



# Diskrete Mathematik

Vorlesung im 1. Fachsemester  
Wirtschaftsinformatik

Prof. Dr. Frank Zimmermann

4. Dezember 2014



# Inhaltsverzeichnis

<b>Danksagung</b>	<b>v</b>
<b>Festlegungen</b>	<b>vii</b>
<b>1 Einleitung</b>	<b>1</b>
1.1 Was ist Mathematik eigentlich? . . . . .	1
1.2 Die Sprache der Mathematik . . . . .	3
1.3 Warum muss ein Wirtschaftsinformatiker Mathematik lernen? . .	4
1.4 Was bedeutet Mathematik lernen? . . . . .	6
<b>2 Mengenlehre</b>	<b>9</b>
2.1 Naive Mengenlehre . . . . .	9
2.2 Mengenbegriff, Elemente . . . . .	11
2.3 Die leere Menge . . . . .	16
2.4 Mengengleichheit und Mengeninklusion . . . . .	18
2.5 Potenzmenge . . . . .	25
2.6 Mengenoperationen und Venn Diagramme . . . . .	27

---

2.7	Kartesisches Produkt . . . . .	34
2.8	Einige Rechenregeln für Mengen . . . . .	39
2.9	Naive und axiomatische Mengenlehre . . . . .	42
<b>3</b>	<b>Logik</b>	<b>45</b>
3.1	Aussagen und Aussageformen . . . . .	45
3.2	Allquantor . . . . .	52
3.3	Existenzquantor . . . . .	60
3.4	Negieren prädikatenlogischer Aussagen . . . . .	66
<b>4</b>	<b>Vollständige Induktion</b>	<b>69</b>
4.1	Peano Axiome . . . . .	69
4.2	Beweise mit vollständiger Induktion . . . . .	72
4.3	Definitionen mit vollständiger Induktion . . . . .	90
<b>5</b>	<b>Relationen</b>	<b>103</b>
5.1	Kartesisches Produkt . . . . .	104
5.2	Allgemeine Relationen und deren Darstellung . . . . .	108
5.2.1	Pfeildiagramme . . . . .	110
5.2.2	Matrixschreibweise . . . . .	111
5.2.3	vereinfachtes Pfeildiagramm . . . . .	111
5.3	Eigenschaften von Relationen . . . . .	118
5.4	Ordnungsrelationen . . . . .	129
5.5	Größte und Maximale Elemente, obere Schranken und Suprema .	136

---

5.6	Verbände . . . . .	146
5.7	Äquivalenzrelationen . . . . .	147
5.8	Restklassen . . . . .	151
5.9	Abbildungen . . . . .	152
<b>6</b>	<b>Algebraische Strukturen</b>	<b>159</b>
6.1	Verknüpfungen . . . . .	160
6.2	Restklassenoperationen . . . . .	167
6.3	Gruppen . . . . .	172
6.4	Restklassengruppen mit Multiplikation . . . . .	177
6.5	Untergruppen . . . . .	185
6.6	Isomorphismen . . . . .	194
6.7	Eine Anwendung aus der Kryptographie . . . . .	197
6.7.1	Grundlagen der Kryptographie . . . . .	197
6.7.2	Diffie Hellman Key Exchange . . . . .	198
6.7.3	Exponentieren durch wiederholtes Quadrieren . . . . .	201
	<b>Index</b>	<b>205</b>



# Danksagung

Vielen Dank an Dr. Röber, der diese Unterlagen über mehrere Jahre hinweg erweitert hat.

Besonderen Dank auch an alle Studenten, die mit viel Geduld Fehler in diesen Unterlagen gesucht und gefunden haben.





# Festlegungen

In dieser Arbeit werden folgende Konventionen benutzt:

Definitionen werden durch grüne Kästen hervorgehoben. Sie werden pro Kapitel nummeriert.

**DEFINITION:**

Definitionen sind das Rückgrat der Mathematik. In ihnen werden die Begriffe mit denen gearbeitet werden muss festgelegt. Jeder Satz und jeder Beweis nutzt sie.

**Definition 0.0.1**  
Definition

Sätze werden durch orangefarbene Kästen hervorgehoben. Sie werden pro Kapitel nummeriert.

**SATZ:**

Sätze sind der Muskel der Mathematik. In ihnen formuliert man die Erkenntnisse in knapper und allgemeiner Weise. Sie bringen die Kraft in die Mathematik.

**Satz 0.0.1** Satz

Beweise sind die Sehnen, die das Skelett mit dem Muskel verbinden. Ohne Sie sind die Muskeln nutzlos, und das Skelett bricht in sich zusammen.

Beispiele werden durch blaue Kästen hervorgehoben. Sie werden pro Kapitel nummeriert.

**Beispiel 0.0.1**

*Beispiele und Anwendungen stellen das Gewand dar, in dem sich uns die Definitionen und Sätze zu präsentieren. Sie sind die Grundlage für ein Verständnis von Schönheit und Sinn der Mathematik.*

Methodische Hinweise werden durch gelbe Kästen hervorgehoben. Sie werden nicht nummeriert.

Prinzip :  
*Prinzipien*

**PRINZIPIEN:**

Stellen das Gehirn dar. Sie Anzuwenden heißt Mathematik zu betreiben. Als methodische Hinweise bringen Sie den Körper der Mathematik eine wohlgeformte Bewegung.

Zur besseren Lesbarkeit werden keine geschlechtsspezifischen Begriffe verwendet. Die männliche Form steht für beide Geschlechter.

# Kapitel 1

## Einleitung

*“Mathematik ist das Alphabet, mit dessen Hilfe Gott das Universum beschrieben hat.”*

—Galileo Galilei (1564-1642), ital. Mathematiker, Physiker u. Astronom

### 1.1 Was ist Mathematik eigentlich?

(vgl. Alexander Ostrowski, Vorlesungen über Differential- und Integralrechnung) Es ist oft sehr schwer, den Gegenstand einer Wissenschaft genau zu umgrenzen. Dies liegt daran, dass eine Wissenschaft in der Regel ein ständig sich entwickelnder Organismus ist, für den häufig weniger der augenblickliche Zustand als die Entwicklungstendenzen charakteristisch sind.

Im Falle der Mathematik liegt die Sache insofern anders, als für die Mathematik weniger ihr Gegenstand, als vielmehr die Art des Schliessens charakteristisch ist. In der Schule wird unter Mathematik häufig Technik des Rechnens verstanden. Vektorrechnung und Infinitesimalrechnung werden erläutert, und es werden in den Klausuren vorher besprochene Rechenaufgaben abgefragt. Die Technik des Beweisens steht im Hintergrund, sie wird selten den Schülern abverlangt.

Mathematik ist das nicht. “Rechnen können” ist nicht das Ziel der Mathematik.

Es gibt drei Arten von Mathematikern:

1. Solche, die zählen können.
2. Solche, die nicht zählen können.

Offensichtlich lässt sich über den Autor dieser Aussage etwas schließen.

Eine wohl in den meisten Fällen zutreffende Charakterisierung der Mathematik ist die folgende:

Jedesmal, wenn man aus einem endlichen, übersichtlich dargestellten System von scharf formulierten Prämissen logisch einwandfreie Schlüsse zieht, treibt man Mathematik.

Dass hierbei die zu ziehenden Schlüsse logisch einwandfrei sind, bedeutet, dass sie sich in Ketten von Einzelschlüssen, sogenannten Syllogismen, lückenlos zerlegen lassen. Die Forderung, dass die Prämissen vollständig scharf formuliert worden sind, ist selbstverständlich, wenn man daraus logisch absolut gesicherte Schlüsse ziehen will. Schliesslich muss auf die Endlichkeit und daneben auf die übersichtliche Darstellung des Prämissensystems Wert gelegt werden, da nur in diesem Falle das exakte Schliessen prinzipiell und praktisch gesichert werden kann.

Insofern kann man nunmehr auch sagen, dass alles das Gegenstand der Mathematik ist, was sich auf endlich viele scharf formulierte Grundtatsachen zurückführen lässt. Solche Grundtatsachen nennt man **Axiome**. Eine derartige Zurückführung der Haupttatsachen eines Wissensgebietes auf endlich viele Grundtatsachen nennt man seine **Axiomatisierung**.

Die Axiome werden dabei als wahr angenommen, ihre Gültigkeit wird nicht hinterfragt. Die abgeleiteten Aussagen bezeichnet man als Sätze. Man spricht in diesem Zusammenhang auch von deduktivem Vorgehen.

Der Weg von den Axiomen zu den Sätzen ist der Beweis. Mathematische Beweise werden nicht mit den klassischen Beweismethoden 'Bestechung', 'Einschüchterung', 'Überredung' und 'Befehl' geführt (diese sind eher eine Domäne der Rechtsanwälte, Militärs oder der Manager). Die einzige gültige Methode ist es, mittels logischer Schlüsse zum gewünschten Ergebnis zu kommen. Dieses Ergebnis ist dann für jedermann, der sich die Mühe macht, die logischen Schlüsse nachzuvollziehen, ohne weitere Hilfsmittel einsehbar.

Es soll nicht verschwiegen werden, dass die mathematischen Schlüsse häufig recht kompliziert sind und ein hohes Maß an Abstraktionsvermögen erfordern.

Deshalb werden wir uns in diesen beiden Semestern auch nicht mit wirklich komplizierten Themen, sondern nur mit den Grundlagen und einigen einfachen Anwendungen beschäftigen. Ziel ist es, sicher zwischen Voraussetzung und Folgerung differenzieren zu können. Gerade diese Fertigkeit spielt eine wesentliche Rolle bei der wissenschaftlichen Arbeit in allen Fachgebieten, z.B. der Betriebswirtschaftslehre und der Rechtslehre. Allerdings ist das Fach Mathematik deutlich besser geeignet, sich logische Denkweise anzueignen, denn in der betrieblichen Praxis spielen häufig viele andere Faktoren eine Rolle als die reine Lehre.

Mathematik ist für viele andere Wissenschaften (z. B. Physik, Astronomie, Informatik, Geophysik, Meteorologie, Ozeanographie, Psychologie, Soziologie) eine Hilfswissenschaft. Sie stellt Beschreibungsmittel zur Verfügung, ermöglicht Modellbildung. Hier steht sie nicht im Vordergrund sondern stellt die Hilfsmittel bereit, um z. B. physikalische Phänomene zu beschreiben und daraus Schlüsse zu ziehen.

Die bedeutsame Rolle der Mathematik bei der systematischen Durchbildung verschiedener Wissenschaften gibt gelegentlich zu etwas übertriebenen Vorstellungen Anlass, so z. B., wenn unter Berufung auf Kant behauptet wird, in jedem Wissensgebiet stecke nur soviel Wissenschaft, als in ihm Mathematik stecke.

## 1.2 Die Sprache der Mathematik

Die Darstellung der Mathematik hat unter allen Umständen in erster Linie der Forderung lückenloser Exaktheit und Klarheit zu genügen, auch dann, wenn dabei eine gewisse stilistische Monotonie in Kauf genommen werden muss. Diese Darstellung muss so gründlich und ausführlich sein, dass Versehen und Fehler dabei ausgeschlossen sind. Es ist nur natürlich, dass die Umgangssprache, die zur Darstellung mathematischer Überlegungen benutzt wird, sich dazu nicht sehr gut eignet, da sie vom Volk, von den Dichtern und Schriftstellern vor allem für andere Zwecke ausgebildet und verfeinert wurde. Daher ist, sobald die „Flucht in die Formeln“ nicht ausreicht, das stilistische Problem für die Mathematik von einer gewissen Bedeutung. Denn eine sprachlich zu schwerfällige, nicht genügend elegante Darstellung ist wenig einprägsam, also schwer zu verstehen und zu behalten.

Trotzdem ist auf die Eleganz bei der mathematischen Darstellung erst in zweiter Linie Rücksicht zu nehmen. Niemals darf die Klarheit der Eleganz geopfert werden. So ist das bekannte Scherzwort zu verstehen, man „solle die Eleganz Sache der Schuster und Schneider sein lassen.“

Eine der häufigsten Fehlerquellen beim Schliessen (beweisen) in der Mathematik liegt im falschen Gebrauch von Definitionen. Eine mathematische Definition muss restlos klar und eindeutig sein, sonst ist sie zum exakten Schliessen unbrauchbar. Es darf aus ihr auch nie mehr heraus gelesen werden, als ihrem exakten Wortlaut entspricht.

Besonders gefährlich sind Begriffe, die zugleich auch im täglichen Leben benutzt werden; denn in einen solchen Begriff legt man leicht nicht nur das hinein, was in der genauen Definition steckt, sondern auch manches, was der etwas vagen, landläufigen Bedeutung des betreffenden Wortes entspricht. Dies ist auch der Grund, warum man sich zur Bezeichnung neu eingeführter Begriffe gern der Fremdwörter oder eigens geprägter Wörter bedient. Die Notwendigkeit, auch gegenüber den zunächst als selbstverständlich erscheinenden Dingen misstrauisch zu sein und sich mit ihnen ausführlich auseinanderzusetzen, bedingt leicht eine Geisteshaltung, die als pedantisch wirkt. Insofern könnte man die Pedanterie als eine „Berufskrankheit der Mathematiker“ bezeichnen. Dennoch vergesse man nie: **Pedantisch scheinen mag peinlich sein, unklar sein aber ist verboten!**

### 1.3 Warum muss ein Wirtschaftsinformatiker Mathematik lernen?

1. Schulung in Prädikatenlogik, um das Erfassen von quantitativen Zusammenhängen zu üben. Solche Zusammenhänge sind:

- die Grundlage der Datenbankmodellierung.  
Eine professionelle Datenbankgestaltung, -dieses Problem ist sicherlich ein zentrales für die Wirtschaftsinformatik- hat zur Grundlage die Fähigkeit, die Realität zu erfassen, von ihr zu abstrahieren und sie modellhaft darzustellen. Dieses setzt einerseits gute kommunikative Kenntnisse voraus, denn nur wer in der Lage ist, mit einem Anwender zu sprechen, wird sich dessen Problemen annehmen können. Andererseits allerdings kann ein tragfähiges Abbild der Realität nur dann gefunden werden, wenn abstrahierte Objekte identifiziert und deren funktionale Abhängigkeiten erkannt werden.
- der Unterschied zwischen „trial and error“ Programmierung und systematischer Programmentwicklung.
- die Grundlage, um (systematisches) Testen zu ermöglichen. Das exakte Formulieren von mathematischen Aussagen und das Verstehen von Bedingungen, unter denen Programme funktionieren, sind verwandte Problemstellungen.

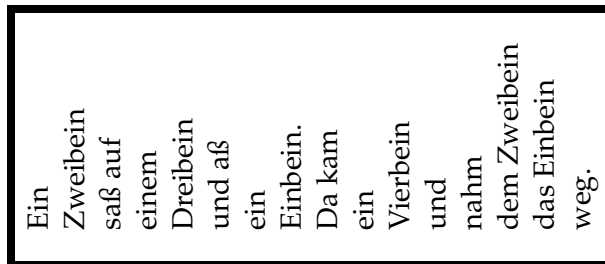
2. Algorithmische Betrachtungsweise von Sätzen, um den Zusammenhang zur Programmierung herzustellen.

Hier sind insbesondere folgende Fragestellungen zu adressieren:

- Es gibt Probleme, die sind durch Algorithmen gar nicht lösbar. Beispiel einer Fragestellung: Hat ein gegebenes Programm Endlosschleifen? Diese auf den ersten Blick einfach anmutende Fragestellung ist der klassische Fall einer nicht berechenbaren Eigenschaft.
  - Es gibt Probleme, die sind nur äußerst ineffizient durch Algorithmen lösbar. Zu dieser Fragestellung gibt es sehr viele unterschiedliche Betrachtungsweisen. Angefangen vom Problem des Handlungsreisenden, der einen optimalen Reiseweg zu allen seinen Kunden sucht, über Funktionen, wie die Ackermann'sche Funktion (Wilhelm Ackermann, Schüler Hilberts, definierte 1928 die nach ihm benannte rekursive Funktion  $\text{ack}(n,m)$ ), die so stark wächst, dass sie mit praktischen Mitteln nicht mehr berechnet werden kann, bis hin zu Verschlüsselungstechnischen Ansätzen, bei denen die nicht-praktische-Berechenbarkeit ganz kalkuliert eingesetzt wird.
  - Es gibt Probleme, die sind gut lösbar, allerdings gibt es auch (naheliegende) schlechte Lösungen.
3. Beschäftigung mit vollständiger Induktion, um rekursives/iteratives Denken, wie es in der Programmierung häufig verwendet wird, zu schulen. Im Prinzip ist die Funktionsweise der vollständigen Induktion nichts anderes als die Funktionsweise einer „for-Schleife“. Die Reduktion auf das Vorhergehende. Induktionsbeweise haben den Vorteil, dass sie häufig starr nach einem Schema ablaufen und deshalb sehr geeignet sind, den Anfänger in die Technik des Beweisens einzuführen.
  4. Das abstrakte Gedankengebäude der Zahlen-/Gruppentheorie kann in der Anwendung einiger Verschlüsselungsverfahren praxisnah vermittelt werden. Gerade hier können mathematische Grunddenkweisen auf spannende und aktuelle Weise vermittelt werden. Durch die Verbreitung des Internets haben Verschlüsselungstechniken einen aktuellen Bezug. Fast jeder, der dieses Medium nutzt, musste sich schon einmal mit diesem Thema auseinandersetzen. Das Faszinierende an dem Thema ist, dass schon recht einfache Techniken ausreichen, um die grundlegenden Techniken der Verschlüsselungstechnik zu verstehen. Viel mehr als ganzzahlige Division mit Rest und ein paar Eigenschaften davon ist eigentlich nicht erforderlich.
  5. Das Gebiet der Logik ist von je her mit dem Gebiet der Informatik eng verbunden.

## 1.4 Was bedeutet Mathematik lernen?

„Mathematik lernen“ kann „Mathematik verstehen“ nicht ersetzen. Ein Beispiel aus dem Buch: Stroh im Kopf? von Vera F. Birkenbihl soll das verdeutlichen. Nehmen Sie vor dem Weiterlesen bitte erst einen Zettel und einen Bleistift zur Hand. Kugelschreiber oder ein anderes Schreibgerät tun es natürlich auch. Lesen Sie den folgenden Text bitte dreimal durch und versuchen Sie dann, den Text aus dem Kopf auf den Zettel zu schreiben.



Ein  
Zweibein  
saß auf  
einem  
Dreibein  
und aß  
ein  
Einbein.  
Da kam  
ein  
Vierbein  
und  
nahm  
dem Zweibein  
das Einbein  
weg.

Haben Sie die Aufgabe geschafft? Wenn ja, dann haben Sie das nur schaffen können, wenn Sie verstanden haben, dass unter 'Zweibein' ein Mensch, unter 'Dreibein' ein dreibeiniger Schemel, unter 'Einbein' ein Hühnerbein und unter 'Vierbein' ein Hund verstanden werden kann.

Ohne dieses Verständnis werden Sie wahrscheinlich Stunden brauchen, um diesen Satz auswendig zu lernen. Und Sie werden den Satz in Stunden vergessen haben. Würde Sie jemand in einer Prüfung nach diesem Satz fragen, überfielen Sie aufgrund der Stresssituation sicherlich beim Rezitieren Zweifel: Wird nun das Zweibein, das Dreibein oder das Vierbein zum Schlagen benutzt? Und wenn der Prüfer nun direkt nach diesem Sachverhalt fragt? Sie haben den Text im Zusammenhang auswendig gelernt. Was für ein gemeiner Prüfer, der sich solch fiese Fragen ausdenkt! Da haben Sie nun so viele Stunden gelernt und fallen trotzdem durch die Prüfung.

Haben Sie aber das Bild vom Menschen und dem Hund im Kopf, dann werden Sie diesen Satz nach höchstens dreimaligen Lesen problemlos wiedergeben können. Sie haben nicht das Gefühl, den Satz auswendig gelernt zu haben. Und trotzdem, wenn Sie jemand in einem halben Jahr fragt, wie der Text geht, werden Sie ohne Nachzudenken korrekt antworten. Und die Prüfungsfragen werden Ihnen leicht und harmlos erscheinen.

Mit mathematischen Sätzen ist es genauso wie mit dem obigen Satz. Man muss sie verstehen und nicht lernen. Wer verstanden hat, braucht nicht zu lernen. Und



wer versucht, auswendig zu lernen, wird „hoffnungslos“ verloren sein. Er wird noch so viele Stunden lernen können, jede kleine Variation der Fragestellung wird ihn aus dem Gleis werfen.

Was nun, wenn ein amöbenhaftes Geistwesen vom Stern Aldebaran versucht, diesen Satz zu lernen? Dieses Wesen wird nicht wissen, was Beine sind. Was würden Sie diesem Wesen empfehlen? Soll es auswendig lernen, oder soll es sich mit der „Theorie der Beine“ auseinandersetzen? Um die Theorie der Beine zu verstehen, wird er sich wahrscheinlich mit für ihn neuen Lebensformen auseinandersetzen müssen. Ich bin der Meinung, das Wesen tut gut daran, sich auch mit anderen Welten auseinanderzusetzen und andere Bewegungsformen kennenzulernen. Auch wenn dieser Ansatz zunächst nach wesentlich mehr Arbeit aussieht, ist doch der Gewinn ungleich höher.

Was lernen Sie aus dieser Betrachtung? Versuchen Sie nicht, große Energie in das Auswendiglernen von Sachverhalten zu stecken. Diese Energie ist verschwendet. Versuchen Sie dagegen, die Sachverhalte zu verstehen. Und wenn Sie die Grundbegriffe nicht parat haben, wie die Amöbe, die keine Beine kennt, tun Sie gut daran, sich zunächst einmal mit den Grundbegriffen ernsthaft auseinanderzusetzen.

Die Frage, wann man einen mathematischen Zusammenhang verstanden hat, ist schwerer zu beantworten als es auf den ersten Blick scheint. Es gibt sicherlich unterschiedliche Ebenen des Verstehens.

„Verstehen“ bedeutet nicht immer dasselbe. Man versteht z. B. eine mathematische Regel 1. wenn man sie anwenden kann oder 2. wenn man ihre Herleitung in allen Teilen überprüft hat oder 3. wenn man ihren Beweis selbständig wiederfinden kann.

Erst auf der dritten Stufe kann man von „verstehen“ im eigentlichen Sinne sprechen. In der Schule reicht es aus, einen Rechenweg einschlagen und nachvollziehen können. Für die Praxis scheint mir diese Stufe aber nicht ausreichend. Gerade die Wirtschaftsinformatik ist ein Gebiet, das einer sehr schnellen Entwicklung unterworfen ist. Techniken, die gestern aktuell und modern waren, sind heute überholt, veraltet und nicht mehr an den „Mann“ zu bringen. Techniken also, die bloß nachvollzogen werden, sind innerhalb eines Zeitraums von 5 Jahren veraltet.

Wir müssen mehr als nur Wissen vermitteln. Wir müssen die Voraussetzung schaffen, Wissen aufzunehmen. Verstehen bedeutet also auch, selber in der Lage zu sein, sich Sachverhalte des Themengebiets zu erarbeiten und Fragestellungen des Themengebiets zu beantworten. Eine noch ehrgeizigere Definition von „Verstehen“ habe ich von einem Hochenergiephysiker:

„Eine Sache zu verstehen, heißt, sie seiner Großmutter erklären zu können.“

Warum ich das sage? Ich möchte Sie darauf hinweisen, dass man selbst häufig nicht weiß, dass man eine Sache nicht (ausreichend) verstanden hat. Mathematische Sachverhalte müssen sorgfältig durchdacht werden, und häufig hat man erst nach Jahren eine Erleuchtung: Aha, darum ist das also so. Mich hat einmal ein sehr brillanter Mathematiker (Michelle Talagrand, der später mit der Fields Medallie, dem Nobelpreis für Mathematiker, ausgezeichnet wurde) mit der Aussage beeindruckt: „Ich habe 6 Jahre gebraucht, um das und das zu verstehen.“ Sein Level des Verständnisses war um Klassen größer als das meine. Übrigens neigte der Mann nicht zum Understatement.

myMethBox100% RegelGeben Sie sich nicht mit „zuwenig“ Verständnis zufrieden. In der Mathematik gibt es keine 80/20 Regel. 20 % nicht verstanden, heißt gar nicht verstanden. Eine logische Kette ist so stark wie ihr schwächstes Glied.

Bleibt noch die häufig gestellte Frage zu klären: „Wozu all das? Warum muss sich ein angehender Wirtschaftsinformatiker durch all diese Sachen quälen?“ (Erfahrungsgemäß ist Mathematik für so manchen Studenten eine Quälerei, ich weiß das.) Nun, im zweiten Abschnitt habe ich versucht, den praktischen Bezug herzustellen. Wem das nicht reicht, für den habe ich nur die folgende Geschichte:

Euklid wurde 330 v. Chr. geboren. Wie Phythagoras (ca. 580-500 v. Chr., der erste „richtige“ Philosoph und Mathematiker) glaubte er an die Suche nach der mathematischen Wahrheit um ihrer selbst Willen und kümmerte sich nicht um praktische Anwendungen seiner Arbeit. Einer Anekdote zur Folge fragte ihn einmal ein Student, was ihm denn die Mathematik nütze, die er lerne. Am Schluss der Vorlesung wandte sich Euklid einem Sklaven zu und befahl: „Gebt dem Jungen eine Münze, da er doch aus allem, was er lernt, Nutzen ziehen will.“ Der Student wurde ausgeschlossen.

## Kapitel 2

# Mengenlehre

*“Aus dem Paradies, das Cantor uns geschaffen hat, soll uns niemand vertreiben können.”*

—David Hilbert 1925, dt. Mathematiker

### 2.1 Naive Mengenlehre

Die Mengenlehre ist durch Georg Cantor (dt. Mathematiker 1845-1918) begründet worden. Sie hat durch ihre Begriffsbildungen, die ihr innewohnenden Ideen und die in ihr enthaltene Problematik fast alle Teile der Mathematik neu befruchtet oder gar zu neuen Disziplinen geführt. Als Beispiele seien genannt die neuere Theorie der reellen Funktionen, die Topologie, die Funktionalanalysis, die moderne Algebra. Sie hat aber auch über die Mathematik hinaus der wissenschaftlichen Logik und Erkenntnistheorie neue Impulse gegeben.

In der Informatik ist die Mengenlehre die zentrale Beschreibungssprache, die immer dann verwendet wird, wenn es um präzise Formulierung von Zusammenhängen geht. Somit ist die Mengenlehre aus der Wissenschaft Informatik nicht wegzudenken.

Im gewöhnlichen Leben denkt man bei einer Menge von Dingen immer nur an endlich viele und zwar mindestens zwei Dinge. In der Mengenlehre wird der Begriff weiter gefasst.

**Definition 2.1.1**  
Naiver  
Mengenbegriff

**NAIVER MENGENBEGRIFF:**

Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.

Selbstverständlich hat Cantor die Worte in dieser Definition wohl überlegt gewählt.

Bemerkung 1: So spricht er von „bestimmten“ Objekten. Damit sagt er aus, dass die Elemente einer Menge festgelegt sein müssen. Für eine Menge muss festliegen, welche Elemente sie hat, und welche nicht. Zum Einen muss also gefordert werden, dass die Elemente nicht eine diffuse Definition besitzen (z. B. die Wassertropfen in einem See oder die Träume des Zeus) und zum Zweiten, dass festgelegt sein muss, ob ein Objekt in der Menge ist oder nicht. Ein „bisschen Element“ einer Menge zu sein, geht nicht.

Bemerkung 2: Wenn von „wohlunterschiedenen“ Elementen gesprochen wird, so bedeutet das, dass Elemente in einer Menge nicht mehrfach vorkommen. Je zwei Elemente einer Menge unterscheiden sich voneinander.

Bemerkung 3: Cantor gibt keine Einschränkungen über die Anzahl der Elemente der Zusammenfassung an. Die Definition lässt es auch zu, weniger als zwei Elemente (also ein oder gar kein Element) „zusammenzufassen“. Insbesondere die Möglichkeit, auch gar kein Element zur sogenannten leeren Menge zusammenzufassen, wird uns im Folgenden noch etwas beschäftigen. Es sind aber auch Zusammenfassungen von unendlich vielen Elementen denkbar. In der Tat stellt sich diese Möglichkeit als eine der fruchtbarsten Eigenschaften der Mengenlehre heraus. Cantor gelingt es aus historischer Sicht zum ersten mal, mit seinem Mengenbegriff die Unendlichkeit zu zähmen und sogar das Rechnen im Unendlichen zu ermöglichen. Da aber die Informatik nicht besonders erfolgreich beim Verarbeiten von „unendlichen“ Mengen ist, wird uns dieser Teil der Theorie nicht weiter begegnen.

Bemerkung 4: In dem Begriff „Zusammenfassung“ wird aber auch ausgedrückt, dass Reihenfolge auch bei mehr als zwei Elementen keine Rolle spielt. Er schreibt eben nicht Auflistung oder Reihung sondern Zusammenfassung.

Bemerkung 5: Die Zusammenfassung zu einem „Ganzen“, die die Menge darstellt, ist als neues Objekt unseres Denkens zu verstehen. Dies bedeutet auch, dass ein Objekt unserer Anschauung oder unseres Denkens verschieden von der Zusammenfassung anzusehen ist, die aus diesem einen Objekt gebildet wird.

**Beispiel 2.1.1**

1. *Man kann aus den Informatikdozenten der Nordakademie eine Menge bilden. Sie enthält die Objekte unserer Anschauung: Brauer, Schröder und Zimmermann. Diese Objekte sind bestimmt, und man kann sie auch von anderen Objekten unterscheiden. Alle diese anderen Objekte sind nicht in dieser Menge.*
2. *Wir können aus den ersten vier natürlichen Zahlen (also 1,2,3,4 ) eine Menge bilden. Bei natürlichen Zahlen handelt es sich um Objekte unseres Denkens, die eindeutig definiert sind und die von anderen Objekten unseres Denkens unterschieden werden können.*
3. *Eine Menge aus Glaube, Liebe und Hoffnung zu machen ist problematisch. Es handelt sich zwar um Begriffe unseres Denkens, jedoch sind diese metaphysischen Begriffe nicht wirklich präzise definiert (Mögen die Theologen diesen Frevel bitte entschuldigen).*
4. *Aus den Wassertropfen der Weltmeere eine Menge zu bilden, ist problematisch, nicht weil es sehr viele wären, sondern weil schwierig festzulegen ist, was einen Wassertropfen der Weltmeere ausmacht.*

**2.2 Mengenbegriff, Elemente****MENGEN- UND ELEMENTBEGRIFF:**

Es sei  $M$  eine Menge, also eine Zusammenfassung von bestimmten wohl unterschiedenen Objekten. Diese Objekte heißen Elemente der Menge. Ist  $x$  ein Element der Menge  $M$ , so schreibt man:

$$x \in M .$$

Man schreibt

$$x \notin M ,$$

falls  $x$  nicht ein Element von  $M$  ist.

**Definition 2.2.1**  
Mengen- und  
Elementbegriff

Ist  $x$  ein Element der Menge  $M$ , so sagt man auch manchmal, dass  $x$  in  $M$  **enthalten** ist oder dass  $x$  **aus**  $M$  ist.

**Beispiel 2.2.1** Erste Beispiele für Mengen

- $\mathbb{N}$  die Menge der natürlichen Zahlen  $1, 2, 3, 4, \dots$

*In diesem Beispiel haben wir es offensichtlich mit Objekten unseres Denkens zu tun. Diese Menge zu betrachten ist sehr nützlich, wenn man Mathematik betreiben möchte. Man kann in dieser Menge zum Beispiel die Rechenoperationen  $+$  und  $\cdot$  definieren.*

- Menge aller Computer im Intranet der Nordakademie.

*Offensichtlich eine Menge mit Objekten unserer Anschauung. In der Praxis dürfte diese Menge schwer zu bestimmen sein, da sie sich mit der Zeit sehr schnell ändert. Streng genommen können wir sogar nur dann von einer Menge sprechen, wenn der Zeitpunkt festgelegt ist. Etwa durch Festlegen des Zeitpunkts auf einen bestimmten Tag und Uhrzeit (Mo. 9.1.2006 12:00:00,0000). Diese Menge zu betrachten, kann nützlich sein, wenn man sich zum Beispiel Gedanken über die Verbindungen im Intranet machen möchte.*

- Menge aller Studenten in Ihrer Centurie.

*Wieder eine Menge mit Objekten unserer Anschauung. Auch diesmal ist die Menge nur dann sinnvoll definiert, wenn klar ist, zu welchem Zeitpunkt die Menge betrachtet werden soll. Also etwa dann, wenn Sie diesen Text lesen. Des weiteren wird von Ihrer Centurie geredet. Hier hängt die Menge von dem Betrachter ab. Das ist unschön. Für mich als Professor der Nordakademie zum Beispiel macht diese Definition gar keinen Sinn. Hier wäre es besser, die Centurie über Ihre Kennung zu identifizieren, z.B. Studenten der I05a am 9.1.2006. Sinnvoll kann eine Betrachtung dieser Menge dann sein, wenn man ein System zur Verwaltung der Studenten der Nordakademie entwerfen möchte. Sie kann helfen, die Eigenschaften des zukünftigen Systems zu beschreiben.*

Wie Sie an den obigen Beispielen sehen, fällt es gar nicht so leicht, eine gute Definition für eine konkrete Menge anzugeben. In der Informatik (und der Mathematik) gibt es zwei unterschiedliche Möglichkeiten, Mengen festzulegen:

## 1. Aufzählung der Elemente

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

beschreibt die Menge der ersten vier natürlichen Zahlen. Bitte beachten Sie, dass die geschweiften Klammern in der Mathematik als Begrenzer für Mengen reserviert sind.

Wichtig ist dabei:

- Es kommt nicht auf die Reihenfolge an:  $\{1, 2, 3, 4\} = \{4, 3, 2, 1\}$
- Elemente werden nur einmal genannt:  $\{1, 1\}$  ist keine erlaubte Schreibweise. Statt dessen schreiben wir nur  $\{1\}$ .

## 2. Angabe einer definierenden Eigenschaft

- $\{x \mid x \text{ ist eine natürliche Zahl} < 5\}$

Gesprochen wird dieser Ausdruck wie folgt: Menge aller  $x$ , für die gilt:  $x$  ist eine natürliche Zahl  $< 5$ .

Bemerkung 6: In dieser Schreibweise verwendet man eine Laufvariable, im Beispiel ist es die Laufvariable  $x$ , und eine Eigenschaft, in der die Laufvariable vorkommt, im Beispiel „ $x$  ist eine natürliche Zahl  $< 5$ “. Die durch die obige Schreibweise definierte Menge enthält nun genau die Objekte  $x$  unserer Anschauung oder unseres Denkens, für die die Eigenschaft zutrifft. Die Laufvariable  $x$  durchläuft also alle Objekte unserer Anschauung und unseres Denkens, und immer wenn die definierende Eigenschaft auf das durchlaufene Objekt zutrifft, ist dieses Objekt Element der Menge. Dies soll durch die folgende (selbstverständlich nicht vollständige) Tabelle verdeutlicht werden:

$x$	$x$ ist eine natürliche Zahl $< 5$	in der Menge
1	wahr	ja
2	wahr	ja
3	wahr	ja
4	wahr	ja
5	wahr	nein
6	falsch	nein
10	falsch	nein
0	falsch	nein
-1,3	falsch	nein
Helmut Kohl	falsch	nein
Bo Derek	falsch	nein

Bitte beachten Sie, dass die Laufvariable  $x$  ausserhalb der Mengenklammern keinen Sinn macht. Wie bei einer Programmiersprache ist es in der Mathematik auch üblich, Variablen zu deklarieren, bevor man sie anwendet. In diesem Sinn ist die Verwendung von  $x$  vor dem senkrechten Strich die Deklaration der Laufvariablen. Diese deklarierte Variable darf dann von dem senkrechten Strich  $|$  bis hin zur schließenden Mengenklammer  $\}$  genutzt werden. An anderen Stellen ist Laufvariable nicht deklariert, man sagt, sie sei **ungebunden**, und ist ungültig.

Als definierende Eigenschaft ist jede „vernünftige“ Eigenschaft zugelassen. Wie diese Eigenschaften aufgebaut sind, werden wir im Kapitel über Prädikatenlogik genauer beschreiben.

**Beispiel 2.2.2** Beim Angeben einer definierenden Eigenschaft sollte man immer darauf achten, dass die Laufvariablen korrekt gebunden sind. Mengenbildungen, bei denen die Laufvariablen falsch verwendet werden, sind sinnlos. Leider gibt es in der Mathematik keinen Compiler, der solche Fehler deutlich macht. Hier ist die Aufmerksamkeit des Autors gefragt.

1.  $\{x|x \text{ ist Informatik Dozent an der Nordakademie}\}$  ist sinnvoll.
2.  $\{x|x \text{ ist Dozent an der Nordakademie}\}$   $x$  arbeitet im Informatikbereich. Dies ist fehlerhaft, weil die Variable  $x$  außerhalb der Mengenklammern benutzt wird.
3. Sei  $x$  ein Dozent der Nordakademie.  $\{x|x \text{ arbeitet im Informatikbereich}\}$ . Dies ist genauso fehlerhaft, weil die Variable  $x$  außerhalb der Mengenklammern benutzt wird.
4.  $\{x| \text{ Informatik Dozent an der Nordakademie}\}$ . Ist fehlerhaft, da die Laufvariable gar nicht verwendet wird.
5.  $\{x|x \text{ ist Informatik Dozent an der } y\}$ . Ist fehlerhaft, weil eine zweite Variable verwendet wird, die nirgendwo festgelegt wird.

**Beispiel 2.2.3** Beispiele von Mengen und Elementen

- $1 \in \{1, 2, 3, 4\}$
- $5 \notin \{x \in \mathbb{N} | x < 5\}$
- $2 \in \{x \in \mathbb{N} | x \text{ ist gerade Primzahl}\}$
- $\text{Müller} \notin \{\text{Brauer, Schröder, Zimmermann}\}$

Bemerkung 7: Sehr häufig stammen die Elemente einer Menge, die durch eine definierende Eigenschaft festgelegt wird, schon aus einer anderen Menge. So ist im Beispiel  $\{x|x \text{ ist natürliche Zahl} < 5\}$  von natürlichen Zahlen die Rede und nur natürliche Zahlen werden zugelassen. Um diese etwas umständliche Schreibweise zu vereinfachen schreibt man die Basismenge auch sehr häufig in die „Deklaration“ der Laufvariablen  $x$ :  $\{x \in \mathbb{N} | x < 5\}$ .



Eine der Stärken der Mengenlehre besteht darin, dass Mengenbildung geschachtelt angewendet werden kann: **Mengen können als Elemente wieder Mengen enthalten**. Laut der Definition von Cantor sind Mengen ja wieder Objekte unseres Denkens und können als Elemente in Mengen auftauchen.

**Beispiel 2.2.4** *Beispiele von Mengen mit Mengen*

- $1 \notin \{\{1, 2\}, \{3, 4\}\}$
- $1 \in \{1, \{1, 2\}\}$
- $\{1, 2\} \in \{1, \{1, 2\}\}$

**Aufgabe 2.1:**

Welche der folgenden Mengen ist korrekt definiert:

1.  $\{x | x \text{ ist natürliche Zahl} \geq 1\}$
2.  $\{x | \text{Marsmännchen} \}$
3.  $\{x | x \text{ ist Marsmännchen} \}$
4.  $\{x \in \mathbb{N} | x^2 + 1 > 0\}$

**Aufgabe 2.2:**

Welche der Aussagen ist richtig?

1.  $\{1\} \in \{1, 2, 3, 4\}$
2.  $\{5\} \notin \{x | x \text{ ist natürliche Zahl} < 5\}$
3.  $2 \in \{x | x \text{ ist gerade Primzahl}\}$
4.  $\text{Brauer} \in \{x | x \text{ ist Informatik Dozent an der Nordakademie}\}$
5.  $\{2, 3\} \in \{\{1, 2\}, \{3, 4\}\}$
6.  $2 \in \{\{1, 2\}, \{3, 4\}\}$

## 2.3 Die leere Menge

Für uns ist es heute selbstverständlich, mit der Null wie mit jeder anderen Zahl zu rechnen.

Die wirkliche Entwicklung war komplizierter, die Null wurde als gleichberechtigte Zahl erst zum Ende des Mittelalters anerkannt. Der deutsche Mathematiker Adam Ries hat durch Untersuchung der existierenden Zahlensysteme herausgearbeitet, dass die Römischen Ziffern für die Schematisierung der Grundrechenarten eine große Hemmschwelle darstellen und gab stattdessen den arabischen Ziffern den Vorzug. Ries erkannte, dass durch das Fehlen der Null eine tabellarische Addition und Subtraktion mit Römischen Ziffern wesentlich erschwert wurde. Im Weiteren zeigte er, dass sich auch die Subtraktionsschreibweise der Römischen Ziffern als sehr störend für eine geordnete, formalisierte Verarbeitung auswirkte. Mit der Etablierung von neuzeitlichem Fn auf Basis der arabischen Ziffern läutete er somit zugleich das Ende der Nutzung von Römischen Ziffern im Alltagsleben ein.

Die Einführung der 0 kann also als ein Meilenstein der kulturellen Entwicklung der Menschheit betrachtet werden. Ihre Einführung, obwohl mit einer zunächst „schwierigen“ Abstraktion verbunden, ermöglicht eine starke Vereinfachung des Umgangs mit Zahlen.

Ähnlich verhält es sich in der Welt der Mengen. Es stellt sich als besonders nützlich heraus, eine Menge ohne Elemente einzuführen.

**Definition 2.3.1**  
Leere Menge

**LEERE MENGE:**

Die Menge, die keine Elemente enthält, heißt **leere Menge**. Sie wird mit  $\emptyset$  oder mit  $\{\}$  bezeichnet.

Bitte beachten Sie, dass die leere Menge zwar keine Elemente zusammenfasst, aber trotzdem als Zusammenfassung ein Objekt darstellt. **Die leere Menge enthält zwar nichts, ist aber selbst nicht Nichts.** Das Ignorieren dieses Zusammenhangs führt häufig zu Missverständnissen und Fehlern.

**KEINE SCHLÜSSE MIT NICHTS:**

Unvorsichtiges Schließen mit dem Begriff „Nichts“ führt zu widersinnigen Resultaten:

- Für den Durstigen ist jedes Getränk besser als nichts.
- Nichts ist besser als Milch.
- Da jedes Getränk besser als nichts und nichts besser als Milch ist, muss auch jedes Getränk besser als Milch sein.

Die letzte Aussage widerspricht aber der zuvor gemachten Aussage, dass nichts besser als Milch ist, ein offensichtlicher Fehlschluss.

In der Mathematik vermeidet man den Umgang mit dem Begriff „Nichts“.

Prinzip :  
*Keine Schlüsse  
mit Nichts*

**Beispiel 2.3.1** Aussagen mit der leeren Menge

- Für jedes Objekt  $x$  unserer Anschauung oder unseres Denkens ist  $x \in \emptyset$  falsch.
- Für jedes Objekt  $x$  unserer Anschauung oder unseres Denkens ist  $x \notin \emptyset$  wahr.
- $1 \in \emptyset$  ist falsch.
- $0 \in \emptyset$  ist falsch.
- $\emptyset \in \emptyset$  ist falsch.
- $\{\emptyset\}$  ist eine Menge mit einem Element, also von  $\emptyset$  verschieden.
- $\emptyset \in \{\emptyset\}$  ist wahr.
- $\emptyset \notin \emptyset$  ist wahr.
- $\text{TokioHotel} \notin \emptyset$  ist wahr.

