 Einige Bemerkungen zu allgemeinen mathematischen Strukturen

In den ersten vier Abschnitten dieses Kapitels haben wir homogene algebraische Strukturen behandelt und einige spezielle klassische Ausprägungen genauer untersucht. Wie schon in der Einleitung erwähnt wird, ist der Strukturbegriff der Mathematik aber viel allgemeiner. Allgemeinere Strukturen werden insbesondere auch in der Informatik verwendet. In diesem Abschnitt stellen wir einige davon vor. Wir tun dies aber nicht in der Präzision und Breite der bisherigen Strukturen, sondern versuchen nur, einen Eindruck davon zu geben, was an Verallgemeinerungen möglich ist und welche prinzipiellen Begriffe und Fragestellungen dabei auftreten.

Eine erste Verallgemeinerung besteht darin, bei algebraischen Strukturen mehr als nur eine Trägermenge zuzulassen. So eine sogenannte **heterogene algebraische Struktur** ist ein Tupel  $(M_1, \dots, M_k, c_1, \dots, c_m, f_1, \dots, f_n)$ , mit  $k \geq 2$ ,  $m \geq 0$  und  $n \geq 1$ . Die Konstanten kommen nun aus irgendeiner der  $k$  Trägermengen und die Operationen sind nun  $s_i$ -stellige und 1-wertige Funktionen über den Trägermengen. Damit ist es nicht mehr möglich, den Typ (die Signatur) durch eine Liste von Zahlen anzugeben. Stattdessen wird die Typisierung beispielsweise oft durch eine Funktion

$$\Sigma : \{c_1, \dots, c_m, f_1, \dots, f_n\} \rightarrow \{M_1, \dots, M_k\}^+$$

angegeben, wobei  $\Sigma(x) = (M_r)$  festlegt, dass  $x \in M_r$ , und  $\Sigma(x) = (M_{s_1}, \dots, M_{s_i}, M_r)$  festlegt, dass  $x : \prod_{j=1}^i M_{s_j} \rightarrow M_r$ . Eine in der Praxis übliche Variante dieser abstrakten Vorgehensweise besteht darin, die Typisierung direkt im Tupel an die Konstanten und Operationen anzufügen, wie etwa im Beispiel

$$(M, N, c : M, d : N, f : M \rightarrow N, g : M \times N \rightarrow N),$$

was offensichtlich viel einfacher zu lesen ist, als die folgende Funktionsdefinition:

$$\begin{aligned} \Sigma : \{c, d, f, g\} &\rightarrow \{M, N\}^+ & \Sigma(c) &= (M) & \Sigma(f) &= (M, N) \\ && \Sigma(d) &= (N) & \Sigma(g) &= (M, N, N) \end{aligned}$$

Bei heterogenen algebraischen Strukturen  $(M_1, \dots, M_k, c_1, \dots, c_m, f_1, \dots, f_n)$  wird manchmal auch nur  $k \geq 1$ ,  $m \geq 0$  und  $n \geq 1$  gefordert. Dann sind homogene algebraische Strukturen spezielle heterogene algebraische Strukturen, bei denen  $k = 1$  gilt.

Eine andere, auch einfacher zu verstehende Vorgehensweise in der Praxis besteht darin, die Typisierung in die Einführung einer heterogenen algebraischen Struktur umgebenden Text zu spezifizieren, beispielsweise zu sagen, dass im Fall der Struktur  $(M, N, c, d, f, g)$  gelten  $c \in M$ ,  $d \in N$ ,  $f : M \rightarrow N$  und  $g : M \times N \rightarrow N$ . Daraus geht implizit hervor, dass  $M$  und  $N$  die Trägermengen sind. Wir verwenden in den folgenden Beispielen die beiden letztgenannten Möglichkeiten.

Eine Klasse von Beispielen für heterogene algebraische Strukturen kennen wir bereits, nämlich die gerichteten Graphen der Art  $(V, P, \alpha, \omega)$  von Abschnitt 7.4. Mit einer Typangabe wird daraus  $(V, P, \alpha : P \rightarrow V, \omega : P \rightarrow V)$ . Man beachte jedoch, dass die ungerichteten Graphen der Art  $(V, K, \iota)$  von Abschnitt 7.4 keine heterogenen algebraischen Strukturen bilden, da die Funktion  $\iota$  als Ziel weder die Menge  $V$  der Knoten noch die Menge  $K$  der

Kanten hat, sondern die Potenzmenge  $\mathcal{P}(V)$ .

Deterministische Transitionssysteme (auch sequentielle Maschinen genannt) sind eine weitere Klasse von heterogenen algebraischen Strukturen. Ein **deterministisches Transitionssystem** ist ein Tripel  $(S, A, \Delta)$ . Dabei ist, wie bei den allgemeinen Transitionssystemen von Abschnitt 6.4,  $S$  eine Menge von Zuständen und  $A$  eine Menge von elementaren Aktionen. Im Gegensatz zu den allgemeinen Transitionssystemen werden bei den deterministischen Transitionssystemen die durch Aktionen bewirkten Zustandsübergänge nicht durch eine dreistellige Relation  $\rightarrow \subseteq S \times A \times S$  spezifiziert, sondern durch eine Funktion  $\Delta : S \times A \rightarrow S$ . Zu  $s \in S$  ist  $\Delta(s, a) \in S$  der durch die Aktion  $a \in A$  bewirkte Folgezustand. Somit entspricht  $\Delta(s, a) = t$  genau der Schreibweise  $s \xrightarrow{a} t$  von Abschnitt 6.4. Im Vergleich zu den allgemeinen Transitionssystemen gibt es bei den deterministischen Transitionssystemen zu jedem Zustand und jeder Aktion genau einen Folgezustand. Die Situation, dass es zu  $s \in S$  kein  $a \in A$  und kein  $t \in S$  mit  $s \neq t$  und  $s \xrightarrow{a} t$  gibt, modelliert man in deterministischen Transitionssystemen dadurch, dass man  $\Delta(s, a) = s$  für alle  $a \in A$  festlegt. Man nennt dann  $s$  einen **Fangzustand**.