## 2.4 Mengengleichheit und Mengeninklusion

**Definition 2.4.1**  
Gleichheit von  
Mengen (Exten-  
sionalitätsprinzip)

### GLEICHHEIT VON MENGEN (EXTENSIONALITÄTSPRINZIP):

Zwei Mengen  $M_1$  und  $M_2$  heißen „gleich“, (genau dann) wenn sie die gleichen Elemente enthalten.

Mit anderen Worten:

1. Jedes Element von  $M_1$  ist Element von  $M_2$ .
- und**
2. Jedes Element von  $M_2$  ist Element von  $M_1$ .

Die Eigenschaft der Mengengleichheit wird durch die Definition 2.4.1 sehr griffig formuliert. Trotzdem muss vor der Arbeit mit der Formulierung „wenn sie die gleichen“ gewarnt werden, weil sie zu viel Komplexität verbirgt. Wie man an der zweiten Formulierung erkennt, kann diese Aussage in zwei einfache Folgerungen zerlegt werden.

Prinzip :  
Vermeiden von  
Äquivalenzbeweisen

### VERMEIDEN VON ÄQUIVALENZBEWEISEN:

In Beweisen geht man immer in kleinen Schritten vor, um logische Fehlschlüsse zu vermeiden. Zwei Implikationen sind einfacher zu bearbeiten als eine Äquivalenzaussage, weil man bei jeder der Implikationen zwischen Voraussetzung und Folgerung unterscheiden kann. Das ist bei einer Äquivalenzaussage nicht der Fall, in der beide Teile sowohl Voraussetzung und Folgerung sind.

Konkret bedeutet das also für Mengengleichheiten:

Prinzip :  
Mengengleichheit  
beweisen

### MENGENGLEICHHEIT BEWEISEN:

Jeder Mengengleichheitsbeweis  $A = B$  wird prinzipiell in zwei Schritten geführt:

1. Jedes Element der Menge A ist Element der Menge B.
2. Jedes Element der Menge B ist Element der Menge A.

Bemerkung 8: Bei der Gleichheit von Mengen kommt es also nur darauf an, welche Elemente die Mengen haben. Nicht auf deren Definition oder die Umstände ihres Zustandekommens. Zum Beispiel bezeichnen die Mengen  $\{\text{Morgenstern}\}$

und  $\{\text{Abendstern}\}$  dieselbe Menge, weil der Morgenstern und der Abendstern beides Namen für ein und denselben Planeten Venus darstellen. Dieses Prinzip wird als „Extensionalitätsprinzip“ bezeichnet. In der natürlichen Sprache verbindet man Morgenstern und Abendstern mit unterschiedlichen Stimmungen, weshalb die Begriffe nicht durcheinander ersetzt werden können. Die natürliche Sprache wäre also nicht extensional.

**Beispiel 2.4.1 Mengengleichheit**

1.  $\{1, 2, 3, 4\} = \{x \in \mathbb{N} | x < 5\}$
2.  $\{\text{Morgenstern}\} = \{\text{Abendstern}\}$

**EIGENSCHAFTEN MENGENGLEICHHEIT:**

Seien  $M, M_1, M_2, M_3$  Mengen, dann gilt:

1.  $M = M$  (Reflexivität).
2. Wenn  $M_1 = M_2$  dann ist  $M_2 = M_1$  (Symmetrie).
3. Wenn  $M_1 = M_2$  und  $M_2 = M_3$  dann ist  $M_1 = M_3$  (Transitivität).

**Satz 2.4.1**  
Eigenschaften  
Mengengleichheit

Um ein Beispiel für Beweistechnik zu geben, wird der Beweis dieses Satzes gegeben.

**Beweis:**

Zu 1.: Um die erste Aussage zu beweisen, müssen wir in die Definition 2.4.1 schauen. Wir können sie nämlich anwenden und zwar für den Fall  $M_1 = M_2 = M$ . Die in 2.4.1 angegebenen Bedingungen lesen sich dann:

1. Jedes Element von  $M$  ist Element von  $M$ .
- und**
2. Jedes Element von  $M$  ist Element von  $M$ .

Sie erkennen aus den Bedingungen wird eine selbstverständlich wahre Aussage.

Prinzip :  
 Kennzeichnung  
 Voraussetzung  
 und Folgerung

#### KENNZEICHNUNG VORAUSSETZUNG UND FOLGERUNG:

Eine Basistechnik des Beweisens besteht darin, die Voraussetzungen und die Folgerungen zu identifizieren. Eine Möglichkeit, dies deutlich zu machen, ist die Voraussetzung grün und die Folgerung rot zu unterstreichen. Logische Schlüsse dürfen immer nur auf Basis der Voraussetzungen (grünen Aussagen) geschlossen werden. Auch verbal sollte die Voraussetzung und die Folgerung deutlich unterschieden werden. Voraussetzungen müssen durch einen Indikativ angezeigt werden, während Folgerungen immer durch: „wir müssen zeigen“ oder „zu zeigen“ angezeigt werden.

Zu 2: Bei dieser Aussage handelt es sich um eine Implikation. Um eine Implikation zu beweisen, startet man bei der Voraussetzung und versucht sie so lange mittels einfacher Schlüsse (Sylogismen) umzuformen, bis die Folgerung dasteht. Um die Voraussetzung  $M_1 = M_2$  nutzen zu können, müssen wir wieder auf die Definition 2.4.1 schauen.

1. Jedes Element von  $M_1$  ist Element von  $M_2$ .
- und**
2. Jedes Element von  $M_2$  ist Element von  $M_1$ .

Da die beiden Punkte aber durch die logische Konjunktion und verknüpft sind, bei der die Reihenfolge keine Rolle spielt, folgt aus der Voraussetzung selbstverständlicherweise.

1. Jedes Element von  $M_2$  ist Element von  $M_1$ .
- und**
2. Jedes Element von  $M_1$  ist Element von  $M_2$ .

Nun hilft wieder ein Blick auf 2.4.1. Um diese Definition anwenden zu können, müssen wir die Rollen von  $M_1$  und  $M_2$  vertauschen:  $M_2$  in der Rolle von  $M_1$  und  $M_1$  in der Rolle von  $M_2$ . Wir erkennen, dass wir nun genau die Definition von  $M_2 = M_1$  hergeleitet haben.

Zu 3.: Die behauptete Aussage hat wieder die Form einer Implikation: Wenn . . . dann . . . Auch hier starten wir wieder mit der Anwendung der Definition 2.4.1, diesmal allerdings wenden wir sie gleich zweimal an:

1. Jedes Element von  $M_1$  ist Element von  $M_2$ .
- (\*)      **und**
2. Jedes Element von  $M_2$  ist Element von  $M_1$ .

1. Jedes Element von  $M_2$  ist Element von  $M_3$ .
- (\*\*)      **und**
2. Jedes Element von  $M_3$  ist Element von  $M_2$ .

Wir müssen eine Mengengleichheit beweisen, und zwar die Mengengleichheit  $M_1 = M_3$ . Wie Sie sicher erraten, wenden wir die Definition an, um zu sehen, was das bedeutet:

1. Jedes Element von  $M_1$  ist Element von  $M_3$ .
- (\*\*  
\*)      **und**
2. Jedes Element von  $M_3$  ist Element von  $M_1$ .

Um diese Aussage zu beweisen, überlegen wir zuerst, dass es sich um ein durch „und“ verknüpft Gebilde aus zwei Teilaussage handelt. Es reicht, jede der beiden Teilaussagen einzeln zu beweisen.

Wenden wir uns zunächst der ersten Teilaussage von (\*\*  
\*) zu: Jedes Element von  $M_1$  ist Element von  $M_3$ . Generalisierungen (gemeint ist hier das Konstrukt „Jedes Element“) lassen sich schwer bearbeiten, insbesondere wenn man mehrere Generalisierungen in einer Aussage hat. Das ist hier zwar nicht der Fall, aber wir werden später solche Fälle zu Hauf haben. Um diese Generalisierung loszuwerden, bedienen wir uns eines kleinen Tricks: Wir nehmen an, dass uns ein Element aus  $M_1$  gegeben wird. Wenn wir dann für dieses gegebene Element die Aussage  $x \in M_3$  beweisen können und der Beweis nichts anderes nutzt, als dass  $x$  aus  $M_1$  ist, haben wir die generalisierte Aussage bewiesen. Sei also  $x \in M_1$  ein beliebiges aber festes Element. Für dieses Element können wir nun die erste Teilaussage von (\*) anwenden. Da jedes Element aus  $M_1$  auch Element von  $M_2$  ist, und  $x$  ein Element von  $M_1$  ist, ist also  $x$  mit Sicherheit auch ein Element aus  $M_2$ . Die erste Teilaussage von (\*\*) sagt, dass jedes Element von  $M_2$  auch Element von  $M_3$  ist.  $x$  ist aber, wie wir eben bewiesen haben, ein Element aus  $M_2$ . Deshalb folgt, dass  $x$  aus  $M_3$  sein muss.

Die zweite Teilaussage von  $\left( \begin{smallmatrix} ** \\ * \end{smallmatrix} \right)$  lässt sich mit fast derselben Argumentation beweisen, es sind nur andere Teilaussagen zu verwenden.

q.e.d.

#### BEWEISTECHNIKEN:

Wie Sie sehen, ist der Beweis aus sehr kleinen Schritten aufgebaut. Dabei werden immer wiederkehrende Elemente genutzt:

- Das Anwenden von Definitionen für bestimmte Elemente. In unserem Beispiel Definition 2.4.1.
- Das Ziehen von Schlüssen aufgrund aussagenlogischer Zusammenhänge. Hier ist insbesondere Kenntnis der aussagenlogischen Verknüpfungen „und“, „oder“ und „wenn ... dann ...“ erforderlich.
- Das Einführen von Variablen, um Generalisierungen zu beweisen. In unserem Beispiel „Sei also  $x \in M_1$  ein beliebiges aber festes Element.“
- Das Anwenden elementarer Schlüsse wie dem Schluss: „Da jedes Element aus  $M_1$  auch Element von  $M_2$  ist, und  $x$  ein Element von  $M_1$  ist, ist also  $x$  mit Sicherheit auch ein Element aus  $M_2$ .“ Diese Schlussweise besitzt übrigens einen Namen: „Syllogismus Barbara“.

Prinzip :  
Beweistechniken

Bemerkung 9: Diese relativ einfachen Aussagen sind nicht spezifisch für die Mengenlehre, sondern sind Eigenschaften des Operators „=“.

#### TEILMENGE:

Eine Menge  $M_1$  heißt „Teilmenge“ der Menge  $M_2$ , wenn jedes Element von  $M_1$  auch Element von  $M_2$  ist. Man schreibt dann:

$$M_1 \subseteq M_2.$$

Die Tatsache, dass  $M_1$  nicht Teilmenge von  $M_2$  ist, wird durch

$$M_1 \not\subseteq M_2$$

ausgedrückt.

Falls  $M_1 \subseteq M_2$  und  $M_1 \neq M_2$  heißt  $M_1$  „echte Teilmenge“ von  $M_2$ . Man verwendet hierfür die Schreibweise

$$M_1 \subsetneq M_2$$

.

**Definition 2.4.2**  
Teilmenge



Machen Sie sich anhand der folgenden Beispiele die Unterschiede zwischen der Element- und der Teilmengenbeziehung deutlich. Insbesondere wenn Mengen wieder Mengen enthalten, führt das häufig zu Verwechslungen.

**Beispiel 2.4.2** *Teilmengen und Elemente*

- $\{1\} \subseteq \{1, \{1, 2\}\}$
- $\{1\} \notin \{1, \{1, 2\}\}$
- $\{1, 2\} \in \{1, \{1, 2\}\}$
- $1 \in \{1, \{1, 2\}\}$
- $2 \notin \{1, \{1, 2\}\}$
- $\{1, 2\} \not\subseteq \{1, \{1, 2\}\}$

Bemerkung 10: Wenn  $M_1 \not\subseteq M_2$  ist, so bedeutet das, dass wenigstens ein Element in  $M_1$  existieren muss, das nicht Element von  $M_2$  ist

**EIGENSCHAFTEN TEILMENGE :**

1. Für jede Menge  $M$  gilt:  $M \subseteq M$
2.  $M_1 = M_2$  genau dann, wenn  $M_1 \subseteq M_2$  und  $M_2 \subseteq M_1$
3. Wenn  $M_1 \subseteq M_2$  und  $M_2 \subseteq M_3$ , dann  $M_1 \subseteq M_3$
4. Für jede Menge  $M$  gilt:  $\emptyset \subseteq M$

**Satz 2.4.2**  
Eigenschaften  
Teilmenge

Bemerkung 11: Die leere Menge ist also Teilmenge jeder Menge, sie ist aber nicht Element jeder Menge. Die leere Menge kann Element einer Menge sein, muss es aber nicht.

**Beispiel 2.4.3** Die folgenden Beispiele sollen den Unterschied zwischen Element- und Teilmengenbeziehung für die leere Menge deutlich machen:

- $\emptyset \subseteq \{1, \{1, 2\}\}$
- $\emptyset \notin \{1, \{1, 2\}\}$
- $\emptyset \in \{\emptyset\}$

**Aufgabe 2.3:**

Welche der folgenden Aussagen sind wahr:

1.  $\{1\} \in \{1, \{1, 2\}\}$
2.  $\{1\} \subseteq \{1, \{1, 2\}\}$
3.  $\{1\} \subsetneq \{1, \{1, 2\}\}$
4.  $\{1\} \not\subseteq \{1, \{1, 2\}\}$
5.  $1 \in \{1, \{1, 2\}\}$
6.  $\emptyset \in \{1, \{1, 2\}\}$
7.  $\emptyset \not\subseteq \{1, \{1, 2\}\}$
8.  $\emptyset \subsetneq \{1, \{1, 2\}\}$
9.  $\emptyset \subseteq \{\emptyset, \{1, 2\}\}$
10.  $\emptyset \in \{\emptyset, \{1, 2\}\}$

**Aufgabe 2.4:**

Warum sind die folgenden Gebilde fehlerhaft:

1.  $1 \subseteq \{1, \{1, 2\}\}$
2.  $1 \subsetneq \{1, \{1, 2\}\}$
3.  $1 \not\subseteq \{1, \{1, 2\}\}$
4. Es gilt:  $\{1, \{1, 2\}\}$

**Aufgabe 2.5:**

Welche Mengen werden durch die folgenden Definitionen beschrieben?

1.  $\{x \in \mathbb{N} \mid x = 2 \wedge x = 4\}$
2.  $\{x \in \mathbb{N} \mid x = 2 \vee x = 4\}$
3.  $\{x \in \mathbb{N} \mid x - 2 = 2\}$
4.  $\{x \in \mathbb{N} \mid x > 2 \wedge x < 4\}$
5.  $\{x \in \mathbb{N} \mid x > 4\}$
6.  $\{x \in \mathbb{N} \mid x < 4\}$
7.  $\{x \in \mathbb{N} \mid x < 2 \vee x > 4\}$
8.  $\{x \in \mathbb{N} \mid x < 2 \vee x = 4\}$

## 2.5 Potenzmenge

Ein wichtiger und häufig angewendeter Begriff der Mengenlehre ist der Begriff der Potenzmenge. Seine Schwierigkeit entsteht dadurch, dass die Potenzmenge Mengen enthält, und somit die Unterscheidung zwischen Element- und Teilmengenbeziehung vielen Neulingen schwerfällt. Legen Sie besonderen Wert auf das Verständnis dieses Aspekts.

**POTENZMENGE:**

Die „Potenzmenge“  $P(M)$  einer Menge  $M$  ist die Gesamtheit aller Teilmengen von  $M$ , einschließlich der leeren Menge und der Menge selbst.

$$P(M) = \{x \mid x \subseteq M\}$$

**Definition 2.5.1**  
Potenzmenge

**Beispiel 2.5.1** 1. Sei  $M = \{1, 2, 3\}$ . Dann ist die Potenzmenge:

$$P(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

2. Sei  $M = \emptyset$ . Dann gilt:  $P(M) = \{\emptyset\} \neq \emptyset$

**Beispiel 2.5.2** Sei  $M$  eine beliebige Menge. Gilt dann:

1.  $M \subseteq P(M)$  ? nein, zum Beispiel nicht für die Menge  $\{1, 2, 3\}$
2.  $M \in P(M)$  ? ja
3.  $\emptyset \in P(M)$  ? ja
4.  $\emptyset \subseteq P(M)$  ? ja

**Definition 2.5.2**  
Mächtigkeit einer Menge

**MÄCHTIGKEIT EINER MENGE:**

Es sei  $S$  eine Menge mit endlich vielen Elementen. Die Anzahl der Elemente, auch „Kardinalität“ oder „Mächtigkeit“ genannt, schreibt man  $|S|$ .

**Beispiel 2.5.3** 1.  $S = \{a, b, c\} \quad |S| = 3$

2.  $|\emptyset| = 0$

Bemerkung 12: Zwei endliche Mengen, die gleich viele Elemente besitzen, heißen **gleichmächtig**. Man kann sie in gewisser Weise miteinander „identifizieren“, indem man jedes Element der einen Menge zu einem „Partner“ oder „Stellvertreter“ genau eines Elements der anderen Menge erklärt. Einfach ausgedrückt, kann man dann vom Standpunkt der Mengenlehre aus (d.h. mit Hilfe der Operatoren , etc.) mit der einen Menge genau dieselben Dinge machen wie mit der anderen. Jeweils ein Element der einen Menge „steht für“ ein Element der anderen Menge, und umgekehrt. (Man kann das auch so sagen: Für jemanden, der nur den Begriff der Menge und die Operatoren der Mengenlehre kennt und alles andere ignoriert, sind die beiden Mengen nicht unterscheidbar). Der Begriff der Mächtigkeit kann für unendliche Mengen, d.h. für Mengen, die unendlich viele Elemente enthalten, verallgemeinert werden. Zwei beliebige Mengen heißen gleichmächtig, wenn jedes Element der einen Menge zu einem „Partner“ oder „Stellvertreter“ genau eines Elements der anderen Menge erklärt werden kann, so dass kein Element der zweiten Menge „übrigbleibt“. Es gibt unendliche Mengen, die nicht gleichmächtig sind. In diesem Sinn können also auch unendliche Mengen „verschieden viele Elemente“ enthalten, also „verschieden groß“ sein. Das wichtigste Beispiel hierfür bilden die Mengen der natürlichen und der reellen Zahlen: Sie besitzen beide unendlich viele Elemente, sind aber nicht gleichmächtig.

Beim Berechnen der Potenzmenge einer Menge vergisst man gerne einige Ele-

mente, da eine systematische Aufzählung der Elemente nicht ganz einfach ist. Deshalb soll der folgende Satz einen schnellen Test ermöglichen, ob man wirklich schon alle Elemente gefunden hat:

**MÄCHTIGKEIT DER POTENZMENGE:**

Sei  $M$  eine beliebige Menge mit endlich vielen Elementen. Wenn  $|M| = n$ , dann hat  $|P(M)| = 2^n$  Elemente.

**Satz 2.5.1**  
Mächtigkeit der Potenzmenge

Beweisidee: Sei  $M$  eine Menge mit  $n$  Elementen, etwa den Elementen  $a_1, \dots, a_n$ . Wir können die Elemente der Potenzmenge, also die Teilmengen von  $\{a_1, \dots, a_n\}$  in einen Entscheidungsbaum einordnen: Bei der ersten Entscheidung unterteilen wir die Teilmengen nach solchen Teilmengen, die  $a_1$  enthalten und solchen Teilmengen, die  $a_1$  nicht enthalten. Der Entscheidungsbaum unterteilt sich also zunächst in zwei Äste. Dann unterteilen wir jeden Ast, nach solchen Teilmengen, die  $a_2$  enthalten und solchen die  $a_2$  nicht enthalten. Jeder Ast wird also wieder in zwei Teiläste zerlegt, und somit haben wir  $2 * 2$  Unterscheidungen. Dieses Verfahren wiederholen wir nun auch für die Elemente  $a_3, \dots, a_n$ . Durch Betrachtung eines zusätzlichen Elements verdoppelt sich die Anzahl der Unterteilungen jedesmal. Damit haben wir nach Betrachtung von  $n$  Elementen genau  $\underbrace{2 * \dots * 2}_{n\text{-mal}} = 2^n$  Unterscheidungen, wobei jede Unterscheidung genau einer Teilmenge entspricht.

**Aufgabe 2.6:**

Zählen Sie die Elemente der Potenzmenge der folgenden Mengen auf:

1.  $M = \{1, 2, 3, 4\}$
2.  $M = \{\{1, 2\}, 1\}$
3.  $M = \{\{1, 2\}, \emptyset\}$

## 2.6 Mengenoperationen und Venn Diagramme

**DURCHSCHNITT ZWEIER MENGEN:**

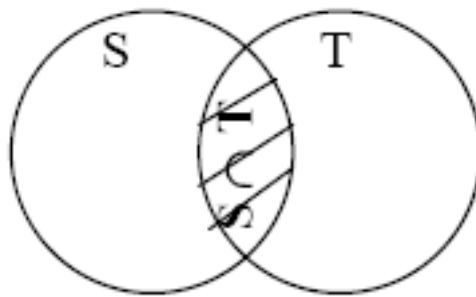
Der „Durchschnitt  $S \cap T$  zweier Mengen  $S, T$  ist die Menge, die aus allen Elementen besteht, die zu  $S$  **und** zu  $T$  gehören.

$$S \cap T = \{x | x \in S \wedge x \in T\}$$

**Definition 2.6.1**  
Durchschnitt zweier Mengen

Bemerkung 13: Für die logische Verknüpfung „und“ wurde in der Definition das Symbol  $\wedge$  verwendet.

Das folgende Venn Diagramm soll die Definition des Durchschnitts veranschaulichen. Dabei werden die Mengen als Kreise symbolisiert und die Elemente der Menge entsprechen der eingeschlossenen Fläche:



Venn-Diagramm

Bemerkung: Das Venn Diagramm wurde nach John Venn (1834-1923), einem englischen Priester benannt. Er lehrte in Cambridge und hat mehrere Bücher geschrieben, darunter zwei über Logik.

**Beispiel 2.6.1** Seien  $S = \{1, 2, 3\}$  und  $T = \{3, 4, 5\}$ . Dann ist  $S \cap T = \{3\}$ .  
 Seien  $S = \{1, \{1, 2\}\}$  und  $T = \{2, \{2, 1\}\}$ . Dann ist  $S \cap T = \{\{1, 2\}\}$ .  
 Seien  $S = \{1, \{1, 2\}\}$  und  $T = \{2, \{2, 3\}\}$ . Dann ist  $S \cap T = \emptyset$ .  
 Seien  $S = \{1, \{1, 2\}\}$  und  $T = \emptyset$ . Dann ist  $S \cap T = \emptyset$ .

**Satz 2.6.1**  
 Durchschnitt ist  
 Teilmenge

**DURCHSCHNITT IST TEILMENGE:**

Seien  $S, T$  beliebige Mengen. Dann gilt:  $S \cap T \subseteq S$

**Beweis:**

Seien  $S, T$  beliebige Mengen. Nach Definition 2.4.2 müssen wir zeigen: Jedes Element von  $S \cap T$  ist Element von  $S$ .

Sei dazu  $x \in S \cap T$  ein beliebiges Element. Nach Definition 2.6.1 ist  $x \in S$  und  $x \in T$ . Wir können die zweite Teilaussage der und Verknüpfung einfach vergessen und erhalten die erforderliche Behauptung  $x \in S$ . **q.e.d.**

#### CHARAKTERISIERUNG TEILMENGE MIT DURCHSCHNITT:

Seien  $S, T$  beliebige Mengen. Dann gilt:  $S \subseteq T \Leftrightarrow S \cap T = S$

**Satz 2.6.2**  
Charakterisierung  
Teilmenge mit  
Durchschnitt

Wir wollen diesen Satz beweisen. Dazu müssen wir zunächst bemerken, dass eine Äquivalenz (also eine genau-dann-wenn-Aussage) zu zeigen ist. Viele Anfänger sind aus Faulheitsgründen versucht, solche Äquivalenzen in einem einzigen Schritt durch Äquivalenzumformungen zu beweisen. Obwohl Faulheit eine der Tugenden von guten Informatikern (sonst fehlt Ihnen der instinktive Drang zur Automation von wiederkehrenden Aufgaben!) ist, ist es an dieser Stelle jedoch nicht angebracht, weil sich zu viele Fehlschlüsse einschleichen. Deshalb werden wir Äquivalenzbeweise immer in zwei Schritten formulieren. In diesem Beispiel bedeutet das: Wir zeigen:  $S \subseteq T \Rightarrow S \cap T = S$  und  $S \subseteq T \Leftarrow S \cap T = S$ .

#### Beweis:

Seien  $S$  und  $T$  beliebige Mengen.

$S \subseteq T \Rightarrow S \cap T = S$ : Die Voraussetzung besagt:  $S \subseteq T$ . Nach Definition 2.4.2 bedeutet das, dass jedes Element von  $S$  ein Element von  $T$  ist. Wir müssen die folgende Behauptung zeigen:  $S \cap T = S$ . Nach Definition 2.4.1 müssen wir also zwei Aussagen beweisen: Jedes Element von  $S \cap T$  ist Element von  $S$  und jedes Element von  $S$  ist Element von  $S \cap T$ . Die erste Teilaussage ist genau der Satz 2.6.2. Bleibt also die zweite Teilaussage zu zeigen. Sei dazu  $x \in S$  beliebig. Nach der Voraussetzung ist nun auch  $x \in T$ , da jedes Element von  $S$  in  $T$  liegt und  $x$  ein Element aus  $S$  ist. Da  $x \in S$  und  $x \in T$  ist, ist nach Definition 2.6.1  $x \in S \cap T$ .

$S \subseteq T \Leftarrow S \cap T = S$ : Jetzt ist die Voraussetzung  $S \cap T = S$ . Wir müssen zeigen, dass  $S \subseteq T$ , d. h. nach Definition 2.4.2 dass jedes Element von  $S$  ein Element von  $T$  ist. Sei also  $x \in S$  ein beliebiges Element. Da nach Voraussetzung  $S \cap T = S$  ist, bedeutet das, dass jedes Element von  $S \cap T$  in  $S$  ist und jedes Element von  $S$  in  $S \cap T$  ist. Wir vergessen die erste Teilaussage und wissen deshalb, dass jedes Element von  $S$  auch Element von  $S \cap T$  ist.  $x$  ist ein Element von  $S$  und ist deshalb auch in  $S \cap T$ . Nach der Definition 2.6.1 des Durchschnitts ist  $x \in S \wedge x \in T$ . Vergessen wir wieder die erste Teilaussage, so folgt  $x \in T$ .

**q.e.d.**

**Definition 2.6.2**  
Disjunkte  
Mengen

**DISJUNKTE MENGEN:**

$S$  und  $T$  heißen „disjunkt“ oder „elementfremd“, falls  $S \cap T = \emptyset$ .

Frage: Wie sieht ein Venn-Diagramm aus, das diese Situation beschreibt?

**Beispiel 2.6.2** 1.  $\{1, 2\}$  und  $\{3, 4, 5\}$  sind disjunkt.

2.  $S = \{1, \{1, 2\}\}$  und  $T = \{2\}$  sind disjunkt.

3.  $S = \{x | x \in \mathbb{N} \text{ ist gerade}\}$  und  $T = \{x | x \in \mathbb{N} \text{ ist ungerade}\}$  sind disjunkt.

4. Manchmal ist es nicht ganz einfach festzustellen, ob zwei Mengen disjunkt sind: Sei  $S = \{x | \text{Es gibt natürliche Zahlen } u, v, \text{ so dass: } x = u^3 + v^3\} = \{2, 9, 16, \dots\}$  und  $T = \{x | \text{Es gibt eine natürliche Zahl } w, \text{ so dass: } x = w^3\} = \{1, 8, 27, \dots\}$ . Sind  $S$  und  $T$  disjunkt?

*Diese Frage ist Teil der berühmten Fermat'schen Vermutung.*

**Bemerkung 14: Die Fermat'sche Vermutung**

Im Jahr 1637 behauptete der Richter und begnadete Amateur-Mathematiker Pierre de Fermat aus Toulouse in einer Randnotiz in seiner Ausgabe des Buches Arithmetica von Diophant: Für jede natürliche Zahl  $n > 2$  gibt es keine ganzzahligen Lösungen  $x, y, z > 0$  der Gleichung  $x^n + y^n = z^n$ .

Leider blieb Fermat den Beweis schuldig. Er schrieb nur: „Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch dieser Rand ist zu schmal, um ihn zu fassen.“ Damit forderte er Generationen von Mathematikern heraus, den Beweis zu finden.

Das Problem ist so einfach zu formulieren; jeder kennt den Satz des Pythagoras und weiss, dass die Gleichung für  $n = 2$  Lösungen hat (sogenannte pythagoräische Tripel:  $3^2 + 4^2 = 5^2$ ). Dennoch dauerte es 357 Jahre, bis 1995 der englische Mathematiker Andrew Wiles (Professor in Princeton) einen vollständigen Beweis für die Unmöglichkeit der Lösbarkeit für  $n > 2$  erbrachte. Sein Beweis, das Ergebnis von zehn Jahren harter Arbeit, ist über 100 Seiten lang und enthält modernste und sehr komplizierte Mathematik. Er weist viele Verbindungen zu anderen Gebieten der Mathematik auf und benutzt Theorien aus Geometrie, Analysis und Algebra, die im 20. Jahrhundert entwickelt wurden. Es ist klar, dass der Beweis, den Fermat behauptet, gefunden zu haben, ein anderer gewesen sein muss.



Zum Glück für uns Mathematiker gibt es immer noch eine Vielzahl ungelöster Probleme, die auf ihre Lösung warten. Die meisten sind zwar nicht so alt wie die Fermatsche Vermutung (oder besser der Satz von Wiles), aber trotzdem faszinierend. Es gibt ein spannendes Buch zum Thema Fermat, das sich liest wie ein Roman: Simon Singh, Fermats letzter Satz, Carl Hanser Verlag 1998.

**VEREINIGUNG ZWEIER MENGEN:**

Die „Vereinigung“ zweier Mengen  $S$  und  $T$  ist die Menge aller Elemente, die zu  $S$  oder zu  $T$  gehören.

$$S \cup T = \{x \mid x \in S \vee x \in T\}$$

**Definition 2.6.3**  
Vereinigung  
zweier Mengen

Bemerkung 15: Für die logische Verknüpfung „oder“ wurde in der Definition das Symbol  $\vee$  verwendet.

Wie sieht das Venn-Diagramm aus?

Bemerkung 16: Ich möchte Sie auf eine mögliche Verwechslungsgefahr aufmerksam machen. Nachlässige Personen merken sich die Vereinigung von zwei Mengen indem die Vereinigung die Elemente der einen Menge und die Elemente der anderen Menge hat. Wenn dann die Definition aufgeschrieben werden soll, setzen sie dieses „und“ in die Definition ein. Mit „und“ wird aber grade der Durchschnitt beschrieben. In der Definition der Vereinigung tritt aber das „oder“ (Zeichen  $\vee$  wie Vereinigung) auf. Ein Informatiker muss aber zwischen „und“ und „oder“ unterscheiden können. Und schon wird aus einer „harmlosen Nachlässigkeit“ ein böser Fehler.

**Beispiel 2.6.3** Seien  $S = \{1, 2, 3\}$  und  $T = \{3, 4, 5\}$ . Dann ist  $S \cup T = \{1, 2, 3, 4, 5\}$ .

In Analogie zu Satz 2.6.2 gilt:

**VEREINIGUNG IST OBERMENGE:**

Seien  $S, T$  beliebige Mengen. Dann gilt:  $T \subseteq S \cup T$ .

**Satz 2.6.3**  
Vereinigung ist  
Obermenge

**Satz 2.6.4**

Charakterisierung  
Teilmenge durch  
Vereinigung

**CHARAKTERISIERUNG TEILMENGE DURCH VEREINIGUNG:**

Seien  $S, T$  beliebige Mengen. Dann gilt:  $S \subseteq T \Leftrightarrow S \cup T = T$ .

**Satz 2.6.5**

Mächtigkeit von  
Vereinigung und  
Durchschnitt

**MÄCHTIGKEIT VON VEREINIGUNG UND DURCHSCHNITT:**

Seien  $S, T$  endliche Mengen. Dann gilt:  $|S \cap T| + |S \cup T| = |S| + |T|$

Beweisidee: Die Elemente des Durchschnitts werden auf beiden Seiten doppelt gezählt.

**Definition 2.6.4**  
Mengendifferenz**MENGENDIFFERENZ:**

Die „Differenz“ zweier Mengen  $S$  und  $T$  ist die Menge aller Elemente von  $S$ , die nicht zu  $T$  gehören.

$$S \setminus T = \{x | x \in S \wedge x \notin T\}$$

Wie sieht das Venn- Diagramm zur Mengendifferenz aus?

**Definition 2.6.5**  
Symmetrische  
Differenz**SYMMETRISCHE DIFFERENZ:**

Die „symmetrische Differenz“ zweier Mengen  $S$  und  $T$  ist die Menge aller Elemente, die zu genau einer der beiden Mengen  $S$  und  $T$  gehören.

$$S \Delta T = \{x | (x \in S \wedge x \notin T) \vee (x \notin S \wedge x \in T)\}$$

Bemerkung 17:

Man erkennt, dass  $S \Delta T = (S \setminus T) \cup (T \setminus S) = (S \cup T) \setminus (S \cap T)$

Wie sieht das Venn-Diagramm aus?

**Satz 2.6.6**

Assoziativgesetz  
für symmetrische  
Differenz

**ASSOZIATIVGESETZ FÜR SYMMETRISCHE DIFFERENZ:**

Für beliebige Mengen  $S, R, T$  gilt das folgende Assoziativgesetz

$$(S \Delta R) \Delta T = S \Delta (R \Delta T)$$

**KOMPLEMENT EINER MENGE:**

Sei  $S \subseteq M$ , eine Teilmenge einer festen Grundmenge  $M$  (das Universum). Das „Komplement“  $\bar{S}$  von  $S$  in  $M$  ist die Menge aller Elemente von  $M$ , die nicht in  $S$  liegen.

$$\bar{S} = M \setminus S = \{x | x \in M \text{ und } x \notin S\}$$

**Definition 2.6.6**  
Komplement  
einer Menge

Wie kann man das Komplement in einem Venn Diagramm fassen? Wie kann man die feste Grundmenge (das Universum) darstellen?

**Beispiel 2.6.4** Sei das Universum  $M = \mathbb{N}$  gegeben. Dann ist

1.  $\overline{\{1, 2, 3, 4\}} = \{5, 6, 7, 8, \dots\}$
2.  $\overline{\{x | x \text{ ungerade}\}} = \{x | x \text{ grade}\}$

**Aufgabe 2.7:**

Berechnen Sie:

1.  $\{1, \{1, 2\}\} \cup \{2, \{2, 1\}\}$
2.  $\{\emptyset, \{1, 2\}\} \cap \{2, \{2, 3\}\}$
3.  $\{1, \{1, 2\}\} \setminus \{2, \{2, 1\}\}$
4.  $\{1, \{1, 2\}\} \setminus \{\emptyset\}$
5.  $\{1, \{1, 2\}\} \Delta \{2, \{2, 1\}\}$
6.  $\{1, \{1, 2\}\} \Delta \emptyset$
7.  $\emptyset \Delta \emptyset$

Zu welchen Ergebnismengen ist die Ergebnismenge aus 1 disjunkt?

**Aufgabe 2.8:**

Zeichnen Sie ein Venn-Diagramm, das den Sachverhalt des Assoziativgesetzes für die symmetrische Differenz darstellt.

**Aufgabe 2.9:**

1. Finden Sie eine Formel, die  $|S \setminus T|$ ,  $|S|$  und  $|S \cap T|$  in Verbindung bringt.
2. Finden Sie eine Formel, die  $|S \Delta T|$ ,  $|S|$ ,  $|T|$  und  $|S \cup T|$  in Verbindung bringt.

### Aufgabe 2.10:

Beweisen Sie den Satz **Vereinigung ist Obermenge**.

### Aufgabe 2.11:

Beweisen Sie den Satz **Charakterisierung Teilmenge durch Vereinigung**.

## 2.7 Kartesisches Produkt

**Definition 2.7.1**  
geordnete Paare

#### GEORDNETE PAARE:

Es seien  $a_1$  und  $a_2$  beliebige Objekte,  $(a_1, a_2)$  heißt geordnetes Paar.  
Zwei geordnete Paare sind gleich:

$$(a_1, a_2) = (b_1, b_2) \Leftrightarrow (a_1 = b_1 \wedge a_2 = b_2)$$

**Bemerkung 18:** Wir haben das geordnete Paar als ein neues Konzept eingeführt. Ein geordnetes Paar ist ein neues Ding unseres Denkens, das nur einem Paar mit denselben Komponenten gleich ist. Das ist ein einfaches, aber vielleicht als unschön empfundenes Verfahren. Schöner würde es von einem Mathematiker angesehen werden, wenn das Konzept des Paares auf das Konzept der Menge zurückgeführt würde. Das ist auch möglich, indem man definiert:  $(a, b) = \{a, \{a, b\}\}$ . Dann muss man allerdings die in der Definition festgelegte Gleichheit beweisen. Wir wählen die einfachere Variante.

**Beispiel 2.7.1** 1.  $(1, 2) = (1, 2)$

2.  $(1, 2) \neq (2, 1)$

3.  $(1, (1, 2)) \neq ((1, 1), 2)$

4.  $(1, \{1\}) \neq (1, 1)$

5.  $(1, \{1\}) = (1, \{x \in \mathbb{N} | x < 2\})$

6.  $(1, 2) \neq \{1, 2\}$

7.  $1 \neq (1, 1)$

**KARTESISCHES PRODUKT:**

Das „Kartesische Produkt“ zweier Mengen  $S$  und  $T$  ist die Menge aller geordneten Paare.  $S \times T = \{x | \text{Es gibt } y \in S \text{ und } z \in T, \text{ so dass } x = (y, z)\}$

**Definition 2.7.2**  
Kartesisches  
Produkt

Bemerkung 19: Zur Vereinfachung der Schreibweise verwendet man die Variante, in der man mit zwei Laufvariablen arbeitet:

$$S \times T = \{(x, y) | x \in S \wedge y \in T\}$$

Die Laufvariablen  $x$  und  $y$  durchlaufen unabhängig voneinander alle Objekte unseres Denkens und unserer Anschauung. Die definierende Eigenschaft schränkt nun die Objekte ein, für die das Paar  $(x, y)$  in der Menge liegt.

Bemerkung 20: Bitte beachten Sie, dass beim Arbeiten mit zwei Laufvariablen  $x$  und  $y$  diese unabhängig ihre Werte annehmen. Das bedeutet insbesondere, dass die angenommenen Werte durchaus identische sein können. Dieser Spezialfall wird häufig übersehen. Im Kern bedeutet das, dass das geordnete Paar  $(x, y)$  durchaus gleich dem geordneten Paar  $(y, x)$  sein kann, nämlich dann, wenn  $x = y$  ist. Obwohl die Laufvariablen unterschiedlich heißen, sind ihre Werte gleich.

Bei der Verwendung von zwei Laufvariablen  $x, y$  gibt es nicht nur bei Paaren Sonderfälle. Auch bei dem Mengenbildungsprinzip „Aufzählen der Elemente“ ist zu beachten, dass zwei Variablen denselben Wert haben können. So kann  $\{x, y\}$  durchaus eine Menge mit nur einem Element sein, wenn nämlich  $x=y$  ist. Obwohl beim Aufzählen konkreter Objekte in der Menge Elemente nicht mehrfach genannt werden dürfen, kann es passieren, dass bei der Verwendung von Variablen gewisse Elemente zusammenfallen. Falls  $x = y$ , so ist dann  $\{x, y\} = \{x\} = \{y\}$

**Beispiel 2.7.2** 1. Sei  $S = \{1, 2\}$  und  $T = \{3, 4, 5\}$  dann ist

$$S \times T = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$$

2.  $\{1, 2\} \times \{2, 3\} = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$

3.  $S \times \emptyset = \emptyset$

4.  $\emptyset \times S = \emptyset$

**N-TUPEL:**

Es seien  $x_1, x_2, x_3, \dots, x_n$  beliebige Objekte. Das geordnete „n-tupel“ ist das Objekt  $(x_1, x_2, x_3, \dots, x_n)$ . Zwei geordnete n-tupel  $(x_1, \dots, x_n) = (y_1, \dots, y_n)$  sind gleich, wenn  $x_1 = y_1$  und  $x_2 = y_2$  und ... und  $x_n = y_n$ .

Das kartesische Produkt von n Mengen  $M_1, \dots, M_n$  ist definiert durch:

$$M_1 \times M_2 \times \dots \times M_n = \{(x_1, x_2, \dots, x_n) | x_1 \in M_1 \wedge x_2 \in M_2 \wedge \dots \wedge x_n \in M_n\}$$

**Definition 2.7.3**  
n-tupel

**Aufgabe 2.12:**

Berechnen Sie die kartesischen Produkte:

1.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}$
2.  $(\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}) \times \{1\}$
3.  $\{1, \{1, 2\}\} \times (\{1, \{1, 2\}\} \times \{1\})$
4.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} \times \{1\}$
5.  $\{\emptyset\} \times \{\emptyset, 1, 2\}$
6.  $\{\emptyset, P(\emptyset)\} \times \emptyset$

**Lösung 2.12:**

1.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} = \{(1, 1), (1, \{1, 2\}), (\{1, 2\}, 1), (\{1, 2\}, \{1, 2\})\}$
2.  $(\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}) \times \{1\}$   
 $= \{((1, 1), 1), ((1, \{1, 2\}), 1), ((\{1, 2\}, 1), 1), ((\{1, 2\}, \{1, 2\}), 1)\}$

3.  $\{1, \{1, 2\}\} \times (\{1, \{1, 2\}\} \times \{1\})$   
 $= \{(1, (1, 1)), (1, (\{1, 2\}, 1)), (\{1, 2\}, (1, 1)), (\{1, 2\}, (\{1, 2\}, 1))\}$
4.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} \times \{1\} = \{(1, 1, 1), (1, \{1, 2\}, 1), (\{1, 2\}, 1, 1), (\{1, 2\}, \{1, 2\}, 1)\}$
5.  $\{\emptyset\} \times \{\emptyset, 1, 2\} = \{(\emptyset, \emptyset), (\emptyset, 1), (\emptyset, 2)\}$
6.  $\{\emptyset, P(\emptyset)\} \times \emptyset = \emptyset$

**Aufgabe 2.13:**

Geben Sie die Menge an:

$$\{\{x, y\} | x \in \{1, 2\} \wedge y \in \{2, 3\}\}$$

**Lösung 2.13:**

Bei dieser Aufgabe muss man darauf achten, dass die Mengenbildung anders funktioniert als die Paarbildung. Eine Menge darf eben nur jedes Element einmal enthalten. Ausserdem kommt es nicht auf die Reihenfolge an.

$$\{\{x, y\} | x \in \{1, 2\} \wedge y \in \{2, 3\}\} = \{\{1, 2\}, \{1, 3\}, \{2\}, \{2, 3\}\}$$

**Aufgabe 2.14:**

Geben Sie eine Formel zur Berechnung von  $|S \times T|$  an.

**Lösung 2.14:**

$$|S \times T| = |S| \cdot |T|$$

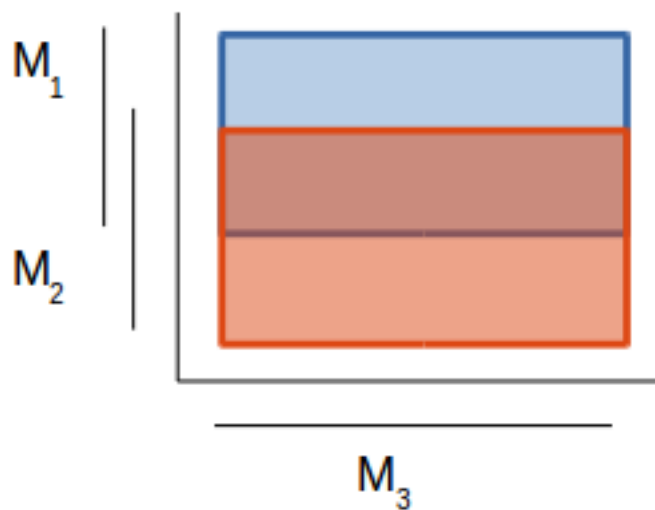
**Aufgabe 2.15:**

Welche der Gleichheiten gilt für beliebige Mengen  $M_1, M_2, M_3, M_4$ ?

1.  $(M_1 \cup M_2) \times M_3 = (M_1 \times M_3) \cup (M_2 \times M_3)$
2.  $(M_1 \cap M_2) \times M_3 = (M_1 \times M_3) \cap (M_2 \times M_3)$
3.  $(M_1 \setminus M_2) \times M_3 = (M_1 \times M_3) \setminus (M_2 \times M_3)$

$$4. (M_1 \cup M_2) \times (M_3 \cup M_4) = (M_1 \times M_3) \cup (M_2 \times M_4)$$

**Lösung 2.15:**



$$1. (M_1 \cup M_2) \times M_3 = (M_1 \times M_3) \cup (M_2 \times M_3) \text{ ist richtig.}$$

Beide Seiten entsprechen dem Bereich, der durch beide Rechtecke dargestellt wird.

$$2. (M_1 \cap M_2) \times M_3 = (M_1 \times M_3) \cap (M_2 \times M_3) \text{ ist richtig.}$$

Beide Seiten entsprechen dem Bereich, der durch die Überschneidung der beiden Rechtecke dargestellt wird.

$$3. (M_1 \setminus M_2) \times M_3 = (M_1 \times M_3) \setminus (M_2 \times M_3) \text{ ist richtig.}$$

Beide Seiten entsprechen dem Bereich, der durch das blaue aber nicht durch das orangefarbene Rechteck dargestellt wird.

$$4. (M_1 \cup M_2) \times (M_3 \cup M_4) = (M_1 \times M_3) \cup (M_2 \times M_4) \text{ ist falsch. Beispiel: } M_1 = \emptyset, M_2 = \{1\}, M_3 = \{1\}, M_4 = \emptyset \text{ Die linke Seite ist dann } \{(1, 1)\} \text{ und die rechte Seite ist } \emptyset.$$



## 2.8 Einige Rechenregeln für Mengen

Machen Sie sich die Aussagen an Hand von Venn Diagrammen klar und wenn Sie viel Lust haben, versuchen Sie sich an den Beweisen.

**KOMMUTATIVGESETZE :**

Es gilt für beliebige Mengen  $A, B$ :

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

**Satz 2.8.1**  
Kommutativgesetze

Alle Sätze dieses Kapitels lassen sich nach demselben Schema beweisen. Beim Übergang von Mengenbeziehungen zu Elementbeziehungen entsprechen alle in diesem Kapitel erwähnten Rechenregeln mit Mengen den entsprechenden Rechenregeln der Booleschen Algebra. Man spricht deshalb von der Booleschen Algebra der Mengen.

**Beweis:**

Wir beweisen nur die erste Gleichheit, da alle anderen nach demselben Prinzip geführt werden können.

Um eine Mengengleichheit zu beweisen muss laut Definition 2.4.1 gezeigt werden, dass „Jedes Element von  $A \cup B$  auch Element von  $B \cup A$  ist“ und „Jedes Element von  $B \cup A$  auch Element von  $A \cup B$  ist“. Wir zeigen zuerst die erste Teilaussage: Sei dazu  $x \in A \cup B$  beliebig. Nach der Definition der Vereinigung bedeutet das, dass  $x \in A \vee x \in B$  wahr ist. Wegen der Vertauschbarkeit der Operanden von „ $\vee$ “ (Kommutativgesetz von  $\vee$ ) folgt, dass  $x \in B \vee x \in A$ . Wendet man ein zweites Mal die Definition von  $\cup$  an, so erhält man:  $x \in B \cup A$ . Die zweite Teilaussage beweist man genauso. **q.e.d.**

Bemerkung 21: Man mag sich darüber streiten, ob es sinnvoll ist, in dem obigen Beweis beide Teilaussagen getrennt beweisen zu wollen. Lassen sich doch die Umformungen als Äquivalenzumformungen auffassen. Hier ist ein Wort der Warnung angebracht: „Äquivalenzbeweise sind für Anfänger äußerst gefährlich.“ Nur zu häufig werden bei Äquivalenzbeweisen Voraussetzung und Folgerung durcheinandergebracht, Äquivalenzumformungen gemacht, die gar keine sind und Argumente nicht auf den Punkt gebracht. Eines der Lernziele dieser Veranstaltung ist es jedoch, dass Sie eine Voraussetzung und eine Folgerung unterscheiden können. Äquivalenzbeweise stehen diesem Lernziel entgegen. **Deshalb sind Äquivalenzbeweise in dieser Veranstaltung prinzipiell verboten.** Zur Ermittlung des Ergebnisses einer Vereinigung von Mengen kommt

es nicht auf die Reihenfolge der Operanden an.

**ASSOZIATIVGESETZE:**

Es gilt für beliebige Mengen  $A, B, C$ :

**Satz 2.8.2**

Assoziativgesetze

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

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

Deshalb kommt es nicht auf die Klammersetzung an.

**DISTRIBUTIVGESETZE:**

Es gilt für beliebige Mengen  $A, B, C$ :

**Satz 2.8.3**

Distributivgesetze

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

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

Distributivgesetze ermöglichen ein „Aus- und Einklammern“.

**DE MORGANSCHEN REGELN:**

Seien  $S, T$  beliebige Teilmengen des Universums  $M$ . Dann gilt

**Satz 2.8.4** De  
Morgansche  
Regeln

$$\overline{S \cup T} = \overline{S} \cap \overline{T}$$

$$\overline{S \cap T} = \overline{S} \cup \overline{T}$$

**PAPIERKORB:**

Es gibt einen Unterschied zwischen der Methode, wie man auf einen Beweis kommt und wie man einen Beweis aufschreibt. Der menschliche Geist ist eher sprunghaft und nicht linear in der Denkweise. Ein Beweis muss aber immer bei der Voraussetzung starten und bei der Folgerung enden. Deshalb ist es normal, dass Überlegungen in den Papierkorb gehören. Es ist kein Zeichen von Dummheit, wenn ein Beweis mehrfach formuliert werden muss. Im Gegenteil, ein guter Beweis muss reifen. Insofern ist der Papierkorb ein sehr wichtiges Arbeitsinstrument. Wenn ein Beweis fertig ist, sollten:

1. Mit der Voraussetzung beginnend logische Schlüsse angewendet werden.
2. Anwendungen von Definitionen und Sätzen deutlich gemacht werden.
3. Ein Schluss auf dem vorhergehenden aufbauen.
4. Am Ende die gesamte Behauptung folgern.
5. Nichts Überflüssiges bewiesen werden.
6. Nichts doppelt beschrieben werden.

Prinzip :  
*Papierkorb*

**Aufgabe 2.16:**

Venn Diagramme für Mengenbeziehungen mit drei Mengen  $A, B, C$  können prinzipiell als Beweis anerkannt werden, weil im Prinzip alle acht Fälle von Zugehörigkeiten zu den Mengen abgebildet werden können. Vergewissern Sie sich davon, indem Sie eine boolesche Wahrheitstabelle mit den drei Einträgen  $x \in A$ ,  $x \in B$  und  $x \in C$  aufstellen und den Zeilen der Wahrheitstabelle den Bereichen eines Venn Diagramms zuordnen.

**Aufgabe 2.17:**

Beweisen Sie eines der Distributivgesetze aus Satz 2.8.3.

**Aufgabe 2.18:**

Disney World

Zum Schluss noch eine Aufgabe, bei der es ohne die Benutzung von Venn Diagrammen sicherlich nicht leicht fällt, den Überblick zu bewahren.

Bei einer Befragung von Kindern, die in Disney World drei verschiedene

Vorführungen sahen, kam folgendes heraus:

- 39 Kinder mochten „Die kleine Meerjungfrau“
- 43 Kinder mochten „101 Dalmatiner!“
- 56 Kinder mochten „Mickey Mouse“
- 7 Kinder mochten „Die kleine Meerjungfrau“ und „101 Dalmatiner“
- 10 Kinder mochten „Die kleine Meerjungfrau“ und „Mickey Mouse“
- 16 Kinder mochten „101 Dalmatiner“ und „Mickey Mouse“
- 4 Kinder mochten „Die kleine Meerjungfrau“, „101 Dalmatiner“ und „Mickey Mouse“
- 6 Kinder mochten keine der Vorführungen.

Beantworten Sie die folgenden Fragen:

- Wie viele Kinder wurden insgesamt befragt?
- Wie viele Kinder mochten nur „Die kleine Meerjungfrau“?
- Wie viele Kinder mochten nur „101 Dalmatiner“?
- Wie viele Kinder mochten nur „Mickey Mouse“?

## 2.9 Naive und axiomatische Mengenlehre

Die von Cantor verfasste Definition über die Menge ist etwas ungenau: Wie wir an Beispielen sehen werden, führt die uneingeschränkte Erzeugung von Mengen nach diesem Standpunkt auf Widersprüche (sogenannte Antinomien). Entdeckungen dieser Art haben seit dem Beginn des 20. Jahrhunderts (beginnend mit Ernst Zermelo) zu einem Überdenken der Grundlagen der Mathematik geführt. In der „axiomatischen Mengenlehre“ wird versucht, Regeln für den Umgang mit Mengen auf formale Weise aus möglichst wenigen Grundannahmen (Axiomen) herzuleiten, so dass Objekte wie die „Menge aller Mengen“ gar nicht erst auftreten.

**Beispiel 2.9.1** *Antinomie des Barbiers*

Nehmen wir einen Barbier (Friseur) eines kleinen Dorfes. Er bekommt von den Dorfältesten den Auftrag, nur all diejenigen zu rasieren, die dies nicht selbst tun können. Hält sich der Barbier streng an seinen Auftrag, so darf er sich selber nicht rasieren, weil ihm das nur bei Leuten gestattet ist, die sich nicht selber rasieren. Rasiert er sich aber nicht, so muss er sich doch rasieren, aus eben demselben Grund. Fazit: Egal was er macht, er macht es falsch und hält sich nicht an seinen Auftrag.

Eng verwandt mit der Antinomie des Barbiers ist das folgende Beispiel:

**Beispiel 2.9.2** *Menge aller Mengen, die sich nicht als Element enthalten*

Wir betrachten die Menge  $M = \{x \mid x \notin x\}$ . Wir fragen uns nun, ob  $M \in M$  oder  $M \notin M$ , genau eine von beiden Situationen muss ja richtig sein. Aus  $M \in M$  folgt aber aus der Definition der Menge sofort  $M \notin M$ . Und aus  $M \notin M$  folgt auch wegen der Definition von  $M$   $M \in M$ . Wir erkennen, dass beide Situationen zu einem Widerspruch führen. Das Bilden der Menge  $M$  ist also nicht sinnvoll.

**Beispiel 2.9.3** *Menge aller Mengen*

Eine andere Antinomie tritt auf, wenn man nach der Mächtigkeit der Menge aller Mengen schlechthin fragt. Man sieht leicht ein, dass man ihr keine Mächtigkeit zuordnen kann, denn wenn sie wirklich alle Mengen enthielte, müsste auch alle Teilmengen dabei sein. Damit ist die Potenzmenge eine Teilmenge der Menge selbst. Die Potenzmenge ist aber, wie wir gesehen haben, stets von höherer Mächtigkeit als die Menge selbst.

Fazit: Die Menge aller Mengen ist daher ein in sich widersprüchlicher Begriff.

Ziel der axiomatischen Mengenlehre ist es nun, das Mengenbildungsprinzip „definierende Eigenschaft“ so zu formulieren, dass widersprüchliche Mengen nicht entstehen können. Also eine präzise Formulierung aller „legalen definierenden Eigenschaften“ zu finden. Dies ist der Hintergrund zu der Aussage von David Hilbert, die als Zitat an den Beginn dieses Kapitels gestellt wurde.

Ein praktischer Standpunkt - den wir auch hier vertreten - ist der, trotz allem die Anschauungen der naiven Mengenlehre zuzulassen, problematische Konstruktionen wie die „Menge aller Mengen“ (oder auch Mengen, die sich selbst

als Element enthalten) aber zu vermeiden.

## Kapitel 3

# Logik

*“Logik ist die Anatomie des Denkens.”*  
—John Locke (1632-1704), engl. Philosoph

### 3.1 Aussagen und Aussageformen

Charakteristisch an der (klassischen) Aussagenlogik ist, dass als Grundelemente nur die Elementaraussagen „wahr“ und „falsch“ zugelassen werden. Man spricht von einer „zweiwertigen“ Logik, weil nur diese zwei Werte zugelassen sind.

**WAHRHEITSWERTE:**

In der Aussagenlogik betrachten wir die zwei **aussagenlogischen Konstanten (Wahrheitswerte)** „wahr“ und „falsch“.

**Definition 3.1.1**  
Wahrheitswerte

**Definition 3.1.2**  
aussagenlogische  
Aussage

**AUSSAGENLOGISCHE AUSSAGE:**

Eine **aussagenlogische Aussage** ist nun ein Konstrukt, in dem die Elementaraussagen „wahr“ und „falsch“ über Operatoren miteinander verknüpft werden. Solche Operatoren sind die Verknüpfung „und“, „oder“, „wenn ... , dann ...“ oder der in der technischen Realisierung wichtige „nand“ Operator. Diese Operatoren werden häufig auch als aussagenlogische Junktoren bezeichnet. Der Wahrheitswert einer solchen zusammengesetzten Aussage ergibt sich nun ausschließlich aus dem Wahrheitswert der beteiligten Elementaraussagen. Diese Forderung bezeichnet man auch als das **Extensionalitätsprinzip** der Aussagenlogik.

**Beispiel 3.1.1** „wenn wahr, dann falsch“, „wahr oder nicht wahr“ „wenn entweder wahr oder falsch dann falsch“ sind Aussagen.

Dem Extensionalitätsprinzip zufolge, muss es für jeden Operator eine Wahrheitstabelle geben. Beispiele für solche Wahrheitstabellen sind:

**Beispiel 3.1.2** Für den aussagenlogischen Junktor „und“ verwendet man das Symbol „ $\wedge$ “. Seine Wahrheitstabelle ist:

A	B	$A \wedge B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	falsch
falsch	falsch	falsch

**Beispiel 3.1.3** Für den aussagenlogischen Junktor „oder“ verwendet man das Symbol „ $\vee$ “. Seine Wahrheitstabelle ist:

A	B	$A \vee B$
wahr	wahr	wahr
wahr	falsch	wahr
falsch	wahr	wahr
falsch	falsch	falsch



**Beispiel 3.1.4** Für den aussagenlogischen Junktor „entweder ... oder ...“ verwendet man das Symbol „ $\dot{\vee}$ “. Seine Wahrheitstabelle ist:

A	B	$A \dot{\vee} B$
wahr	wahr	falsch
wahr	falsch	wahr
falsch	wahr	wahr
falsch	falsch	falsch

**Beispiel 3.1.5** Für den aussagenlogischen Junktor „wenn ... dann ...“ verwendet man das Symbol „ $\Rightarrow$ “. Seine Wahrheitstabelle ist:

A	B	$A \Rightarrow B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	wahr
falsch	falsch	wahr

Aussagen, deren äusserer Junktor ein „ $\Rightarrow$ “ ist, werden auch Implikation genannt.

**Beispiel 3.1.6** Für den aussagenlogischen Junktor „genau dann ... wenn ...“ verwendet man das Symbol „ $\Leftrightarrow$ “. Seine Wahrheitstabelle ist:

A	B	$A \Leftrightarrow B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	falsch
falsch	falsch	wahr

Aussagen, deren äusserer Junktor ein „ $\Leftrightarrow$ “ ist, werden auch Äquivalenz genannt.

**Beispiel 3.1.7** Von besonderer Bedeutung ist der einstellige Junktor „nicht“. Man verwendet das Symbol „ $\neg$ “. Seine Wahrheitstabelle ist:

A	$\neg A$
wahr	falsch
falsch	wahr

**Definition 3.1.3**  
aussagenlogische  
Aussageform

**AUSSAGENLOGISCHE AUSSAGEFORM:**

Eine **aussagenlogische Aussageform** (über den Variablen  $x_1, \dots, x_n$ ) ist nun ein sprachliches Konstrukt, in dem Wahrheitswerte (wahr, falsch) und aussagenlogische Variablen  $x_1, \dots, x_n$  über aussagenlogische Operatoren miteinander verknüpft werden.

Durch Einsetzen von Wahrheitswerten für die aussagenlogischen Variablen  $x_1, \dots, x_n$  erhält man eine aussagenlogische Aussage.

Ergibt sich aus einer aussagenlogischen Aussageform über den Variablen  $x_1, \dots, x_n$  unabhängig von den für die Variablen eingesetzten Wahrheitswerte eine wahre (falsche) Aussage, so heißt die Aussageform eine **Tautologie** (**Kontradiktion**).

**Beispiel 3.1.8** Beispiele für aussagenlogische Aussageformen:

- „wahr  $\vee x_1$ “ ist eine aussagenlogische Aussageform.
- „ $x_1 \vee \neg x_1$ “ ist eine Tautologie.
- „ $x_1 \wedge \neg x_1$ “ ist eine Kontradiktion

Um die Realität beschreiben zu können muss man die Zerlegung von Aussagen noch weiter treiben, als in der Aussagenlogik üblich. Es reicht nicht mit den Elementaraussagen wahr und falsch zu arbeiten, sondern man will mit Aussagen wie „Bremen liegt an der Weser“, „No. 5 lebt“ oder „Lessing schrieb Minna von Barnhelm“ arbeiten. Solche sprachlichen Gebilde eignen sich zum Aufbau einer Logik, da sie ja genau einen Wahrheitswert haben. Darüberhinaus verwenden sie aber Dinge unserer Anschauung oder unseres Denkens (Bremen, Weser, No. 5, Lessing, Minna von Barnhelm) und Beziehungen zwischen diesen: „liegt an“, „lebt“ oder „schrieb“. Solche Beziehungen nennt man in der Logik „Prädikate“.

**Definition 3.1.4**  
Prädikat

**PRÄDIKAT:**

Ein  $n$ -stelliges Prädikat ordnet jedem  $n$ -tupel von Objekten unserer Anschauung oder unseres Denkens einen Wahrheitswert zu.

**Beispiel 3.1.9** Beispiele für Prädikate in dem obigen Text:

- „liegt an“, „schrieb“ sind zweistellige Prädikate
- „lebt“ ist ein einstelliges Prädikat

Bemerkung 22: Um die Stelligkeit eines Prädikats hervorzuheben, kann man für jede Stelle des Prädikats einen  $\cdot$  setzen:

- „ $\cdot$  liegt an  $\cdot$ “, „ $\cdot$  schrieb  $\cdot$ “ sind zweistellige Prädikate
- „ $\cdot$  lebt“ ist ein einstelliges Prädikat

Wir werden im Folgenden statt der elementaren Wahrheitwerte „wahr“ und „falsch“ Prädikate verwenden. Also statt die Aussage „wenn wahr dann wahr“ zu untersuchen, werden wir in Zukunft Aussagen der Form „Wenn Bremen an der Weser liegt, dann schrieb Lessing Minna von Barnhelm.“ betrachten. Solche Konstrukte werden **prädikatenlogische Aussagen** genannt.

Bemerkung 23: Prädikatenlogische Aussagen enthalten

- Prädikate die einen Wahrheitswert „wahr“ oder „falsch“ ergeben, indem sie
- Objekte unserer Anschauung oder unsres Denkens in Beziehung setzen. Sowie
- Aussagenlogische Junktoren, die die Prädikate miteinander verbinden.

Prädikatenlogische Aussagen haben immer einen Wahrheitswert „wahr“ oder „falsch“.

Bemerkung 24: Bitte beachten Sie die besondere Bedeutung die dem Extensionalitätsprinzip nun zufällt: Der Wahrheitswert der Gesamtaussage hängt nur von dem Wahrheitswert der Einzelaussagen ab. Es wird also in dem Satz „Wenn Bremen an der Weser liegt, dann schrieb Lessing Minna von Barnhelm.“ nicht untersucht, ob ein kausaler Zusammenhang zwischen der Tatsache, dass Bremen an der Weser liegt und dass Lessing Minna von Barnhelm schrieb gesucht. Allein der Wahrheitsgehalt der Einzelaussagen bestimmt den Wahrheitsgehalt der Gesamtaussage.

Entsprechend den aussagenlogischen Variablen werden wir nun auch prädikatenlogische Objektvariablen einführen, die beliebige Objekte repräsentieren können. Wir werden also Konstrukte betrachten wie „ $x$  liegt an der Weser“ oder „ $x_1$  liegt an der  $x_2$ “. Entsprechend der aussagenlogischen Aussageform aus Definition 3.1.3 führen wir den Begriff der prädikatenlogischen Aussageform ein:

Bemerkung 25: Prädikatenlogische Aussageformen enthalten

- Prädikate
- Objekte unserer Anschauung oder unseres Denkens
- Variablen für Objekte unserer Anschauung oder unseres Denkens
- Aussagenlogische Junktoren, die die Prädikate miteinander verbinden.

Da prädikatenlogische Aussageformen immer Variablen enthalten, denen keine Werte zugewiesen sind (wir sprechen von sogenannten **freien Variablen**), kann man ihnen keinen Wahrheitswert zuordnen.

Bemerkung 26: Wir haben schon im Kapitel Mengenlehre intensiv von prädikatenlogischen Aussageformen Gebrauch gemacht, wenn wir Mengen durch definierende Eigenschaften festgelegt haben. Zum Beispiel benutzt die Definition der Menge der Lebewesen  $L = \{x|x \text{ lebt}\}$  das einstellige Prädikat „lebt“.

Jede prädikatenlogische Aussageform  $Q(x)$  mit einer freien Variablen definiert also eine Menge  $\{x|Q(x)\}$ . Umgekehrt definiert jede Menge  $M$  auch eine prädikatenlogische Aussageform  $x \in M$ .

Bemerkung 27: Der aufmerksame Leser mag sich zwei Fragen (welch Unterstellung! wenn Sie sich das nicht fragen, sind Sie dann etwa nicht aufmerksam?!) stellen.

1. Warum betrachtet man prädikatenlogische Aussageformen, wenn ihnen doch kein Wahrheitswert zugeordnet ist?
2. Warum wurden Bemerkungen zur prädikatenlogischen Aussage und zur prädikatenlogischen Aussageform nicht als Definition formuliert? Schließlich haben Sie sich schon so an das Arbeiten mit Definitionen gewöhnt, dass Ihnen etwas fehlt!

Der Grund dafür ist, dass uns noch ein wesentlicher Bestandteil von prädikatenlogischen Aussagen fehlt: Man kann Aussageformen, in denen eine prädikatenlogische Variable vorkommt, durch eine „Mengenangabe“ für diese Variable in eine prädikatenlogische Aussage umwandeln. Beispielfhaft sei die Aussage „Alle Männer sind Schweine.“ genannt sein. Das Wort Männer steht eigentlich für eine prädikatenlogische Variable, die alle Männer durchläuft, und für deren Ausprägungen behauptet wird, dass sie Schweine seien. Wir starten also mit einer prädikatenlogischen Aussageform „ $x$  ist ein Schwein“. Da die Variable  $x$  nicht weiter festgelegt ist, hat diese Aussageform keinen Wahrheitswert.

Aber durch eine **Generalisierung** „Für alle  $x$ , die Mann sind“ wird sie zu einer prädikatenlogischen Aussage, hat dann also einen Wahrheitswert (ich sage nicht welchen ;-)). Neben einer Generalisierung werden wir als „Mengenangabe“ auch die **Partikularisierungen**, also eine Aussage über eine Existenz, besprechen. Generalisierungen und Partikularisierungen bezeichnet man gemeinsam als **Quantifizierungen** und die sprachlichen Konstrukte, die die Quantifizierungen ausdrücken als **Quantoren**.

**Aufgabe 3.1:**

Bestimmen Sie, ob es sich bei den folgenden sprachlichen Konstrukten um aussagenlogische/prädikatenlogische Aussagen/Aussageformen handelt.

1. wahr  $\vee$  falsch
2. Das Ulmer Münster steht in Münster
3. Das Ulmer Münster steht in  $x$
4. Wenn das Ulmer Münster in  $x$  steht, dann liegt  $x$  an der Donau
5. (Das Ulmer Münster steht in  $x$ )  $\Rightarrow$  ( $x$  liegt an der Donau)
6. (Das Ulmer Münster steht in  $x$ )  $\Rightarrow$  ( $y$  liegt an der Donau)
7. wahr  $\vee x$
8. ( Das Ulmer Münster steht in  $x$ )  $\Rightarrow x$

**Aufgabe 3.2:**

Bestimmen Sie in den folgenden Aussagen Prädikate und deren Stelligkeit:

1. Boris Becker gewann Wimbledon.
2. Hans ist doof.
3. Ralf Schuhmacher ist Formel 1 Weltmeister.
4. Ralf Schuhmacher ist der Bruder von Michael Schuhmacher.
5. Rotkäppchen ist Waise.
6. Der bürgerliche Name von Rotkäppchen ist Anna Moik.
7.  $2 > 5$
8.  $2 + 3 = 5$

### 3.2 Allquantor

Wir führen zunächst den Allquantor ein. Der Allquantor beschreibt die Situation, dass eine Aussageform für alle Dinge eines Betrachtungsbereichs richtig ist. Wir werden Beispiel für Aussagen mit Allquantoren geben. Dabei starten wir mit der einfachen Situation mit nur einem Allquantor und schauen uns dann an, was passiert, wenn mehr als ein Allquantor in einer Aussage vorkommt.

Betrachten wir also zum Beispiel die Aussageform „ $x$  ist Schwein“. Dann wäre eine Generalisierung: „Für alle Männer  $x$  gilt:  $x$  ist Schwein“. Beachten Sie bitte, dass die Variable  $x$  in der zweiten Aussage nicht mehr frei wählbar ist, sondern durch den Allquantor „Für alle Männer  $x$ “ gebunden wird. Dadurch können wir der Aussage einen Wahrheitswert zuordnen.

#### ALLQUANTOR:

Sei  $Q(x_1, \dots, x_n)$  eine prädikatenlogische Aussageform mit  $n$  freien Variablen  $x_1, \dots, x_n$ , unter denen  $x_i$  eine ist. Dann bezeichnet

$$\forall x_i : Q(x_1, \dots, x_n)$$

eine prädikatenlogische Aussageform mit  $n-1$  Variablen. Im Spezialfall  $n = 1$  erhalten wir eine prädikatenlogische Aussage, die genau dann wahr ist, wenn  $Q(x_1)$  für alle Dinge unserer Anschauung oder unseres Denkens wahr ist.

**Definition 3.2.1**  
Allquantor

**Beispiel 3.2.1**  $x = x$  ist eine prädikatenlogische Aussageform mit einer freien Variablen  $x$ . Das Prädikat ist der zweistellige Vergleichsoperator „ $=$ “. Da der Variablen  $x$  kein Wert zugeordnet ist, wollen wir der Aussageform auch keinen Wahrheitswert zuordnen. Schreiben wir allerdings  $\forall x : x = x$  so haben wir die Variable  $x$  an den Allquantor  $\forall$  gebunden und erhalten nun eine prädikatenlogische Aussage, denn es kommt keine freie Variable mehr vor. Diese Aussage ist wahr.

**Beispiel 3.2.2**  $x = 42$  ist eine prädikatenlogische Aussageform mit einer freien Variablen  $x$ . Das Prädikat ist der zweistellige Vergleichsoperator „ $=$ “, der allerdings durch die Verwendung der Konstanten 42 zu einem einstelligen Prädikat wird.  $\forall x : x = 42$  ist eine falsche Aussage, da z.B. für  $x = \text{Saturn}$  die Aussage „Saturn=42“ falsch ist.

**Beispiel 3.2.3**  $\forall x : x = 42 \vee x \neq 42$  ist eine prädikatenlogische Aussage, die wahr ist.

**Beispiel 3.2.4**  $x = y$  ist eine prädikatenlogische Aussageform mit zwei freien Variablen  $x$  und  $y$ .  $\forall x : x = y$  ist eine prädikatenlogische Aussageform mit einer freien Variablen  $y$ . Die andere Variable  $x$  wird durch den Allquantor gebunden. Auch dieser Aussageform ist kein Wahrheitswert zugeordnet. Erst wenn auch die zweite Variable durch einen Quantor gebunden wird, entsteht eine prädikatenlogische Aussage:  $\forall y : \forall x : x = y$  ist falsch.

Bitte bedenken Sie, dass diese Ihnen sicher sinnlos erscheinende Aussage in der Praxis häufig geäußert wird: Das ist hier doch alles dieselbe Sch... .

In der Definition 3.2.1 des Allquantors lassen wir die Laufvariable uneingeschränkt durch alle Objekte unserer Anschauung oder unseres Denkens laufen. Diese Form der Allaussage ist sehr selten, da man üblicherweise den Betrachtungsbereich für seine Objekte einschränken möchte. Wir möchten eben nur Aussagen über alle Männer treffen und nicht über alle Objekte unseres Denkens oder unserer Anschauung. Dazu betrachten wir die Menge  $M = \{x | x \text{ ist Mann}\}$  aller Männer und wollen so etwas definieren wie:  $\forall x \in M : x \text{ ist Schwein}$ .

#### EINGESCHRÄNKTER ALLQUANTOR:

Sei  $Q(x)$  eine prädikatenlogische Aussageform, in der die freie Variable  $x$  vorkommt und  $M$  eine beliebige Menge.

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

ist äquivalent zu:

$$\forall x : x \in M \Rightarrow Q(x)$$

**Definition 3.2.2**  
eingeschränkter  
Allquantor

**Bemerkung 28:** Manche Autoren verwenden statt des Symbols  $\forall$  das Symbol  $\bigwedge$ . Die Aussage  $\bigwedge x \in \{x_1, x_2, \dots, x_n, \dots\} : Q(x)$  soll an die Aussage  $Q(x_1) \wedge Q(x_2) \wedge \dots \wedge Q(x_n) \wedge \dots$  erinnern.

Bitte beachten Sie die besondere Bedeutung der Implikation  $\Rightarrow$ . Nach ihrer Wahrheitstafel spielt die Eigenschaft  $Q(x)$  nur dann eine Rolle, wenn  $x \in M$ . Ist  $x$  außerhalb von  $M$ , ist die Aussage sowieso wahr. Die Verwendung der Im-

plikation in Verbindung mit dem Allquantor ist fast so etwas wie eine goldene Regel:

Verwende  $\forall$  nur in Verbindung mit „ $\Rightarrow$ “ als äußerem logischen Junktor.

**Beispiel 3.2.5** Wir betrachten die Menge  $I05a$  aller Studenten der Wirtschaftsinformatik der Nordakademie, die in der  $I05a$  sind. Die Aussage „ $\forall x \in I05a : x$  ist anwesend in der Vorlesung“ ist gleichwertig zu der Aussage „ $\forall x : x \in I05a \Rightarrow$  ist anwesend in der Vorlesung“. Für alle Studenten, die nicht in der  $I05a$  sind, wird nichts ausgesagt. Genau so wenig wie über „ $x = \text{Saturn}$ “ oder „ $x = 42$ “.

**Beispiel 3.2.6** Wir wollen den Wahrheitswert der Aussage „Alle meine Entchen schwimmen auf dem See“ ermitteln. Dazu wollen wir das zunächst in eine prädikatenlogische Aussage umformen. Wir betrachten die Menge  $ME = \{x | x \text{ ist mein Entchen}\}$ , sowie das einstellige Prädikat „schwimmt auf dem See“. Dann formuliert man die Aussage „Alle meine Entchen schwimmen auf dem See“ mit Hilfe von Quantoren durch:  $\forall x \in ME : x \text{ schwimmt auf dem See}$ . Bei dieser Aussage handelt es sich also um eine sehr einfache Generalisierung: Wir benutzen einen eingeschränkten Allquantor und ein einstelliges Prädikat. Da keine freie prädikatenlogische Variable in der Aussage mehr vorkommt, kann man dieser Aussage einen Wahrheitswert zuordnen. Was meinen Fall betrifft, so muss ich zugeben, dass die Menge meiner Entchen leer ist. Somit stellt sich die Frage, ob diese Aussage auch wahr sein kann, wenn die Einschränkung so groß ist, dass gar keine Elemente betrachtet werden. Ohne lang zu mutmaßen und zu grübeln, lassen Sie uns die Definition 3.2.2 des eingeschränkten Allquantors anwenden, wir müssen prüfen, ob die Aussage

$$\forall x : x \in \emptyset \Rightarrow x \text{ schwimmt auf dem See}$$

wahr ist. Nach der Definition des Allquantors ist das genau dann der Fall, wenn für alle Objekte  $x$  unseres Denkens und unserer Anschauung die Aussage „ $x \in \emptyset \Rightarrow x$  schwimmt auf dem See“ wahr ist. Nun ist die Aussage  $x \in \emptyset$  aber für alle Objekte unseres Denkens und unserer Anschauung falsch. Wegen der Wahrheitstafel von  $\Rightarrow$  folgt aber, dass die Implikation ohne Ansehen des Prädikats „ $x$  schwimmt auf dem See“ wahr wird. Mit anderen Worten, weil es unmöglich ist, dass „ $x \in \emptyset$ “ wahr wird, ist die Aussage „Alle meine Entchen schwimmen auf dem See“ eine wahre Aussage.



**Beispiel 3.2.7** Casanova pflegte zu sagen: „Ich liebe alle Frauen.“ Wir wollen dies in eine prädikatenlogische Aussage umformen. Dazu benötigen wir zuerst eine Menge als Betrachtungsbereich. Dies ist die Menge  $F = \{x | x \text{ ist Frau}\}$ . Dann noch ein einstelliges Prädikat „Ich liebe“.

Als Generalisierung formuliert bedeutet das  $\forall x \in F : \text{Ich liebe } x$ .

Überlassen wir die Wahrheit dieser Aussage den Geschichtsschreibern.

**Beispiel 3.2.8** Mit der Prädikatenlogik sind wir in der Lage, Definitionen, die wir verbal formuliert haben präzise zu formulieren. Beispiel: Definition der Teilmenge: Seien  $S, T$  zwei beliebige Mengen. Wir definieren:  $S \subseteq T \Leftrightarrow \forall x \in S : x \in T$ . Oder mit dem uneingeschränkten Allquantor:  $S \subseteq T \Leftrightarrow \forall x : x \in S \Rightarrow x \in T$ .

Die natürliche Sprache hat viele Möglichkeiten, einen Allquantor auszudrücken. Ein Informatiker sollte diese Möglichkeiten kennen, denn er muss in der Lage sein, Aussagen, die ein Auftraggeber - im allgemeinen ein Betriebswirt - macht, auf ihren inneren Gehalt hin zu analysieren und im Zweifelsfall nachzufragen. Hier eine kurze Auswahl:

- Schlüsselwörter wie „Alle“ oder „Jede“ deuten offensichtlich auf eine Generalisierung hin.
- In der Aussage „Ein Hund frisst gern Knochen.“ wird der unbestimmte Artikel „ein“ genutzt um eine Generalisierung anzudeuten. Gemeint ist natürlich: „Alle Hunde fressen gerne Knochen.“ Der Duden spricht hier von einer **existenziellen Generalisierung**.
- Manchmal ist es auch ein bestimmter Artikel, der eine Generalisierung anzeigt. In den 60'er Jahren gab es einen Werbespruch: „Drei Dinge braucht der Mann.“ Auch hier eine Aussage über alle Männer.
- Manchmal steht auch nur einfach ein Plural: „Real programmers don't use Pascal.“ Eine Generalisierung über alle „Wahren Programmierer“.

Wir wollen noch ein paar Beispiele zum Wahrheitswert für prädikatenlogische Aussagen machen.

**Beispiel 3.2.9** Beispiele für Aussagen mit Allquantoren:

- Die Aussage  $\forall y \in \mathbb{N} : y \geq 1$  ist offensichtlich wahr.
- Die Aussage  $\forall y \in \mathbb{N} : y > 1$  ist offensichtlich falsch, wie das Gegenbeispiel  $y = 1$  zeigt.
- Die Aussage  $\forall y \in \mathbb{N} : y > x$  ist keine prädikatenlogische Aussage, sondern eine prädikatenlogische Aussageform, da sie noch eine freie Variable  $x$  enthält. Als Aussageform ist ihr kein Wahrheitswert zugeordnet.
- Die Aussage  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : y > x$  ist falsch. Wie können wir das einsehen? Es reicht ein Beispiel für  $x$  zu finden, so dass die Aussageform  $\forall y \in \mathbb{N} : y > x$  eine falsche Aussage wird, wenn wir den Wert für  $x$  einsetzen. Zum Beispiel für  $x = 1$  entsteht die falsche Aussage:  $\forall y \in \mathbb{N} : y > 1$ .
- Die Aussage  $\forall y \in \mathbb{N} : \forall x \in \mathbb{N} : y > x$  ist falsch. Wie können wir das einsehen? Es reicht ein Beispiel für  $y$  zu finden, so dass die Aussageform  $\forall x \in \mathbb{N} : y > x$  eine falsche Aussage wird, wenn wir den Wert für  $y$  einsetzen. Etwa für  $y = 1$  entsteht die falsche Aussage:  $\forall x \in \mathbb{N} : 1 > x$ .

Der Unterschied der letzten beiden Beispiele besteht in der Reihenfolge der Quantoren.

**VERTAUSCHBARKEIT VON ALLQUANTOREN:**

Sei  $Q(x, y)$  eine Aussageform mit zwei freien Variablen. Dann ist:

$$(\forall x : \forall y : Q(x, y)) \Leftrightarrow (\forall y : \forall x : Q(x, y))$$

oder in der Form mit eingeschränkten Allquantoren.

Dafür seien  $M$  und  $N$  beliebige Mengen:

$$(\forall x \in M : \forall y \in N : Q(x, y)) \Leftrightarrow (\forall y \in N : \forall x \in M : Q(x, y))$$

**Satz 3.2.1**

Vertauschbarkeit  
von Allquantoren

Bemerkung 29: Bei der Verwendung der Generalisierungen muss man aufpassen, wie Klammern gesetzt werden. Die Aussage „Männer sind unrasiert.“ und „Männer sind liederlich.“ ist äquivalent zur Aussage „Männer sind unrasiert und liederlich.“ Aber eine Aussage „Männer sind langweilig oder vergeben.“ ist nicht äquivalent zu: „Männer sind langweilig.“ oder „Männer sind vergeben.“ Im ersten Fall nämlich hängt die „Langweiligkeit“ vom einzelnen Mann ab. Manche sind so, andere anders, jeder aber wenigstens eins von beiden. In der zweiten Aussage wird behauptet, dass alle Männer langweilig sind, oder dass

alle Männer vergeben sind.

Wir formulieren diese Bemerkung als Satz:

**KONJUNKTION UND ALLQUANTOREN:**

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Dann ist:

$$(\forall x : P(x)) \wedge (\forall x : Q(x)) \Leftrightarrow \forall x : P(x) \wedge Q(x)$$

**Satz 3.2.2**  
Konjunktion und  
Allquantoren

Bemerkung 30: Da Allquantoren im Kern verallgemeinerte Konjunktionen sind, ist dieser Satz so etwas wie ein Kommutativgesetz, denn wenn wir die beiden Seiten als Konjunktionen schreiben, verändert sich nur die Reihenfolge der Operanden.

Bemerkung 31: Die Variable  $x$  wird in der obigen Aussage dreimal gebunden. Man könnte statt dessen auch schreiben:

$$(\forall x : P(x)) \wedge (\forall y : Q(y)) \Leftrightarrow \forall z : P(z) \wedge Q(z)$$

**DISJUNKTIONEN VON ALLQUANTOREN:**

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Aus

$$(\forall x : P(x)) \vee (\forall x : Q(x))$$

folgt

$$\forall x : P(x) \vee Q(x)$$

**Satz 3.2.3**  
Disjunktionen von  
Allquantoren

Die beiden Aussagen sind im **Allgemeinen nicht äquivalent**.

Bemerkung 32: Die fehlende Äquivalenz ist nicht erstaunlich, wenn wir beachten, dass der Allquantor nichts anderes ist als eine verallgemeinerte Konjunktion. Konjunktionen und Disjunktionen lassen sich eben nicht beliebig umordnen.

**Satz 3.2.4**  
Implikation und  
Allquantoren

**IMPLIKATION UND ALLQUANTOREN:**

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Aus

$$(\forall x : P(x) \Rightarrow Q(x))$$

folgt

$$(\forall x : P(x)) \Rightarrow (\forall x : Q(x))$$

Die beiden Aussagen sind im **Allgemeinen nicht äquivalent**.

**Satz 3.2.5**  
Äquivalenz und  
Allquantoren

**ÄQUIVALENZ UND ALLQUANTOREN:**

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Aus

$$(\forall x : P(x) \Leftrightarrow Q(x))$$

folgt

$$(\forall x : P(x)) \Leftrightarrow (\forall x : Q(x))$$

Die beiden Aussagen sind im **Allgemeinen nicht äquivalent**.

**Aufgabe 3.3:**

Definieren Sie für die folgenden Behauptungen in natürlicher Sprache Prädikate und schreiben Sie sie als eingeschränkte und uneingeschränkte Generalisierungen. Machen Sie eine Aussage zum Wahrheitsgehalt.

1. Alle Nordakademiedozenten sind lieb.
2. Alle Nordakademiedozenten lieben alle Nordakademiestudenten.
3. Männer sterben an Herzinfarkt.
4. Männer bestechen durch ihr Geld und ihre Lässigkeit.
5. Männer lieben Autos. Benutzen Sie ein einstelliges Prädikat.
6. Männer lieben Autos. Benutzen Sie ein zweistelliges Prädikat.
7. Alle Marsmännchen sind Mitglieder im deutschen Bundestag.