Die **partiellen heterogenen algebraischen Strukturen** sind eine nochmalige Verallgemeinerung. Sie sind heterogene algebraische Strukturen, bei denen die Operationen auch partielle Funktionen sein dürfen. Seit vielen Jahren werden sie in der Informatik dazu verwendet, Datenstrukturen abstrakt zu spezifizieren. Ein Beispiel ist etwa die **algebraische Spezifikation des abstrakten Datentyps der linearen Listen** über einer Grundmenge. Sie ist gegeben durch die partielle heterogene algebraische Struktur

$$(M, L, e : L, \text{kopf} : L \rightarrow M, \text{rest} : L \rightarrow L, \text{anf} : M \times L \rightarrow L)$$

und die folgenden vier Eigenschaften der Konstanten  $e$  und Operationen  $\text{kopf}$ ,  $\text{rest}$  und  $\text{anf}$ , welche für alle Elemente  $a \in M$  und  $s \in L$  gefordert werden:

$$\begin{array}{ll} \text{kopf}(\text{anf}(a, s)) = a & \text{kopf}(e) \text{ ist undefiniert} \\ \text{rest}(\text{anf}(a, s)) = s & \text{rest}(e) \text{ ist undefiniert} \end{array}$$

Durch das 6-Tupel wird die Schnittstelle des abstrakten Datentyps der linearen Listen spezifiziert, wobei  $L$  für die Menge der linearen Listen steht und  $e$  für die leere Liste. Die drei Listenoperationen kennen wir bereits von Abschnitt 3.2, wobei wir dort die Operation des Linksanfügens durch einen Doppelpunkt und in Infix-Schreibweise notiert haben. Was genau sie bewirken wird durch die Eigenschaften der Struktur spezifiziert.

Natürlich gibt es auch **partielle homogene algebraische Strukturen**. Wenn man diesen Ansatz wählt, dann kann man bei den Körpern auch die Inversenbildung hinsichtlich der Multiplikation zu den Operationen hinzunehmen.

Algebraische Strukturen bestehen aus Trägermengen und Funktionen auf ihnen, sowie gegebenenfalls einigen Konstanten. Ersetzt man die Funktionen durch Relationen auf den Trägermengen, auch mehrstelligen Relationen, so erhält man **relationale Strukturen**. Auch hierzu haben wir schon Beispiele kennengelernt, etwa geordnete Mengen  $(M, \sqsubseteq)$ , gerichtete Graphen  $g = (V, P)$  und Transitionssysteme  $(S, A, \rightarrow)$ . Alle diese relationalen Strukturen besitzen keine Konstanten. Es gibt aber auch Varianten mit Konstanten, etwa

**fundierte geordnete Mengen**  $(M, \perp, \sqsubseteq)$ , wo gefordert wird, dass  $\perp$  das kleinste Element von  $M$  ist, oder **Transitionssysteme mit einem Anfangszustand**  $(S, A, \rightarrow, s)$ , wo  $s$  ein ausgezeichneter Zustand ist, bei dem das Transitionssystem, wenn es als Maschine angesehen wird, die Berechnung startet.

Schließlich gibt es noch algebraisch-relationale Strukturen, in denen sowohl Funktionen als auch Relationen vorkommen dürfen. Ein bekanntes Beispiel hierfür ist die Struktur eines **angeordneten Körpers**. Dies ist ein 7-Tupel  $(K, 0, 1, +, \cdot, -, \sqsubseteq)$  mit den folgenden Eigenschaften:

- (1) Es ist  $(K, 0, 1, +, \cdot, -)$  ein Körper.
- (2) Es ist  $(K, \sqsubseteq)$  eine linear geordnete Menge.
- (3) Für alle  $x, y, z \in K$  gelten:

$$x \sqsubseteq y \Rightarrow x + z \sqsubseteq y + z \quad 0 \sqsubseteq x \wedge 0 \sqsubseteq y \Rightarrow 0 \sqsubseteq x \cdot y$$

Beispielsweise bilden die rationalen Zahlen mit den üblichen Operationen und der üblichen Ordnung einen angeordneten Körper. Auch die reellen Zahlen bilden mit den üblichen Operationen und der üblichen Ordnung einen angeordneten Körper. Diese letztgenannte Struktur hat die zusätzliche Eigenschaft, dass jede nichtleere Teilmenge, zu der es eine obere Schranke gibt, auch ein Supremum besitzt. Bis auf Isomorphie ist  $(\mathbb{R}, 0, 1, +, \cdot, -, \leq)$  sogar der einzige angeordnete Körper mit dieser Eigenschaft. Dazu ist natürlich der Begriff „Isomorphie“ geeignet zu erweitern. Zwei angeordnete Körper  $(K_1, 0_1, 1_1, +_1, \cdot_1, -, \sqsubseteq_1)$  und  $(K_2, 0_2, 1_2, +_2, \cdot_2, -, \sqsubseteq_2)$  heißen isomorph, falls es einen Körperisomorphismus  $\Phi : K_1 \rightarrow K_2$  im Sinne von Abschnitt 8.2 gibt, der für alle  $x, y \in K_1$  erfüllt

$$x \sqsubseteq_1 y \iff \Phi(x) \sqsubseteq_2 \Phi(y).$$

Man sagt, dass der Körper der reellen Zahlen bis auf Isomorphie der einzige ordnungsvollständig angeordnete Körper ist. Wenn in einem Analysis-Buch oder einer Analysis-Vorlesung die reellen Zahlen nicht konstruktiv, sondern axiomatisch eingeführt werden, dann sind die entsprechenden Axiome genau die eines ordnungsvollständig angeordneten Körpers. In diesem Zusammenhang nennt man die Forderung, dass jede nichtleere Teilmenge von  $\mathbb{R}$ , zu der es eine obere Schranke gibt, auch ein Supremum besitzt, das **Vollständigkeitsaxiom**.

Zum Ende dieses Abschnitts wollen wir noch auf mathematische Strukturen eingehen, die **Mengensysteme** bilden, d.h. Paare bestehend aus einer Trägermenge  $M$  und einer Teilmenge  $\mathcal{M}$  der Potenzmenge  $\mathcal{P}(M)$ , wobei  $\mathcal{M}$  bestimmte Eigenschaften zu erfüllen hat. Ungerichtete Graphen  $g = (V, K)$  gehören zu dieser Klasse von Strukturen. Hier gilt  $K \subseteq \mathcal{P}(V)$  und die zu erfüllende Eigenschaft ist, dass  $|k| = 2$  für alle  $k \in K$  gilt. Auch Hypergraphen sind Mengensysteme, wenn man sie ohne parallele Hyperkanten in der Form  $g = (V, K)$  definiert und die Hyperkanten  $k \in K$  als nicht leere Mengen von Knoten festlegt. Als ein weiteres Beispiel betrachten wir noch Hüllensysteme, weil diese in vielen Bereichen der Informatik und der Mathematik eine bedeutende Rolle spielen und wir durch ein spezielles Hüllensystem die reflexiv-transitiven Hüllen unter einem anderen Blickwinkel nochmals aufgreifen können.

Ein Paar  $(M, \mathcal{H})$  heißt ein **Hüllensystem**, falls  $\mathcal{H}$  eine Teilmenge von  $\mathcal{P}(M)$  ist und für alle  $\mathcal{M} \subseteq \mathcal{H}$  gilt  $\bigcap \mathcal{M} \in \mathcal{H}$ . Ist  $M$  endlich, so ist  $(M, \mathcal{H})$  genau dann ein Hüllensystem, wenn  $\mathcal{H} \subseteq \mathcal{P}(M)$ ,  $M \in \mathcal{H}$  und für alle  $A, B \in \mathcal{H}$  gilt  $A \cap B \in \mathcal{H}$ . Die Menge  $\mathcal{RT}_X$  der reflexiven und transitiven Relationen auf einer vorgegebenen Menge  $X$  ist ein Hüllensystem  $(X \times X, \mathcal{RT}_X)$ , denn es gilt  $\mathcal{RT}_X \subseteq \mathcal{P}(X \times X)$  und der beliebige Durchschnitt reflexiver und transitiver Relationen auf  $X$  ist wiederum eine reflexive und transitive Relation auf  $X$ . Dieses spezielle Hüllensystem  $(X \times X, \mathcal{RT}_X)$  führt nun auf eine weitere Weise zu reflexiv-transitiven Hüllen, denn es gilt für alle Relationen  $R$  auf der Menge  $X$  die folgende Gleichung:

$$R^* = \bigcap \{S \in \mathcal{RT}_X \mid R \subseteq S\}$$

Diese Eigenschaft besagt, dass die reflexiv-transitive Hülle von  $R$  bezüglich der Inklusionsordnung die kleinste reflexive und transitive Relation auf  $X$  ist, welche  $R$  enthält.

Man rechnet relativ einfach nach, dass eine Relation  $S$  auf  $X$  genau dann reflexiv und transitiv ist, wenn  $\mathbf{I}_X \cup SS \subseteq S$  gilt. Dazu startet man mit

$$\begin{aligned} S \text{ reflexiv} &\iff \forall x \in X : x S x \\ &\iff \forall x, y \in X : x = y \Rightarrow x S y \\ &\iff \forall x, y \in X : x \mathbf{I}_X y \Rightarrow x S y \\ &\iff \mathbf{I}_X \subseteq S \end{aligned}$$

und der nur wenig komplizierteren Rechnung

$$\begin{aligned} S \text{ transitiv} &\iff \forall x, y, z \in X : x S y \wedge y S z \Rightarrow x S z \\ &\iff \forall x, z \in X : \forall y \in X : x S y \wedge y S z \Rightarrow x S z \\ &\iff \forall x, z \in X : (\exists y \in X : x S y \wedge y S z) \Rightarrow x S z \\ &\iff \forall x, z \in X : x (SS) z \Rightarrow x S z \\ &\iff SS \subseteq S, \end{aligned}$$

wobei in diesen logischen Umformungen nur die Definitionen der Reflexivität und der Transitivität von Relationen, der Inklusion von Mengen (hier: Relationen), der speziellen Relation  $\mathbf{I}_X$  und der Komposition  $SS$  von  $S$  mit sich selbst sowie einige bekannte logische Regeln angewendet werden. Dann verwendet man noch die Äquivalenz

$$S \text{ reflexiv} \wedge S \text{ transitiv} \iff \mathbf{I}_X \subseteq S \wedge SS \subseteq S \iff \mathbf{I}_X \cup SS \subseteq S,$$

welche sich unmittelbar aus den obigen Resultaten ergibt. Dadurch kann man nun die obige Gleichung umformen zu

$$\begin{aligned} R^* &= \bigcap \{S \in \mathcal{RT}_X \mid R \subseteq S\} \\ &= \bigcap \{S \in \mathcal{P}(X \times X) \mid R \subseteq S \wedge \mathbf{I}_X \cup SS \subseteq S\} \\ &= \bigcap \{S \in \mathcal{P}(X \times X) \mid R \cup \mathbf{I}_X \cup SS \subseteq S\} \\ &= \mu(\Phi), \end{aligned}$$

mit  $\mu(\Phi)$  als den kleinsten Fixpunkt der Funktion  $\Phi : \mathcal{P}(X \times X) \rightarrow \mathcal{P}(X \times X)$  mit der Definition  $\Phi(S) = R \cup \mathbf{I}_X \cup SS$ . Diese Funktion  $\Phi$  erfüllt nämlich (wie einfache Überlegungen zeigen) die Monotonie-Voraussetzung des Fixpunktsatzes 4.1.3 und  $R \cup \mathbf{I}_X \cup SS \subseteq S$  ist äquivalent zu  $\Phi(S) \subseteq S$ . Startet man nun mit der leeren Relation  $\emptyset$  auf  $X$  und wendet

immer wieder  $\Phi$  an, dann erhält man die folgende aufsteigende Kette von Relationen, wobei  $\Phi^i$  die  $i$ -fache Anwendung von  $\Phi$  bezeichnet:

$$\emptyset \subseteq \Phi(\emptyset) = \bigcup_{i=0}^1 R^i \subseteq \Phi^2(\emptyset) = \bigcup_{i=0}^2 R^i \subseteq \Phi^3(\emptyset) = \bigcup_{i=0}^4 R^i \subseteq \Phi^4(\emptyset) = \bigcup_{i=0}^8 R^i \subseteq \dots$$

Ist  $X$  endlich mit  $|X| = n$ , dann gibt es maximal  $\mathcal{O}(\log_2(n))$  unterschiedliche Kettenglieder und das letzte Kettenglied stimmt mit  $R^*$  überein. Deshalb ist das auf der obigen Kette beruhende Verfahren zur Berechnung von  $R^*$  schneller als das, welches auf der  $n$ -fachen Vereinigung  $R^* = \bigcup_{i=0}^{n-1} R^i$  beruht.