**Aufgabe 3.4:**

Beweisen Sie durch eine Wahrheitstafel:

$x \Rightarrow (y \Rightarrow z)$  ist äquivalent zu  $(x \wedge y) \Rightarrow z$ .

Benutzen Sie das, um zu zeigen, dass für beliebige Mengen  $M, N$  und beliebige prädikatenlogische Aussageformen  $Q(x, y)$  mit zwei freien Variablen  $x, y$ :

$$(\forall x \in M : \forall y \in N : Q(x, y)) \Leftrightarrow (\forall y : \forall x : (x \in M \wedge y \in N) \Rightarrow Q(x, y))$$

### Aufgabe 3.5:

Handelt es sich bei den folgenden Konstrukten um Aussagen oder um Aussageformen:

1.  $\forall x \in \mathbb{N} : x > y$
2.  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : (x + y)^2 > 3 * x$
3.  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : x > 10 \Rightarrow (x + y)^2 > 127$
4.  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : x > 10 \Rightarrow y + x > 20$
5.  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : y * x > 20 * z$

### Aufgabe 3.6:

Bestimmen Sie die freien und gebundenen Variablen in den folgenden Konstrukten:

1.  $\forall x \in \mathbb{N} : x > x$
2.  $\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : (x + y)^2 > z$
3.  $\forall x \in \mathbb{N} : z > 0 \Rightarrow (\forall y \in \mathbb{N} : (x + y)^2 > z)$

### Aufgabe 3.7:

Welche der folgenden Konstrukte sind sinnvoll:

1.  $\forall x \in \mathbb{N} : x > x$
2.  $\forall x \in \mathbb{N} : \forall x \in \mathbb{N} : (x + y)^2 > x$

$$3. \forall x \in \mathbb{N} : \forall y \in \mathbb{N} : y + z > 127$$

**Aufgabe 3.8:**

Zeigen Sie, dass die Aussagen in Satz 3.2.4 nicht äquivalent sind. Mit anderen Worten: Finden Sie Prädikate  $P(x)$  und  $Q(x)$ , so dass

$$(\forall x : P(x)) \Rightarrow (\forall x : Q(x))$$

wahr ist, während

$$(\forall x : P(x) \Rightarrow Q(x))$$

falsch ist.

**Aufgabe 3.9:**

Zeigen Sie, dass die Aussagen in Satz 3.2.5 nicht äquivalent sind.

**3.3 Existenzquantor**

Der Existenzquantor beschreibt die Situation, dass eine Aussageform für wenigstens ein Ding des Betrachtungsbereichs richtig ist. Wir wollen die Aussage „Es gibt Freizeit an der Nordakademie“ näher ansehen. Betrachten wir also zum Beispiel die Aussageform „ $x$  ist Freizeit an der Nordakademie“. Dann wäre eine Anwendung des Existenzquantors: „Es gibt einen Zeitpunkt  $x$ :  $x$  ist Freizeit an der Nordakademie“. Beachten Sie bitte, dass die Variable  $x$  in der zweiten Aussage nicht mehr frei wählbar ist, sondern durch den Existenzquantor „Es gibt einen Zeitpunkt  $x$ “ gebunden wird. Dadurch können wir der Aussage einen Wahrheitswert zuordnen.

**EXISTENZQUANTOR:**

Sei  $Q(x_1, \dots, x_n)$  eine prädikatenlogische Aussageform mit  $n$  freien Variablen  $x_1, \dots, x_n$ , unter denen  $x_i$  eine ist. Dann bezeichnet

$$\exists x_i : Q(x_1, \dots, x_n)$$

eine prädikatenlogische Aussageform mit  $n-1$  Variablen. Im Spezialfall  $n = 1$  erhalten wir eine prädikatenlogische Aussage, die genau dann wahr ist, wenn  $Q(x_1)$  für wenigstens ein Ding unserer Anschauung oder unseres Denkens wahr ist.

**Definition 3.3.1**  
Existenzquantor

**Beispiel 3.3.1** Beispiele für Aussagen mit dem Existenzquantor.

- $\exists x : x = x$  ist eine wahre Aussage
- $\exists x : x \neq x$  ist eine falsche Aussage

Ähnlich der Situation beim Allquantor hat man auch beim Existenzquantor Betrachtungsbereiche. So ist im Einführungsbeispiel die Menge aller Zeitpunkte der Betrachtungsbereich. Deshalb definieren wir:

**EINGESCHRÄNKTER EXISTENZQUANTOR:**

Sei  $Q(x)$  eine prädikatenlogische Aussageform, in der die freie Variable  $x$  vorkommt und  $M$  eine beliebige Menge.

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

ist äquivalent zu:

$$\exists x : x \in M \wedge Q(x)$$

**Definition 3.3.2**  
eingeschränkter  
Existenzquantor

**Beispiel 3.3.2** 1.  $\exists x \in \mathbb{N} : x > 2$  ist eine wahre Aussage. Ein  $x \in \mathbb{N}$  reicht, um die Wahrheit zu beweisen. Ein solches  $x$  könnte 3 sein.

2.  $\exists x \in \mathbb{N} : x^2 - 10x + 24 = 0$  ist auch eine wahre Aussage, denn z.B.  $x = 6$  löst die Gleichung. Bitte beachten Sie, dass ein Lösungsweg nicht gefordert ist, um die Wahrheit der Aussage zu beweisen.

3.  $\exists x \in \mathbb{N} : 1 > x$  ist falsch.

4.  $\exists x \in \mathbb{N} : 2 > x$  ist wahr.

5.  $\exists y \in \mathbb{N} : \exists x \in \mathbb{N} : y > x$  ist eine wahre Aussage. Zum Beispiel für  $y = 2$  ergibt sich die Aussage des vorigen Beispiels, die als wahr erkannt wurde. Bitte beachten Sie, dass ein Unglücklicher, der den Versuch  $y = 1$  unternimmt, die falsche Aussage des vorletzten Beispiels erhält. Das reicht natürlich nicht aus, um die Falschheit der Aussage dieses Beispiels zu beweisen.

Bemerkung 33: Manche Autoren verwenden statt des Symbols  $\exists$  das Symbol  $\vee$ . Die Aussage  $\vee x \in \{x_1, x_2, \dots, x_n, \dots\} : Q(x)$  soll an die Aussage  $Q(x_1) \vee Q(x_2) \vee \dots \vee Q(x_n) \vee \dots$  erinnern.

Bemerkung 34: Bitte beachten Sie die Verwendung der Konjunktion  $\wedge$  in der Definition 3.3.2. Während der Allquantor mit der Implikation verheiratet ist, ist der Existenzquantor mit der Konjunktion verheiratet. Aussagen wie:

$$\exists x : x \in M \Rightarrow Q(x)$$

$$\forall x : x \in M \wedge Q(x)$$

sind immer wahr (falsch) und deshalb wertlos, um Situationen zu beschreiben.

Wir merken uns die zweite goldene Regel:

Verwende  $\exists$  nur in Verbindung mit „ $\wedge$ “ als äußerem logischen Junktor.

Es kann durchaus passieren, dass eine prädikatenlogische Aussage mehrere Existenzquantoren enthält. Dann ist die Reihenfolge der Existenzquantoren unerheblich:

**VERTAUSCHBARKEIT VON EXISTENZQUANTOREN:**

Sei  $Q(x, y)$  eine Aussageform mit zwei freien Variablen. Dann ist:

$$(\exists x : \exists y : Q(x, y)) \Leftrightarrow (\exists y : \exists x : Q(x, y))$$

oder in der Form mit eingeschränkten Allquantoren:

Dafür seien  $M$  und  $N$  beliebige Mengen:

$$(\exists x \in M : \exists y \in N : Q(x, y)) \Leftrightarrow (\exists y \in N : \exists x \in M : Q(x, y))$$

**Satz 3.3.1**  
Vertauschbarkeit  
von Existenz-  
quantoren



**Beispiel 3.3.3** •  $\exists x \in \mathbb{N} : \exists y \in \mathbb{N} : x > y$  ist eine wahre Aussage. Das Beispiel  $x = 2$  und  $y = 1$  zeigt es.

- $\exists x \in \mathbb{N} : \exists y \in \mathbb{N} : \exists z \in \mathbb{N} : x^2 + y^2 = z^2$  ist eine wahre Aussage, wie das Beispiel  $x = 3, y = 4, z = 5$  zeigt.
- $\exists x \in \mathbb{N} : \exists y \in \mathbb{N} : \exists z \in \mathbb{N} : x^3 + y^3 = z^3$  ist eine falsche Aussage. Der Beweis dieser Aussage ist aber nicht einfach (Siehe Ausführungen über Fermat in Kapitel 2).
- $\exists x \in \{f | f \text{ ist Frau}\} : \text{Hans liebt } x$ . Selbst wenn Hans nicht so ein Frauenheld ist, wie Casanova, ist das wahrscheinlich eine wahre Aussage, weil Hans wohl doch seine Mutter liebt, oder?
- Dasselbe gilt eigentlich für jeden Mann:  $\exists x \in \{f | f \text{ ist Frau}\} : \text{Klaus liebt } x$  und  $\exists x \in \{f | f \text{ ist Frau}\} : \text{Herbert liebt } x$ . Die Frau ist aber höchstwahrscheinlich immer eine andere. Sie hängt von der Person des Mannes ab.

#### DISJUNKTIONEN UND EXISTENZQUANTOREN:

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Dann ist:

$$(\exists x : P(x)) \vee (\exists x : Q(x)) \Leftrightarrow \exists x : P(x) \vee Q(x)$$

**Satz 3.3.2**  
Disjunktionen  
und Existenz-  
quantoren

Bemerkung 35: Da Existenzquantoren im Kern verallgemeinerte Disjunktionen sind, ist dieser Satz so etwas wie ein Kommutativgesetz, denn wenn wir die beiden Seiten als Disjunktionen schreiben, verändert sich nur die Reihenfolge der Operanden.

#### KONJUNKTIONEN UND EXISTENZQUANTOREN:

Seien  $Q(x)$  und  $P(x)$  Aussageformen mit der freien Variablen  $x$ . Aus

$$\exists x : P(x) \wedge Q(x)$$

folgt

$$(\exists x : P(x)) \wedge (\exists x : Q(x))$$

.

Die beiden Aussagen sind im **Allgemeinen nicht äquivalent**.

**Satz 3.3.3**  
Konjunktionen  
und Existenz-  
quantoren

Die erste Formulierung behauptet nämlich  $P(x) \wedge Q(x)$  für dasselbe  $x$ , während

in der zweiten Formulierung zwei  $x$  angesprochen werden, die durchaus unterschiedlich sein können.

Bemerkung 36: Diese Aussage ist nicht so erstaunlich, wenn wir beachten, dass der Existenzquantor nichts anderes ist als eine verallgemeinerte Disjunktion. Konjunktionen und Disjunktionen lassen sich eben nicht beliebig umordnen.

Man kann All- und Existenzquantoren unter sich beliebig vertauschen. Wenn sie jedoch gemeinsam auftreten, gilt das nicht:

**Beispiel 3.3.4** Sei  $M = \{x | x \text{ ist Mann}\}$  die Menge aller Männer und  $F = \{x | x \text{ ist Frau}\}$  die Menge aller Frauen. Wir betrachten das zweistellige Prädikat „liebt“.

Die Aussage  $\forall y \in M : \exists x \in F : y \text{ liebt } x$  ist wahr, denn wir nehmen -wie oben schon- einfach an, dass alle Männer ihre Mutter lieben.

Nun aber fragen wir nach der Wahrheit der folgenden Aussage:  $\exists x \in F : \forall y \in M : y \text{ liebt } x$ . Da stellt sich die Frage, ob es eine Frau gibt, die alle Männer lieben. Meine Versuche, die Studenten davon zu überzeugen, dass Pamela Anderson oder Dolly Buster eine solche Frau wäre, sind kläglich gescheitert. Also handelt es sich um eine falsche Aussage.

In der ersten Aussage darf die Frau vom Mann abhängen (im logischen nicht im materiellen Sinne), in dem zweiten Fall nicht. Die Reihenfolge der Quantoren legt also eine Abhängigkeit zwischen den Variablen fest.

**Beispiel 3.3.5** Die Aussage  $\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : y > x$  ist eine wahre Aussage. Wir können als  $y$  einfach  $x + 1$  nehmen, denn da der Existenzquantor der innere Quantor ist, darf die Variable  $y$  von der Variablen  $x$  abhängig gewählt werden.

Die Aussage  $\exists y \in \mathbb{N} : \forall x \in \mathbb{N} : y > x$  ist eine falsche Aussage, denn es gibt bekanntermaßen keine größte natürliche Zahl.

#### REIHENFOLGE EXISTENZ UND ALLQUANTOR:

Sei  $Q(x, y)$  eine prädikatenlogische Aussageform mit den freien Variablen  $x$  und  $y$ . Dann gilt:

$$\exists x : \forall y : Q(x, y) \Rightarrow \forall y : \exists x : Q(x, y)$$

Die umgekehrte Richtung ist im Allgemeinen falsch.

**Satz 3.3.4**  
Reihenfolge  
Existenz und  
Allquantor

**Aufgabe 3.10:**

Formulieren Sie die folgenden Aussagen mit Quantoren und einem zweistelligen Prädikat:

- Für jeden Mann gibt es einen Hut, der dem Mann passt.
- Es gibt einen Hut, der jedem Mann passt.

Welche der beiden Aussagen ist wahr, und welche Rolle spielt die Frage, ob es sich bei der Pudelmütze um einen Hut handelt?

**Aufgabe 3.11:**

Benutzen Sie als Betrachtungsbereiche die Menge  $S$  der Studenten der Nordakademie und die Menge  $P$  der Prüfungen. Wir haben ein zweistelliges Prädikat, das Bestehen einer Prüfung: „ $\cdot$  besteht  $\cdot$ “. Formulieren Sie folgende Aussagen mit Quantoren:

1. Alle Studenten bestehen eine Prüfung.
2. Es gibt einen Studenten, der alle Prüfungen besteht.
3. Wenigstens ein Student besteht wenigstens eine Prüfung nicht.
4. Es gibt eine Prüfung, die alle Studenten bestehen.
5. Es gibt eine Prüfung, die kein Student besteht.
6. Niemand hat jemals irgendeine Prüfung bestanden.

**Aufgabe 3.12:**

Drücken Sie die folgenden Behauptungen in Worten aus und geben Sie an, ob die Aussagen wahr oder falsch sind.

1.  $\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : x = y + y$
2.  $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \exists z \in \mathbb{N} : y > x \Rightarrow y = x + z$
3.  $\exists x \in \mathbb{N} : \exists y \in \mathbb{N} : (x \neq y) \wedge (x^y = y^x)$
4.  $\exists x \in \mathbb{N} : \forall y \in \mathbb{N} : \exists z \in \mathbb{N} : y > x \Rightarrow y = x * z$

### 3.4 Negieren prädikatenlogischer Aussagen

Wir wollen nun Aussagen, die Generalisierungen und Partikularisierungen enthalten, negieren. Dabei stellt sich heraus, dass beim Negieren Generalisierungen in Partikularisierungen überführt werden und umgekehrt.

Betrachten wir das Beispiel einer negierten Generalisierung:

Nicht alle Nordakademiedozenten sind lieb. Das bedeutet doch, dass wenigstens ein Nordakademiedozent böse (böse ist gleichbedeutend mit nicht lieb) ist. Wenn wir das mit Quantoren schreiben:

$$\neg \forall x \in D : x \text{ ist lieb.} \Leftrightarrow \exists x \in D : x \text{ ist böse.}$$

Formulieren wir das allgemeiner als Satz:

**NEGATION VON ALLAUSSAGEN:**

Sei  $Q(x)$  eine prädikatenlogische Aussageform mit der freien Variablen  $x$ . Dann gilt:

$$(\neg \forall x : Q(x)) \Leftrightarrow (\exists x : \neg Q(x))$$

und in eingeschränkter Form:

$$(\neg \forall x \in M : Q(x)) \Leftrightarrow (\exists x \in M : \neg Q(x))$$

**Satz 3.4.1**  
Negation von  
Allaussagen

**Beispiel 3.4.1** Wir wollen die Aussage  $\forall x \in \mathbb{N} : x > 2$  negieren und erhalten:  $\exists x \in \mathbb{N} : \neg x > 2$ . Aus dem Kindergarten wissen wir: Wenn ich nicht mehr Spielzeug habe als mein Nachbar, dann habe ich höchstens genausoviel. Mit anderen Worten:  $\neg x > 2$  ist äquivalent zu  $x \leq 2$ . Schreiben wir die ganze Negation noch einmal hin:  $\exists x \in \mathbb{N} : x \leq 2$ .

Negieren wir die Existenzaussage „Es gibt Freizeit an der Nordakademie.“ Wir erhalten „Die gesamte Zeit an der Nordakademie wird gearbeitet.“ Die Negation einer Partikularisierung ist eine Generalisierung des Gegenteils (das Gegenteil von Freizeit ist Arbeitszeit).

**NEGATION VON EXISTENZAUSSAGEN:**

Sei  $Q(x)$  eine prädikatenlogische Aussageform mit der freien Variablen  $x$ .  
Dann sind gleichwertig:

$$(\neg \exists x : Q(x)) \Leftrightarrow (\forall x : \neg Q(x))$$

und in eingeschränkter Form:

$$(\neg \exists x \in M : Q(x)) \Leftrightarrow (\forall x \in M : \neg Q(x))$$

**Satz 3.4.2**

Negation von  
Existenzaussagen

**Aufgabe 3.13:**

Negieren Sie alle Aussagen aus den Aufgaben des letzten Kapitels.

**Aufgabe 3.14:**

Negieren Sie die Aussage: Alle Marsmännchen sind Mitglieder des Deutschen Bundestages. Schreiben Sie die Aussage und deren Negation mit Quantoren. Welche der Aussagen sind wahr und welche falsch?

**Aufgabe 3.15:**

1) Die Firma Cantor Bräu ist Hersteller jeder Menge Biermarken. Sie beschäftigt eine Menge Mitarbeiter in einer Menge Abteilungen. Seien

$$M = \{m \mid m \text{ ist Mitarbeiter der Firma Cantor Bräu} \}$$

$$A = \{a \mid a \text{ ist Abteilung der Firma Cantor Bräu} \}$$

$$B = \{b \mid b \text{ ist Biermarke der Firma Cantor Bräu} \}$$

Betrachten Sie die folgenden Aussagen der Geschäftsleitung.

1. Unsere Mitarbeiter sind glücklich. Ergänzen Sie den Quantor:

.....  $m \in M : m$  ist glücklich.

2. Jeder Mitarbeiter stellt mindestens eine Biermarke her. Ergänzen Sie den Lückentext durch geeignete Quantoren:

.....  $m \in M : \dots\dots\dots b \in B : m$  stellt  $b$  her

Negieren Sie diese Aussage:

..... :  $m$  stellt  $b$  nicht her

und formulieren Sie daraus einen deutschen Satz.

3. Können Sie auch die Aussage „Jede Abteilung hat eine Biermarke, die ihre Mitarbeiter herstellen“ mit Quantoren formulieren?

..... $m$  arbeitet In  $a$  ..... $m$  stellt  $b$  her

4. Formulieren Sie die umgangssprachlichen Aussagen „Ein Mitarbeiter arbeitet in einer Abteilung“. „Ein Mitarbeiter stellt zwei Biermarken her.“ Achten Sie auf die Betonung!

### Aufgabe 3.16:

Die Firma Fraenkelbräu ist eine andere global vertretene Brauerei. Sei  $K$  die Menge aller Kunden,  $R$  die Menge der Vertriebsregionen und  $V$  die Menge der Vertriebsmitarbeiter. Übertragen Sie die folgenden Aussagen des Vertriebsleiters Adolf Abraham Halevi Fraenkel in prädikatenlogische Ausdrücke mit Quantoren. Folgende Prädikate sollen verwendet werden: Kunde **gehört zu** Vertriebsregion. Vertriebsmitarbeiter **betreut** Kunde.

1. Alle Kunden sind einer Vertriebsregion zugeordnet.
2. Jeder Vertriebsmitarbeiter betreut in wenigstens einer Region alle Kunden.
3. Ein Kunde wird von einem Vertriebsmitarbeiter betreut.
4. Manche Kunden werden von mehr als einem Vertriebsmitarbeiter betreut.

Negieren Sie die zweite Aussage und schreiben Sie sie so, dass keine Quantoren negiert vorkommen.

## Kapitel 4

# Vollständige Induktion

*“Die natürlichen Zahlen hat der liebe Gott gemacht, alles andere ist  
Menschenwerk.”*

—L. Kronecker (1823-1892)

Wir haben in dem Kapitel über Mengenlehre die natürlichen Zahlen  $\mathbb{N}$  definiert, indem wir die Elemente aufgezählt haben:  $\{1, 2, 3, 4, \dots\}$ . Dies ist natürlich nicht wirklich eine mathematische Definition, da die drei Punkte keine unmissverständliche Aussage darstellen. Hier müssen wir die Definition der natürlichen Zahlen etwas präziser fassen.

### 4.1 Peano Axiome

It's Domino Day. Stellen Sie sich eine Kette von Dominosteinen vor, die unendlich lang ist. Diese Kette sollte in Ihrer Vorstellung keine Verzweigungen haben. Will man (aus mathematischer Sicht) beweisen, dass alle Dominosteine fallen, so muss man zwei Sachen sicherstellen:

1. Der erste Stein muss fallen.
2. Wenn ein Stein fällt, darf er von seinem Folgestein nur so weit entfernt sein, dass er den Folgestein umstößt.

Sind beide Bedingungen sichergestellt, so ist es zwingend erforderlich, dass alle Steine fallen.

Das ist genau das Prinzip der vollständigen Induktion. Dieses Prinzip beschreibt die charakteristische Eigenschaft der natürlichen Dominosteine, Entschuldigung Zahlen. Die Peano (Guiseppe Peano, 1858-1932, italienischer Mathematiker) Axiome sind die definierenden Eigenschaften der natürlichen Zahlen.

**PEANO AXIOME:**

Unter den natürlichen Zahlen verstehen wir eine Menge  $\mathbb{N}$ , für die eine Nachfolgeroperation definiert ist, und die die folgenden Eigenschaften hat:

P1) 1 ist eine natürliche Zahl.

P2) Jede natürliche Zahl  $n \in \mathbb{N}$  hat genau einen Nachfolger  $n' \in \mathbb{N}$ .

P3) Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.

P4)  $1 \in \mathbb{N}$  ist nicht Nachfolger einer natürlichen Zahl.

P5) Sei  $P$  eine beliebige Eigenschaft von natürlichen Zahlen.

Wenn die folgenden zwei Aussagen wahr sind:

(a) Induktionsanfang:  $P(1)$  ist wahr.

(b) Induktionsschluss:  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n')$

Dann gilt:  $\forall n \in \mathbb{N} : P(n)$

**Definition 4.1.1**  
Peano Axiome

Unter dem Nachfolger einer natürlichen Zahl  $n$  muss man sich die Zahl  $n+1$  vorstellen. Die Peano Axiome werden üblicherweise mit der Nachfolgeroperation formuliert und nicht mit der Operation  $+$ , weil sie dann einfacher gestaltet sind.

Von der Zahl 1 ist schon in der Definition der natürlichen Zahlen die Rede. Der aufgrund von P2 eindeutige Nachfolger von 1 heißt 2. Der wiederum aufgrund von P2 eindeutige Nachfolger von 2 heißt 3. usw.

Bemerkung 37: Das 5. Peanoaxiom ist das eigentlich interessante. Es stellt ein Beweisprinzip dar, das es erlaubt die Aussage  $\forall n \in \mathbb{N} : P(n)$  für eine beliebige Eigenschaft von natürlichen Zahlen zu beweisen. Dieses Beweisprinzip heißt **vollständige Induktion**. Das ist deshalb so bemerkenswert, weil es eigentlich das einzige Beweisprinzip ist, das es erlaubt Aussagen über eine unendliche Menge von Objekten herzuleiten. Beweise über endliche Mengen zu führen, ist „einfach“, weil man die Aussage zumindest prinzipiell für alle Objekte überprüfen kann, es sind ja nur endlich viele. Bei unendlichen geht das nicht mehr. Dabei ist entscheidend, dass diese Aussage eine „unbedingte“ Aussage ist, das heißt, dass nichts bekannt ist, was wir schon über unendlich viele



Elemente wissen. Sozusagen aus dem „Nichts“ beweisen wir eine Aussage über unendlich viele Elemente, obwohl wir sie mit Sicherheit nicht durch Nachprüfen beweisen können.

Der „Trick“ der vollständigen Induktion besteht also darin, das die unbedingte Aussage

$$\forall n \in \mathbb{N} : P(n)$$

nicht direkt bewiesen wird, sondern in Form von zwei Teilen:

Induktionsanfang:  $P(1)$

Induktionsschluss:  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n + 1)$

Der Induktionsanfang ist dabei eine Aussage, die nur über ein Objekt getroffen wird. (Ein Element ist eine endliche Anzahl, oder?)

Der Induktionsschluss ist zwar eine Aussage über eine unendliche Menge, allerdings ist sie eine **bedingte** Aussage. Eine bedingte Aussage ist aber einfacher zu beweisen als eine unbedingte Aussage, weil eine zusätzliche Voraussetzung vorliegt.

Zusammenfassend kann man vollständige Induktion als eine Technik ansehen, die es erlaubt, eine unbedingte Aussage über eine unendliche Menge von Objekten zu beweisen, indem man eine Aussage über eine endliche Menge und eine bedingte Aussage über eine unendliche Menge beweist.

Bemerkung 38: Vielen Studenten fällt das Verständnis der Peano Axiome schwer. Das ist schon verständlich, denn es wird eine Aussage über alle Eigenschaften (Prädikate) generalisiert. In dem Kapitel über Prädikatenlogik haben wir nur Objekte generalisiert und nicht Prädikate. Diese Art der Generalisierung ist neu und komplex. Man spricht, wenn man Generalisierung von Objekten formuliert, von der sog. Prädikatenlogik 1. Stufe. Das Generalisieren von Prädikaten ist Teil der Prädikatenlogik zweiter Stufe. Die meisten Sachverhalte, die Informatiker beschäftigen, lassen sich sehr gut mit der Prädikatenlogik erster Stufe beschreiben. Deshalb haben wir uns in dem Kapitel Logik auch nur mit der Prädikatenlogik 1. Stufe beschäftigt. Aber es gibt einige Ausnahmen von dieser Regel:

- Die vollständige Induktion als Instrument zur Beherrschung von Schleifen und allen Konstrukten, die sich mit „...“ beschreiben lassen.
- Die Stücklistenauflösung in der Logistik. Wir werden auf dieses Problem zu sprechen kommen, wenn wir über die transitive Hülle einer Relation sprechen.

Alle bekannten Rechenoperationen  $+, *, **$  und Vergleichsoperatoren  $<, \leq$  können auf Basis der Nachfolgeroperation definiert werden. So ist  $+$  nichts anderes als die iterierte Nachfolgebildung,  $*$  nichts anderes als iterierte Addition,  $<$  nichts anderes als die transitive Hülle der Nachfolgeroperation, etc. Wir verzichten jedoch auf eine detaillierte Herleitung.

Das Axiom P5 kann man zum Beweisen von Aussagen über die natürlichen Zahlen verwenden. Lassen Sie uns das an einigen Beispielen demonstrieren:

## 4.2 Beweise mit vollständiger Induktion

Vollständige Induktion ist eine Beweistechnik, die nach dem folgenden Schema abläuft:

### **VOLLSTÄNDIGE INDUKTION:**

Behauptung:  $\forall n \in \mathbb{N} : P(n)$

... (Hier formulieren Sie die Behauptung)

1. Induktionsanfang:  $P(1)$

... (Hier zeigen Sie die Aussage  $P(1)$ )

2. Induktionsschluss:  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Sei dazu  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

... (Hier formulieren Sie die Aussageform  $P(n)$ )

2.2 Induktionsbehauptung:  $P(n+1)$

... (Hier formulieren Sie die Aussageform  $P(n+1)$ )

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$

... (Hier führen Sie den Schritt von  $n$  nach  $n+1$  aus.)

Prinzip :  
Vollständige  
Induktion



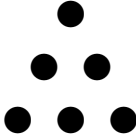
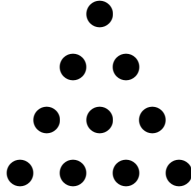
Wir wollen das Prinzip der vollständigen Induktion zunächst an einigen einfachen Summenformeln erläutern:

**DREIECKSZAHLEN:**

$$\forall n \in \mathbb{N} : \sum_{k=1}^n k = \frac{n \cdot (n+1)}{2}$$

**Satz 4.2.1**  
Dreieckszahlen

Die in dem Satz angesprochenen Zahlen werden auch „Dreieckszahlen“ genannt, weil sie sich als Gesamtzahl von Kugeln ergeben, wenn man versucht Kugeln in einem Dreiecksmuster anzuordnen.

			
$n = 1: 1 \text{ Kugel}$	$n = 2: 3 \text{ Kugeln}$	$n = 3: 6 \text{ Kugeln}$	$n = 4: 10 \text{ Kugeln}$

Bemerkung 39: Beachten Sie bitte die Verwendung des Zeichens  $\sum$ . Auf diese Weise werden Summen mit einer variablen Anzahl von Summanden geschrieben. Wir verwenden eine Laufvariable  $k$ , deren Werte von der unteren Grenze 1 bis zur oberen Grenze  $n$  variieren. Die Summe enthält nun alle Summanden, die entstehen, indem man nacheinander die Werte für  $k$  (in 1-er Schritten) einsetzt und den Wert, der nach dem Summenzeichen steht, ermittelt. So bedeutet:

$$\sum_{k=1}^4 k = 1 + 2 + 3 + 4$$

oder

$$\sum_{k=1}^4 (2 \cdot k - 1) = 1 + 3 + 5 + 7$$

Bitte beachten Sie, dass in dem Ausdruck „ $\sum_{k=1}^n k$ “ die Variable  $k$  gebunden und die Variable  $n$  frei vorkommt.

Der Beweis des Satzes erfolgt nach einem strengen Schema, das immer gleich ist. Prägen Sie sich dieses Schema ein. Der Beweis läuft dann „wie auf Schienen“.

**Beweis:**

1. Induktionsanfang: Richtigkeit der Aussage  $P(1)$ :

Wir haben zu zeigen, dass die Formel für  $n = 1$  richtig ist. Dazu rechnen wir einfach beide Seiten aus:

Linke Seite  $n = 1$  eingesetzt:  $\sum_{k=1}^1 k = 1$

Rechte Seite  $n = 1$  eingesetzt:  $\frac{1 \cdot (1+1)}{2} = \frac{2}{2} = 1$

Die Übereinstimmung der beiden Seiten zeigt, dass der Induktionsanfang richtig ist. (vgl. Peano Axiom 5 Unterpunkt (a))

## 2. Induktionsschluss: $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Wir nehmen uns ein beliebiges  $n \in \mathbb{N}$  her und haben zu zeigen, dass aus der Gültigkeit von  $P(n)$  die Gültigkeit von  $P(n+1)$  folgt. (vgl. P5 b). Um die Übersichtlichkeit zu erhöhen, formulieren wir die Voraussetzung noch einmal ausführlich:

### 2.1 Induktionsvoraussetzung: $P(n)$

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

### 2.2 Induktionsbehauptung: $P(n+1)$

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

### 2.3 Induktionsschritt: $P(n) \Rightarrow P(n+1)$ Wir zeigen $P(n+1)$ als eine Kette von Gleichungen:

$$\sum_{k=1}^{n+1} k = \left( \sum_{k=1}^n k \right) + (n+1) \quad (4.1)$$

$$= \frac{n \cdot (n+1)}{2} + (n+1) \quad (4.2)$$

$$= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} \quad (4.3)$$

$$= \frac{(n+2) \cdot (n+1)}{2} \quad (4.4)$$

$$= \frac{(n+1) \cdot ((n+1)+1)}{2} \quad (4.5)$$

In dieser Kette gilt die Gleichheit (1), weil die Summe bis  $n+1$  aufgesplittet werden kann in die Summe bis  $n$  und den  $n+1$  sten Summanden. Die Gleichheit (2) gilt, weil wir hier die Induktionsvoraussetzung anwenden können. Die Gleichungen (3) - (5) sind elementare Umformungen. Bitte beachten Sie, dass dies genau die Aussage ist, wenn man für die freie Variable  $n$  den Wert  $n+1$  einsetzt.

q.e.d.

Bemerkung 40: In dem letzten Beweis der Schritt 1 ist von besonderem Interesse. Es handelt sich dabei um einen Trick, der es ermöglicht die Situation auf der Stufe von  $n+1$  auf die Stufe von  $n$  zurückzuführen. Der Trick besteht in unserem Fall darin, dass die Summe, die eigentlich  $n+1$  Summanden hat, aufzuspalten, in einen Teil, der  $n$  Summanden hat und einen Teil der nur einen Summanden hat. Dieser Trick ist bei allen Beweisen, in denen Summen vorkommen, derselbe. Die vollständige Induktion kann man auch in vielen anderen Situationen anwenden. Summenformeln sind nur ein Beispiel dafür. Dann kann der „Trick“ anders aussehen. In jedem Fall ist mit diesem Trick eine gewisse Raffinesse verbunden.



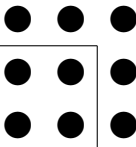
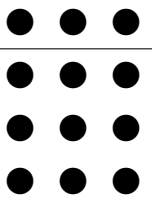
Machen wir eine zweite Anwendung der vollständigen Induktion:

#### QUADRATZAHLEN:

$$\forall n \in \mathbb{N} : \sum_{k=1}^n (2 \cdot k - 1) = n^2$$

**Satz 4.2.2**  
Quadratzahlen

Die in dem Satz angesprochenen Zahlen ergeben sich als Gesamtzahl von Kugeln, wenn man versucht Kugeln in einem Quadrat anzuordnen.

			
$n = 1: 1 \text{ Kugel}$	$n = 2: 4 \text{ Kugeln}$	$n = 3: 9 \text{ Kugeln}$	$n = 4: 16 \text{ Kugeln}$

**Beweis:**

1. Induktionsanfang: Richtigkeit der Aussage  $P(1)$ :

Wir haben zu zeigen, dass die Formel für  $n = 1$  richtig ist. Dazu rechnen wir einfach beide Seiten aus:

Linke Seite  $n = 1$  eingesetzt:  $\sum_{k=1}^1 (2 \cdot k - 1) = 2 \cdot 1 - 1 = 1$

Rechte Seite  $n = 1$  eingesetzt:  $1^2 = 1$

Die Übereinstimmung der beiden Seiten zeigt, dass der Induktionsanfang richtig ist. (vgl. Peano Axiom 5 Unterpunkt (a))

2. Induktionsschluss:  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Sei  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

$$\sum_{k=1}^n (2 \cdot k - 1) = n^2$$

2.2 Induktionsbehauptung:  $P(n+1)$

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

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$  Wir zeigen  $P(n+1)$  als eine Kette von Gleichungen:

$$\begin{aligned} \sum_{k=1}^{n+1} (2 \cdot k - 1) &= \left( \sum_{k=1}^n (2 \cdot k - 1) \right) + 2 \cdot (n+1) - 1 \\ &= n^2 + (2 \cdot n + 2) - 1 \\ &= n^2 + 2 \cdot n + 1 \\ &= (n+1)^2 \end{aligned}$$

In dieser Kette gilt die erste Gleichheit, weil die Summe bis  $n+1$  aufgesplittet werden kann in die Summe bis  $n$  und den  $n+1$ sten Summanden. Dies ist der Induktionstrick.

Die zweite Gleichheit gilt, weil wir hier die Induktionsvoraussetzung anwenden können. Die anderen Gleichungen sind elementare Umformungen. Bitte beachten Sie, dass dies genau die Aussage ist, wenn man für die freie Variable  $n$  den Wert  $n+1$  einsetzt.

q.e.d.

**Satz 4.2.3**  
Pyramidenzahlen

**PYRAMIDENZAHLEN:**

$$\forall n \in \mathbb{N} : \sum_{k=1}^n k^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}$$

Die im Satz angesprochenen Zahlen werden auch „Pyramidenzahlen“ genannt, weil sie sich ergeben, wenn man versucht, Kugeln gleicher Größe in der Form einer vierseitigen Pyramide anzuordnen.

**Beweis:**

1. Induktionsanfang: Richtigkeit der Aussage  $P(1)$ :

Wir haben zu zeigen, dass die Formel für  $n = 1$  richtig ist. Dazu rechnen wir einfach beide Seiten aus:

Linke Seite  $n = 1$  eingesetzt:  $\sum_{k=1}^1 k^2 = 1^2 = 1$

Rechte Seite  $n = 1$  eingesetzt:  $\frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = \frac{6}{6} = 1$

Die Übereinstimmung der beiden Seiten zeigt, dass der Induktionsanfang fertig ist.

2. Induktionsschluss:  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Sei  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

$$\sum_{k=1}^n k^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}$$

2.2 Induktionsbehauptung:  $P(n+1)$

$$\sum_{k=1}^{n+1} k^2 = \frac{(n+1) \cdot ((n+1)+1) \cdot (2 \cdot (n+1) + 1)}{6}$$

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$

Wir können  $P(n+1)$  mit eine Kette von Gleichungen zeigen. Allerdings müssten wir dann sehr aufpassen, welche elementaren Umformungen wir machen. Einfacher ist die Linke Seite/Rechte Seite Methode:

Linke Seite:

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= \left( \sum_{k=1}^n k^2 \right) + (n+1)^2 \\ &= \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6} + (n+1)^2 \\ &= \frac{2 \cdot n^3 + 9 \cdot n^2 + 13 \cdot n + 6}{6} \end{aligned}$$

In dieser Kette gilt die erste Gleichheit, weil die Summe bis  $n + 1$  aufgesplittet werden kann. (Der Induktionstrick!). Die zweite Gleichheit gilt, weil wir hier die Induktionsvoraussetzung anwenden können. Die letzte Gleichung erhält man durch elementares Ausmultiplizieren. Rechte Seite:

$$\frac{(n+1) \cdot ((n+1)+1) \cdot (2 \cdot (n+1)+1)}{6} = \frac{2 \cdot n^3 + 9 \cdot n^2 + 13 \cdot n + 6}{6}$$

Dies ist nichts als elementares Ausmultiplizieren. Wir stellen mit Genugtuung fest, dass die rechte und die linke Seite übereinstimmen. Damit ist bewiesen, dass die Formel für die Pyramidenzahlen richtig ist.

**q.e.d.**

Ein Beispiel soll verdeutlichen, dass nicht nur Summenformeln mit vollständiger Induktion bewiesen werden können.

**Satz 4.2.4**  
Bernoullische  
Ungleichung

**BERNOULLISCHE UNGLEICHUNG:**

(Jacob (1654-1715) und Johann (1667-1748) B, Schweizer Mathematiker)

Sei  $p > -1$  eine beliebige reelle Zahl. Dann gilt:

$$\forall n \in \mathbb{N} : (1 + p)^n \geq 1 + n \cdot p$$

Diese Formel besagt eigentlich nichts anderes, als dass ein Kapital, das mit Zinseszins über  $n$  Jahre verzinst wird, mehr ergibt, als wenn es ohne Zinseszins angelegt wird. Die linke Seite ist nämlich die Formel für eine Kapitalanlage mit Zinseszins und die rechte Seite die Formel für eine Kapitalanlage ohne Zinseszins. Sage noch mal einer, dass Mathematik nichts mit BWL zu tun hat.

**Beweis:**

Sei  $p > -1$  eine beliebige reelle Zahl.

Behauptung: Es soll bewiesen werden  $\forall n \in \mathbb{N} : P(n)$

$$\forall n \in \mathbb{N} : (1 + p)^n \geq 1 + n \cdot p$$

1. Induktionsanfang: wir beweisen  $P(1)$



Linke Seite:  $(1 + p)^1 = 1 + p$

Rechte Seite:  $1 + 1 \cdot p = 1 + p$

Die linke Seite ist „ $\geq$ “ als die rechte Seite, deshalb ist der Induktionsanfang fertig.

2. Induktionsschluss: wir beweisen  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n + 1)$

Sei dazu  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

$$(1 + p)^n \geq 1 + n \cdot p$$

2.2 Induktionsbehauptung:  $P(n + 1)$

$$(1 + p)^{(n+1)} \geq 1 + (n + 1) \cdot p$$

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n + 1)$

Leider können wir, wenn wir mit Ungleichungen arbeiten, die „linke Seite ausrechnen/rechte Seite ausrechnen Technik“ nicht vorteilhaft verwenden. Deshalb müssen wir eine Kette von Ungleichungen hinschreiben:

$$(1 + p)^{(n+1)} = (1 + p)^n \cdot (1 + p) \quad (4.1)$$

$$\geq (1 + n \cdot p) \cdot (1 + p) \quad (4.2)$$

$$= 1 + n \cdot p + p + n \cdot p^2 \quad (4.3)$$

$$= 1 + (n + 1)p + n \cdot p^2$$

$$\geq 1 + (n + 1) \cdot p \quad (4.4)$$

Die erste Gleichung (1) ist eine elementare Umformung, um in die Lage zu kommen, die Induktionsvoraussetzung anwenden zu können. Hier ist der Induktionstrick also eine einfache Anwendung der Potenzrechengesetze. Der zweite Schritt (2) wendet die Induktionsvoraussetzung an. Beachten Sie bitte, dass hier verwendet wird, dass  $p \geq -1$ , denn sonst wäre der Faktor  $(1 + p)$  negativ und die Ungleichungsrichtung würde sich umdrehen.

Der nächste Schritt (3) ist wieder eine elementare Umformung (Ausmultiplizieren), und der letzte Schritt (4) nutzt aus, dass immer  $p^2 \geq 0$  ist.

Damit haben wir die Ungleichung für  $n + 1$  bewiesen und die vollständige Induktion ist abgeschlossen.

q.e.d.

Ein Beispiel soll zeigen, wie man mit vollständiger Induktion arbeitet, wenn die Aussage nicht für alle  $n \in \mathbb{N}$  sondern nur für alle  $n \in \mathbb{N}_{n_0} = \{x \in \mathbb{N} | x \geq n_0\}$  gilt. Schauen wir uns dazu eine Wertetabelle an:

$n$	$n^2$	$2^n$
0	0	1
1	1	2
2	4	4
3	9	8
4	16	16
5	25	32
6	36	64
7	49	128

Es sieht so aus, als wäre  $2^n \geq n^2$  falls  $n \geq 4$  ist. Formulieren wir das als Satz:

**Satz 4.2.5**  
Potenz wächst  
schneller als  
Quadrat

**POTENZ WÄCHST SCHNELLER ALS QUADRAT:**

$$\forall n \in \mathbb{N}_4 : 2^n \geq n^2$$

**Beweis:**

In dem Induktionsanfang starten wir nun mit dem kleinsten möglichen  $n$ :

1. Induktionsanfang: wir beweisen  $P(n_0)$

Linke Seite:  $2^4 = 16$

Rechte Seite:  $4^2 = 16$

Da die linke Seite größergleich der rechten Seite ist, ist der Induktionsanfang fertig.