## 8.7 Übungsaufgaben

### Aufgabe

Geben Sie Beispiele an für algebraische Strukturen  $(M, f)$  des Typs (2), bei denen die Operation  $f : M^2 \rightarrow M$

- (1) nicht assoziativ ist,
- (2) nicht kommutativ ist,
- (3) assoziativ aber nicht kommutativ ist,
- (4) kommutativ aber nicht assoziativ ist.

### Aufgabe

Eine algebraische Struktur  $(V, \sqcup, \sqcap)$  des Typs (2, 2) (mit infixnotierten Operationen) heißt ein Verband, falls für alle  $x, y, z \in V$  die folgenden Verbands-Axiome gelten:

- (1)  $x \sqcup y = y \sqcup x$  und  $x \sqcap y = y \sqcap x$ .
- (2)  $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$  und  $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ .
- (3)  $x \sqcup (y \sqcap x) = x$  und  $x \sqcap (y \sqcup x) = x$ .

Geben Sie drei Beispiele für Verbände an.

### Aufgabe

Geben Sie ein Beispiel für einen Verband  $(V, \sqcup, \sqcap)$  an, in dem die beiden Distributivgesetze  $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$  und  $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$  für alle  $x, y, z \in V$  gelten.

### Aufgabe

Es sei  $(V, \sqcup, \sqcap)$  ein Verband. Beweisen Sie für alle  $x, y \in V$  die folgenden Eigenschaften:

- (1)  $x \sqcup x = x$  und  $x \sqcap x = x$ .
- (2) Es gilt  $x \sqcup y = y$  genau dann, wenn  $x \sqcap y = x$  gilt.
- (3) Es gilt  $x \sqcup y = x \sqcap y$  genau dann, wenn  $x = y$  gilt.

### Aufgabe

Es sei  $(M, \sqsubseteq)$  eine geordnete Menge mit der Eigenschaft, dass für alle  $x, y \in M$  sowohl das Supremum  $\sqcup\{x, y\}$  als auch das Infimum  $\sqcap\{x, y\}$  existieren. Beweisen Sie: Definiert man zwei Operationen  $\sqcup, \sqcap : M^2 \rightarrow M$  auf  $M$  in Infix-Schreibweise durch die Festlegungen

$$x \sqcup y = \sqcup\{x, y\} \quad x \sqcap y = \sqcap\{x, y\}$$

für alle  $x, y \in M$ , so bildet das Tripel  $(M, \sqcup, \sqcap)$  einen Verband.

### Aufgabe

Es sei  $(V, \sqsubseteq, \sqcap)$  ein Verband. Beweisen Sie: Definiert man eine Relation  $\sqsubseteq$  auf der Menge  $V$  durch die Festlegung

$$x \sqsubseteq y \iff x \sqcap y = x$$

für alle  $x, y \in V$ , so gelten die folgenden Eigenschaften:

- (1) Das Paar  $(V, \sqsubseteq)$  ist eine geordnete Menge.
- (2) Für alle  $x, y \in V$  ist in dieser geordnete Menge  $x \sqcup y$  das Supremum  $\sqcup\{x, y\}$  der Menge  $\{x, y\}$  und  $x \sqcap y$  das Infimum  $\sqcap\{x, y\}$  der Menge  $\{x, y\}$ .
- (3) In der geordneten Menge  $(V, \sqsubseteq)$  besitzt jede endliche Teilmenge  $X$  von  $V$  sowohl ein Supremum  $\sqcup X$  als auch ein Infimum  $\sqcap X$ .

### Aufgabe

Spezialisieren Sie die in Abschnitt 8.2 eingeführten Strukturmorphismen auf die algebraische Struktur eines Verbands.

### Aufgabe

Spezialisieren Sie die in Abschnitt 8.3 und 8.4 eingeführten Unterstrukturen, Produkt- und Quotientenbildungen auf die algebraische Struktur eines Verbands.

### Aufgabe

Definieren Sie Ringe in der traditionellen Auffassung als algebraische Strukturen  $(R, +, \cdot)$  des Typs  $(2, 2)$  und beweisen Sie, dass Ringe in der traditionellen Auffassung nicht gleichungsdefinierbar sind.

### Aufgabe

Es sei  $(G, 1, \cdot, ^{-1})$  eine Gruppe. Eine Untergruppe  $U \subseteq G$  heißt ein Normalteiler (oder eine normale Untergruppe) von  $(G, 1, \cdot, ^{-1})$ , falls für alle  $x \in G$  und  $y \in U$  gilt  $xux^{-1} \in U$ . Zeigen Sie die folgenden Eigenschaften:

- (1) Ist  $(G, 1, \cdot, ^{-1})$  eine kommutative Gruppe, so ist jede Untergruppe auch ein Normalteiler.

- (2) Ist  $U$  ein Normalteiler von  $(G, 1, \cdot, ^{-1})$  und definiert man eine Relation  $\equiv$  auf  $G$  durch die Festlegung

$$x \equiv y \iff xy^{-1} \in U$$

für alle  $x, y \in G$ , so ist  $\equiv$  eine Kongruenz.

Man bezeichnet die Quotientengruppe modulo der Kongruenz  $\equiv$  oft durch  $G/U$ .

### Aufgabe

Definieren Sie

- (1) sich an der Isomorphie von ungerichteten Graphen orientierend einen Isomorphiebegriff für gerichtete Graphen und
- (2) sich an der Isomorphie von angeordneten Körpern orientierend einen Isomorphiebegriff für angeordnete Mengen.

Erweitern Sie diese beiden Isomorphiebegriffe auf allgemeine homogene relationale Strukturen  $(M, R_1, \dots, R_n)$  mit gegebenenfalls auch mehrstelligen Relationen auf der Trägermenge  $M$ .

### Aufgabe

Beweisen Sie: Ist  $(K, 0, 1, +, \cdot, -, \sqsubseteq)$  ein angeordneter Körper, so kann die Menge  $K$  nicht endlich sein.

### Aufgabe

Zeigen Sie, dass, wie oben behauptet,

- (1) die Menge  $\mathcal{RT}_X$  der reflexiven und transitiven Relationen auf einer Menge  $X$  tatsächlich ein Hüllensystem  $(X \times X, \mathcal{RT}_X)$  bildet,
- (2) für alle Relationen  $R$  auf einer Menge  $X$  die reflexiv-transitive Hülle  $R^*$  das kleinste Element der Teilmenge  $\{S \in \mathcal{RT}_X \mid R \subseteq S\}$  von  $\mathcal{P}(X \times X)$  in der geordneten Menge  $(\mathcal{P}(X \times X), \subseteq)$  ist.

### Aufgabe

Es sei  $M$  eine nicht endliche Menge und  $\mathcal{E}_M$  die Menge der endlichen Teilmengen von  $M$ . Bildet  $(M, \mathcal{E}_M)$  ein Hüllensystem (mit Begründung)?

### Aufgabe

Eine Struktur  $(M, d)$ , bestehend aus einer Menge  $M$  und einer Funktion  $d : M \times M \rightarrow \mathbb{R}_{\geq 0}$ , heißt ein metrischer Raum, falls für alle  $x, y, z \in M$  die folgenden Eigenschaften gelten:

$$d(x, y) = 0 \Leftrightarrow x = y \quad d(x, y) = d(y, x) \quad d(x, y) \leq d(x, z) + d(z, y)$$

Beweisen Sie, dass die Menge der reellen Zahlen mit der Funktion  $d : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ , definiert durch  $d(x, y) = |x - y|$ , einen metrischen Raum  $(\mathbb{R}, d)$  bildet.

## 9 Einige Literaturhinweise

Aufgrund des einführenden Charakters werden alle in dem Text vorgestellten mathematischen Gebiete nur auf relativ elementarem Niveau behandelt. Nachfolgend geben wir zu den einzelnen Kapiteln noch einige Literaturhinweise an, in denen der behandelte Stoff teilweise beträchtlich vertieft wird und auch viele weitere Beispiele zu finden sind. Wir beschränken uns dabei auf (in der Regel) Lehrbücher neueren Datums und vermeiden Hinweise auf Originalartikel aus Zeitschriften oder Konferenzbänden. Es ist jedoch auch reizvoll und sogar für einen Anfänger manchmal hilfreich, einen Blick in Originalarbeiten zu werfen.

Die mengentheoretischen Grundlagen werden, mehr oder minder ausführlich und in der Regel dem naiven Ansatz folgend, in allen einführenden Mathematikbüchern behandelt. Dabei ist es nicht wesentlich, ob es sich etwa um eine Analysis-Einführung handelt oder eine Einführung in die lineare Algebra oder die diskrete Mathematik. Ein Buch, das sich nur der naiven Mengenlehre als einzigmem Thema widmet, ist das nachfolgend unter (1) aufgeführte. Das nachfolgende Buch (2) stellt hingegen eine Einführung in die axiomatische Mengenlehre dar. Es beginnt mit einem sehr interessanten Kapitel über die historische Entwicklung der Mengenlehre, das auch deutlich aufzeigt, wie sehr insbesondere anfangs unter den Mathematikern um die Cantorschen Ideen gerungen wurde,

- (1) P. Halmos, Naive Mengenlehre (5. Auflage), Vandenhoeck und Ruprecht, 1994.
- (2) A. Oberschelp, Allgemeine Mengenlehre, BI-Wissenschaftsverlag, 1994.

Ähnlich wie die Mengenlehre wird auch die Logik normalerweise in allen einführenden Mathematikbüchern naiv und mehr oder minder ausführlich behandelt. Die folgenden zwei Bücher stellen hingegen umfassende Einführungen in die formale mathematische Logik dar, indem etwa zwischen Syntax und Semantik und Gültigkeit und Beweisbarkeit genau unterschieden wird.

- (3) H.-D. Ebbinghaus, J. Flum, W. Thomas, Einführung in die mathematische Logik, Spektrum Akademischer Verlag, 1996.
- (4) W. Rautenberg, Einführung in die mathematische Logik (3. Auflage), Vieweg+Teubner, 2008.

Auch der Stoff von Abschnitt 3.1 ist Standard in vielen einführenden Mathematikbüchern und wird in der Regel ähnlich präsentiert wie in dem vorliegenden Text. Die darauf aufbauende Behandlung von Datenstrukturen der Informatik geschieht hingegen normalerweise nur in Informatikbüchern und dort teils auch nicht in der gewohnten mathematischen Notation, sondern in Programmiersprachen-Notation. Unsere Darstellung orientiert sich an der Vorgehensweise, wie sie typisch für das funktionale Programmieren ist. Das nachfolgende Buch stellt eine Einführung in diese Art der Programmierung anhand von vier funktionalen Programmiersprachen dar, darunter auch das von uns in Abschnitt 3.2 erwähnte Haskell.

- (5) P. Pepper, Funktionale Programmierung in Opal, ML, Haskell und Gofer (2. Auflage), Springer Verlag, 2003.