2. Induktionsschluss: wir beweisen  $\forall n \in \mathbb{N}_{n_0} : P(n) \Rightarrow P(n+1)$

Sei dazu  $n \in \mathbb{N}_{n_0}$  beliebig aber fest.

- 2.1 Induktionsvoraussetzung:  $P(n)$

$$2^n \geq n^2$$

- 2.2 Induktionsbehauptung:  $P(n+1)$

$$2^{(n+1)} \geq (n+1)^2$$

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$ 

Wir schreiben wieder eine Kette von Ungleichungen:

$$\begin{aligned}
 2^{(n+1)} &= 2^n \cdot 2 && \text{Induktionstrick} \\
 &\geq n^2 \cdot 2 = n^2 + n \cdot n && \text{Induktionsvoraussetzung} \\
 &\geq n^2 + 4 \cdot n = n^2 + 2 \cdot n + 2 \cdot n && \text{da } n \geq 4 \\
 &\geq n^2 + 2 \cdot n + 8 && \text{da } n \geq 4 \\
 &\geq n^2 + 2 \cdot n + 1 && \text{da } 8 \geq 1 \\
 &= (n+1)^2 && \text{1. Binomische Formel}
 \end{aligned}$$

**q.e.d.**

Bemerkung 41:

Wenn wir versuchen würden, den Satz mit  $n \geq 3$  zu beweisen, würde der Induktionsanfang schief gehen. Der Beweis durch vollständige Induktion wäre dann nicht vollständig.

Versuchen wir dasselbe mit  $n \geq 2$ , so kann man (ich finde das witzig :-)) den Induktionsanfang wieder durchführen, aber die Ungleichungen des Induktionsschlusses werden falsch.

Die Wahl eines geeigneten Startpunkts für eine vollständige Induktion kann den Induktionsanfang vereinfachen. Ein Beispiel hierfür ist der folgende Satz. Sei dazu  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ .

**GEOMETRISCHE REIHE:**

Sei  $q \neq 1$  eine beliebige reelle Zahl.

$$\forall n \in \mathbb{N}_0 : \sum_{k=0}^n q^k = \frac{1 - q^{n+1}}{1 - q}$$

**Satz 4.2.6**  
Geometrische  
Reihe

**Beweis:**

Behauptung:  $\forall n \in \mathbb{N}_0 : \sum_{k=0}^n q^k = \frac{1 - q^{n+1}}{1 - q}$

1. Induktionsanfang: Ich zeige die Aussage für  $n = 0$

$$\text{Linke Seite: } \sum_{k=0}^0 q^k = q^0 = 1$$

$$\text{Rechte Seite: } \frac{1 - q^{0+1}}{1 - q} = \frac{1 - q}{1 - q} = 1$$

2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}_0$  beliebig aber fest.

2.1 Induktionsvoraussetzung:

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

2.2 Induktionsbehauptung:

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

2.3 Induktionsschritt:

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^n q^k + q^{n+1} \quad (4.1)$$

$$= \frac{1 - q^{n+1}}{1 - q} + q^{n+1} \quad (4.2)$$

$$= \frac{1 - q^{n+1} + (1 - q)q^{n+1}}{1 - q} \quad (4.3)$$

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

$$= \frac{1 - q^{(n+1)+1}}{1 - q}$$

(1) ist das inzwischen bekannte Aufsplitten der Summe, (2) das Anwenden der Induktionsvoraussetzung, (3) bringt die Teile auf den Hauptnenner und die restlichen Gleichungen sind elementare Umformungen.

**q.e.d.**

Ein anderes Beispiel für einen anderen Startpunkt als 1 ist eine Aussage der Form:

**Satz 4.2.7**

Teilbarkeitsbeispiel

**TEILBARKEITSBEISPIEL:**

$$\forall n \in \mathbb{N}_0 : n^3 - n \text{ ist durch 3 teilbar.}$$

**Beweis:**

Behauptung:  $\forall n \in \mathbb{N}_0 : n^3 - n$  ist durch 3 teilbar.

1. Induktionsanfang:  $P(0)$

$0^3 - 0 = 0$  ist durch 3 teilbar.

2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}_0$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

$n^3 - n$  ist durch 3 teilbar.

2.2 Induktionsbehauptung:  $P(n+1)$

$(n+1)^3 - (n+1)$  ist durch 3 teilbar.

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - (n+1) \quad (4.1)$$

$$= \underbrace{n^3 - n}_{(3)} + \underbrace{3 \cdot (n^2 + n)}_{(4)} \quad (4.2)$$

Der Induktionstrick ist das Anwenden der binomischen Formel (1) und das Sortieren der Terme in (2), so dass die Induktionsvoraussetzung angewendet werden kann: Nach der Induktionsvoraussetzung ist nämlich (3) durch 3 teilbar und dass (4) ein Vielfaches von 3 ist, ist auch die Summe von (3) und (4) durch 3 teilbar.<sup>1</sup>

**q.e.d.**

In der Informatik wird vollständige Induktion auch häufig angewendet, wenn es um ganz andere Dinge geht als Zahlen. Ein schönes Beispiel stammt aus dem Buch von Douglas Hofstdter: Gdel, Escher, Bach und trgt den Namen „Das MIU Rtsel“.

<sup>1</sup>Mit etwas mehr Sorgfalt ist auch zu schließen, dass  $n^3 - n$  durch 6 teilbar ist.  $n^2 + n = n \cdot (n+1)$  ist immer durch 2 teilbar, weil entweder  $n$  oder  $n+1$  gerade ist. Damit kann man dann leicht den Induktionsschritt fhren.

Das MIU-System handelt von Wörtern (Zeichenketten), die nur aus den drei Buchstaben M, I, und U bestehen.

Beispiele für solche Wörter sind:

- MI
- MIII
- MIIUIU
- MU
- ...

Aber nicht alle möglichen Wörter bestehend aus M, I oder U sind Wörter des MIU-Systems, sondern nur solche, die nach gewissen Regeln aus dem Wort „MI“ erzeugt werden können. Hier sind die Regeln:

Regel 1: Bei einer Kette, deren letzter Buchstabe I ist, darf ein U hinten angefügt werden.

Beispiel:  $MI \rightarrow MIU$ . Man sagt MIU wird aus MI abgeleitet. Die Ableitung wird durch den Pfeil  $\rightarrow$  dargestellt.

Regel 2: Aus einer Kette der Form  $Mx$  darf man die Kette  $Mxx$  ableiten. Dabei steht  $x$  für eine beliebige Zeichenkette.

Beispiele:  $MI \rightarrow MII$ ,  $MIUUI \rightarrow MIUUIIUI$ .

Beachte, dass  $x$  immer die gesamte Kette ausser dem M umfasst.

Regel 3: Wenn in einer Kette die Teilkette III vorkommt, darf man diese durch ein U ersetzen.

Beispiele:  $MIII \rightarrow MU$ ,  $U \underbrace{III}_{\text{III}} IM \rightarrow UUIM$ ,  $UI \underbrace{III}_{\text{III}} M \rightarrow UIUM$ .

Regel 4: Wenn in einer Kette die Teilkette UU vorkommt darf man sie streichen.

Beispiele:  $UUU \rightarrow U$ ,  $MUUUIII \rightarrow MUIII$ .

Die Regeln dürfen natürlich nur genau in der angegebenen Weise verwendet werden. Offensichtlich gibt es Situationen, in denen mehrere Regeln anwendbar sind. Dann darf man sich eine aussuchen.

Alle Wörter, die aus MI mit beliebiger Anwendung der Regeln erzeugt werden können, heissen „die Wörter des MIU-Systems“.

Beispiel für eine korrekte Ableitung:

MI

→ MIU Regel 1

→ MIUIU Regel 2

→ MIUIUIIU Regel 2

Man sagt dass MIUIUIIU ein Wort des MIU-Systems ist genau dann wenn MIUIUIIU aus MI ableitbar ist.

Nun kommen wir zur eigentlichen Aufgabe, dem MU-Rätsel. Dies ist ganz einfach die Frage:

Ist MU ein Wort des MIU-Systems?

Zunächst wird man etwas herumprobieren und zusehen, ob man die Zeichenkette MU irgendwie bekommen kann. Wenn es einem zu langweilig geworden ist, fragt man sich vielleicht, ob es nicht systematischer geht, denn es entsteht die Vermutung, dass MU nicht im MIU System liegt. Es reicht nicht, zu zeigen dass eine bestimmte Art der Erstellung von MU nicht erfolgreich ist, sondern man muss alle möglichen Ableitungen als „ergebnislos“ nachweisen. Leider ist es aufgrund der nicht festgelegten Reihenfolge der Regelanwendungen nicht einfach.

Folgender Satz beweist, dass MU nicht erzeugt werden kann:

**MIU SYSTEM:**

Die Anzahl der I in einem Wort des MIU Systems ist nicht durch 3 teilbar.

**Satz 4.2.8** MIU System

MU kann also nicht erzeugt werden, weil die Anzahl der I in MU durch 3 teilbar ist.

Wie kann man aber den Satz beweisen? Erstaunlicherweise kann uns hier die vollständige Induktion weiterhelfen. Aber es kommt in der Aussage nicht einmal eine natürliche Zahl vor. Wie soll das gehen?

Dazu müssen wir zu einem kleinen Trick greifen, der eine natürliche Zahl einführt. Wie wir wissen, geht ja jedes Wort des MIU Systems durch Anwendungen von Regeln aus MU hervor. Wir formulieren den Satz etwas anders:

**Satz 4.2.9**

Induktion über  
Regelanwendun-  
gen

**INDUKTION ÜBER REGELANWENDUNGEN:**

Für alle  $n \in \mathbb{N}_0$ :

Ist ein Wort des MIU Systems in  $n$  Regelanwendungen ableitbar, dann ist die Anzahl der I nicht durch 3 teilbar.

Da jedes Wort des MIU Systems durch eine endlich Anzahl von Regelanwendungen entstehen muss, sind die beiden letzten Sätze äquivalent.

Da wir aber in Satz 4.2.9 in die Anzahl der Regelanwendungen als neue Variable eingeführt haben, können wir zum Beweis die vollständige Induktion nutzen. Wir sprechen bei dem Induktionsbeweis nun von einer vollständigen Induktion über die Anzahl der Regelanwendungen.

**Beweis:**

Behauptung: Es soll bewiesen werden

$\forall n \in \mathbb{N}_0$  : Ist ein Wort des MIU Systems in  $n$  Regelanwendungen ableitbar, dann ist die Anzahl der I nicht durch 3 teilbar.

1. Induktionsanfang: wir beweisen  $P(0)$ 

Mit  $n = 0$  Regeln ist nur MI ableitbar. Die Anzahl der I's in MI ist nicht durch 3 teilbar.

2. Induktionsschluss: wir beweisen  $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$ 

Sei dazu  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$ 

Ist ein Wort des MIU Systems in  $n$  Regelanwendungen ableitbar, dann ist die Anzahl der I nicht durch 3 teilbar.

2.2 Induktionsbehauptung:  $P(n+1)$ 

Ist ein Wort des MIU Systems in  $n+1$  Regelanwendungen ableitbar, dann ist die Anzahl der I nicht durch 3 teilbar.

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$ 

Sei  $w_{n+1}$  ein Wort, dass sich durch  $n+1$  Regelanwendungen ableiten lässt. Dann entsteht dieses Wort durch Anwenden einer der Regeln 1-4 auf ein Wort  $w_n$ , dass sich durch Anwenden von  $n$  Regeln ableiten lässt. Nach der Induktionsvoraussetzung ist die Anzahl der I in  $w_n$  nicht durch 3 teilbar. Wir machen nun eine Fallunterscheidung, je nachdem welche der 4 Regeln zum Erzeugen von  $w_{n+1}$  aus  $w_n$  angewendet wurde:



Regel 1: Die Anzahl der I in  $w_{n+1}$  ist dann gleich der Anzahl der I in  $w_n$ .

Regel 2: Die Anzahl der I in  $w_{n+1}$  ist dann gleich der 2 mal Anzahl der I in  $w_n$ .

Regel 3: Die Anzahl der I in  $w_{n+1}$  ist dann gleich der Anzahl der I in  $w_n$  minus 3.

Regel 4: Die Anzahl der I in  $w_{n+1}$  ist dann gleich der Anzahl der I in  $w_n$ .

In keinem Fall also ist die Anzahl der I in  $w_{n+1}$  durch 3 teilbar.

q.e.d.

#### REGELSYSTEM DEFINIEREN:

Induktionsanfang:

Es werden Startobjekte  $b_1, \dots, b_n$  festgelegt.

Induktionsschluss:

Es werden ein oder mehrere Regeln  $R_1, \dots, R_m$  festgelegt, wie man aus bestehenden Objekten neue Objekte konstruiert.

Alle Objekte, die aus dem Startobjekten  $b_1, \dots, b_n$  durch kein, ein oder mehrmaliges Anwenden der Regeln  $R_1, \dots, R_m$  hergeleitet werden können, gehören zu dem durch das Regelsystem definierten Objektmenge.

Prinzip :  
Regelsystem  
definieren

#### INDUKTION ÜBER REGELANWENDUNGEN:

Induktionsanfang:

Eigenschaft für die Startobjekte  $b_1, \dots, b_n$  nachweisen.

Induktionsschluss:

Sei  $o$  ein Objekt des Regelsystems, das die Eigenschaft hat.

Wenn man  $o$  durch die Regeln  $R_1, \dots, R_m$  transformiert, haben die neuen Objekte auch die Eigenschaft.

Prinzip :  
Induktion über  
Regelanwendungen

#### Aufgabe 4.1:

Beweisen Sie:

$$\forall n \in \mathbb{N} : \sum_{k=1}^n (3 \cdot k - 2) = \frac{n}{2} \cdot (3 \cdot n - 1)$$

#### Aufgabe 4.2:

Beweisen Sie:

$$\forall n \in \mathbb{N} : \sum_{k=1}^n (4 \cdot k - 3) = n(2 \cdot n - 1)$$

### Aufgabe 4.3:

Beweisen Sie:

$$\forall n \in \mathbb{N} : \sum_{k=1}^n \frac{1}{k \cdot (k+1)} = 1 - \frac{1}{n+1}$$

### Aufgabe 4.4:

Beweisen Sie für geeignete  $n$  durch vollständige Induktion:

$$2^n \geq 2 \cdot n^2$$

### Aufgabe 4.5:

Beweisen Sie:

$$\forall n \in \mathbb{N} : n^5 - n \text{ ist durch 5 teilbar.}$$

### Aufgabe 4.6:

Beweisen Sie durch vollständige Induktion über die Anzahl der Regelanwendungen: Im modifizierten MIU System kann man MU nicht erzeugen:

Modifiziertes MIU System:

Startzeichenkette: MI

Regel 1: Bei einer Kette, deren letzter Buchstabe I ist darf ein U hinten angefügt werden.

Regel 2: Aus einer Kette der Form  $Mx$  darf man die Kette  $MxxI$  ableiten. Dabei steht  $x$  für eine beliebige Zeichenkette. Beachte, dass  $x$  immer die gesamte Kette ausser dem M umfasst.

Regel 3: Wenn in einer Kette die Teilkette II vorkommt, darf man diese durch ein U ersetzen.

Regel 4: Wenn in einer Kette die Teilkette UU vorkommt darf man sie streichen.

#### Aufgabe 4.7:

Ein Klammergebirge ist eine Zeichenkette, von öffnenden und schließenden Klammern, die aus der Startzeichenkette  $()$  entsteht, indem man eine der beiden zwi folgenden Regeln anwendet:

Regel 1: Wenn  $w$  ein Klammergebirge ist, dann ist  $(w)$  ein Klammergebirge.

Regel 2: Wenn  $w_1$  und  $w_2$  Klammergebirge sind, dann ist  $w_1w_2$  ein Klammergebirge.

So sind zum Beispiel  $()$ ,  $(( ))$ ,  $()()$ ,  $(( ))()$  und  $(( ( )))$  Klammergebirge. Beweisen Sie folgende Behauptungen durch vollständige Induktion über die Anzahl der Regelanwendungen:

1. In einem Klammergebirge ist die Anzahl der öffnenden Klammern gleich der Anzahl der schließenden Klammern.
2. Die Breite  $b(w)$  eines Klammergebirges ist die Anzahl der Zeichen in  $w$ . Beispielsweise haben  $(( ))$  und  $(( ( )))$  die Breite 6.  
Beweisen Sie: Die Breite eines Klammergebirges ist eine grade Zahl.
3. Zerlegt man ein Klammergebirge  $w$  an beliebiger Stelle in einen Anfang und ein Ende  $w = uv$ , dann ist die Anzahl der öffnenden Klammern in  $u$  immer mindestens so groß, wie die Anzahl der schließenden Klammern.
4. Den Überschuss an öffnenden Klammern in einem Anfang  $u$  des Klammergebirges  $w$  bezeichnen wir als Höhe  $h(w, u)$  des Klammergebirges  $w$  an der Stelle  $u$ . So hat zum Beispiel  $(( ))$  die Höhe 2 an der Stelle  $(($  und die Höhe 1 an der Stelle  $(( )$ .

Die maximale Höhe, die ein Klammergebirge  $w$  an einem Anfang  $u$  hat bezeichnen wir als Höhe des Klammergebirges:

$$h(w) = \max_{u \text{ Anfang von } w} h(w, u)$$

So hat  $(( ))$  die Höhe 2 und  $(( ( )))$  die Höhe 3.

Zeigen Sie: Für jedes Klammergebirge  $w$  gilt:

$$h(w) \leq \frac{b(w)}{2}$$

### 4.3 Definitionen mit vollständiger Induktion

Vollständige Induktion kann nicht nur als Beweistechnik eingesetzt werden. In der Informatik fast noch häufiger wird vollständige Induktion für Definitionszwecke eingesetzt. Wir schauen uns das an dem Beispiel der Definition der Fakultätsfunktion an. Bekanntermassen definiert man

$$\forall n \in \mathbb{N} : n! = 1 \cdot 2 \cdot \dots \cdot n$$

Diese Definition ist zwar sehr verständlich, hat aber den großen Nachteil mathematisch nicht exakt zu sein. Das stört für das Verständnis zunächst gar nicht, aber wenn es darum geht Eigenschaften der Fakultätsfunktion zu beweisen, fehlt die solide Grundlage.

**Definition 4.3.1**  
Fakultät

**FAKULTÄT:**

Wir definieren für alle  $n \in \mathbb{N}_0$  den Wert  $n!$  (sprich: n Fakultät) durch:

1.  $0! = 1$
2.  $\forall n \in \mathbb{N}_0 : (n+1)! = (n+1) \cdot n!$

**Beispiel 4.3.1** Wir berechnen:

$$\begin{aligned} 1! &= 1 \cdot 0! = 1 \cdot 1 = 1 \\ 2! &= 2 \cdot 1! = 2 \cdot 1 = 2 \\ 3! &= 3 \cdot 2! = 3 \cdot 2 = 6 \\ 4! &= 4 \cdot 3! = 4 \cdot 6 = 24 \end{aligned}$$

Diese Definition legt den Wert für  $n!$  eindeutig fest, denn er ist für 0 eindeutig festgelegt und wenn er für  $n$  eindeutig festgelegt ist, ist er auch für  $n+1$  eindeutig festgelegt.

Prinzip :  
Definition durch  
vollständige  
Induktion

**DEFINITION DURCH VOLLSTÄNDIGE INDUKTION:**

Es ist für alle  $n \in \mathbb{N}$   $a_n$  zu definieren.

1. Induktionsanfang:  $n = 1$   
Definieren Sie  $a_1$ .
2. Induktionsschluss: Definieren Sie  $a_{n+1}$  unter Bezugnahme auf  $a_n$

Wir wollen als Beispiel einen Satz beweisen, der die Fakultätsfunktion verwendet.

**SUMMENFORMEL FÜR FAKULTÄT:**

$$\forall n \in \mathbb{N}_0 : \sum_{k=0}^n (k \cdot k!) = (n+1)! - 1$$

**Satz 4.3.1**  
Summenformel  
für Fakultät

**Beweis:**

Behauptung:  $\forall n \in \mathbb{N}_0 : \sum_{k=0}^n (k \cdot k!) = (n+1)! - 1$

1. Induktionsanfang:  $P(0)$

Linke Seite:  $\sum_{k=0}^0 (k \cdot k!) = 0 \cdot 0! = 0$

Rechte Seite:  $(0+1)! - 1 = 1! - 1 = 0$

2. Induktionsschluss:  $\forall n \in \mathbb{N}_0 : P(n) \Rightarrow P(n+1)$

Sei dazu  $n \in \mathbb{N}_0$  beliebig aber fest.

2.1 Induktionsvoraussetzung:  $P(n)$

$$\sum_{k=0}^n (k \cdot k!) = (n+1)! - 1$$

2.2 Induktionsbehauptung:  $P(n+1)$

$$\sum_{k=0}^{(n+1)} (k \cdot k!) = ((n+1)+1)! - 1$$

2.3 Induktionsschritt:  $P(n) \Rightarrow P(n+1)$

$$\sum_{k=0}^{n+1} (k \cdot k!) = \left( \sum_{k=0}^n (k \cdot k!) \right) + (n+1) \cdot (n+1)! \quad (4.1)$$

$$= (n+1)! - 1 + (n+1) \cdot (n+1)! \quad (4.2)$$

$$= ((n+1)+1) \cdot (n+1)! - 1 \quad (4.3)$$

$$= ((n+1)+1)! - 1 \quad (4.4)$$

Das Aufsplitten der Summe ist der bekannte Trick, der in (1) angewendet wurde. Dabei wurde gleich der Wert  $n+1$  für  $k$  in den Ausdruck  $k \cdot k!$  eingesetzt. (2) ist das Anwenden der Induktionsvoraussetzung. (3) klammert den Term  $(n+1)!$  aus und (4) verwendet die Definition der Fakultät für  $n+1$  an der Stelle von  $n$ . Wie Sie erkennen ergänzen sich Definition und Beweis hervorragend.

**q.e.d.**

Ein klassisches Beispiel für eine Definition durch vollständige Induktion sind die Fibonaccizahlen. Fibonacci, der eigentlich Leonardo von Pisa heißt, lebte um 1200 im mittelalterlichen Pisa. Während noch das (primitive) römische Zahlensystem vorherrschte, rechnete er mit der indischen Zahldarstellung, die ähnlich den heute benutzten arabischen Zahlen die 0 kennt. Sein Hauptwerk „Liber Abbaci“ handelt von kaufmännischen Rechnungen. Da werden Pferde gekauft, Zinsen und Gewinne ermittelt, fünf Leute finden einen Geldbeutel und müssen für die Verteilung des Geldes fünf Gleichungen mit fünf Unbekannten lösen. Selbst Kaiser Friederich II soll das Werk gelesen haben.

Architekten und Künstler kennen die Fibonacci Zahlen, weil sie wissen, dass sie den goldenen Schnitt, ein besonders angenehmes Verhältnis von Höhe zu Breite, besonders gut annähern. (Goldener Schnitt: ein Zahlenverhältnis, das an Kunstwerken als Maßverhältnis oder bei den Proportionen des menschlichen Körpers oft heraus gelesen werden kann. Eine Strecke ist nach dem G.S. in zwei Abschnitte geteilt, wenn sich der kleinere Abschnitt zum größeren so verhält wie dieser zur ganzen Strecke. Einen Näherungswert gibt 5:8).

Für uns werden die Fibonacci Zahlen ein schönes Feld zum Üben der Beweistechnik „Vollständige Induktion“ darstellen.

**Definition 4.3.2**  
Fibonacci Zahlen

**FIBONACCI ZAHLEN:**

Die Fibonacci Zahlen sind die Folge von Zahlen  $f_n$   $n \in \mathbb{N}_0$  die den Bedingungen genügen:

- a)  $f_0 = 1$  und  $f_1 = 1$
- b)  $\forall n \in \mathbb{N}_2 : f_n = f_{n-1} + f_{n-2}$

Wenn wir die ersten 20 Glieder der Folge aufschreiben erhalten wir:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 243, 387, 630, 1017, 1647, 2664, 4311, 6975

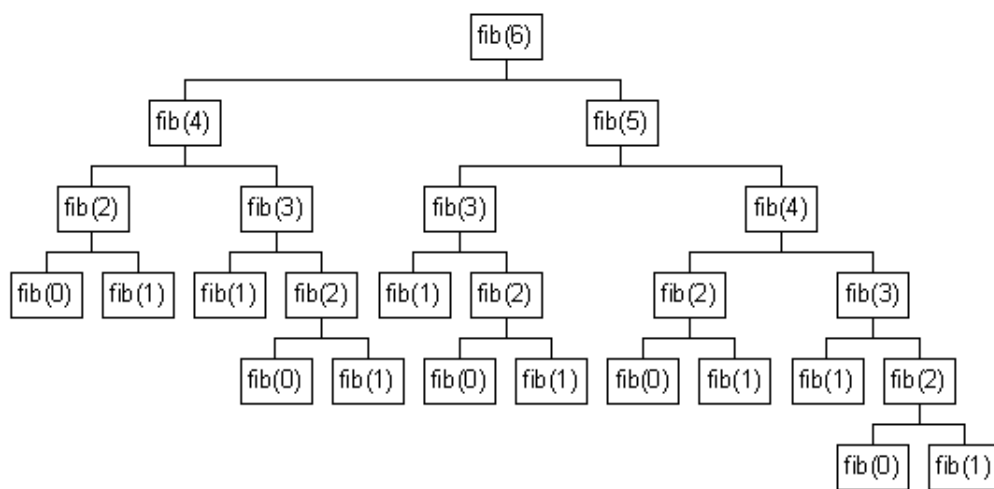
Die einfachste Möglichkeit, die Fibonacci Zahlen algorithmisch zu berechnen, würde in PASCAL so aussehen:

Algorithmus 1: Fibonacci rekursiv

```
function fib(n:integer):integer;
begin
  if (n<2) then return 1
    else return fib(n-1)+fib(n-2)
```

end

Diese auf den ersten Blick besonders elegante und gelungene Art, die Fibonacci Zahlen zu berechnen, hat einen wesentlichen Nachteil: Sie ist sehr, sehr langsam. Dies wird deutlich, wenn Sie sich z. B. den Aufrufbaum von  $\text{fib}(6)$  ansehen:



Wie Sie erkennen, erfolgt die Berechnung von  $f_6$  und  $f_5$  einmal, die Berechnung von  $f_4$  zweimal, die Berechnung von  $f_3$  dreimal, die Berechnung von  $f_2$  fünfmal und schließlich die Berechnung von  $f_1$  achtmal. Das kann nicht als besonders effizient bezeichnet werden.

Wie Sie erkennen, hat der Aufrufbaum von  $\text{fib}(6)$  genau  $f_6$  Blätter. Das ist ein allgemeines Gesetz, weil sich die Anzahl der Blätter in dem Aufrufbaum nach demselben Gesetz addieren, wie die Fibonacci Zahlen. Wie viele Blätter hat denn nun der Baum. Eine grobe Abschätzung gibt der folgende Satz:

#### WACHSTUM FIBONACCI ZAHLEN:

$$\forall n \in \mathbb{N}_2 : f_n \geq 2^{n/2}$$

#### Satz 4.3.2

Wachstum  
Fibonacci Zahlen

#### Beweis:

Behauptung:  $\forall n \in \mathbb{N}_2 : f_n \geq 2^{n/2}$

1. Induktionsanfang: Wir zeigen die Aussage für  $n = 2$ .

Linke Seite:  $f_2 = 2$

Rechte Seite:  $2^{2/2} = 2$

## 2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}_2$  beliebig aber fest.

### 2.1 Induktionsvoraussetzung:

$$f_n \geq 2^{n/2}$$

### 2.2 Induktionsbehauptung:

$$f_{n+1} \geq 2^{(n+1)/2}$$

### 2.3 Induktionsschritt:

$f_{n+1} = f_n + f_{n-1}$	Definition Fibonacci Zahlen
$\geq 2^{n/2} + 2^{(n-1)/2}$	Induktionsvoraussetzung
$= 2^{n/2} + 2^{n/2} \cdot 2^{-1/2}$	Potenzrechengesetze
$= 2^{n/2}(1 + 1/\sqrt{2})$	Ausklammern
$\geq 2^{n/2}\sqrt{2}$	$(1 + 1/\sqrt{2}) \geq \sqrt{2}$
$= 2^{(n+1)/2}$	

**q.e.d.**

Aber halt, der obige Beweis hat eine Lücke. In der zweiten Zeile des Induktionsschrittes verwenden wir die Induktionsvoraussetzung für  $f_n$  **und** für  $f_{n-1}$ . Das ist ohne weiteres nicht zulässig. Schließlich haben wir uns große Mühe gegeben, die Voraussetzung sauber hinzuschreiben. Ist der Beweis nun falsch? Streng genommen ja. allerdings können wir ihn mit einem kleinen Trick reparieren. Wir modifizieren die Behauptung so, dass zwei Aussagen als Induktionsvoraussetzung zur Verfügung stehen.

**Beweis:**

Behauptung:  $\forall n \in \mathbb{N}_3 : f_n \geq 2^{n/2}$  und  $f_{n-1} \geq 2^{(n-1)/2}$

## 1. Induktionsanfang: Wir zeigen die Aussage für $n = 3$ .

Linke Seite:  $f_3 = 3$  und  $f_2 = 2$

Rechte Seite:  $2^{3/2} = 2\sqrt{2}$  und  $2^{2/2} = 2$

## 2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}_3$  beliebig aber fest.



## 2.1 Induktionsvoraussetzung:

$$f_n \geq 2^{n/2} \text{ und } f_{(n-1)} \geq 2^{(n-1)/2}$$

## 2.2 Induktionsbehauptung:

$$f_{n+1} \geq 2^{(n+1)/2} \text{ und } f_{(n+1)-1} \geq 2^{((n+1)-1)/2}$$

## 2.3 Induktionsschritt:

Wir müssen beide Teile der Behauptung zeigen. Der zweite Teil der Behauptung ist aber nichts anderes als der erste Teil der Induktionsvoraussetzung. Der erste Teil ist genau die Berechnung aus dem letzten Beweis:

$$\begin{aligned}
 f_{n+1} &= f_n + f_{n-1} && \text{Definition Fibonacci Zahlen} \\
 &\geq 2^{n/2} + 2^{(n-1)/2} && \text{Induktionsvoraussetzung Teil 1 und 2} \\
 &= 2^{n/2} + 2^{n/2} \cdot 2^{-1/2} && \text{Potenzrechengesetze} \\
 &= 2^{n/2}(1 + 1/\sqrt{2}) && \text{Ausklammern} \\
 &\geq 2^{n/2}\sqrt{2} && (1 + 1/\sqrt{2}) \geq \sqrt{2} \\
 &= 2^{(n+1)/2}
 \end{aligned}$$

**q.e.d.**

Wie in diesem Beweis erkennen, müssen wir nur im Induktionsanfang ein wenig mehr arbeiten. Die Rechnungen im Induktionsschritt sind 100% ig dieselben. Obwohl wir also mehr beweisen, ist die Arbeit (fast) dieselbe. Wir können diese Technik noch etwas verallgemeinern. Sei  $\mathbb{N}_{\leq n} = \{x | x \in \mathbb{N} \wedge x \leq n\} = \{1, 2, \dots, n\}$ . Wir betrachten statt der Aussage

$$\forall n \in \mathbb{N} : P(n)$$

die folgende allgemeinere Aussage:

$$\forall n \in \mathbb{N} : \forall k \in \mathbb{N}_{\leq n} : P(k)$$

Aus der zweiten Aussage folgt offensichtlich die erste, denn es ist  $n \in \mathbb{N}_{\leq n}$ . Umgekehrt folgt aus der ersten Aussage auch die zweite, weil eben für alle  $n \in \mathbb{N} : P(n)$  gilt. Die beiden Aussage sind also gleichwertig. Was müssen wir tun, um die zweite Aussage per vollständiger Induktion zu beweisen?

Behauptung:

$$\forall n \in \mathbb{N} : \forall k \in \mathbb{N}_{\leq n} : P(k)$$

## 1. Induktionsanfang:

$$\forall k \in \mathbb{N}_{\leq 1} : P(k)$$

Das ist aber nichts anderes als die Aussage  $P(1)$ .

## 2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}$  beliebig aber fest.

## 2.1 Induktionsvoraussetzung:

$$\forall k \in \mathbb{N}_{\leq n} : P(k)$$

## 2.2 Induktionsbehauptung:

$$\forall k \in \mathbb{N}_{\leq n+1} : P(k)$$

## 2.3 Induktionsschritt:

Wie Sie erkennen, ist die für  $k \leq n$  schon in der Voraussetzung enthalten. Damit brauchen wir eigentlich nur die Aussage  $P(n+1)$  zu beweisen. Als Voraussetzung dürfen wir aber benutzen:  $\forall k \in \mathbb{N}_{\leq n} : P(k)$ . Das ist mehr als wir in der „normalen Induktion dürfen.“

Wir haben damit das allgemeine Schema für die vollständige Induktion:

**VOLLSTÄNDIGE INDUKTION****ALLGEMEINES SCHEMA:**

Behauptung:  $\forall n \in \mathbb{N}_{n_0} : P(n)$

## 1. Induktionsanfang:

$$P(n_0)$$

## 2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}_{n_0}$  beliebig aber fest.

## 2.1 Induktionsvoraussetzung:

$$\forall k \in \mathbb{N}_{\leq n} : P(k)$$

## 2.2 Induktionsbehauptung:

$$P(n+1)$$

## 2.3 Induktionsschritt:

$$[\forall k \in \mathbb{N}_{\leq n} : P(k)] \Rightarrow P(n+1)$$

Prinzip :  
Vollständige  
Induktion  
Allgemeines  
Schema

Obwohl der rekursive Ansatz zunächst sehr elegant aussieht, ist ein iterativer Ansatz mit einer Schleife wesentlich effizienter.

Etwas weniger elegant, aber um so effizienter ist die Berechnung der Fibonacci Zahlen mittels einer Schleife: Man merkt sich in der Schleife immer die beiden zuletzt berechneten Fibonacci Zahlen.

## Algorithmus 2: Fibonacci mit Schleifen

```

function fib(n:integer):integer;
var k, fk, fkminus1, temp:integer;
begin
  fk=0; fkminus1=1; k=1;
  while (k<n) do
    begin
      temp=fk;
      fk=fk+fkminus1;
      fkminus1=temp;
      k = k + 1
    end;
  return fk;
end

```

Wie Sie sehen, kommt dieser Algorithmus mit  $n - 1$  Schleifendurchgängen aus, um  $\text{fib}(n)$  zu berechnen.

Es gibt aber noch geschicktere Algorithmen, um die Fibonacci Zahlen zu berechnen. Dazu benötigen wir einen kleinen Satz:

**REKURSIONSFORMEL FÜR  $f_{2n}$  UND  $f_{2n+1}$ :**

Für alle  $n \in \mathbb{N}$  gilt:

$$f_{2n} = f_n^2 + f_{n-1}^2$$

$$f_{2n+1} = f_n^2 + 2f_n \cdot f_{n-1}$$

**Satz 4.3.3**  
Rekursionsformel  
für  $f_{2n}$  und  $f_{2n+1}$

Bitte machen Sie sich keine Gedanken, wie es zu diesen Formeln kommen kann. Um das zu durchblicken, müssten wir sehr viel tiefer in die Materie einsteigen. Vielleicht würden wir dann auch etwas mehr von der Genialität von Fibonacci mitbekommen, aber für angewandte Wissenschaftler zählt einzig das Umsetzen von Ideen, nicht deren Entstehung. Und die bekannte Formel mit vollständiger Induktion zu beweisen ist um vieles einfacher, als sich die Formel ausdenken zu müssen. Mit ein wenig Umsicht und etwas Vertrauen, läuft der Beweis wie auf Schienen.

**Beweis:**

Zweiter Versuch

Behauptung:  $\forall n \in \mathbb{N} : f_{2n} = f_n^2 + f_{n-1}^2$  und  $f_{2n+1} = f_n^2 + 2f_n \cdot f_{n-1}$

1. Induktionsanfang: Wir beweisen die Aussage für  $n = 1$ :

Linke Seite:  $f_{2 \cdot 1} = f_2 = 2$  und  $f_{2 \cdot 1 + 1} = f_3 = 3$  Rechte Seite:  $f_1^2 + f_{1-1}^2 = 1^2 + 1^2 = 2$  und  $f_1^2 + 2f_1f_0 = 1^2 + 2 \cdot 1 \cdot 1 = 3$

2. Induktionsschluss:

Sei dazu  $n \in \mathbb{N}$  beliebig aber fest.

2.1 Induktionsvoraussetzung:

$$f_{2n} = f_n^2 + f_{n-1}^2 \text{ und } f_{2n+1} = f_n^2 + 2f_n \cdot f_{n-1}$$

2.2 Induktionsbehauptung:

$$f_{2(n+1)} = f_{n+1}^2 + f_n^2 \text{ und } f_{2(n+1)+1} = f_{(n+1)}^2 + 2f_{(n+1)} \cdot f_n$$

2.3 Induktionsschritt:

Wir zeigen beide Formeln:

$$\begin{aligned} f_{2(n+1)} &= f_{2n+2} = f_{2n+1} + f_{2n} && \text{Definition der Fibonacci Zahlen} \\ &= (f_n^2 + 2f_n \cdot f_{n-1}) + (f_n^2 + f_{n-1}^2) && \text{Induktionsvoraussetzung} \\ &= (f_n^2 + 2f_n \cdot f_{n-1} + f_{n-1}^2) + f_n^2 && \text{Umsortieren} \\ &= (f_n + f_{n-1})^2 + f_n^2 && \text{1. Binomische Formel} \\ &= f_{n+1}^2 + f_{(n+1)-1}^2 && \text{Definition der Fibonacci Zahlen} \\ \\ f_{2(n+1)+1} &= f_{2n+3} = f_{2n+2} + f_{2n+1} && \text{Definition der Fibonacci Zahlen} \\ &= (f_{n+1}^2 + f_n^2) + f_{2n+1} && \text{obige Formel} \\ &= (f_{n+1}^2 + f_n^2) + (f_n^2 + 2f_n \cdot f_{n-1}) && \text{Induktionsvoraussetzung} \\ &= f_{n+1}^2 + 2f_n \cdot (f_n + f_{n-1}) && \text{Umsortieren} \\ &= f_{n+1}^2 + 2f_{n+1} \cdot f_n && \text{Definition der Fibonacci Zahlen} \end{aligned}$$

**q.e.d.**

Wir wollen  $f_{730}$  berechnen. Dazu wenden wir Satz 4.3 1 für  $2n = 730$  an. Damit können wir die Berechnung von  $f_{730}$  auf die Berechnung von  $f_{366}$  und  $f_{365}$  reduzieren. Dies ist in der Matrix in der zweiten Zeile dargestellt.

Rechenweg in Paaren						Dualdarstellung von 730	Wertigkeit
730						0	1
366,365	365,364					1	2
	183,182					0	4
	92,91	91,90				1	8
		46,45	45,44			1	16
			23,22			0	32
			12,11	11,10		1	64
				6,5	5,4	1	128
					3,2	0	256
					2,1	1	512

Bedauerlicherweise sind diese zwei Zahlen nicht in der Form  $2n$  und  $2n + 1$  sondern in der Form  $2n$ ,  $2n - 1$ , denn die ungerade Zahl ist die kleinere. Wir wenden die Definition der Fibonacci Zahlen an, und führen die Berechnung von  $f_{366}$  auf die Berechnung von  $f_{365}$  und  $f_{364}$  zurück. Dies wird durch die zweite Zeile, zweite Spalte ausgedrückt. Durch diesen kleinen Trick haben wir wieder Zahlen der Form  $2n$  und  $2n+1$ , wobei die gerade die kleine der beiden Zahlen ist. Wir können die Berechnung dieser Fibonacci Zahlen mit dem Satz 1 auf die Berechnung von  $f_{183}$ ,  $f_{182}$  zurückführen, wie der dritten Zeile zu entnehmen ist. Hier ist die größere der beiden Zahlen ungerade, deshalb können wir Satz 4.3 1 direkt anwenden. In der vierten Zeile stehen deshalb 92 und 91. Dieses Verfahren kann weitergeführt werden, bis wir bei dem Paar 2,1 enden. Bitte beachten Sie, dass wir nicht mehr als 9 Berechnungsschritte (Schleifendurchläufe) brauchen. Das ist doch deutlich weniger als 730, wie bei dem Schleifengesteuerten Algorithmus, nicht wahr? Wenn wir dieses Verfahren in ein Programm umsetzen wollen, haben wir mit einer Schwierigkeit fertig zu werden: Die Berechnung der Fibonacci Zahlen erfolgt startend mit der letzten Zeile. Deshalb ist es erforderlich sich zu überlegen, wann die Definition der Fibonaccizahlen und wann der Satz angewendet werden muss. Als entscheidendes Kriterium ist dafür die Dualdarstellung der Zahl 730 angegeben.

Das folgende Programmstück in Java (wegen der BigInteger) setzt Satz 4.3 1 in ein Programm um. Die Java Methode `bitLength` gibt die Länge der Binärdarstellung einer Zahl an, die Methode `testBit(k)` testet, ob das  $k$ -te Bit der Binärdarstellung gesetzt ist.

Algorithmus 3: Fibonacci logarithmisch

```
public static BigInteger fibonacci2(BigInteger i) {
    if (i.compareTo(BigInteger.valueOf(0)) < 0) return null;
    if (i.compareTo(BigInteger.valueOf(1)) <= 0 ) return i;

    BigInteger fnminus1 = BigInteger.valueOf(0);
    BigInteger fn = BigInteger.valueOf(1);

    BigInteger fnhoch2, temp;
    for (int k = i.bitLength()-2; k>=0; k--) {
        fnhoch2 = fn.multiply(fn);
        fn = fnhoch2.add(fnminus1.multiply(
            fn.multiply(BigInteger.valueOf(2))));
        fnminus1 = fnhoch2.add(fnminus1.multiply(fnminus1));
        if ( i.testBit(k) ) {
            temp = fn;
            fn = fn.add(fnminus1);
        }
    }
}
```

```

        fnminus1 = fn;
    }
}
return fn;
}

```

**Aufgabe 4.8:**

Wir definieren Zahlen  $g_n$  für alle  $n \in \mathbb{N}$  durch:

$$g_1 = 1$$

$$g_n = \begin{cases} g_{n/2} & : n \text{ gerade} \\ g_{3n+1} & : n \text{ ungerade} \end{cases}$$

Berechnen Sie  $g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9$

Erläutern Sie, wo das Problem bei Definition liegt.

**Aufgabe 4.9:**

Berechnen Sie die Fibonacci Zahlen  $f_{20}$  und  $f_{40}$  mittels des rekursiven Algorithmus in einer Programmiersprache Ihrer Wahl.

Wie lange glauben Sie, dauert die Berechnung von  $f_{730}$ ?

**Aufgabe 4.10:**

Berechnen Sie  $f_{730}$  mit dem Schleifenalgorithmus mit einer Programmiersprache Ihrer Wahl. Auf welches Problem stoßen Sie.