Lineare Listen werden, wie in Abschnitt 3.2 erwähnt, im Kontext der formalen Sprachen auch als Wörter bezeichnet. Sie sind ein unentbehrliches Hilfsmittel in vielen Teilen der theoretischen Informatik, dem Gebiet der Informatik, dem auch die formalen Sprachen zugeordnet werden. Eine sehr umfangreiche Einführung in wichtige Teilgebiete dieses Gebiets, wo Wörter immer wieder vorkommen, ist etwa das nachfolgende Buch (6). Als wesentlich knappere Einführung in die theoretische Informatik sei noch das Buch (7) genannt.

- (6) J.E. Hopcroft, R. Motwani, J.D. Ullman, Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie, Pearson Studium, 2002.
- (7) K. Wagner, Einführung in die Theoretische Informatik, Springer Verlag, 1994.

Was ein mathematischer Beweis im Sinne eines formalen Kalküls ist, wird in der formalen mathematischen Logik definiert. Damit kann man auch die Grenzen dessen aufzeigen, was beweisbar ist. Beweise im täglichen mathematischen Leben werden hingegen wie in diesem Text geführt. Der Stil ist dabei jedoch nicht einheitlich. Manche Autoren bevorzugen den umgangssprachlichen Stil, also den unseres ersten Kapitels, andere ziehen es hingegen vor, soweit wie möglich mit logischen Symbolen und logischen Umformungen, Gleichungsketten  $E_1 = E_2 = E_3 = \dots$  und Ketten von Ordnungsbeziehungen  $E_1 \sqsubseteq E_2 \sqsubseteq E_3 \sqsubseteq \dots$  zu arbeiten. Insbesondere von einer Gruppe von Informatikern, die sich mit der formalen Entwicklung von korrekten Programmen aus mathematischen Problem-Spezifikationen beschäftigen, wird der letztgenannte Stil bevorzugt. In der englischen Literatur spricht man dann von „calculational program development“. Das nachfolgende Buch enthält viele Beispiele zu dieser Vorgehensweise.

- (8) R. Backhouse, Program Construction, Wiley, 2003.

Es gibt mittlerweile auch einige Bücher, die Mathematik und das mathematische Denken und Beweisen unter sehr allgemeinen Gesichtspunkten betrachten. Als Beispiele hierzu seien die nachfolgend unter (9) und (10) aufgeführten Bücher genannt. Einen Spezialfall stellt das Buch (11) dar. Es geht auf eine Idee des ungarischen Mathematikers Paul Erdös (1913-1996) zurück. Dieser sprach von einem Buch, genannt „The Book“, in dem Gott die schönsten und perfektesten aller mathematischen Beweise sammeln würde. Das Buch (11) enthält eine Folge von Beweisen aus verschiedenen mathematischen Bereichen, von denen die Autoren annehmen, dass sie in Gottes Buch aufgenommen würden.

- (9) A. Beutelspacher, Das ist o.B.d.A. trivial (5. Auflage), Vieweg Verlag, 1999.
- (10) G. Polya, Schule des Denkens. Vom Lösen mathematischer Probleme, Francke Verlag, 1980.
- (11) M. Aigner, G.M. Ziegler, Proofs from THE BOOK (3. Auflage), Springer Verlag, 1994.

Die in Abschnitt 5.1 eingeführten Klassen von Funktionen kommen praktisch in allen einführenden Mathematikbüchern vor und werden dort mehr oder weniger vertieft behandelt. Wesentlich ausführlicher wird der Stoff von Abschnitt 5.2 in Büchern über Mengenlehre behandelt, so auch in den oben angegebenen Büchern (1) und (2). Das Wachstum von

speziellen Funktionen im Hinblick auf den Aufwand von Algorithmen, den sie abschätzen, wird intensiv in Büchern über Algorithmik und Komplexitätstheorie behandelt. Ein Standardtext zur Algorithmik ist das folgende Buch (12). Nachfolgend haben wir noch ein weiteres Buch (13) angegeben, welches sich insbesondere mit der Lösung von sehr schweren Problemen durch spezielle Techniken beschäftigt.

- (12) T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, Introduction to Algorithms (3. Auflage), MIT Press, 2009.
- (13) J. Hromcovic, Algorithms for Hard Problems, Springer Verlag, 2001.

In eigentlich allen einführenden Mathematikbüchern werden auch Relationen ziemlich am Anfang relativ knapp eingeführt. Äquivalenzrelationen werden dann insbesondere in Büchern zur Algebra und zur Zahlentheorie vertieft. In beiden Bereichen spielt etwa die Modulo-Relation  $\equiv_m$  samt ihrer Verallgemeinerungen eine herausragende Rolle. In der Informatik sind in vielen Teilbereichen Ordnungsrelationen wesentlich wichtiger als Äquivalenzrelationen. Geordnete Mengen und wichtige Teilklassen, insbesondere Verbände, werden in den folgenden zwei Büchern (14) und (15) ausführlich behandelt.

- (14) B.A. Davey, H.A. Priestley, Introduction to Lattices and Orders (2. Auflage), Cambridge University Press, 2002.
- (15) R. Berghammer, Ordnungen, Verbände und Relationen mit Anwendungen (2. Auflage), Springer Vieweg, 2012.

Hinsichtlich gerichteter Graphen verweisen wir auf das folgende Buch (16) als vertiefende Literatur. Viele Teile der Graphentheorie überschneiden sich mit der diskreten Mathematik. Eine Einführung in dieses Gebiet stellt das nachfolgende Buch (17) dar. Auch in Büchern zum Thema Algorithmik, wie den oben unter (12) und (13) genannten, sind Graphen sehr populär, da viele der dort behandelten Algorithmen graphentheoretische Probleme lösen.

- (16) R. Diestel, Graphentheorie (4. Auflage), Springer Verlag, 2010.
- (17) M. Aigner, Diskrete Mathematik, Vieweg Studium, 1993.

Schon im 19. Jahrhundert wurde (u.a. von A. de Morgan und E. Schröder) versucht, Relationen algebraisch zu behandeln, also nicht mittels der objektbehafteten Beziehungen  $x R y$ , sondern nur unter Verwendung der auf ihnen definierten Operationen (wie Komposition, Vereinigung und Durchschnitt). Tarski führte, auf diese Arbeiten aufbauend, den Begriff einer (axiomatischen) Relationenalgebra ein. Dieser hat sich als sehr vorteilhaft für viele Gebiete sowohl der Mathematik als auch der Informatik erwiesen. Die Grundlagen der Relationenalgebra und eine Fülle von Anwendungen findet man beispielsweise im zweiten Teil des schon genannten Buchs (15) und auch in dem folgenden Buch.