**Aufgabe 4.11:**

Beweisen Sie folgende Formel für die Fibonacci Zahlen:

$$f_n = \frac{1}{\sqrt{5}} (\Phi^{n+1} - \Psi^{n+1})$$

mit dem goldenen Schnitt  $\Phi$

$$\Phi = \frac{1 + \sqrt{5}}{2} \text{ und } \Psi = 1 - \Phi = \frac{1 - \sqrt{5}}{2}$$

Tipp: Benutzen Sie dass  $\Phi^2 = \Phi + 1$  und  $\Psi^2 = \Psi + 1$  (Kann man nachrechnen!)

**Aufgabe 4.12:**

Beweisen Sie durch vollständige Induktion:

$$\forall n \in \mathbb{N}_0 : f_n \leq 2^n$$

**Aufgabe 4.13:**

Beweisen Sie durch vollständige Induktion:

$$\forall n \in \mathbb{N}_0 : \sum_{k=0}^n f_k = f_{n+2} - 1$$

**Aufgabe 4.14:**

Schreiben Sie ein Programm, das die folgende, rekursiv definierte Funktion berechnet:

Für  $m, n \in \mathbb{N}_0$ :

$$ack(n, m) = \begin{cases} m + 1 & : n = 0 \\ ack(n - 1, 1) & : m = 0 \wedge n > 0 \\ ack(n - 1, ack(n, m - 1)) & : m > 0 \wedge n > 0 \end{cases}$$

n \ m	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	6
2	3	5	7	9	11
3	5	13	29	61	125
4	13				
5					

Beispiele für die Ackermann Funktion

Berechnen Sie mit Ihrem Programm:  $ack(3,2)$ ,  $ack(4,0)$ ,  $ack(4,1)$ ,  $ack(6,0)$ .

Diese Funktion ist die sogenannte Ackermannsche Funktion. Sie spielt in der Berechenbarkeitstheorie eine große Rolle.

Alternativ kann man mit dieser Funktion auch Vorstandsgehälter vorhersagen. Die beiden Parameter haben dabei die folgende Interpretation:

- $n$  ist die Gierigkeitsstufe, die der Vorstandsvorsitzende erreicht hat
- $m$  ist das Jahr seiner Vorsitzendenfunktion

Die Frage ist: Welches Unternehmen kann sich einen Vorstandsvorsitzenden der Gierigkeitsstufe 6 einstellen? Und vielleicht sind das ja auch nur Peanuts.

**Aufgabe 4.15:**

Beweisen Sie, dass für die Funktion  $ack$  folgende Eigenschaft erfüllt:

$$\forall m \in \mathbb{N}_0 : ack(1, m) = m + 2$$

**Aufgabe 4.16:**

Beweisen Sie, dass für die Funktion  $ack$  folgende Eigenschaft erfüllt:

$$\forall m \in \mathbb{N}_0 : ack(2, m) = 2m + 3$$

**Aufgabe 4.17:**

Beweisen Sie, dass für die Funktion  $ack$  folgende Eigenschaft erfüllt:

$$\forall m \in \mathbb{N}_0 : ack(3, m) = 2^{m+3} - 3$$

**Aufgabe 4.18:**

Beweisen Sie, dass für die Funktion  $ack$  folgende Eigenschaft erfüllt:

$$\forall m \in \mathbb{N}_0 : ack(4, m) = \underbrace{2^{\left(2^{\left(\dots^{(2^2)}\right)}\right)}}_{m+3\text{-mal}} - 3$$



## Kapitel 5

# Relationen

*“Ordnung ist die Tochter der Überlegung”*

—Georg Christoph Lichtenberg (1742-99), dt. Aphoristiker u. Physiker

In der Informatik werden Relationen benutzt, um Beziehungen zwischen Objekten darzustellen. Als mathematisches Werkzeug sind sie in der mehr theoretisch ausgerichteten Wissenschaft nicht wegzudenken. (Wer wollte auch schon ohne Bohrmaschine heimwerkern? ) Aber spätestens seit dem Durchbruch der relationalen Datenbanken ist Relationenalgebra in Form der SQL auch für den Praktiker von großer Bedeutung. Wer professionell Datenbanken bauen möchte, sollte sich mit den Begriffen funktionale Abhängigkeit und Normalisierung schon auskennen.

Es ist nicht Ziel dieser Veranstaltung einer Datenbankvorlesung vorzugreifen. Wir werden den Begriff der Relation in harmlosen Zusammenhängen zur Beschreibung von Ordnungen und Äquivalenzen nutzen. Ordnungen finden in vielen Bereichen eine Anwendung als Basis für Programmierverfahren oder mathematische Beweisansätze. Äquivalenzen bilden die Grundlage jeder Abstraktion, einem wissenschaftlichen Grundprinzip. Damit haben wir zwei Basistechniken, bei denen es sich lohnt, sie etwas genauer anzusehen. Und es gibt ausreichend Feinheiten, die das logische Denken trainieren.

## 5.1 Kartesisches Produkt

### Definition 5.1.1 geordnete Paare

#### GEORDNETE PAARE:

Es seien  $a_1$  und  $a_2$  beliebige Objekte,  $(a_1, a_2)$  heißt geordnetes Paar.

Zwei geordnete Paare sind gleich:

$$(a_1, a_2) = (b_1, b_2) \Leftrightarrow (a_1 = b_1 \wedge a_2 = b_2)$$

Bemerkung 42: Wir haben das geordnete Paar als ein neues Konzept eingeführt. Ein geordnetes Paar ist ein neues Ding unseres Denkens, das nur einem Paar mit denselben Komponenten gleich ist. Das ist ein einfaches, aber vielleicht als unschön empfundenes Verfahren. Schöner würde es von einem Mathematiker angesehen werden, wenn das Konzept des Paares auf das Konzept der Menge zurückgeführt würde. Das ist auch möglich, indem man definiert:  $(a, b) = \{a, \{a, b\}\}$ . Dann muss man allerdings die in der Definition festgelegte Gleichheit beweisen.<sup>1</sup> Wir wählen die einfachere Variante.

#### Beispiel 5.1.1

1.  $(1, 2) = (1, 2)$
2.  $(1, 2) \neq (2, 1)$
3.  $(1, (1, 2)) \neq ((1, 1), 2)$
4.  $(1, \{1\}) \neq (1, 1)$
5.  $(1, \{1\}) = (1, \{x \in \mathbb{N} | x < 2\})$
6.  $(1, 2) \neq \{1, 2\}$
7.  $1 \neq (1, 1)$

### Definition 5.1.2 Kartesisches Produkt

#### KARTESISCHES PRODUKT:

Das „Kartesische Produkt“ zweier Mengen  $S$  und  $T$  ist die Menge aller geordneten Paare.  $S \times T = \{x | \text{Es gibt } y \in S \text{ und } z \in T, \text{ so dass } x = (y, z)\}$

Bemerkung 43: Mit Quantoren kann man schreiben  $S \times T = \{x | \exists y \in S : \exists z \in T : x = (y, z)\}$

<sup>1</sup>Diese Definition geht auf Kuratowski zurück. Andere Mathematiker haben andere Definitionen für das Kartesische Produkt gewählt. Welche davon Verwendung findet ist Geschmackssache. Es lohnt sich den Wikipediartikel zum Thema Geordnetes Paar zu lesen.

Bemerkung 44: Zur Vereinfachung der Schreibweise verwendet man die Variante, in der man mit zwei Laufvariablen arbeitet:

$$S \times T = \{(x, y) | x \in S \wedge y \in T\}$$

Die Laufvariablen  $x$  und  $y$  durchlaufen unabhängig voneinander alle Objekte unseres Denkens und unserer Anschauung. Die definierende Eigenschaft schränkt nun die Objekte ein, für die das Paar  $(x, y)$  in der Menge liegt.

Bemerkung 45: Bitte beachten Sie, dass beim Arbeiten mit zwei Laufvariablen  $x$  und  $y$  diese unabhängig ihre Werte annehmen. Das bedeutet insbesondere, dass die angenommenen Werte durchaus identische sein können. Dieser Spezialfall wird häufig übersehen. Im Kern bedeutet das, dass das geordnete Paar  $(x, y)$  durchaus gleich dem geordneten Paar  $(y, x)$  sein kann, nämlich dann, wenn  $x = y$  ist. Obwohl die Laufvariablen unterschiedlich heißen, sind ihre Werte gleich.

Bei der Verwendung von zwei Laufvariablen  $x, y$  gibt es nicht nur bei Paaren Sonderfälle. Auch bei dem Mengenbildungsprinzip „Aufzählen der Elemente“ ist zu beachten, dass zwei Variablen denselben Wert haben können. So kann  $\{x, y\}$  durchaus eine Menge mit nur einem Element sein, wenn nämlich  $x=y$  ist. Obwohl beim Aufzählen konkreter Objekte in der Menge Elemente nicht mehrfach genannt werden dürfen, kann es passieren, dass bei der Verwendung von Variablen gewisse Elemente zusammenfallen. Falls  $x = y$ , so ist dann  $\{x, y\} = \{x\} = \{y\}$

**Beispiel 5.1.2** 1. Sei  $S = \{1, 2\}$  und  $T = \{3, 4, 5\}$  dann ist

$$S \times T = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$$

2.  $\{1, 2\} \times \{2, 3\} = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$

3.  $S \times \emptyset = \emptyset$

4.  $\emptyset \times S = \emptyset$

#### N-TUPEL:

Es seien  $x_1, x_2, x_3, \dots, x_n$  beliebige Objekte. Das geordnete „n-tupel“ ist das Objekt  $(x_1, x_2, x_3, \dots, x_n)$ . Zwei geordnete n-tupel  $(x_1, \dots, x_n) = (y_1, \dots, y_n)$  sind gleich, wenn  $x_1 = y_1$  und  $x_2 = y_2$  und ... und  $x_n = y_n$ .

Das kartesische Produkt von n Mengen  $M_1, \dots, M_n$  ist definiert durch:

$$M_1 \times M_2 \times \dots \times M_n = \{(x_1, x_2, \dots, x_n) | x_1 \in M_1 \wedge x_2 \in M_2 \wedge \dots \wedge x_n \in M_n\}$$

**Definition 5.1.3**  
n-tupel

**Aufgabe 5.1:**

Berechnen Sie die kartesischen Produkte:

1.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}$
2.  $(\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}) \times \{1\}$
3.  $\{1, \{1, 2\}\} \times (\{1, \{1, 2\}\} \times \{1\})$
4.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} \times \{1\}$
5.  $\{\emptyset\} \times \{\emptyset, 1, 2\}$
6.  $\{\emptyset, P(\emptyset)\} \times \emptyset$

**Lösung 5.1:**

1.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} = \{(1, 1), (1, \{1, 2\}), (\{1, 2\}, 1), (\{1, 2\}, \{1, 2\})\}$
2.  $(\{1, \{1, 2\}\} \times \{1, \{1, 2\}\}) \times \{1\}$   
 $= \{((1, 1), 1), ((1, \{1, 2\}), 1), ((\{1, 2\}, 1), 1), ((\{1, 2\}, \{1, 2\}), 1)\}$
3.  $\{1, \{1, 2\}\} \times (\{1, \{1, 2\}\} \times \{1\})$   
 $= \{(1, (1, 1)), (1, (\{1, 2\}, 1)), (\{1, 2\}, (1, 1)), (\{1, 2\}, (\{1, 2\}, 1))\}$
4.  $\{1, \{1, 2\}\} \times \{1, \{1, 2\}\} \times \{1\} = \{(1, 1, 1), (1, \{1, 2\}, 1), (\{1, 2\}, 1, 1), (\{1, 2\}, \{1, 2\}, 1)\}$
5.  $\{\emptyset\} \times \{\emptyset, 1, 2\} = \{(\emptyset, \emptyset), (\emptyset, 1), (\emptyset, 2)\}$
6.  $\{\emptyset, P(\emptyset)\} \times \emptyset = \emptyset$

**Aufgabe 5.2:**

Geben Sie die Menge an:

$$\{\{x, y\} \mid x \in \{1, 2\} \wedge y \in \{2, 3\}\}$$

**Lösung 5.2:**

Bei dieser Aufgabe muss man darauf achten, dass die Mengenbildung anders funktioniert als die Paarbildung. Eine Menge darf eben nur jedes Element einmal enthalten. Ausserdem kommt es nicht auf die Reihenfolge an.

$$\{\{x, y\} | x \in \{1, 2\} \wedge y \in \{2, 3\}\} = \{\{1, 2\}, \{1, 3\}, \{2\}, \{2, 3\}\}$$

**Aufgabe 5.3:**

Geben Sie eine Formel zur Berechnung von  $|S \times T|$  an.

**Lösung 5.3:**

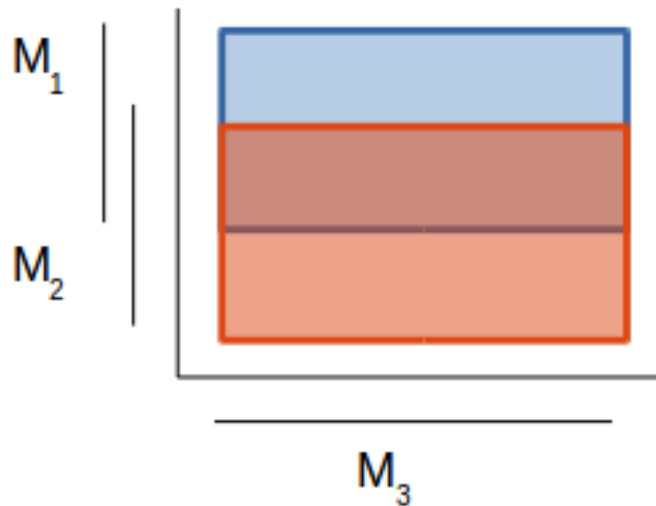
$$|S \times T| = |S| \cdot |T|$$

**Aufgabe 5.4:**

Welche der Gleichheiten gilt für beliebige Mengen  $M_1, M_2, M_3, M_4$ ?

1.  $(M_1 \cup M_2) \times M_3 = (M_1 \times M_3) \cup (M_2 \times M_3)$
2.  $(M_1 \cap M_2) \times M_3 = (M_1 \times M_3) \cap (M_2 \times M_3)$
3.  $(M_1 \setminus M_2) \times M_3 = (M_1 \times M_3) \setminus (M_2 \times M_3)$
4.  $(M_1 \cup M_2) \times (M_3 \cup M_4) = (M_1 \times M_3) \cup (M_2 \times M_4)$

**Lösung 5.4:**



1.  $(M_1 \cup M_2) \times M_3 = (M_1 \times M_3) \cup (M_2 \times M_3)$  ist richtig.  
Beide Seiten entsprechen dem Bereich, der durch beide Rechtecke dargestellt wird.
2.  $(M_1 \cap M_2) \times M_3 = (M_1 \times M_3) \cap (M_2 \times M_3)$  ist richtig.  
Beide Seiten entsprechen dem Bereich, der durch die Überschneidung der beiden Rechtecke dargestellt wird.
3.  $(M_1 \setminus M_2) \times M_3 = (M_1 \times M_3) \setminus (M_2 \times M_3)$  ist richtig.  
Beide Seiten entsprechen dem Bereich, der durch das blaue aber nicht durch das orangefarbene Rechteck dargestellt wird.
4.  $(M_1 \cup M_2) \times (M_3 \cup M_4) = (M_1 \times M_3) \cup (M_2 \times M_4)$  ist falsch. Beispiel:  $M_1 = \emptyset, M_2 = \{1\}, M_3 = \{1\}, M_4 = \emptyset$  Die linke Seite ist dann  $\{(1, 1)\}$  und die rechte Seite ist  $\emptyset$ .

## 5.2 Allgemeine Relationen und deren Darstellung

Der Begriff der Relation, den wir in diesem Kapitel auf den Begriff der Menge und des kartesischen Produkts zurückführen, ist im Kern inhaltsgleich mit den zweistelligen Prädikaten. Zweistellige Prädikate beschreiben „Beziehungen“ zwischen Objekten aus einem, oder allgemeiner gesehen aus zwei möglicherweise verschiedenen Betrachtungsbereichen. Genau das können wir

auch mit der Betrachtung von Paaren erreichen. Es fragt sich nur welche Paare wir betrachten wollen. Das wird aber durch eine Mengenbildung beantwortet werden.

Wir werden Relationen als Mengen einführen, weil sich mit Mengen so schön rechnen lässt.

**RELATION:**

Eine (binäre) Relation  $R$  zwischen zwei Mengen  $M$  und  $N$  ist eine beliebige Teilmenge des kartesischen Produkts  $M \times N$  (siehe Mengenlehre).

$$R \subseteq M \times N$$

**Definition 5.2.1**  
Relation

Manche könnten sich durch die Allgemeinheit der Definition 5.2.1 irritieren lassen. Denn unter einer Beziehung zwischen Objekten versteht man im gewöhnlichen Leben üblicherweise einen realen Zusammenhang. Die Beziehung „liebt“ schafft einen Zusammenhang zwischen Männern und Frauen (streng katholisch patriarchisch gesehen), die Beziehung „kauft seine Brötchen bei“ zwischen Menschen und Bäckereibetrieben (und neuerdings auch Tankstellen). Wenn wir eine Relation als eine Teilmenge des kartesischen Produktes definieren, verstehen wir das so, dass für Paare  $(x, y)$ , die in der Teilmenge stehen, das  $x$  in Beziehung zu dem  $y$  steht. In der Definition 5.2.1 fehlt nun jeglicher Bezug auf eine konkrete Beziehung. Es wird nur auf abstrakter Ebene ein Zusammenhang zwischen Objekten der Menge  $M$  und Objekten der Menge  $N$  geschaffen, der nicht weiter hinterfragt wird. Es ist völlig nebensächlich, welche Beziehung die Relation erzeugt, es ist nicht einmal vorausgesetzt, dass es überhaupt solch eine Beziehung gibt. Diese Definition

Identifiziert man die Menge  $R$  mit einem zweistelligen Prädikat  $R$ , so kann man statt  $(x, y) \in R$  auch  $x R y$  und sagt:

- $x$  und  $y$  stehen in der Relation  $R$  oder
- $x$  steht in der Relation  $R$  zu  $y$

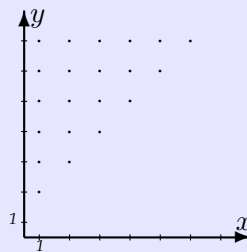
**Beispiel 5.2.1** Betrachten wir die Menge  $M$  aller Männer und  $F$  aller Frauen. Die Beziehung „ist Gatte von“ kann man sich als Relation vorstellen, wobei ein Paar  $(x,y)$  in der Relation vorkommt, immer wenn „ $x$  ist Gatte von  $y$ “ wahr ist:

Nehmen wir also an  $M = \{Hans, Klaus, Peter\}$  und  $F = \{Lisa, Mona\}$  und Hans ist verheiratet mit Mona und Klaus ist verheiratet mit Lisa. Dann wäre die Relation im Sinne der Definition 5.2.1 gegeben durch:

$$R = \{(Hans, Mona), (Klaus, Lisa)\}$$

**Beispiel 5.2.2** In der Menge der natürlichen Zahlen  $\mathbb{N}$  kann man das zweistellige Prädikat „ $\cdot < \cdot$ “ auch als Relation verstehen. Das Paar  $(x,y)$  ist in der Relation (Menge)  $R_{<}$ , genau dann, wenn  $x < y$ . Wir werden diese Identifikation von  $<$  mit der Menge aller Paare  $R_{<}$  im Rest des Skriptes stillschweigend machen.

Visuell kann man sich  $R_{<}$  wie folgt vorstellen: In dem kartesischen Koordinatensystem sind die Punkte aus  $\mathbb{N} \times \mathbb{N}$ , die zur Relation  $R_{<}$  gehören, dargestellt:

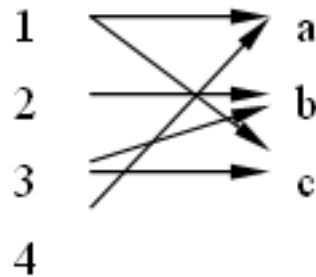


Zur visuellen Veranschaulichung von Relationen stehen verschiedene Methoden zur Verfügung:

### 5.2.1 Pfeildiagramme

$$M = \{1, 2, 3, 4\} \quad N = \{a, b, c\} \quad R = \{(1, a), (1, c), (2, b), (3, b), (3, c), (4, a)\}$$





### 5.2.2 Matrixschreibweise

$$M = \{1, 2, 3, 4\} N = \{a, b, c\} R = \{(1, a), (1, c), (2, b), (3, b), (3, c), (4, a)\}$$

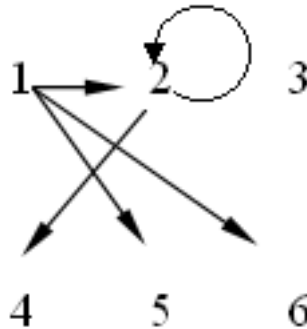
$M \setminus N$	a	b	c
1	1	0	1
2	0	1	0
3	0	1	1
4	1	0	0

Die in diesem Unterabschnitt dargestellte Matrix wird auch Adjazenzmatrix genannt.

### 5.2.3 vereinfachtes Pfeildiagramm

Sind die beiden Mengen  $M$  und  $N$  identisch, dann bietet es sich an, das Pfeildiagramm zu vereinfachen:  $M = N = \{1, 2, 3, 4, 5, 6\}$

$$R = \{(1, 2), (1, 5), (1, 6), (2, 2), (2, 4)\}$$



Bemerkung 1: Eine kleine Abschätzung der möglichen Relationen in der Menge  $\{1, 2, 3, 4, 5, 6\}$ :

- Anzahl der möglichen Paare: 36
- Anzahl der möglichen Relationen:  $2^{36} \approx 64$  Milliarden (Alle Teilmengen des Kreuzprodukts sind Relationen. Eine Menge mit  $n$  Elementen hat  $2^n$  Teilmengen.

**Definition 5.2.2**  
Inverse Relation

**INVERSE RELATION:**

Es seien  $M, N$  beliebige Mengen und  $R \subseteq M \times N$  eine Relation.

Die inverse Relation  $R^{-1} \subseteq N \times M$  ist:

$$R^{-1} = \{(y, x) | (x, y) \in R\}$$

**Beispiel 5.2.3** In den Verwandtschaftsbeispielen setzen wir aus Vereinfachungsgründen immer streng katholische Familienverhältnisse voraus: keine unehelichen Kinder keine geschiedenen Ehen, ....

$M = N = \{m | m \text{ ist Mensch}\}$

$R = \{(m, k) \in M \times M | m \text{ „ist Vater von“ } k\}$

$R^{-1} = \{(k, m) \in M \times M | k \text{ „hat als Vater“ } m\}$

**Beispiel 5.2.4** In der Matrixschreibweise erhält man die inverse Relation durch Spiegelung an der Nebendiagonale:

$M \setminus N$	$a$	$b$	$c$		$N \setminus M$	$1$	$2$	$3$	$4$
$1$	$1$	$0$	$1$	$\xrightarrow{\text{spiegeln}}$	$a$	$1$	$0$	$0$	$1$
$2$	$0$	$1$	$0$		$b$	$0$	$1$	$1$	$0$
$3$	$0$	$1$	$1$		$c$	$1$	$0$	$1$	$0$
$4$	$1$	$0$	$0$						

**Beispiel 5.2.5** Inverse Relation im Pfeildiagramm: Pfeilrichtung umdrehen

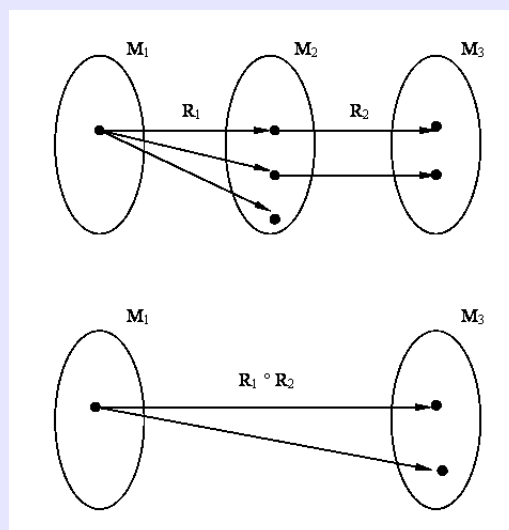
#### VERKETTUNG VON RELATIONEN:

Seien  $M_1, M_2$  und  $M_3$  beliebige Mengen. Es seien  $R_1 \subseteq M_1 \times M_2$  und  $R_2 \subseteq M_2 \times M_3$  binäre Relationen. Die **Verkettung** oder auch **Komposition**  $R_1 \circ R_2$  ist dann folgende Relation zwischen  $M_1$  und  $M_3$ :

$$R_1 \circ R_2 \subseteq M_1 \times M_3$$

$$R_1 \circ R_2 = \{(x, z) | x \in M_1 \wedge z \in M_3 \wedge \exists y \in M_2 : (x, y) \in R_1 \wedge (y, z) \in R_2\}$$

**Definition 5.2.3**  
Verkettung von  
Relationen



**Beispiel 5.2.6**

**Beispiel 5.2.7**  $M_1 = M_2 = M_3 = \{\text{Karl, Otto, Ilse, Fritz, Berta, Anna}\}$

$$\begin{aligned} R_1 &= \text{„ist Vater von“} \\ &= \{(\text{Karl, Otto}), (\text{Karl, Fritz}), (\text{Otto, Berta})\} \end{aligned}$$

$$\begin{aligned} R_2 &= \text{„ist verheiratet mit“} \\ &= \{(\text{Otto, Ilse}), (\text{Fritz, Berta}), (\text{Karl, Anna}), \\ &\quad (\text{Ilse, Otto}), (\text{Berta, Fritz}), (\text{Anna, Karl})\} \end{aligned}$$

$$\begin{aligned} R_1 \circ R_2 &= \text{„ist Schwiegervater von“} \\ &= \{(\text{Karl, Ilse}), (\text{Karl, Berta}), (\text{Otto, Fritz})\} \end{aligned}$$

Otto ist Schwiegervater von Fritz, weil Fritz Berta, die Tochter seines Bruders (oder vielleicht Halbbruders) Otto geheiratet hat. Das ist zumindest in unserem Kulturkreis nicht üblich! Es könnte natürlich sein, dass Ilse Berta mit in die Ehe gebracht hat, sie also mit Otto gar nicht verwandt ist. Also ist dieses Beispiel eher unchristlich zu bezeichnen.

Bemerkung 2: Verkettung mit der leeren Menge gibt die leere Menge.

Wenn  $R \subseteq M_1 \times M_2$  und  $\emptyset \subseteq M_2 \times M_3$  dann  $R \circ \emptyset = \emptyset$  Zum Abschluss noch zwei Sätze, die die Verkettung betreffen:

**Satz 5.2.1**  
Assoziativgesetz  
Verkettung

**ASSOZIATIVGESETZ VERKETTUNG:**

Es seien:  $R_1 \subseteq M_1 \times M_2, R_2 \subseteq M_2 \times M_3, R_3 \subseteq M_3 \times M_4$  Relationen, dann gilt:

$$(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$$

Anmerkung zum Verständnis:  $R_1 \circ R_2 \subseteq M_1 \times M_3$  und  $R_2 \circ R_3 \subseteq M_2 \times M_4$ .

Das Assoziativgesetz besagt, dass Kammersetzung bei der Auswertung von mehreren Verkettungen nicht erforderlich ist. Die Reihenfolge in der die Relationen stehen ist aber sehr wichtig.

**RECHENREGELN INVERSE RELATION:**

Es seien  $R_1 \subseteq M_1 \times M_2$  und  $R_2 \subseteq M_2 \times M_3$  Relationen, dann ist

1.

$$(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$$

Anmerkung zum Verständnis:

$$R_1 \circ R_2 \subseteq M_1 \times M_3 \text{ und } R_2^{-1} \circ R_1^{-1} \subseteq M_3 \times M_1$$

2.

$$(R_1^{-1})^{-1} = R_1$$

**Satz 5.2.2**  
Rechenregeln  
Inverse Relation

Beweis zu a) 1) Zu zeigen:  $(R_1 \circ R_2)^{-1} \subseteq R_2^{-1} \circ R_1^{-1}$  :

Sei  $(z, x) \in (R_1 \circ R_2)^{-1}$  beliebig. Nach der Definition der inversen Relation gilt:  $(x, z) \in R_1 \circ R_2$ . Dann gibt es ein  $y \in M_2$  für das gilt:  $(x, y) \in R_1$  und  $(y, z) \in R_2$ . Also gilt:  $(y, x) \in R_1^{-1}$  und  $(z, y) \in R_2^{-1}$ . Nach der Definition von  $\circ$  bedeutet das:  $(z, x) \in R_2^{-1} \circ R_1^{-1}$

2) Noch zu zeigen  $R_2^{-1} \circ R_1^{-1} \subseteq (R_1 \circ R_2)^{-1}$ :

Sei  $(z, x) \in R_2^{-1} \circ R_1^{-1}$  beliebig. Es gibt ein  $y$  aus  $M_2$  für das gilt:  $(y, x) \in R_1^{-1}$  und  $(z, y) \in R_2^{-1}$ . Nach der Definition der inversen relation gilt:  $(x, y) \in R_1$  und  $(y, z) \in R_2$ . Also folgt  $(x, z) \in R_1 \circ R_2$ . Mit der Definition der inversen Relation folgt:  $(z, x) \in (R_1 \circ R_2)^{-1}$

**Aufgabe 5.5:**

Seien  $M$  und  $N$  beliebige Mengen und  $R \subseteq M \times N$  eine Relation. Welche der Aussagen ist richtig:

1.  $\emptyset$  ist eine Relation zwischen  $M$  und  $N$ .
2.  $M \times N$  ist eine Relation zwischen  $M$  und  $N$ .
3.  $R^{-1}$  ist nur definiert, wenn  $R \neq \emptyset$ .
4.  $R^{-1} = \{(x, y) | (y, x) \in R\}$ .
5.  $\emptyset^{-1} = \emptyset$ .

**Lösung 5.5:**

1.  $\emptyset$  ist eine Relation zwischen  $M$  und  $N$  ist richtig, da auch  $\emptyset$  eine Teilmenge von  $M \times N$  ist, wie in der Definition einer Relation gefordert.
2.  $M \times N$  ist eine Relation zwischen  $M$  und  $N$  ist richtig, da auch  $M \times N$  eine Teilmenge von  $M \times N$  ist, wie in der Definition einer Relation gefordert.
3.  $R^{-1}$  ist nur definiert, wenn  $R \neq \emptyset$  ist falsch, da in der Definition der inversen Relation keine Bedingung an die Relation  $R$  gestellt wird.
4.  $R^{-1} = \{(x, y) | (y, x) \in R\}$  ist richtig, da  $x$  und  $y$  nur "lokale" Variablennamen sind. Wichtig ist nur, dass die Reihenfolge vor und nach dem senkrechten Strich vertauscht wird.
5.  $\emptyset^{-1} = \emptyset$  ist richtig, da  $\emptyset^{-1} = \{(y, x) | (x, y) \in \emptyset\} = \emptyset$

#### Aufgabe 5.6:

1. Wie lautet die inverse Relation  $R = \text{"ist Bruder von"}$  in der Menge der Menschen?
2. Wie lautet die inverse Relation  $R = \text{"ist Kind von"}$  in der Menge der Menschen?
3. Wie lautet die inverse Relation  $R = \text{"liebt"}$  in der Menge der Menschen?
4. Sei  $M$  eine Menge von Mitarbeitern und  $A$  eine Menge von Abteilungen. Die Relation  $R$  sei die Relation "arbeitet in" zwischen  $M$  und  $A$ . Wie bezeichnet man die inverse Relation zu  $R$ ?

#### Lösung 5.6:

1. "hat als Bruder"
2. "ist Elternteil von"
3. "wird geliebt von"
4. "beschäftigt"

#### Aufgabe 5.7:

Seien  $M_1, M_2, M_3$  beliebige Mengen und  $R \subseteq S \subseteq M_1 \times M_2$  sowie  $T \subseteq M_2 \times M_3$  beliebige Relationen. Beweisen oder widerlegen Sie:

1.  $R^{-1} \subseteq S^{-1}$
2.  $S^{-1} \subseteq R^{-1}$
3.  $R \circ T \subseteq S \circ T$

**Lösung 5.7:**

1. Die Aussage ist richtig. Beweis: Sei  $(x, y) \in R^{-1}$  beliebig. Dann gilt laut Definition der inversen Relation  $(y, x) \in R$ . Da  $R \subseteq S$  vorausgesetzt ist, folgt  $(y, x) \in S$  und deshalb wieder nach der Definition der inversen Relation  $(x, y) \in S$ .
2. Die Aussage ist falsch.  $M_1 = M_2 = \{1\}$  und  $R = \emptyset, S = (1, 1)$  ist ein Gegenbeispiel, da  $R^{-1} = \emptyset$  und  $S^{-1} = \{(1, 1)\}$ .
3. Die Aussage ist richtig. Beweis: Sei  $(x, z) \in R \circ T$  beliebig. Dann gibt es nach der Definition der Verkettung ein  $y \in M_2$ , so dass  $(x, y) \in R$  und  $(y, z) \in T$ . Da  $R \subseteq S$  vorausgesetzt wird, ist  $(x, y) \in S$  und daher wieder nach der Definition der Verkettung  $(x, z) \in S \circ T$ .

**Aufgabe 5.8:**

Geben Sie Beispiele für Relationen  $R_1 \subseteq M_1 \times M_2$  und  $R_2 \subseteq M_2 \times M_1$ , so dass

1.  $R_1 \circ R_2 = \emptyset$  und  $R_2 \circ R_1 \neq \emptyset$
2.  $R_1 \circ R_2 = M_1 \times M_1$  und  $R_2 \circ R_1 \neq M_2 \times M_2$

**Lösung 5.8:**

1.  $M_1 = M_2 = \{1, 2\}$  und  $R_1 = \{(1, 1)\}$  und  $R_2 = \{(2, 1)\}$ . Dann ist  $R_1 \circ R_2 = \emptyset$  und  $R_2 \circ R_1 = \{(2, 1)\}$ .
2.  $M_1 = M_2 = \{1, 2\}$  und  $R_1 = \{(1, 1), (2, 1)\}$  und  $R_2 = \{(1, 1), (1, 2)\}$ . Dann ist  $R_1 \circ R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$  und  $R_2 \circ R_1 = \{(1, 1)\}$ .

### 5.3 Eigenschaften von Relationen

In diesem Kapitel betrachten wir nur Relationen einer festen Grundmenge  $M$ :  $R \subseteq M \times M$ .

#### EIGENSCHAFTEN VON RELATIONEN:

Es sei  $M$  eine nichtleere Menge,  $R$  eine Relation,  $R \subseteq M \times M$ .

1. Die „Identische“ Relation ist  $I = \{(x, x) : x \in M\}$
2. Die Relation  $R$  heißt „reflexiv“, wenn:  $I \subseteq R$  oder anders:

$$\forall x \in M : (x, x) \in R$$

3. Eine Relation  $R$  heißt „irreflexiv“, wenn  $I \cap R = \emptyset$  oder anders:

$$\forall x \in M : (x, x) \notin R$$

4. Eine Relation  $R$  heißt „symmetrisch“, wenn:  $R \subseteq R^{-1}$  oder anders:

$$\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$$

5. Eine Relation  $R$  heißt „asymmetrisch“, wenn:  $R \cap R^{-1} = \emptyset$  m.a.W.:

$$\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \notin R$$

6. Eine Relation  $R$  heißt „antisymmetrisch“, wenn:  $R \cap R^{-1} \subseteq I$  oder anders:

$$\forall x, y \in M : (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$$

oder noch anders

$$\forall x, y \in M : (x, y) \in R \wedge x \neq y \Rightarrow (y, x) \notin R$$

oder noch anders

$$\forall x, y \in M : (x, y) \in R \Rightarrow x = y \vee (y, x) \notin R$$

7. Eine Relation  $R$  heißt „transitiv“, wenn:  $R \circ R \subseteq R$  oder anders wenn

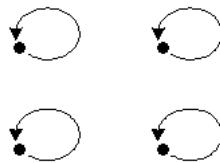
$$\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$$

**Definition 5.3.1**  
Eigenschaften  
von Relationen



Bemerkung 3:

1. Bezüglich  $I$  steht jedes Element aus  $M$  zu sich selbst in Relation, aber keine zwei verschiedenen Elemente stehen in der Relation  $I$ . Der Graph von  $I$  hat an jedem Knoten eine Schlinge und sonst keine Pfeile.



In der Matrixdarstellung wird  $I$  durch die Einheitsmatrix dargestellt.

2. Der Graph einer reflexiven Relation hat also ebenfalls an jedem Punkt eine Schlinge (und möglicherweise noch andere Pfeile).
3. Es ist  $R$  genau dann reflexiv, wenn das Komplement (als Teilmenge von  $M \times M$ ) von  $R$  irreflexiv ist. Im Graphen einer irreflexiven Relation trägt kein Punkt eine Schlinge.

Bemerkung: Eine Relation kann auch weder reflexiv noch irreflexiv sein.  $R$  ist nicht reflexiv bedeutet also nur, dass es mindestens ein  $x \in M$  gibt mit  $(x, x) \notin R$ .

4. Im Graphen einer symmetrischen Relation gibt es genau dann einen Pfeil von  $x$  nach  $y$ , wenn es auch einen Pfeil von  $y$  nach  $x$  gibt. Der gerichtete Graph ist also symmetrisch.

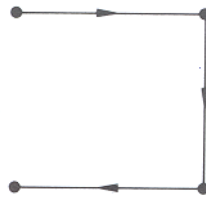


symmetrische Relation

In der Matrixdarstellung wird eine symmetrische Relation durch eine symmetrische Matrix dargestellt (Matrix geht durch Spiegelung an der Hauptdiagonalen - von links oben nach rechts unten - in sich über).

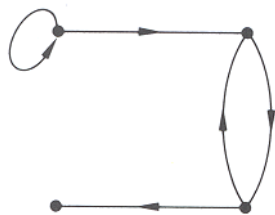
Die Bedingung der Symmetrie findet man häufig auch durch  $\forall x, y \in M : (x, y) \in R \Leftrightarrow (y, x) \in R$  beschrieben. In der Tat sind diese beiden Definitionen auch gleichwertig, was man formal auch dadurch herleiten kann, indem man die Variablen  $x$  und  $y$  in der Definition vertauscht.

5. Im Graphen einer asymmetrischen Relation gibt es zwischen zwei Punkten also höchstens einen Pfeil in einer Richtung, aber keinesfalls beide Richtungen. Eine asymmetrische Relation ist sicher irreflexiv (keine Schlingen im Graphen), denn aus  $(x, x) \in R \Rightarrow (x, x) \notin R$ , also ein Widerspruch.



asymmetrische Relation

Bemerkung: Eine Relation ist nicht entweder symmetrisch oder asymmetrisch. „Nicht symmetrisch“ bedeutet nur, dass es mindestens einen Pfeil  $(x, y)$  gibt, für den der Pfeil  $(y, x)$  in der umgekehrten Richtung fehlt.



nicht symmetrische und  
nicht asymmetrische  
Relation

6. Im Graphen einer antisymmetrischen Relation kann es daher zwischen verschiedenen Punkten höchstens einen Pfeil (eben in einer der beiden möglichen Richtungen) geben, aber es können auch Schlingen vorkommen im Unterschied zu asymmetrischen Relationen.
7. Für den Graphen der Relation  $R$  bedeutet die Transitivität, dass aus der Existenz von Pfeilen von  $x$  nach  $y$  und von  $y$  nach  $z$  die Existenz eines Pfeils von  $x$  nach  $z$  folgt.

Bemerkung 4: Bitte beachten Sie, dass die Aussageformen 4-7 der Definition 5.3.1 bedingte Aussagen sind. Keine der Eigenschaften symmetrisch, asymmetrisch, antisymmetrisch oder transitiv, läßt den Schluss auf eine existierende Beziehung zu.

Die Eigenschaften aus Definition 5.3.1 sind im Kern unabhängig voneinander. Zusammenhänge werden in folgendem Satz dargestellt:

**Beispiel 5.3.1** Betrachten Sie die folgende Relation in der Menge  $M = \{a, b, c\}$ :

$$R = \{(a, a), (a, b), (b, b), (b, a)\}$$

Wenn wir feststellen wollen, welche Eigenschaften diese Relation hat, dann kann man das durch eine Wertetabelle machen. Diese Tabelle hat für die Eigenschaften reflexiv und irreflexiv eine Variablenspalte und für die Eigenschaften symmetrisch und asymmetrisch zwei Variablenspalten und für die Eigenschaft antisymmetrisch sogar drei Variablenspalten.

$x$	$(x, x) \in R$	$(x, x) \notin R$
$a$	wahr	falsch
$b$	wahr	falsch
$c$	falsch	wahr

Wie diese Wertetafel ergibt, ist die Relation weder reflexiv noch irreflexiv.

$x$	$y$	$(x, y) \in R \Rightarrow (y, x) \in R$	$(x, y) \in R \Rightarrow (y, x) \notin R$	$(x, y) \in R \Rightarrow (y, x) \notin R \vee x = y$
$a$	$a$	wahr	falsch	wahr
$a$	$b$	wahr	falsch	falsch
$a$	$c$	wahr	wahr	wahr
$b$	$a$	wahr	falsch	falsch
$b$	$b$	wahr	falsch	wahr
$b$	$c$	wahr	wahr	wahr
$c$	$a$	wahr	wahr	wahr
$c$	$b$	wahr	wahr	wahr
$c$	$c$	wahr	wahr	wahr

Diese Wertetafel zeigt, dass die Relation symmetrisch, nicht asymmetrisch und nicht antisymmetrisch ist.

**Satz 5.3.1**  
Zusammenhänge  
unter den  
Eigenschaften

**ZUSAMMENHÄNGE UNTER DEN EIGENSCHAFTEN:**

- Jede asymmetrische Relation ist irreflexiv.
- Jede asymmetrische Relation ist antisymmetrisch.
- Jede irreflexive Relation ist nicht reflexiv.
- Jede reflexive Relation ist nicht irreflexiv.