- (18) G. Schmidt, Relational Mathematics, Cambridge University Press, 2011.

Hinsichtlich weiterführender Literatur zur Kombinatorik sei auf das folgende Buch verwiesen, sowie auf das schon erwähnte Buch (17) zur diskreten Mathematik. Wie bei der Graphentheorie überschneiden sich nämlich auch Teile der Kombinatorik mit der diskreten Mathematik.

- (19) M. Aigner, Kombinatorik I. Grundlagen und Zähltheorie, Springer Verlag, 1975.

Kombinatorik und Graphentheorie werden auch in der folgenden Einführung in die diskrete Mathematik ausführlicher als in dem vorliegenden Text behandelt.

- (20) A. Steger, Diskrete Strukturen 1: Kombinatorik, Graphentheorie (2. Auflage), Springer Verlag, 2007.

In den oben angegebenen Büchern (16) und (20) werden nicht nur gerichtete Graphen behandelt, sondern auch ungerichtete. Auch für diese Art von Graphen bietet insbesondere das Buch (16) eine Fülle weiterer Informationen und Resultate an. In Büchern zur diskreten Mathematik und zur Kombinatorik werden auch oft ungerichtete Graphen betreffende Fragestellungen diskutiert. Eine Behandlung von Graphen mittels relationaler Methoden findet man in (15) und (18).

Hinsichtlich weiterführender Literatur zum letzten Kapitel sind viele der nunmehr klassischen Algebra-Bücher geeignet. Nachfolgend geben wir jeweils ein solches Buch in Deutsch und Englisch an.

- (21) C. Karpfinger und K. Meyberg, Algebra: Gruppen – Ringe – Körper, Spektrum Akademischer Verlag, 2010.

- (22) S. Lang, Algebra, Springer Verlag, 2002.

Falls sich Leserinnen oder Leser für Details hinsichtlich der universellen Algebra interessieren, so kann das folgende klassische Werk immer noch empfohlen werden:

- (23) G. Grätzer. Universal Algebra, Van Nostrand, 1968.

Auch in Büchern über Verbandstheorie, Boolesche Algebra (einem wichtigen Teilgebiet der Verbandstheorie) und Modelltheorie (einem wichtigen Teilgebiet der Logik) findet man oft Bezüge zur und Resultate aus der universellen Algebra, ebenso in Informatik-Büchern zu den sogenannten Algebraischen Spezifikationen.

# Index

- $k$ -Teilmengen, 197  
Äquivalenz, 33  
Äquivalenzklasse, 152  
Äquivalenzrelation, 149
- Abelsche Gruppe, 227  
abgeschlossene Teilmenge, 243  
Absolutbetrag, 28  
Ackermann-Peter-Funktion, 169  
additive Gruppe, 231  
Allquantor, 33  
Anfangsknoten, 172  
angeordneter Körper, 268  
antisymmetrische Relation, 159  
arithmetischer Mittelwert, 88  
Assoziativgesetz, 226  
asymptotische Beschränkung, 141  
Außengrad, 172  
Aufzählungsform, 1  
Aussage, 2  
Aussagenlogik, 35  
Auswahlaxiom, 125  
Auswahlfunktion, 125
- Baum, 211  
Baumkonstruktion, 73  
Baumoperationen, 73  
Bedeutung der Junktoren, 37  
Beschreibungsform, 3  
Beschreibungsform mit Typisierung, 5  
Beweis durch Kontraposition, 84  
bijektive Funktion, 119  
Bildmenge, 122  
Binomialkoeffizient, 196  
Binomischer Lehrsatz, 201  
bipartites Pfeildiagramm, 116
- definierende Äquivalenz, 24  
definierende Gleichheit, 8  
deskriptive Mengenbeschreibung, 3  
deterministisches Transitionssystem, 267  
Digraph, 172  
direkter Beweis, 81  
direktes Produkt, 21  
Disjunktion, 33
- echt absteigende unendliche Kette, 168  
echte Teilmenge, 5  
eindeutige Relation, 24  
eineindeutige Beziehung, 121  
Eins-zu-Eins-Beziehung, 121  
Einschieben in Permutation, 192  
Einschränkungen von Operation, 243  
Einselement, 231  
Endknoten, 172, 203  
Endlichkeit, 17  
Enthaltenseinsrelation, 4  
erreichbar, 174  
Eulersche Polyederformel, 218  
Existenzquantor, 33  
explizite Darstellung, 1  
Exponentialfunktion, 138
- Fakultät, 189  
Fallunterscheidung bei Funktionen, 28  
Familie, 63  
Fibonacci-Zahl, 166  
Fixpunktsatz von Knaster, 82  
Folge, 63  
Formeln der Aussagenlogik, 35  
frei induktiv definiert, 77  
frei induktiv definierte Menge, 77  
freie Variable, 48  
Funktion, 25  
Funktionalität, 25  
Funktionsanwendung, 25  
Funktionsapplikation, 25  
Funktionskomposition, 118
- ganzzahlige Division, 157  
ganzzahlige Quadratwurzel, 84  
ganzzahliger dualer Logarithmus, 30  
gebundene Variable, 34  
geometrischer Mittelwert, 103  
gerichteter Graph, 172  
Gittergraph, 206  
Gleichheit von Binärbäumen, 73  
Gleichheit von Funktionen, 26  
Gleichheit von linearen Listen, 66  
Gleichheit von Mengen, 5  
Gleichheit von Paaren, 26

Gleichheit von Relationen, 26  
Gleichheit von Tupeln, 63  
größtes Element, 161  
größter gemeinsamer Teiler, 28  
graphentheoretische Kreislänge, 174  
graphentheoretische Weglänge, 174  
Gruppe, 227  
Gruppenhomomorphismus, 238  
Gruppenisomorphismus, 238