**Beispiel 5.3.2** Es sei  $M$  eine Menge aller Geraden in der 2 dimensionalen Ebene  $\mathbb{R}^2$   
Die Relation  $R = \text{„ist orthogonal zu“}$  ist

- *nicht reflexiv*
- *irreflexiv*
- *symmetrisch*
- *nicht asymmetrisch*
- *nicht antisymmetrisch*
- *nicht transitiv*

**Beispiel 5.3.3** Es sei  $M$  eine Menge aller Geraden in der 2 dimensionalen Ebene  $\mathbb{R}^2$   
Die Relation  $R = \text{„ist parallel zu“}$  ist

- *reflexiv* (Das ist eine Frage der genauen Definition von Parallelität. In der Geometrie wird die Definition typischerweise so formuliert, dass die Relation reflexiv ist.)
- *nicht irreflexiv*
- *symmetrisch*
- *nicht asymmetrisch*
- *nicht antisymmetrisch*
- *transitiv*

**Beispiel 5.3.4** *Gesucht: eine Menge  $M$  und eine Relation  $R$ , deren Eigenschaften nicht symmetrisch und nicht asymmetrisch sind;*

*Sei  $M = \{1, 2\}$  und  $R = \{(1, 1), (1, 2)\}$   $R$  ist*

- 1. nicht symmetrisch, weil  $(2, 1) \notin R$*
- 2. nicht asymmetrisch, weil nicht gilt:  $(1, 1) \notin R$*

**Beispiel 5.3.5** *Es sei  $M$  die Menge aller Menschen und  $R$  die Relation „ist Bruder von“.*

*Die Relation ist:*

- nicht symmetrisch, weil  $(\text{Hänsel}, \text{Gretel}) \in R$   
und  $(\text{Gretel}, \text{Hänsel}) \notin R$*
- nicht asymmetrisch, weil  $(\text{Castor}, \text{Pollux}) \in R$   
und  $(\text{Pollux}, \text{Castor}) \in R$*
- irreflexiv, weil keiner sein eigener Bruder ist.*

*Bitte beachten Sie, dass die Relation auch **nicht** transitiv ist. Der Grund hierfür ist etwas versteckt: Castor ist Bruder von Pollux und Pollux ist Bruder von Castor. Aber Castor ist nicht Bruder von Castor.*

Die Eigenschaft der Transitivität lässt sich einfach dadurch darstellen, dass eine Verbindung von  $x$  nach  $z$  über einen Umweg  $y$  existiert, dass gibt es auch immer eine direkte Verbindung von  $x$  nach  $z$ . Man kann durch Hinzunehmen von neuen Verbindungen in einer Relation eine Relation immer transitiv machen. So kann man zum Beispiel die Relation „ist Kind von“ betrachten, die nicht transitiv ist. Lässt man jedoch indirekte Verbindungen zu, dann erhält man die Relation „stammt ab von“. Diese Relation ist transitiv.

**Definition 5.3.2**  
transitiv  
(reflexive) Hülle

**TRANSITIV (REFLEXIVE) HÜLLE:**

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

Die Relation  $R^+$ , die durch die folgende Gleichung definiert wird:

$$R^+ = \{(x, y) \in M \times M \mid \exists m \geq 1, z_0, z_1, \dots, z_m \in M : z_0 = x \wedge z_m = y \\ \wedge (z_0, z_1) \in R \wedge (z_1, z_2) \in R \wedge \dots \wedge (z_{m-1}, z_m) \in R\}$$

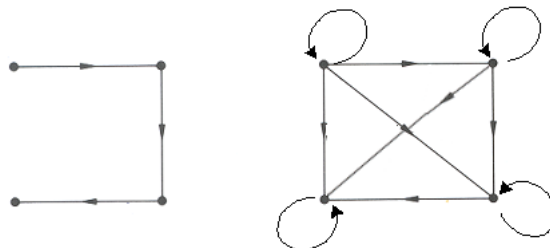
heißt **transitive Hülle** von  $R$ .

Die Relation  $R^*$ , die durch die folgende Gleichung definiert wird:

$$R^* = \{(x, y) \in M \times M \mid x = y \vee \exists m \geq 1, z_0, z_1, \dots, z_m \in M : z_0 = x \wedge z_m = y \\ \wedge (z_0, z_1) \in R \wedge (z_1, z_2) \in R \wedge \dots \wedge (z_{m-1}, z_m) \in R\}$$

heißt **transitiv reflexive Hülle** von  $R$ .

Bemerkung 5: Im Graphen der Relation  $R$  bedeutet dies: Wenn man indirekt von  $x$  nach  $y$  kommen kann, kann man es auch direkt.



Bilden der transitiv reflexiven Hülle

Der Unterschied zwischen der transitiven und der transitiv reflexiven Hülle ist, dass die transitiv reflexive Hülle immer reflexiv ist. Im obigen Beispiel würden also die Eselsohren nicht dazukommen.

**Beispiel 5.3.6** Ein sehr typisches Beispiel für die Bildung einer transitiven Hülle sind Ordnungshierarchien. In einem Unternehmen wird die Aufbauorganisation durch die Relation „berichtet an“ beschrieben:

$M = \{\text{Vorstand, AbteilungVertrieb, AbteilungEinkauf, AbteilungInternetVertrieb, AbteilungLadenVertrieb, SachbearbeiterLadenVertrieb, SachbearbeiterEinkauf}\}$

$R_{\text{berichtetAn}} = \{(\text{AbteilungVertrieb, Vorstand}), (\text{AbteilungEinkauf, Vorstand}), (\text{AbteilungInternetVertrieb, AbteilungVertrieb}), (\text{AbteilungLadenVertrieb, AbteilungVertrieb}), (\text{SachbearbeiterLadenVertrieb, AbteilungLadenVertrieb}), (\text{SachbearbeiterEinkauf, AbteilungEinkauf})\}$

Häufig ist es interessant, wer nun alles auch indirekt an wen berichtet. Zum Beispiel:

$(\text{SachbearbeiterEinkauf, Vorstand}) \in R_{\text{berichtetAn}}^+$   
 $(\text{SachbearbeiterLadenVertrieb, AbteilungVertrieb}) \in R_{\text{berichtetAn}}^+$   
 $(\text{SachbearbeiterLadenVertrieb, AbteilungEinkauf}) \notin R_{\text{berichtetAn}}^+$

Bemerkung 6: Die Definition 5.3.2 der transitiven Hülle einer Relation scheint besonders schwer zu sein, da in der Definition drei Punkte verwendet werden. In strengem mathematischen Sinn ist das **keine** Definition. Man fragt sich, ob Definition 5.3.2 eine ungünstige Formulierung wählt. Leider ist das nicht der Fall. Wir erreichen tatsächlich die Grenzen der Beschreibungsmöglichkeiten der von uns eingeführten Prädikatenlogik 1. Stufe. Dieselbe Beschränkung trifft auch die Datenbankanfragesprache SQL, die sich als Standard zum Auswerten relationaler Datenbankbestände durchgesetzt hat. Konkret bedeutet das, dass mit der Sprache SQL keine Anfrage formuliert werden kann, die als Resultat alle „indirekt“ an den Vorstand berichtenden Organisationseinheiten ermittelt. SQL ist maximal in der Lage eine feste Anzahl von „Indirektionsstufen“ zu ermitteln. Nur durch den Einsatz einer Programmiersprache, die nacheinander mehrere SQL Anfragen absetzt, ist die Frage zu beantworten.

#### CHARAKTERISIERUNG DER TRANSITIV REFLEXIVEN HÜLLE:

$R^*$  ist die kleinste transitive und reflexive Relation, die  $R$  umfasst. Oder anders:

1.  $R^* \supseteq R$  ist transitiv und reflexiv.
2. Ist  $S$  eine beliebige transitive und reflexive Relation mit  $S \supseteq R$  dann ist  $S \supseteq R^*$

**Satz 5.3.2**  
Charakterisierung  
der transitiv  
reflexiven Hülle

Bemerkung 7: Satz 5.3.2 kann auch als Definition der transitiv reflexiven Hülle verwendet werden. Bitte beachten Sie, dass dann keine Punkte verwendet werden. Allerdings kauft man sich diese Eigenschaft dadurch ein, dass man eine

Generalisierung über alle Relationen machen muss. Wir haben es dann mit einer Definition zu tun, die die Prädikatenlogik zweiter Stufe verwendet.

**Beweis:**

zu 1: Um zu zeigen dass  $R^* \supseteq R$  ist, nehmen wir uns ein beliebiges  $(x, y) \in R$  her. Ich setze  $m = 1$ ,  $z_0 = x$  und  $z_1 = y$ . Dann sieht man, dass die Existenzforderung aus Definition 5.3.2 erfüllt ist, so dass  $(x, y)$  auch in  $R^*$  sein muss.

Dass  $R^*$  reflexiv ist, folgt sofort aus der Definition 5.3.2, weil  $R^*$  unter anderem die Elemente  $(x, y) \in M \times M$  enthält, für die  $x = y$  ist.

Schließlich ist noch zu zeigen, dass  $R^*$  transitiv ist. Sei dazu  $(x, y) \in R^*$  und  $(y, z) \in R^*$  beliebig. Es ist zu zeigen, dass  $(x, z) \in R^*$ . Wenn  $x = y$  oder  $y = z$  ist, ist diese Folgerung Teil der Voraussetzung und somit wahr. Wenn  $x \neq y$  und  $y \neq z$  ist, so muss es

$m \geq 1, z_0, z_1, \dots, z_m \in M$  geben, so dass  $z_0 = x \wedge z_m = y \wedge (z_0, z_1) \in R \wedge (z_1, z_2) \in R \wedge \dots \wedge (z_{m-1}, z_m) \in R$

und

$\tilde{m} \geq 1, \tilde{z}_0, \tilde{z}_1, \dots, \tilde{z}_{\tilde{m}} \in M$  geben, so dass  $\tilde{z}_0 = y \wedge \tilde{z}_{\tilde{m}} = z \wedge (\tilde{z}_0, \tilde{z}_1) \in R \wedge (\tilde{z}_1, \tilde{z}_2) \in R \wedge \dots \wedge (\tilde{z}_{\tilde{m}-1}, \tilde{z}_{\tilde{m}}) \in R$

Hängen wir die beiden Verbindungsketten von  $z$ 's und  $\tilde{z}$ 's zusammen erhalten wir eine Verbindungskette mit  $m + \tilde{m} + 1$  Elementen:  $z_0, z_1, \dots, z_m = \tilde{z}_0, \tilde{z}_1, \dots, \tilde{z}_{\tilde{m}}$  wobei  $z_0 = x$  und  $\tilde{z}_{\tilde{m}} = z$ . Das beweist  $(x, z) \in R^*$ .

Zu 2: Sei  $S$  eine beliebige transitive und reflexive Relation mit  $S \supseteq R$ . Wir müssen dann beweisen, dass  $S \supseteq R^*$ . Sei dazu  $(x, y) \in R^*$  beliebig. Nach Definition 5.3.2 ist  $x = y$  oder es gibt  $m \geq 1, z_0, z_1, \dots, z_m \in M$ , so dass  $z_0 = x \wedge z_m = y \wedge (z_0, z_1) \in R \wedge (z_1, z_2) \in R \wedge \dots \wedge (z_{m-1}, z_m) \in R$ . Im Fall  $x = y$  ist  $(x, y) \in S$ , da  $S$  reflexiv ist. Im anderen Fall nutzen wir, dass  $R \subseteq S$ . Dann muss gelten:  $(z_0, z_1) \in S \wedge (z_1, z_2) \in S \wedge \dots \wedge (z_{m-1}, z_m) \in S$ . Da  $S$  auch transitiv war, folgt durch  $m-1$  maliges Anwenden der Transitivität:  $(z_0, z_m) \in S$ , was nichts anderes bedeutet als  $(x, y) \in S$ . **q.e.d.**

**Aufgabe 5.9:**

Erstellen Sie eine Wertetabelle für die transitiv Eigenschaft der Relation  $M = \{a, b, c\}$  und  $R = \{(a, a), (a, b), (b, b), (b, a)\}$  (Die Tabelle deckt 27 Kombinationen ab). Ist die Relation transitiv?

**Lösung 5.9:**



Wie diese Wertetafel ergibt, ist die Relation transitiv.

x	y	z	$(x, y) \in R \wedge (y, z) \in R$	$(x, z) \in R$	$(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$
a	a	a	wahr	wahr	wahr
a	a	b	wahr	wahr	wahr
a	a	c	falsch	falsch	wahr
a	b	a	wahr	wahr	wahr
a	b	b	wahr	wahr	wahr
a	b	c	falsch	falsch	wahr
a	c	a	falsch	wahr	wahr
a	c	b	falsch	wahr	wahr
a	c	c	falsch	falsch	wahr
b	a	a	wahr	wahr	wahr
b	a	b	wahr	wahr	wahr
b	a	c	falsch	falsch	wahr
b	b	a	wahr	wahr	wahr
b	b	b	wahr	wahr	wahr
b	b	c	falsch	falsch	wahr
b	c	a	falsch	wahr	wahr
b	c	b	falsch	wahr	wahr
b	c	c	falsch	falsch	wahr
c	a	a	falsch	falsch	wahr
c	a	b	falsch	falsch	wahr
c	a	c	falsch	falsch	wahr
c	b	a	falsch	falsch	wahr
c	b	b	falsch	falsch	wahr
c	b	c	falsch	falsch	wahr
c	c	a	falsch	falsch	wahr
c	c	b	falsch	falsch	wahr
c	c	c	falsch	falsch	wahr

#### Aufgabe 5.10:

Geben Sie Beispiele für Relationen die

1. reflexiv, symmetrisch und nicht transitiv
2. irreflexiv, antisymmetrisch und transitiv
3. antisymmetrisch und nicht asymmetrisch

sind.

**Lösung 5.10:**

Es gibt viele Beispiele für solche Relationen, die Beispiele hier sind also nur Beispiele für Beispiele. Für alle Teilaufgaben ist  $M = \{1, 2, 3\}$ .

1.  $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$
2.  $R = \{\}$
3.  $R = \{(1, 1)\}$

**Aufgabe 5.11:**

Ist die Vereinigung (Durchschnitt, Differenz, symmetrische Differenz) zweier reflexiver (irreflexiver, symmetrischer, asymmetrischer, antisymmetrischer, transitiver) Relationen eine reflexive (irreflexive, symmetrische, asymmetrische, antisymmetrische, transitive) Relation?

**Lösung 5.11:**

Hier eine tabellarische Aufstellung der Ergebnisse. Die Einträge müssen durch einen Beweis oder ein Gegenbeispiel belegt werden. Wenn in der Tabelle nichts steht, dann bedeutet das, dass die Ergebnisrelation im Allgemeinen diese Eigenschaft nicht hat. Es kann passieren, dass es Beispiele gibt, in denen die Eigenschaft vorliegt oder nicht vorliegt.

	Durchschnitt	Differenz	symmetrische Differenz
reflexiv	reflexiv	irreflexiv	irreflexiv
irreflexiv	irreflexiv	irreflexiv	irreflexiv
symmetrisch	symmetrisch	symmetrisch	symmetrisch
asymmetrisch	asymmetrisch	asymmetrisch	
antisymmetrisch	antisymmetrisch	antisymmetrisch	
transitiv	transitiv	transitiv	

Hier exemplarisch ein Gegenbeispiel

Symmetrische Differenz von transitiven Relationen braucht nicht transitiv zu sein:  $M = \{1, 2, 3\}$  und  $R = \{(1, 2)\}$  sowie  $S = \{(2, 3)\}$

**Aufgabe 5.12:**

Welche Eigenschaften haben die Relationen „ist Geschwisterkind von“ und „ist verheiratet mit“ in der Menge der Menschen? Gehen Sie von Familienverhältnissen aus, die als streng katholisch bezeichnet werden können.

**Lösung 5.12:**

Die Relation „ist Geschwisterkind von“ hat folgende Eigenschaften: nicht reflexiv, irreflexiv, symmetrisch, nicht asymmetrisch, nicht antisymmetrisch, nicht transitiv.

Die Relation „ist verheiratet mit“ hat folgende Eigenschaften: nicht reflexiv, irreflexiv, symmetrisch, nicht asymmetrisch, nicht antisymmetrisch, nicht transitiv.

**Aufgabe 5.13:**

Welche Eigenschaften hat die Relation „ist Bruder von“ in der Menge der Männer bzw. in der Menge der Menschen.

**Lösung 5.13:**

Die Relation ist nicht reflexiv, irreflexiv, nicht symmetrisch, nicht asymmetrisch, nicht antisymmetrisch, nicht transitiv.

**Aufgabe 5.14:**

Gegeben sei die Menge  $M = \{1, 2, 3, 4, 5\}$  und die Relation  $R = \{(1, 2), (2, 3), (1, 4), (4, 5), (5, 4)\}$

Stellen Sie die Relation als Pfeildiagramm dar. Bestimmen Sie die transitiv reflexive Hülle  $R^*$ .

## 5.4 Ordnungsrelationen

Einem Sprichwort zufolge ist Ordnung das halbe Leben. In der Tat ist eine sinnvolle Arbeitsorganisation ohne ein gewisses Maß an Ordnung nicht denkbar. Auch das Suchen in einem Datenbestand ist ohne Ordnung praktisch unmöglich. Jede Datenbank, jeder effiziente Suchalgorithmus basiert auf einer Reihenfolge, in der die Elemente abgelegt wurden.

Wir wollen in diesem Kapitel Ordnungen mit mathematischen Mitteln beschreiben. Neben einfachen Sequenzen, wo die Elemente wie an einer Schnur aufge-

reicht werden, wollen wir aber auch Fälle mit einbeziehen, in denen es möglich ist, dass Elemente in mehreren „Strängen“ angeordnet werden. Innerhalb eines Stranges liegt eine paarweise Vergleichbarkeit vor, ausserhalb der Stranggrenzen jedoch nicht.

**(STRIKTE) ORDNUNGSRELATION:**

Eine Relation  $R$  in der Menge  $M$  heißt „Ordnungsrelation“ oder kurz eine Ordnung in  $M$ , wenn sie

1. reflexiv,
2. antisymmetrisch und
3. transitiv

ist.

Eine Relation  $R$  in einer Menge  $M$  heißt „strikte Ordnungsrelation“ in  $M$ , wenn sie

1. asymmetrisch und
2. transitiv

ist.

**Definition 5.4.1**  
(strikte)  
Ordnungsrelation

Bemerkung 8: Nimmt man alle Elemente  $(x, x)$  für  $x \in M$  aus einer Ordnungsrelation heraus, erhält man eine strikte Ordnungsrelation. Nimmt man alle Elemente  $(x, x)$  für  $x \in M$  zu einer strikten Ordnungsrelation hinzu, so erhält man offensichtlich eine Ordnungsrelation.

Bemerkung 9: Wir verwenden  $\sqsubseteq$  als allgemeines Symbol für eine Ordnungsrelationen. Es soll an die Relation  $\leq$  zwischen Zahlen erinnern.

Ebenso verwenden wir  $x \sqsubset y$  statt  $x \sqsubseteq y$  und  $x \neq y$  als allgemeines Symbol für eine strikte Ordnungsrelation.

**Beispiel 5.4.1** Die Relation  $\leq$  zwischen natürlichen Zahlen ist eine Ordnungsrelation, wie man leicht durch nachprüfen der definierenden Eigenschaften von Ordnungsrelationen nachweist.

**Beispiel 5.4.2** Sei  $M$  eine beliebige nichtleere Menge und  $P$  die Potenzmenge von  $M$ . Dann ist  $\subseteq$  eine Ordnungsrelation in  $P$ .

**Beispiel 5.4.3** Für je zwei natürliche Zahlen  $a, b \in \mathbb{N}_0$  sei die Teilbarkeitsrelation definiert durch:  
 $a|b$  genau dann, wenn es ein  $c \in \mathbb{N}_0$  gibt, so dass  $ac = b$ .  
 $|$  ist eine Ordnungsrelation in  $\mathbb{N}_0$ .

**Beispiel 5.4.4** Für je zwei ganze Zahlen  $a, b \in \mathbb{Z}$  sei die Teilbarkeit als Erweiterung der Definition definiert durch:  
 $a|b$  genau dann wenn es ein  $c \in \mathbb{Z}$  gibt, so dass  $ac = b$ .  
 $|$  ist nun keine Ordnungsrelation in  $\mathbb{Z}$  mehr, weil es nicht antisymmetrisch ist, denn  $-1|1$  und  $1|-1$  aber nicht  $1 = -1$ .

#### TOTALE ORDNUNGSRELATION:

Eine Ordnung  $R$  in der Menge  $M$  heißt „total“, wenn je zwei Elemente von  $M$  bezüglich  $R$  vergleichbar sind.

$$\forall x, y \in M : (x, y) \in R \vee (y, x) \in R$$

**Definition 5.4.2**  
 totale  
 Ordnungsrelation

Bemerkung 10: Andernfalls heißt  $R$  „partielle“ Ordnung oder Teilordnung.

**Beispiel 5.4.5**  $\leq$  ist eine totale Ordnungsrelation in  $\mathbb{N}$ , denn für je zwei natürliche Zahlen  $x$  und  $y$  gilt  $x \leq y$  oder  $y \leq x$ . Den Fall, dass zwei natürliche Zahlen nicht vergleichbar sind, gibt es nicht.

**Beispiel 5.4.6**  $\subseteq$  ist i.a. keine totale Ordnungsrelation, denn hat die Menge  $M$  mindestens zwei verschiedene Elemente  $a, b$ , dann sind  $\{a\}$  und  $\{b\}$  jeweils nicht Teilmengen voneinander.

**Beispiel 5.4.7**  $|$  ist auch nur partielle Ordnung (in der Menge der natürlichen Zahlen), denn 2 teilt nicht 3 und 3 teilt nicht 2. D.h. in Bezug auf die Relation  $|$  sind 2 und 3 unvergleichbar.

Zur besseren Veranschaulichung von Ordnungsrelationen verwendet man den Begriff der Nachbarschaftsrelation.

**NACHBARSCHAFTSRELATION:**

Es sei  $\sqsubset$  eine strikte Ordnungsrelation in der Menge  $M$ . Die Nachbarschaftsrelation  $\sqsubset^N$  ist:

**Definition 5.4.3**

Nachbarschaftsrelation

$$x \sqsubset^N y \Leftrightarrow x \sqsubset y \text{ und es gibt kein } z \in M : x \sqsubset z \wedge z \sqsubset y$$

Für eine Ordnungsrelation  $\sqsubseteq$  ist die Nachbarschaftsrelation die Nachbarschaftsrelation der zugehörigen strikten Ordnungsrelation.

Bemerkung 11: Die Nachbarschaftsrelation  $\sqsubset^N$  ( $\sqsubseteq^N$ ) ist nicht transitiv und nicht reflexiv.

**Beispiel 5.4.8** Es sei  $\subseteq$  die Ordnungsrelation Teilmenge oder gleich in der Potenzmenge  $P(A)$  der Menge  $A = \{1, 2, 3\}$ .

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

Dann ist die Nachbarschaftsrelation  $\subseteq^N$  gegeben durch

$$\begin{aligned} \subseteq^N = & \{(\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{3\}), \\ & (\{1\}, \{1, 2\}), (\{1\}, \{1, 3\}), \\ & (\{2\}, \{1, 2\}), (\{2\}, \{2, 3\}), \\ & (\{3\}, \{1, 3\}), (\{3\}, \{2, 3\}), \\ & (\{1, 2\}, \{1, 2, 3\}), \\ & (\{1, 3\}, \{1, 2, 3\}), \\ & (\{2, 3\}, \{1, 2, 3\})\} \end{aligned}$$

Ein sehr nützliches Hilfsmittel zur Veranschaulichung von Ordnungsrelationen ist das „Hasse Diagramm“ (Helmut Hasse 1898-1979, deutscher Mathematiker, lehrte u.a. in Kiel, Halle, Marburg, Göttingen und Berlin).

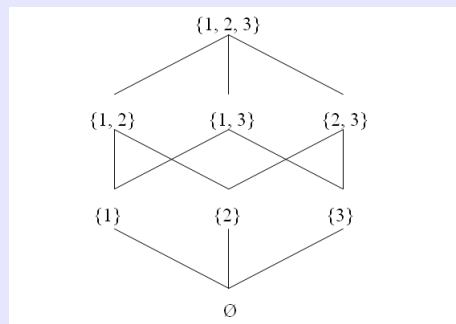
**HASSE DIAGRAMM:**

Das „Hasse Diagramm“ einer Ordnungsrelation ist das Pfeildiagramm der Nachbarschaftsrelation.

**Definition 5.4.4**  
Hasse Diagramm

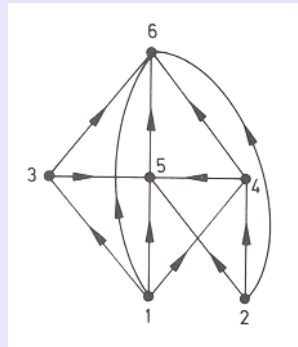
Oder etwas mehr „down to earth“: Ein Hasse Diagramm entsteht, wenn man die Elemente einer Menge so auf dem Papier anordnet, dass gemäß der Ordnungsrelation größere Elemente oberhalb der kleineren stehen, und zwei in der Ordnungsrelation direkt benachbarte Elemente miteinander verbindet (aus Gründen der Übersichtlichkeit werden reflexive und transitive Verbindungen weggelassen).

**Beispiel 5.4.9** Aufgrund der vorgegebenen Pfeilrichtung (von unten nach oben) kann man die Pfeilspitzen weglassen. Damit sieht das Hasse Diagramm der Relation aus Beispiel 5.4.8 folgendermaßen aus.

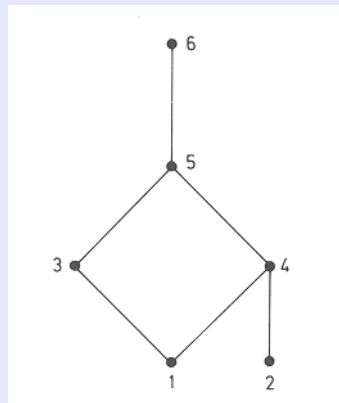


Hasse Diagramm der Teilmengenbeziehung in  $P(\{1, 2, 3\})$ .

**Beispiel 5.4.10** Eine strikte Ordnung auf  $M = \{1, 2, 3, 4, 5, 6\}$  sei durch ihren Graphen gegeben:



Das Hasse Diagramm hat dann folgende Gestalt:



**INFORMATIONSERHALTUNGSSATZ FÜR HASSE DIAGRAMME:**

Es sei  $\sqsubseteq$  eine Ordnungsrelation in der Menge  $M$ .

Ist  $\sqsubseteq$  eine endliche Menge, dann gilt:

$$(\sqsubseteq^N)^* = \sqsubseteq$$

Ist  $\sqsubseteq$  eine beliebige Menge, dann gilt wenigstens immer noch:

$$(\sqsubseteq^N)^* \subseteq \sqsubseteq$$

**Satz 5.4.1**

Informationserhaltungssatz  
für Hasse  
Diagramme

**Bemerkung 12:** Der Satz besagt, dass es zur Beschreibung einer Ordnungsrelation in einer endlichen Menge vollständig ausreicht, die Nachbarschaftsrelation



zu kennen. Durch bilden der transitiv reflexiven Hülle kann man die Relation immer vollständig rekonstruieren. Damit ist das Hasse Diagramm eine sinnvolle Darstellungsmöglichkeit für Ordnungsrelationen. Obwohl es nicht alle Beziehungen darstellt, können alle Beziehungen aus ihm hergeleitet werden.

**Beispiel 5.4.11** *So einfach und fast selbstverständlich die Situation für endliche Mengen ist, so problematisch wird die Darstellung durch das Hasse Diagramm bei unendlichen Mengen.*

*Betrachten wir die gewöhnliche  $\leq$  Ordnung der natürlichen Zahlen. Hier bringt die Nachbarschaftsrelation jede Zahl  $n$  mit ihrem Nachfolger  $n + 1$  in Beziehung, denn zwischen diesen beiden Zahlen gibt es keine dritte. Bildet man die transitive Hülle dieser Nachbarschaftsrelation, so kann man problemlos die Ordnung rekonstruieren. Wenn wir dagegen die gewöhnliche Anordnung der reellen Zahlen betrachten, haben wir das Problem, dass zwischen zwei reellen Zahlen immer noch eine dritte liegt. Das führt dazu dass die Nachbarschaftsrelation leer ist. Aus der leeren Nachbarschaftsrelation können wir die Ordnung der reellen Zahlen natürlich nicht rekonstruieren. Wie haben als einen totalen Informationsverlust.*

*Für die Darstellung von Ordnungsrelationen in unendlichen Mengen ist das Hasse Diagramm keine geeignete Darstellungsmethode, da hier ein Informationsverlust zu befürchten ist.*

*Ein weiteres sehr häufig verwendetes Beispiel für eine Ordnungsrelation, bei der ein Informationsverlust auftritt ist die Ordnung, die man in einem Lexikon anwendet. Je zwei Einträge in einem Lexikon stehen in einer festgelegten Reihenfolge, und jeder, der ein Lexikon benutzt kennt sie, sonst würde er keinen Eintrag finden. Diese Ordnung trägt den Namen lexikografische Ordnung. Die transitive Hülle dieser Nachbarschaftsrelation würde zwar die Einträge „a“, „aa“, „aaa“ usw. wieder in Beziehung setzen, nicht jedoch „a“ und „ab“. Es tritt ein partieller Informationsverlust auf. Zur Darstellung der lexikografischen Ordnung eignet sich das Hasse Diagramm also nicht.*

Bemerkung 13:: Wenn man eine Teileliste (Ordnungsrelation „ist enthalten in“) hat, will man wissen, welche Teile zu einem Auto gehören. Dabei sind wir an allen Teilen interessiert: Baugruppen und Fertigteile. (Die Frage wäre in der Praxis: Wie viele Teile brauche ich, um das Auto herzustellen. Die Anzahl spielt hier allerdings erst mal keine Rolle). Wenn man alle Enthaltenseinsbeziehungen abspeichern würde, sind das sehr viele. Der Satz sagt: Man braucht nur die Nachbarschaftsrelation abzuspeichern und schon kann man den gesamten Rest wieder konstruieren, ohne etwas zu viel oder zu wenig zu haben.

## 5.5 Größte und Maximale Elemente, obere Schranken und Suprema

**Definition 5.5.1**  
größte und  
maximale  
Elemente

### GRÖSSTE UND MAXIMALE ELEMENTE:

Es sei  $\sqsubseteq$  eine Ordnungsrelation in der Menge  $M$ . Es sei  $A \subseteq M$  eine beliebige Teilmenge.

- $b$  heißt „größtes“ Element von  $A$ , falls  $b \in A$  und für alle  $x \in A$  gilt  $x \sqsubseteq b$   
( $\forall x \in A : x \sqsubseteq b$ )
- $b$  heißt „maximales“ Element von  $A$ , falls  $b \in A$  und es gibt kein  $x \in A$  mit  $b \sqsubset x$   
( $\neg \exists x \in A : b \sqsubset x$ )

Ein größtes Element der Menge  $A$  hat also drei Eigenschaften:

- Es gehört zu der Menge  $A$ .
- Es ist mit allen Elementen aus  $A$  vergleichbar.
- Bei dem Vergleich stellt sich heraus, dass es größer als die Elemente der Menge ist.

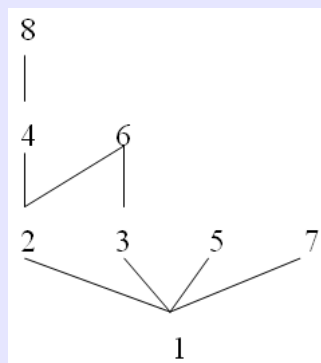
Ein maximales Element hat dagegen die folgenden „abgeschwächten“ Eigenschaften.

- Es gehört zur Menge  $A$ .
- Es ist nicht unbedingt mit allen Elementen vergleichbar.
- Wenn es allerdings vergleichbar ist, dann ist es das größere.

Bemerkung 14:: Mit der „es gibt kein ...“ Aussage lässt sich häufig schwer etwas anfangen. Deshalb formuliert man die negative Aussage gerne in eine positive um.

$$\begin{aligned}
 \neg \exists x \in A : b \sqsubseteq x &\Leftrightarrow \forall x \in A : \neg(b \sqsubseteq x) \\
 &\Leftrightarrow \forall x \in A : \neg(b \sqsubseteq x \wedge x \neq b) \\
 &\Leftrightarrow \forall x \in A : (\neg b \sqsubseteq x) \vee x = b \\
 &\Leftrightarrow \forall x \in A : b \sqsubseteq x \Rightarrow x = b
 \end{aligned}$$

**Beispiel 5.5.1** Es sei  $M$  die Menge  $M = \{1, 2, 3, 4, 5, 6, 7, 8\}$  und „teilt“ die auf  $M$  definierte Ordnungsrelation. Das zugehörige Hasse Diagramm ist:



- 6 ist größtes und maximales Element von  $A = \{2, 3, 6\}$
- 2, 3 sind maximale Elemente von  $B = \{2, 3\}$ .  $B$  hat kein größtes Element.
- 5, 6 sind maximale Elemente von  $C = \{2, 3, 5, 6\}$ .  $C$  hat kein größtes Element.
- 5, 6, 7, 8 sind maximale Elemente von  $M$  und  $M$  hat kein größtes Element.

#### EIGENSCHAFTEN VON GRÖSSTEN ELEMENTEN:

Sei  $M$  eine beliebige Menge mit einer Ordnungsrelation  $\sqsubseteq$ . Sei  $A \subseteq M$  eine beliebige Teilmenge. Dann gilt:

1. Es gibt höchstens ein größtes Element in einer Menge  $A$ .
2. Jedes größte Element der Menge  $A$  ist auch maximales Element von  $A$ .

**Satz 5.5.1**  
Eigenschaften  
von größten  
Elementen

#### Beweis:

Zu Teil 1: Um eine „es gibt höchstens ein ...“ Aussage zu beweisen, zeigt man,

dass zwei Elemente, die die geforderte Eigenschaft besitzen, notwendigerweise gleich sind. Also hier:

Seien  $g_1 \in A$  und  $g_2 \in A$  größte Elemente von  $A$ . Dann gilt:

$g_2 \sqsubseteq g_1$  da  $g_1$  größtes Element von  $A$  ist und  $g_2 \in A$

und

$g_1 \sqsubseteq g_2$  da  $g_2$  größtes Element von  $A$  ist und  $g_1 \in A$

Da  $\sqsubseteq$  als Ordnungsrelation antisymmetrisch ist, folgt  $g_1 = g_2$ .

Der Beweis der zweiten Teilaussage bleibt als Übung. **q.e.d.**

**Bemerkung 15:** In dieser Aussage haben wir es zum ersten Mal mit einer Eindeutigkeitsaussage zu tun gehabt. „Es gibt höchstens ein größtes Element“. Es ist nicht erforderlich, dass ein größtes Element existiert, damit diese Aussage richtig wird. Insofern ist es nicht verwunderlich, dass eine Eindeutigkeitsaussage **keine Existenzaussage** ist, sonder eine **Generalisierung**.

**Beispiel 5.5.2** Viele kennen den Film „Der Highlander“. Ein zentrales Thema in diesem Film wird mit dem Satz „Es kann nur einen geben“ umschrieben. Als Konsequenz zu dieser Aussage müssen sich je zwei so lange bekämpfen, bis nur noch einer übrigbleibt. Genauso beweist man in der Mathematik eine Eindeutigkeitsaussage: Man nimmt an, dass zwei Elemente die geforderte Eigenschaft haben und beweist, dass die beiden Elemente identisch sind. In der Mathematik wäre die im Film verfolgte Lösung nur schwer denkbar.

#### ES GIBT HÖCHSTES EIN . . . :

Eine Eindeutigkeitsaussage (Es gibt höchstens ein . . .) wird dadurch bewiesen, dass man annimmt, es gäbe zwei, und man beweist, dass diese beiden identisch sein müssen.

Prinzip :  
Es gibt höchstes  
ein . . .

**SUPREMUM/INFIMUM:**

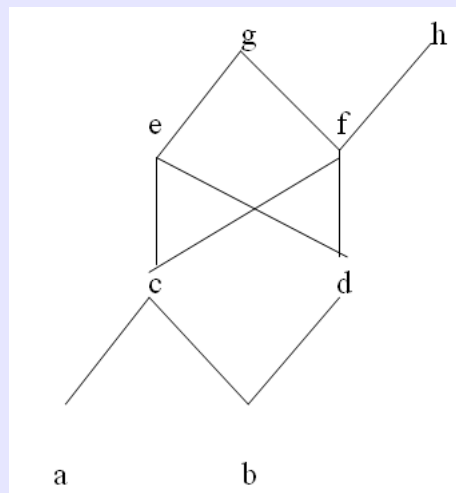
Es sei  $\sqsubseteq$  eine Ordnungsrelation in der Menge  $M$ . Es sei  $A \subseteq M$  eine beliebige Teilmenge.

1.  $g \in M$  heißt obere (untere) Schranke von  $A$ , falls  $\forall x \in A : x \sqsubseteq g$  ( $g \sqsubseteq x$ )
2.  $g \in M$  heißt obere (untere) Grenze von  $A$ , falls  $g$  minimales (maximales) Element der Menge der oberen (unteren) Schranken ist.
3.  $g \in M$  heißt Supremum (Infimum), falls  $g$  kleinstes (größtes) Element der Menge der oberen (unteren) Schranken ist. Wir schreiben  $g = \sup A$  ( $g = \inf A$ ).

**Definition 5.5.2**  
Supremum/Infimum

Da die Ordnungsrelation im Prinzip beliebig strukturiert sein kann, kann es passieren, dass es zu einer Menge keine unteren (oberen) Schranken gibt. In diesem Fall gibt es dann weder untere (obere) Grenzen noch Infima (Suprema). Wenn allerdings ein Supremum (Infimum) existiert, dann ist es eindeutig, da eine Menge immer nur ein größtes (kleinstes) Element hat. Deshalb ist die Schreibweise  $\sup A$  und  $\inf A$  gerechtfertigt.

**Beispiel 5.5.3** Es sei  $\sqsubseteq$  eine Ordnungsrelation in der Menge  $M$ , die durch das folgende Hasse Diagramm gegeben ist.



Hasse Diagramm .

Untersuchen Sie die folgenden Teilmengen  $\{a, b\}$ ,  $\{c, d\}$  und  $\{f, g, h\}$  auf obere Schranken, obere Grenzen und Suprema.

- $A = \{a, b\}$ 
  - hat obere Schranken  $c, e, f, g, h$
  - hat eine obere Grenze  $c$
  - hat ein Supremum  $c = \sup A$ .
- $\{c, d\}$ 
  - hat obere Schranken  $e, f, g, h$
  - hat obere Grenzen  $e, f$
  - hat kein Supremum
- $\{f, g, h\}$ 
  - hat keine obere Schranken
  - hat keine obere Grenzen
  - hat kein Supremum

**EXISTENZSATZ SUPREMUM:**

Eine Menge hat wenigstens ein Supremum (Infimum), wenn sie nur eine obere (untere) Grenze hat.

**Satz 5.5.2**  
Existenzsatz  
Supremum

**Aufgabe 5.15:**

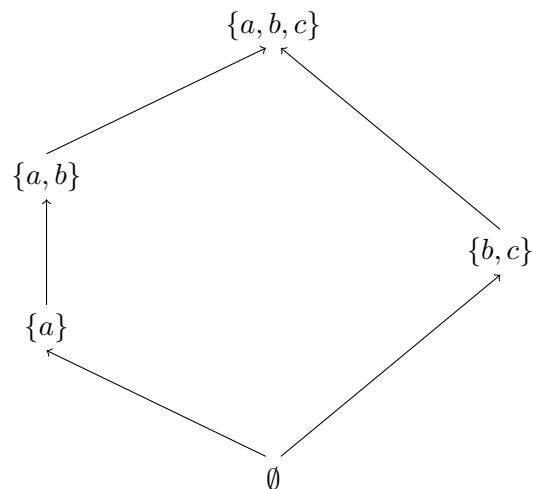
Geben Sie das Hasse Diagramm für die Relation

1.  $\subseteq$  in der Menge  $M = \{\emptyset, \{a, b\}, \{b, c\}, \{a, b, c\}, \{a\}\}$
2.  $|$  (teilt) in der Menge  $M = \{2, 3, 4, 5, 6, 8, 10\}$
3.  $|$  (teilt) in der Menge  $M = \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$

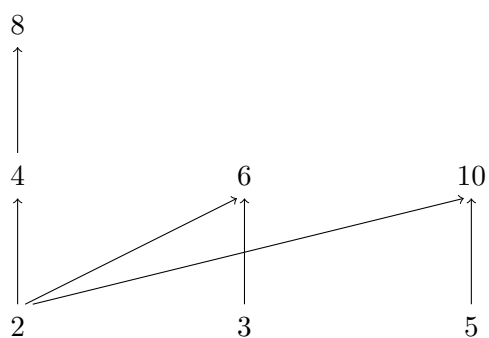
(Bemerkung:  $x|0$  für jedes  $x \in M$ )

**Lösung 5.15:**

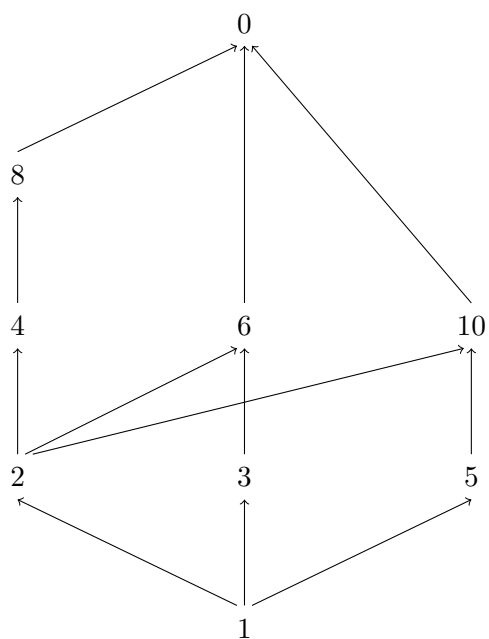
1. Hassediagramm von  $\subseteq$  in der Menge  $M = \{\emptyset, \{a, b\}, \{b, c\}, \{a, b, c\}, \{a\}\}$ .



2. Hassediagramm von  $|$  (teilt) in der Menge  $M = \{2, 3, 4, 5, 6, 8, 10\}$ .



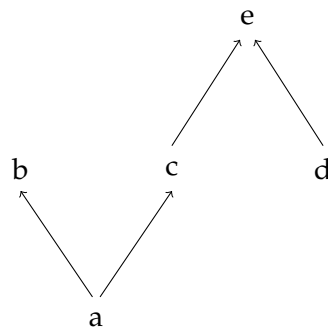
3. Hassediagramm von  $|$  (teilt) in der Menge  $M = \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$ .



### Aufgabe 5.16:

Gegeben ist das folgende Hasse Diagramm:





Geben Sie die zugehörige Ordnungsrelation an.

**Lösung 5.16:**

$M = \{a, b, c, d, e\}$  und  $R = \{(a, b), (a, c), (c, e), (d, e), (a, a), (b, b), (c, c), (d, d)\}$

**Aufgabe 5.17:**

Betrachten Sie das kleine lateinische Alphabeth  $A = \{a, b, \dots, z\}$  das Symbol  $\leq_a$  bezeichne die gewöhnliche Anordnung des Alphabeths. Die Menge der Wörter  $W$  sei die Menge aller endlichen nichtleeren Folgen  $z_1 z_2 z_3 \dots z_n$  von Buchstaben des Alphabeths, also die Menge:

$$W = \{a, aa, aaa, \dots, ab, aba, abaa, \dots, b, ba, \dots, z, \dots, zz, \dots, zzz, \dots\}$$

In der Menge der Wörter definiert man die lexikografische Ordnung  $\leq_{lex}$  (also die Ordnung in der Wörter in einem Lexikon vorkommen:

$$x_1 x_2 x_3 \dots x_n \leq_{lex} z_1 z_2 z_3 \dots z_m$$

genau dann, wenn

$(n \leq m \wedge x_1 = z_1 \wedge x_2 = z_2 \wedge x_3 = z_3 \wedge \dots \wedge x_n = z_n)$  oder (Es gibt ein  $k < n, m$  und  $x_1 = z_1 \wedge x_2 = z_2 \wedge x_3 = z_3 \wedge \dots \wedge x_k = z_k \wedge x_{k+1} \neq z_{k+1} \wedge x_{k+1} \leq_a z_{k+1}$ )

1. Zeigen Sie, dass  $\leq_{lex}$  eine Ordnungsrelation ist.
2. Sei  $A$  die Menge der Wörter, die mit „anna“ anfangen. Geben Sie größte und kleinste Elemente, Suprema und Infima dieser Menge an.