Höhe eines Binärbaums, 73  
Hüllensystem, 269  
Hasse-Diagramme, 20  
heterogene algebraische Struktur, 266  
homogene algebraische Struktur, 225  
Hypergraph, 222

identische Funktion, 118  
identische Relation, 149  
Identitätsprinzip von Leibniz, 115  
Implikation, 33  
indirekter Beweis, 83  
Indexmenge, 63  
Induktion über Baumhöhe, 98  
Induktion über Listenlänge, 98  
Induktion bei Bäumen, 98  
Induktion bei Graphen, 182  
Induktion bei Listen, 96  
Induktionsbeginn, 91  
Induktionsbeweis, 90  
Induktionshypothese, 91  
Induktionsschluss, 91  
Induktionsvoraussetzung, 91  
induktiv definiert, 76  
induktiv definierte Menge, 76  
Infimum, 163  
injektive Funktion, 115  
Inklusion, 5  
Innengrad, 172  
Inverse, 121  
inverses Element, 228

Körper, 234  
Kardinalität, 17  
Kardinalitätsvergleiche, 127  
kleinstes Element, 161  
Knotengrad, 203  
knotenmarkierter Binärbaum, 72

Knotenmenge, 172  
kommutative Gruppe, 227  
kommutativer Ring, 231  
Kommutativgesetz, 226  
komponentenweise Gleichheit, 63  
Kongruenz, 253  
Konjunktion, 33  
Kontraposition, 84  
Kreis, 174  
kreisfrei, 174  
Kreuzchentabelle, 24

Landau-Symbol, 142  
leere Liste, 64  
leere Menge, 6  
leere Relation, 113  
leerer Binärbaum, 72  
leeres Tupel, 64  
Lemma von Bezout, 256  
lineare Liste, 64  
lineare Relation, 159  
linker Teilbaum, 73  
Linksanfügen, 65  
Linksinverse, 119  
linksneutrales Element, 226  
Listenkonkatenation, 65  
Listenkopf, 65  
Listenlänge, 65  
Listenoperationen, 65  
Listenrest, 65  
Logarithmusfunktion, 138  
logische Äquivalenz, 38  
logische Implikation, 43

mathematische Formelsprache, 34  
maximales Element, 161  
mehrstellige Relation, 185  
Menge, 1  
Menge der Binärbaummarken, 73  
Mengendifferenz, 7  
Mengendurchschnitt, 7  
Mengengleichheit, 5  
Mengenkomplement, 9  
Mengensystem, 268  
Mengenvereinigung, 7  
metrischer Raum, 272  
minimales Element, 161  
Modulo-Relation, 155

Monoid, 226  
multiplikative Gruppe, 231  
  
Nachbar, 203  
Negation, 33  
neutrales Element, 226  
nichtleere Liste, 64  
Noethersche Induktion, 165  
Noethersche Ordnung, 164  
Nullelement, 231  
  
obere Schranke, 163  
Ordnung, 159  
Ordnungsdiagramm, 20  
  
Paar, 21  
Partition, 150  
Pascalschen Dreiecks, 199  
Permutation, 192  
Pfad, 178  
Pfeildiagramm, 24  
Pfeilrelation, 172  
planare linealische Graphzeichnung, 215  
planarer Graph, 216  
Polyeder, 214  
Potenzfunktion, 135  
Potenzierung in Monoiden, 226  
Potenzmenge, 15  
Prädikatenlogik, 44  
Primzahl, 46  
Produktstruktur, 249  
  
Quantoren mit typisierten Variablen, 35  
Quotientenstruktur, 253  
  
rechter Teilbaum, 73  
Rechtsinverse, 119  
rechtsneutrales Element, 226  
reflexiv-transitive Hülle, 177  
reflexive Relation, 149  
Regeln von de Morgan, 15  
Rekursion, 28  
Relation, 23  
relationale Komposition, 175  
relationale Struktur, 267  
relationales Datenbankmodell, 185  
Ring, 231  
Ringhomomorphismus, 240  
Ringisomorphismus, 240  
  
Satz von Cantor, 130  
Satz von Euklid I, 86  
Satz von Euklid II, 87  
Satz von Euklid III, 87  
Satz von Pascal, 196  
Satz von Schröder/Bernstein, 131  
Schubfachprinzip, 88  
Signatur, 225  
Spezifikation von Relationen, 24  
Stelligkeit einer Funktion, 61  
streng monoton, 116  
Striktordnung, 160  
Strukturhomomorphismus, 237  
Strukturisomorphismus, 237  
Summenformel von Gauß, 81  
Supremum, 163  
surjektive Funktion, 115  
symmetrische Relation, 149  
  
Teilbarkeitsrelation, 23  
teilerfremde Zahlen, 46  
Teilmenge, 5  
termerzeugte Menge, 77  
topologische Sortierung, 184  
totale Relation, 24  
Trägermenge, 225  
Transitionssystem, 186  
transitive Hülle, 177  
transitive Relation, 149  
Transposition von Relationen, 32  
Tupel, 59  
Tupeling von Funktionen, 249  
  
Umkehrfunktion, 121  
ungerichteter Graph, 202  
untere Schranke, 163  
Untergruppe, 244  
Unterring, 245  
Unterstruktur, 243  
Urbildmenge, 122  
  
Venn -Diagramm, 8  
Verband, 270  
verträgliche Funktionen, 237  
verträgliche Relation, 253  
Vertretersystem, 152  
vollständige Induktion, 91  
vollständiger Graph, 208

Vollständigkeitsaxiom, 268  
Wahrheitswerte, 36  
Wald, 211  
Weg, 174  
Wertigkeit einer Funktion, 61  
Widerlegen durch Gegenbeispiel, 90  
Widerspruchsbeweis, 85  
Wurzelfunktion, 137  
Wurzelmarkierung, 73  
  
Zahlenmengen, 4  
Zerlegung, 150  
Zermelo-Mengenkomprehension, 21  
zusammengesetzter Binärbaum, 72  
zyklische Gruppe, 247