**Aufgabe 5.18:**

Erfolg im Leben misst sich z. B. in Geld oder in Liebe<sup>2</sup>. Ein Erdenbürger kann in jeder dieser Kategorien 0 (nichts), 1 (wenig) oder 2 (viel) haben.

Die Stufen des Erfolgs sind also:

- $(0,0)$  = kein Geld, keine Liebe
- $(1,0)$  = wenig Geld, keine Liebe
- $(0,1)$  = kein Geld, wenig Liebe
- $(0,2)$  = kein Geld, viel Liebe
- ...
- $(2,2)$  = viel Geld, viel Liebe

„erfolgreicher (oder gleich) sein“ bedeutet mehr oder gleich viel Geld zu haben **und** mehr oder gleich viel Liebe zu haben.

Beispiel:  $(2,1)$  ist erfolgreicher als  $(1,1)$  aber  $(1,0)$  ist nicht erfolgreicher als  $(0,1)$

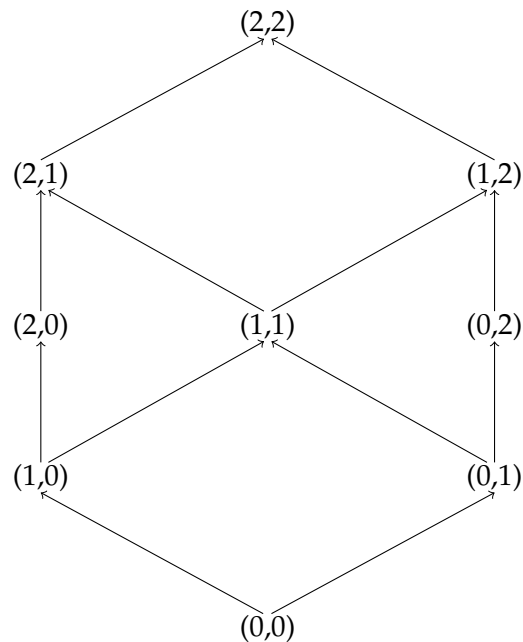
1. Stellen Sie die Relation „ist erfolgreicher als“ als Hasse Diagramm dar.
2. Ermitteln Sie die oberen Grenzen und Suprema für die Mengen:  $\{(0,1), (1,0)\}$ ,  $\{(1,1), (2,0)\}$  und  $\{(0,1), (1,1)\}$
3. Können Sie eine Formel zur Berechnung des Supremums angeben? Benutzen Sie die Funktion  $\max(a,b)$  deren Wert der größere der beiden Zahlen  $a$  und  $b$  ist.

### Lösung 5.18:

1. Hasse Diagramm der Relation „Geld oder Liebe“:

---

<sup>2</sup>„Geld oder Liebe“ war eine Spielshow mit Jürgen von der Lippe. Vom 28. September 1989 bis zum 9. Juni 2001 gab es 90 Folgen.



	$A$	obere Grenzen	Supremum
2.	$\{(0,1), (1,0)\}$	$(1,1), (1,2), (2,1), (2,2)$	$(1,1)$
	$\{(1,1), (2,0)\}$	$(2,1), (2,2)$	$(2,1)$
	$\{(0,1), (1,1)\}$	$(1,1), (1,2), (2,1), (2,2)$	$(1,1)$

3.  $\text{Supremum}\{(a_1, a_2), (b_1, b_2)\} = (\max(a_1, b_1), \max(a_2, b_2)).$

### Aufgabe 5.19:

Beweisen Sie die folgende Aussage:

Gegeben sei eine Ordnungsrelation in einer Menge  $M$  und eine Teilmenge  $A \subseteq M$ . Wenn es ein größtes Element  $g$  in  $A$  gibt, dann sind alle maximalen Elemente gleich diesem  $g$ .

### Lösung 5.19:

Sei  $\sqsubseteq$  eine Ordnungsrelation in  $M$ ,  $A \subseteq M$  eine beliebige Teilmenge von  $A$  und  $g$  ein größtes und  $m$  ein maximales Element von  $A$ . Dann gilt

1.  $g \in A$
2.  $\forall a \in A : a \sqsubseteq g$
3.  $m \in A$

$$4. \forall a \in A : m \sqsubseteq a \Rightarrow m = a$$

Wegen 3 und 2 folgt  $m \sqsubseteq g$ . Deshalb und wegen 1 kann man 4 für  $a = g$  anwenden und erhält  $m = g$ .

## 5.6 Verbände

In dem Kapitel über Mengenlehre haben wir uns mit der Charakterisierung der Teilmengeneigenschaft *subsetq* durch die Vereinigung  $\cup$  und durch den Durchschnitt  $\cap$  beschäftigt. Es wurden die beiden Aussagen bewiesen:

$$A \subseteq B \Leftrightarrow A \cup B = B$$

$$A \subseteq B \Leftrightarrow A \cap B = A$$

Umgekehrt kann man die Teilmengeneigenschaft verwenden um den Durchschnitt und die Vereinigung zu definieren.  $A \cap B$  ist das Infimum der der beiden Elemente  $A, B$  bezüglich der Ordnung  $\subseteq$  und  $A \cup B$  ist das Supremum.

### VERBAND:

Sei  $\sqsubseteq$  eine Ordnung in der festen Menge  $M$ , derart, dass zu je zwei Elementen  $a, b \in M$  das Supremum  $\sup\{a, b\}$  und das Infimum  $\inf\{a, b\}$  existiert. Wir definieren Operationen  $\sqcap$  und  $\sqcup$  durch:

$$a \sqcup b = \sup\{a, b\}$$

$$a \sqcap b = \inf\{a, b\}$$

**Definition 5.6.1**  
Verband

### RECHENGESETZE VERBAND:

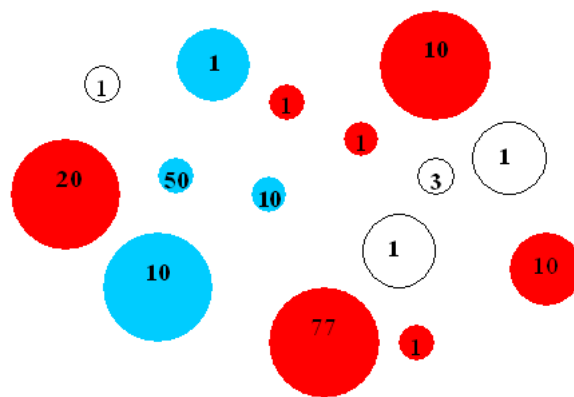
Die in Definition 5.6.1 festgelegten Operation erfüllen folgende Gesetze:

1.  $\forall a \in M : a \sqcap a = a \wedge a \sqcup a = a$  (Idempotenzgesetz)
2.  $\forall a, b \in M : a \sqcup b = b \sqcup a \wedge a \sqcap b = b \sqcap a$  (Kommutativgesetz)
3.  $\forall a, b, c \in M : (a \sqcap b) \sqcap c = a \sqcap (b \sqcap c) \wedge (a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$  (Assoziativgesetz)
4.  $\forall a, b \in M : (a \sqcap b) \sqcup a = a \wedge (a \sqcup b) \sqcap a = a$  (Absorbtionsgesetz)

**Satz 5.6.1**  
Rechengesetze  
Verband

## 5.7 Äquivalenzrelationen

Eines der wichtigsten Prinzipien der Mathematik, wie in jeder Wissenschaft ist die Abstraktion. Das Zusammenfassen von Objekten, die sich in bestimmten Eigenschaften gleichen, aber gleichzeitig das Nichtbeachten von Unterschieden in anderen Eigenschaften. Betrachten Sie folgende Menge von „Münzen“.



Wir können diese Menge unter unterschiedlichen Gesichtspunkten betrachten:

- Größe,
- Farbe,
- Nennwert

sind nur einige Kriterien. Der Abstraktionsvorgang ist nun nichts anderes, als sich ein Merkmal herauszunehmen und alle anderen zu ignorieren. So könnten wir z.B. die Größe herausnehmen und alle anderen Eigenschaften vernachlässigen. Wir betrachten dann zwei Münzen als äquivalent, wenn sie die gleiche Größe haben, andernfalls sind sie nicht äquivalent. Äquivalenzrelationen sind eine Verallgemeinerung dieses Vorgehens. Sie fassen die wesentlichen Eigenschaften von Relationen wie „hat gleiche Farbe“ und „hat gleiche Größe“ zusammen.

**Definition 5.7.1**  
Äquivalenzrelation

**ÄQUIVALENZRELATION:**

Sei  $M$  eine Menge und  $R \subseteq M \times M$  eine Relation in  $M$ .

$R$  heißt Äquivalenzrelation, falls

1.  $R$  ist reflexiv
2.  $R$  ist symmetrisch
3.  $R$  ist transitiv

Äquivalenzrelationen bezeichnet man gerne mit dem Symbol  $\equiv$ . Will man mehrere Äquivalenzrelationen unterscheiden, so kann man das Symbol  $\equiv$  mit einem Index versehen. Etwa  $\equiv_{Farbe}$  oder  $\equiv_{Wert}$ .

Hat man eine Äquivalenzrelation gegeben, kann man die Äquivalenzklassen bilden. Äquivalenzklassen sind die Zusammenfassung der Objekte, die in der betrachteten Eigenschaft übereinstimmen. Die Äquivalenzklassen sind die abstrahierten Objekte. In unserem Beispiel haben wir folgende Äquivalenzklassen:

**Definition 5.7.2**  
Äquivalenzklassen

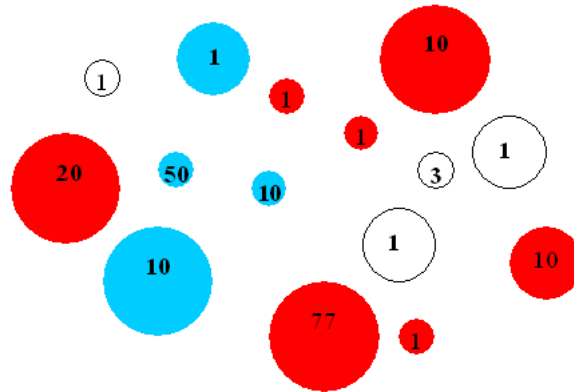
**ÄQUIVALENZKLASSEN:**

Sei  $M$  eine Menge und  $\equiv$  eine Äquivalenzrelation. Für jedes  $x \in M$  ist die Äquivalenzklasse  $[x]$  gegeben durch:

$$[x] = \{y \in M : y \equiv x\}$$

Unter den Äquivalenzklassen von  $\equiv$  versteht man die Elemente der Menge:  $\{[x] : x \in M\}$ .

Das folgende Beispiel zeigt die Äquivalenzklassen, wenn die Unterscheidung nach der Größe erfolgt:



Äquivalenzklassen haben zwei wichtige Eigenschaften: Erstens ergeben Sie zusammengenommen die ganze Menge und zweitens überschneiden sie sich nicht. Mathematisch formulieren wir das in dem folgenden Satz:

#### EIGENSCHAFTEN VON ÄQUIVALENZKLASSEN:

Sei  $M$  eine Menge und  $\equiv$  eine Äquivalenzrelation in  $M$ . Dann gilt für beliebige  $x, y, z \in M$ :

1.  $x \in [x]$
2.  $y \in [x] \Rightarrow x \in [y]$
3.  $(z \in [y] \wedge y \in [x]) \Rightarrow z \in [x]$

**Satz 5.7.1**  
Eigenschaften  
von  
Äquivalenzklassen

#### Beweis:

Die drei Eigenschaften sind nicht anderes als eine Umformulierung der Reflexivität, Symmetrie bzw. der Transitivität der Relation. **q.e.d.** Eine wesentliche Folgerung aus den Eigenschaften der Äquivalenzrelationen ist der folgende Satz:

#### ZERLEGUNG IN ÄQUIVALENZKLASSEN:

Sei  $M$  eine Menge und  $\equiv$  eine Äquivalenzrelation in  $M$ . Die Menge der Äquivalenzklassen  $\{[x] : x \in M\}$  bildet eine Zerlegung der Menge  $M$  in disjunkte Mengen. Das bedeutet:

1. 
$$\bigcup_{x \in M} [x] = M$$
2. 
$$\forall x, y \in M : [x] \cap [y] = \emptyset \vee [x] = [y]$$

**Satz 5.7.2**  
Zerlegung in  
Äquivalenzklassen

**Beweis:**

Die erste Eigenschaft ist einfach zu beweisen, denn alle Äquivalenzklassen sind Teilmengen von  $M$ . Deshalb gilt auch  $\bigcup_{x \in M} [x] \subseteq M$ . Da  $\forall x \in M : x \in [x]$  ist auch umgekehrt  $M \subseteq \bigcup_{x \in M} [x]$ .

Um die zweite Eigenschaft nachzuweisen, sei  $x, y \in M$  mit  $[x] \cap [y] \neq \emptyset$ . Wir müssen dann zeigen, dass  $[x] = [y]$ .

$[x] \subseteq [y]$ : Die Voraussetzung bedeutet, dass es ein  $z \in M$  gibt mit  $z \in [x] \cap [y]$ . Dann ist  $z \in [x]$  und  $z \in [y]$ . Wegen Satz 5.7.1 b gilt  $x \in [z]$  und wegen Satz 5.7.1 c folgt aus  $x \in [z]$  und  $z \in [y]$  die Aussage  $x \in [y]$ . Sei nun  $w \in [x]$  beliebig. Dann folgt wegen Satz 5.7.1 c aus  $w \in [x]$  und  $x \in [y]$  auch  $w \in [y]$ .

Die Inklusion  $[y] \subseteq [x]$  beweist man genauso. **q.e.d.**

**Aufgabe 5.20:**

Gegen Sie mindestens sechs unterschiedliche Beispiele für Äquivalenzrelationen in der obigen Menge von Münzen. Welche Äquivalenzrelation würde man als grösste, welche als feinste bezeichnen.

**Aufgabe 5.21:**

Geben Sie Äquivalenzklassen für mindestens zwei der obigen Äquivalenzrelationen.

**Aufgabe 5.22:**

Können Äquivalenzklassen auch leer sein?

**Aufgabe 5.23:**

Gilt Satz 5.7.1 auch wenn man (b) durch

(b'):  $\forall x, y \in M : \text{Entweder } [x] \cap [y] = \emptyset \text{ oder } [x] = [y]$ .

ersetzt?

**Aufgabe 5.24:**

Geben Sie alle 15 Äquivalenzrelationen in der Menge  $M = \{1, 2, 3, 4\}$  an. Ordnen Sie diese bezüglich der Teilmengenbeziehung.



## 5.8 Restklassen

Wir werden uns in diesem Abschnitt mit speziellen Äquivalenzrelationen beschäftigen, nämlich der Kongruenz modulo  $m \in \mathbb{N}$ . Diese Definition wird im weiteren Verlauf dieser Vorlesung wieder aufgenommen. Stellen Sie also bitte sicher, dass Sie die Sachverhalte dieses Abschnitts verstanden haben.

Wiederholen Sie die Definition der Teilbarkeitsrelation:  $\mid \subseteq \mathbb{Z} \times \mathbb{Z} : a \mid b \Leftrightarrow \exists t \in \mathbb{Z} : a \odot t = b$

### KONGRUENZ MODULO $m$ :

Sei  $m \in \mathbb{N}$  beliebig aber fest. Zwei Zahlen  $a, b \in \mathbb{Z}$  heißen kongruent modulo  $m$ , in Zeichen  $a \equiv_m b$ , genau dann wenn  $m \mid b - a$ .

**Definition 5.8.1**  
Kongruenz modulo  $m$

Natürlich wird durch diese Definition auch eine Relation  $\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$  festgelegt.

### $\equiv_m$ ALS ÄQUIVALENZRELATION:

$\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$  ist eine Äquivalenzrelation.

**Satz 5.8.1**  $\equiv_m$   
als  
Äquivalenzrelation

### Beweis:

Wir müssen die drei Eigenschaften einer Äquivalenzrelation nachrechnen.

1. Reflexivität: Sei  $a \in \mathbb{Z}$ . Dann ist  $a \equiv_m a$ , denn  $m \mid a - a = 0$ , weil  $m * 0 = 0$ .
2. Symmetrie: Seien  $a, b \in \mathbb{Z}$ . Ist  $a \equiv_m b$ , so gibt es ein  $t \in \mathbb{Z}$ , so daß  $m * t = b - a$ . Dann gilt natürlich  $m * (-t) = a - b$ , also  $b \equiv_m a$ .
3. Transitivität: Seien  $a, b, c \in \mathbb{Z}$ . Ist  $a \equiv_m b$  und  $b \equiv_m c$ , dann gibt es  $t_1, t_2 \in \mathbb{Z}$ , so dass  $m * t_1 = b - a$  und  $m * t_2 = c - b$ . Addiert man beide Gleichungen erhält man:  $m * (t_1 + t_2) = (c - b) + (b - a) = c - a$ . Das heißt aber nichts anderes als  $a \equiv_m c$ .

q.e.d.

### RESTKLASSEN:

Die Äquivalenzklassen der Relation  $\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$  heißen Restklassen modulo  $m$ . Für  $a \in \mathbb{Z}$  wird Restklasse  $[a]_m$  geschrieben. Die Menge aller Restklassen modulo  $m$  wird mit  $\mathbb{Z}/m$  bezeichnet.

**Definition 5.8.2**  
Restklassen

**Beispiel 5.8.1** Gerade und Ungerade Zahlen

Die Äquivalenzklassen der Relation  $\equiv_2$  sind als gerade Zahlen und ungerade Zahlen bekannt.

gerade Zahlen  $= [0]_2 = [2]_2 = \{0, 2, 4, 6, 8, 10, 12, \dots, -2, -4, -6, -8, -10, -12, \dots\}$ .

ungerade Zahlen  $= [-1]_2 = [1]_2 = \{1, 3, 5, 7, 9, 11, \dots, -1, -3, -5, -7, -9, -11, \dots\}$ .

**Beispiel 5.8.2** Restklassen mod 10

Die Äquivalenzklassen der Relation  $\equiv_{10}$  sind:

$$\begin{aligned} [0]_{10} &= \{0, 10, 20, 30, \dots, -10, -20, -30, \dots\} \\ [1]_{10} &= \{1, 11, 21, 31, \dots, -9, -19, -29, \dots\} \\ [2]_{10} &= \{2, 12, 22, 32, \dots, -8, -18, -28, \dots\} \\ [3]_{10} &= \{3, 13, 23, 33, \dots, -7, -17, -27, \dots\} \\ [4]_{10} &= \{4, 14, 24, 34, \dots, -6, -16, -26, \dots\} \\ [5]_{10} &= \{5, 15, 25, 35, \dots, -5, -15, -25, \dots\} \\ [6]_{10} &= \{6, 16, 26, 36, \dots, -4, -14, -24, \dots\} \\ [7]_{10} &= \{7, 17, 27, 37, \dots, -3, -13, -23, \dots\} \\ [8]_{10} &= \{8, 18, 28, 38, \dots, -2, -12, -22, \dots\} \\ [9]_{10} &= \{9, 19, 29, 39, \dots, -1, -11, -21, \dots\} \\ [10]_{10} &= [0]_{10} \end{aligned}$$

Den Namen Restklassen erklärt der folgende Satz:

**Satz 5.8.2**  
Charakterisierung  
von Restklassen

**CHARAKTERISIERUNG VON RESTKLASSEN:**

Sei  $m \in \mathbb{N}$  fest, dann liegen zwei Zahlen  $a, b \in \mathbb{Z}$  genau dann in derselben Äquivalenzklasse bezüglich  $\equiv_m$ , wenn  $a$  und  $b$  bei ganzzahliger Division durch  $m$  denselben Rest lassen.

**Aufgabe 5.25:**

Geben Sie die Restklassen zu den Relationen  $\equiv_5$  und  $\equiv_{11}$  an.

## 5.9 Abbildungen

Abbildungen spielen in der Mathematik eine sehr wichtige Rolle. In diesem Kapitel werden die grundlegenden Definitionen und Notationen eingeführt.

Eigentlich ist eine Abbildung ein mathematisches Objekt, das festlegt, wie den Elementen einer Menge, der sog. Urbildmenge, Elemente einer anderen Menge, der sog. Bildmenge, zugeordnet werden. Dabei muss die Zuordnungsvorschrift eindeutig sein, d.h. einem Element des Urbildes darf höchstens ein Element des Bildes zugeordnet sein. Damit ist der Begriff der Abbildung mit zwei Eigenschaften verknüpft:

1. Existenz
2. Eindeutigkeit

Es stellt sich an dieser Stelle die (ein weiteres mal) Frage, wie man Eindeutigkeit mit Quantoren ausdrücken kann, also die Tatsache, dass höchstens ein Element mit gewissen Eigenschaften existiert. Wie Sie wissen, bedeutet der Existenzquantor die Existenz mindestens eines Elements.

Um möglichst genau die Eigenschaft der Eindeutigkeit herauszustellen formulieren wir zunächst die folgende Definition:

**LINKS- (RECHTS)EINDEUTIGKEIT:**

Seien  $M_1, M_2$  beliebige Mengen und  $R \subseteq M_1 \times M_2$  eine beliebige Relation.  $R$  heißt links-(rechts)eindeutig falls

$$\forall x_1, x_2 \in M_1 : \forall y \in M_2 : (x_1, y) \in R \wedge (x_2, y) \in R \Rightarrow x_1 = x_2$$

$$(\forall y_1, y_2 \in M_2 : \forall x \in M_1 : (x, y_1) \in R \wedge (x, y_2) \in R \Rightarrow y_1 = y_2)$$

**Definition 5.9.1**

Links-  
(Rechts)eindeutigkeit

Bemerkung 16: Linkseindeutigkeit kann man folgendermassen interpretieren: Wenn zwei Pfeile bei  $y$  ankommen, dann muss der Ausgangspunkt dieser zwei Pfeile identisch sein, also liegt eigentlich nur ein Pfeil vor. Anders ausgedrückt: Bei jedem  $y \in M_2$  kommt höchstens ein Pfeil an.

Entsprechend bedeutet Rechtseindeutigkeit: Von jedem  $x \in M_1$  geht höchstens ein Pfeil aus.

Wir haben in Definition 5.2.2 den Begriff der inversen Relation eingeführt. Mit ihm können wir den Zusammenhang zwischen Links- und Rechtseindeutigkeit sehr leicht formulieren:

**Satz 5.9.1**  
Zusammenhang  
Links- und Recht-  
seindeutigkeit

**ZUSAMMENHANG LINKS- UND RECHTSEINDEUTIGKEIT:**

Seien  $M_1, M_2$  beliebige Mengen und  $R \subseteq M_1 \times M_2$  eine beliebige Relation.  
 $R$  ist genau dann links-(rechts)eindeutig, wenn  $R^{-1}$  rechts-(links)eindeutig ist.

Als kleine Wiederholung schauen sie sich bitte die Definition 5.2.3 der Verkettung von zwei Relationen an. Wir werden später viel mit dieser Verkettung arbeiten. Bezüglich der Eindeutigkeit verhält sich die Verkettung eigenschaftserhaltend:

**Satz 5.9.2**  
Verkettung und  
Eindeutigkeit

**VERKETTUNG UND EINDEUTIGKEIT:**

Seien  $M_1, M_2, M_3$  beliebige Mengen und  $R_1 \subseteq M_1 \times M_2$  bzw.  $R_2 \subseteq M_2 \times M_3$  beliebige links-(rechts)eindeutige Relationen. Dann ist  $R_1 \circ R_2$  links-(rechts)eindeutig.

**Beweis:**

Wir können uns auf den Beweis mit der Eigenschaft der Linkseindeutigkeit beschränken, weil der Beweis mit der Rechtseindeutigkeit genauso geführt werden kann. (Oder Man wendet Satz 5.9.1 in Verbindung mit Satz 5.2.2 an.) Seien  $M_1, M_2, M_3, R_1$  und  $R_2$  wie im Satz beschrieben gegeben. Wir haben zu zeigen, dass

$$\forall x_1, x_2 \in M_1 \forall z \in M_3 : (x_1, z) \in R_1 \circ R_2 \wedge (x_2, z) \in R_1 \circ R_2 \Rightarrow x_1 = x_2$$

Sei dazu  $x_1, x_2 \in M_1$  und  $z \in M_3$  beliebig gegeben mit:  $(x_1, z) \in R_1 \circ R_2$  und  $(x_2, z) \in R_1 \circ R_2$ . Nach zweimaliger unabhängiger Anwendung der Definition 5.2.3 der Verkettung muss es  $y_1, y_2 \in M_2$  geben, so dass  $(x_1, y_1) \in R_1$   $(y_1, z) \in R_2$  und  $(x_2, y_2) \in R_1$  und  $(y_2, z) \in R_2$ . Da  $R_2$  linkseindeutig ist folgt dass  $y_1 = y_2$  ist. Nun können wir auch die Linkseindeutigkeit der Relation  $R_1$  anwenden um zu schließen, dass  $x_1 = x_2$ . **q.e.d.**

Man kann es nicht oft genug sagen:

Prinzip :  
Eindeutigkeit

**EINDEUTIGKEIT:**

Eine Eindeutigkeitsaussage ist eine Allaussage und keine Existenzaussage.  
Die generelle Struktur einer Eindeutigkeitsaussage für die Eigenschaft  $P$  ist:

$$\forall x_1, x_2 : P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2$$

Neben der Eindeutigkeit spielt Existenz bei der Definition von Abbildungen eine Rolle. Deshalb die Definition

**LINKS- (RECHTS)TOTALITÄT:**

Seien  $M_1, M_2$  beliebige Mengen und  $R \subseteq M_1 \times M_2$  eine beliebige Relation.  $R$  heißt links-(rechts)total falls

$$\forall x \in M_1 : \exists y \in M_2 : (x, y) \in R$$

$$(\forall y \in M_2 : \exists x \in M_1 : (x, y) \in R)$$

**Definition 5.9.2**  
Links-  
(Rechts)totalität

Entsprechend Satz 5.9.1 gilt natürlich auch:

**ZUSAMMENHANG LINKS- UND RECHTSTOTALITÄT:**

Seien  $M_1, M_2$  beliebige Mengen und  $R \subseteq M_1 \times M_2$  eine beliebige Relation.  $R$  ist genau dann links-(rechts)total, wenn  $R^{-1}$  rechts-(links)total ist.

**Satz 5.9.3**  
Zusammenhang  
Links- und  
Rechtstotalität

**VERKETTUNG UND TOTALE RELATIONEN:**

Seien  $M_1, M_2, M_3$  beliebige Mengen und  $R_1 \subseteq M_1 \times M_2$  bzw.  $R_2 \subseteq M_2 \times M_3$  beliebige links-(rechts)totale Relationen. Dann ist  $R_1 \circ R_2$  links-(rechts)total.

**Satz 5.9.4**  
Verkettung und  
totale Relationen

**ABBILDUNG:**

Seien  $M_1, M_2$  beliebige Mengen. Eine Relation  $R$  zwischen  $M_1$  und  $M_2$  (also  $R \subseteq M_1 \times M_2$ ) heißt Abbildung (synonym Funktion) von  $M_1$  nach (in)  $M_2$ , genau dann, wenn  $R$  rechtseindeutig und linkstotal ist.

Mit anderen Worten: Zu jedem  $x \in M$  ein und nur ein („genau ein“)  $y \in M_2$  existiert, sodass  $(x, y) \in R$ .

Mit Quantoren schreibt man dies:

$$1. \forall x \in M_1 \exists y \in M_2 : (x, y) \in R$$

$$2. \forall x \in M_1 \forall y_1, y_2 \in M_2 : (x, y_1) \in R \wedge (x, y_2) \in R \Rightarrow y_1 = y_2$$

**Definition 5.9.3**  
Abbildung

Bemerkung 17: Schreibweisen und Bezeichnungen:

Wenn  $R$  eine Abbildung von  $M_1$  nach  $M_2$  bezeichnet, schreibt man auch  $R : M_1 \rightarrow M_2$ .

Ist  $(x, y) \in R$ , so nennt man  $y$  „das“ Bild von  $x$  und schreibt:

$$y = R(x) \text{ oder } R : x \mapsto y$$

Für Abbildungen verwendet man häufig auch kleine Buchstaben:  $f, g, \dots$

**Definition 5.9.4**  
Definitionsbereich  
und Bild

**DEFINITIONSBEREICH UND BILD:**

Sei  $f : A \rightarrow B$  eine Abbildung von  $M_1$  nach  $M_2$ .  $M_1$  heißt auch Definitionsbereich  $D_f$  der Abbildung  $f$ .  $M_2$  heißt Wertebereich der Abbildung.

Unter dem Bild der Abbildung  $f$  versteht man die Menge aller Bildelemente, also  $B_f = \{y \in M_2 \mid \exists x \in M_1 : y = f(x)\}$ .

**Definition 5.9.5**  
Sur- In und  
Bijektivität

**SUR- IN UND BIJEKTIVITÄT:**

Eine Abbildung  $f : M_1 \rightarrow M_2$  heißt

- surjektiv, wenn  $f$  rechtstotal
- injektiv, wenn  $f$  linkseindeutig
- bijektiv, wenn  $f$  linkseindeutig und rechtstotal

ist.

Kennzeichen von injektiven Abbildungen im Pfeildiagramm: Jedes Element des Wertebereichs  $M_2$  wird von höchstens einem Pfeil getroffen. Gibt es eine injektive Abbildung  $F : M_1 \rightarrow M_2$ , dann hat  $M_2$  mindestens so viele Elemente wie  $M_1$ .

Für injektive Abbildungen wurde in der Mathematik das Unwort eineindeutig geprägt, weil die Abbildung in beide Richtungen eindeutig ist. Manchmal findet man in Fernsehkrimis dieses Unwort in Zusammenhang mit „eineindeutigen Beweisen“, die wohl besonders eindeutig sein sollen. Hier weiß der Autor nicht, wovon er redet.

Kennzeichen von surjektiven Abbildungen im Pfeildiagramm: Jedes Element des Wertebereichs  $M_2$  wird von mindestens einem Pfeil getroffen. Gibt es eine surjektive Abbildung  $F : M_1 \rightarrow M_2$ , dann hat  $M_1$  mindestens so viele Elemente wie  $M_2$ .

Kennzeichen von bijektiven Abbildungen im Pfeildiagramm: Jedes Element des Wertebereichs  $M_2$  wird von genau einem Pfeil getroffen. Gibt es eine bijektive Abbildung  $F : M_1 \rightarrow M_2$ , dann hat  $M_1$  genau so viele Elemente wie  $M_2$ .

Als einfache Folgerung der Sätze 5.9.2 und 5.9.4 ergibt sich:

**VERKETTUNG UND ABBILDUNGSEIGENSCHAFTEN:**

Seien  $M_1, M_2, M_3$  beliebige Mengen und  $R_1 : M_1 \rightarrow M_2$  bzw.  $R_2 : M_2 \rightarrow M_3$  beliebige (surjektive resp. injektive resp. bijektive) Abbildungen. Dann ist  $R_1 \circ R_2 : M_1 \rightarrow M_3$  eine (surjektive resp. injektive resp. bijektive) Abbildung.

**Satz 5.9.5**

Verkettung und Abbildungseigenschaften

Man kann sich fragen, ob die Sur- (In)jektivität der Ursprungsabbildungen auch eine notwendige Bedingung ist, damit die Verkettung sur- (in)jektiv ist. Die Situation wird durch folgenden kleinen Satz geklärt:

**NOTWENDIGE BEDINGUNG FÜR SUR-(IN)JEKTIVITÄT DER VERKETTUNG:**

Seien  $M_1, M_2, M_3$  beliebige Mengen und  $R_1 : M_1 \rightarrow M_2$  bzw.  $R_2 : M_2 \rightarrow M_3$  beliebige Abbildungen. Ist  $R_1 \circ R_2 : M_1 \rightarrow M_3$  eine surjektive (injektive) Abbildung, dann ist  $R_2 (R_1)$  sur-(in)jektiv.

**Satz 5.9.6**

Notwendige Bedingung für Sur-(In)jektivität der Verkettung

Aus der Definition der bijektiven Abbildung in Verbindung mit den Sätzen 5.9.1 und 5.9.3 ergibt sich folgendes Sätzchen:

**BIJEKTIVE ABBILDUNGEN:**

Eine Abbildung  $f : A \rightarrow B$  ist genau dann bijektiv, wenn ihre Umkehrrelation auch eine Abbildung (von B in A) ist.

**Satz 5.9.7**

Bijektive Abbildungen

**Aufgabe 5.26:**

Beweisen Sie Satz 5.9.6.

**Aufgabe 5.27:**

Zeigen Sie durch Beispiele, dass in Satz 5.9.6 nicht auf die Surjektivität von  $R_1$  (Injektivität von  $R_2$ ) geschlossen werden kann.

**Aufgabe 5.28:**

Beweisen Sie Satz 5.9.3.

**Aufgabe 5.29:**

Beweisen Sie Satz 5.9.4.





## Kapitel 6

# Algebraische Strukturen

*“Wer sich keinen Punkt denken kann, der ist einfach zu faul dazu.”*

— *Mathematiklehrer Brenneke in „Eduards Traum“ von Wilhelm Busch*  
(1832 - 1908)

Mathematik nutzt das deduktive Schließen. Ausgehend von mathematischen Begriffsbildungen werden aufgrund von logischen Schlüssen Sätze abgeleitet. Die Anwendung der Mathematik erfolgt dadurch, dass die Realität mit mathematischen Begriffen modelliert werden kann. Die Sätze liefern dann Ergebnisse, die in Aussagen der Realität zurückübersetzt werden können. Eine der häufigsten Anwendungen der Mathematik besteht in der Aufgabe, Lösungen von Gleichungen zu finden. Aufgaben dieser Art entstehen in der Betriebswirtschaftslehre, dem Ingenieurwesen und vielen anderen angewandten Wissenschaften. So führt zum Beispiel die Frage nach dem Nutzen von Outsourcing von Abteilungen in Unternehmen auf das Konzept der internen Leistungsverrechnung. Beschreibt man dieses Problem mit mathematischen Mitteln, stößt man auf ein Gleichungssystem, das es zu lösen gilt.

Wir wollen das Lösen von Gleichungen mit mathematischen Mitteln von Grund auf untersuchen. Dabei muss zunächst beschrieben werden, was überhaupt ein Gleichungssystem ist. Um das Problem mit einer in der Mathematik üblichen Allgemeinheit anpacken zu können, werden wir den Begriff der Verknüpfung einführen. Aus der Schule kennt man die Verknüpfungen Addition und Multiplikation von ganzen, rationalen und reellen Zahlen.

Neben einer Lösungsformel interessieren den Mathematiker natürlich auch Existenz und Eindeutigkeitssätze. Damit führen wir die Untersuchungen, die wir in den vorhergehenden Kapiteln besprochen haben, weiter. Die Frage, wel-

che Voraussetzungen man braucht, um generell gültige Existenz- und Eindeutigkeitssätze für das Lösen von Gleichungen zu erhalten, wird durch die Einführung der algebraischen Struktur der Gruppe beantwortet. Es soll nicht verschwiegen werden, dass dieser Begriff auch viele Motivationen hat, die nicht angesprochen werden. Für uns ist die Gruppe nur ein „Spielzeug“, um den Umgang mit mathematischen Aussagen, insbesondere Existenz und Eindeutigkeit, zu üben.

In diesem Kapitel soll auch das Arbeiten mit Axiomensystemen geübt werden. Als Voraussetzung ist nur zugelassen, was in den Axiomen festgelegt ist oder was schon als Satz bewiesen wurde.

## 6.1 Verknüpfungen

Um den Begriff einer Gleichung mathematisch allgemein formulieren zu können, starten wir mit einer Menge von Objekten, mit denen wir rechnen wollen. Dazu müssen zwei Dinge festliegen:

- Mit welchen Objekten wird gerechnet?
- Was bedeutet rechnen überhaupt?

In der Schule lernt man mit Zahlen zu rechnen. Wir verallgemeinern dies und lassen als Grundmenge beliebige Rechenobjekte zu. Das können Zahlen sein, müssen es aber nicht. Welcher Art diese Objekte sind, ist zunächst einmal egal: Murmeln, Farbplättchen eines Lück-Mathematik-Kastens, Mengen, Relationen, Abbildungen oder Zahlen. Wichtig ist nur, dass wir uns auf eine Menge der möglichen Rechenobjekte festlegen.

Zahlen werden in der Schule addiert, multipliziert, subtrahiert und dividiert. Auch hier geht man von einer allgemeineren Sichtweise aus: Was Rechnen bedeutet, wird völlig offen gelassen, es ist nur wichtig, dass das Ergebnis immer eindeutig festgelegt ist.

**VERKNÜPFUNG:**

Sei  $M$  eine beliebige nichtleere Menge. Eine Verknüpfung  $\circ$  in der Menge  $M$  ist eine Abbildung:

$$\circ : M \times M \rightarrow M$$

Für Verknüpfungen hat sich die Infix Notation eingebürgert. Sind  $x, y \in M$  zwei Elemente des Rechenbereichs  $M$ , dann wird das Verknüpfungsergebnis mit  $x \circ y$  bezeichnet.

Das Paar  $(M, \circ)$  wird algebraische Struktur genannt.

**Definition 6.1.1**  
Verknüpfung

Bemerkung 18:  $x \circ y$  spricht man „x kringel y“.

Eine Verknüpfung liegt also dann vor, wenn je zwei Rechenobjekten immer ein Rechenergebnis zugeordnet wird.

**Beispiel 6.1.1** Sei  $M = \mathbb{N}$ , dann ist die Addition von natürlichen Zahlen eine Verknüpfung in  $\mathbb{N}$ .  $(\mathbb{N}, +)$  ist also eine algebraische Struktur.

**Beispiel 6.1.2** Sei  $M = \mathbb{Z}$ , dann ist die Addition von ganzen Zahlen eine Verknüpfung in  $\mathbb{Z}$ .  $(\mathbb{Z}, +)$  ist also eine zweite algebraische Struktur.

**Beispiel 6.1.3** Sei  $M = \mathbb{N}$ , dann ist die Subtraktion von natürlichen Zahlen keine Verknüpfung in  $\mathbb{N}$ , weil durch die Subtraktion der Bereich der natürlichen Zahlen verlassen wird.

Durch Erweiterung des Rechenbereiches kann jedoch eine algebraische Struktur erzeugt werden:

**Beispiel 6.1.4** Sei  $M = \mathbb{Z}$ , dann ist die Subtraktion von ganzen Zahlen eine Verknüpfung in  $\mathbb{Z}$ .  $(\mathbb{Z}, -)$  ist also eine algebraische Struktur.

Das Verfahren, durch Hinzunehmen von neuen Zahlen einen Zahlenbereich bezüglich einer Verknüpfung abgeschlossen zu machen, ist ein sehr verbreite-

tes. Auf diese Weise entstehen die Brüche (rationalen Zahlen) und die komplexen Zahlen.

Aus dem Rechnen mit Zahlen sind die Kommutativ- und Assoziativgesetze bekannt. Im Kontext der algebraischen Struktur kann man formulieren:

**Definition 6.1.2**  
Kommutativgesetz

**KOMMUTATIVGESETZ:**

Die algebraische Struktur  $(M, \circ)$  heißt kommutativ, falls

$$\forall x, y \in M : x \circ y = y \circ x$$

**Definition 6.1.3**  
Assoziativgesetz

**ASSOZIATIVGESETZ:**

Die algebraische Struktur  $(M, \circ)$  heißt assoziativ, falls

$$\forall x, y, z \in M : (x \circ y) \circ z = x \circ (y \circ z)$$

In assoziativen algebraischen Strukturen spielt Klammersetzung keine Rolle.

**Beispiel 6.1.5** *Assoziative und kommutative algebraische Strukturen*

- $(\mathbb{Z}, +)$  ist kommutativ und assoziativ.
- $(\mathbb{Z}, *)$  ist kommutativ und assoziativ.
- $(\mathbb{Z}, -)$  ist nicht kommutativ und nicht assoziativ.
- $(\mathbb{Q} \setminus \{0\}, /)$  ist nicht kommutativ und nicht assoziativ.

Verknüpfungstabellen können genutzt werden, um eine algebraische Struktur zu beschreiben.

**Beispiel 6.1.6** Betrachten wir die Menge  $M$  aller Bijektionen  $R : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ . Die Hintereinanderausführung ist eine Verknüpfung in dieser Menge. Diese Menge enthält die folgenden Elemente, die jeweils durch eine Wertetabelle festgelegt sind:

$R_1$	1	2	3
	2	1	3

$R_2$	1	2	3
	1	3	2

$R_3$	1	2	3
	3	1	2

$R_4$	1	2	3
	2	3	1

$R_5$	1	2	3
	1	2	3

$R_6$	1	2	3
	3	2	1

Damit ergibt sich für die Verkettung folgende Verknüpfungstafel

$\circ$	$R_1$	$R_2$	$R_3$	$R_4$	$R_5$	$R_6$
$R_1$	$R_5$	$R_3$	$R_2$	$R_6$	$R_1$	$R_4$
$R_2$	$R_4$	$R_5$	$R_6$	$R_1$	$R_2$	$R_3$
$R_3$	$R_6$	$R_1$	$R_4$	$R_5$	$R_3$	$R_2$
$R_4$	$R_2$	$R_6$	$R_5$	$R_3$	$R_4$	$R_1$
$R_5$	$R_1$	$R_2$	$R_3$	$R_4$	$R_5$	$R_6$
$R_6$	$R_3$	$R_4$	$R_1$	$R_2$	$R_6$	$R_5$

#### KOMMUTATIVGESETZ UND VERKNÜPFUNGSTAFEL:

Eine algebraische Struktur ist genau dann kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch an der Diagonalen ist.

Prinzip :  
Kommutativgesetz  
und Ver-  
knüpfungstafel

Leider gibt es keine einfache Methode, ein Assoziativgesetz an der Verknüpfungstafel zu erkennen.

Wenn wir von dem Lösen einer Gleichung in einer algebraischen Struktur reden, gehen wir davon aus, dass wir bei gegebenen  $a, b \in M$  ein  $x \in M$  suchen, so dass

$$a \circ x = b$$

oder je nach Aufgabenstellung

$$x \circ a = b$$

Vorgegeben sind also das Ergebnis und ein Operand und gesucht ist der zweite Operand.

Bei algebraischen Strukturen, in denen kein Kommutativgesetz gilt, muss man zwischen dem Lösen einer Gleichung mit der Unbekannten rechts ( $a \circ x = b$ ) und einer Gleichung mit der Unbekannten links unterscheiden.

**Definition 6.1.4**  
Existenzsatz

**EXISTENZSATZ:**

Sei  $(M, \circ)$  eine algebraische Struktur. Wir sagen, dass ein Existenzsatz für das Lösen von Gleichungen gilt, falls

$$\forall a, b \in M : \exists x \in M : a \circ x = b$$

$$(\forall a, b \in M : \exists x \in M : x \circ a = b)$$

**Definition 6.1.5**  
Eindeutigkeitssatz

**EINDEUTIGKEITSSATZ:**

Sei  $(M, \circ)$  eine algebraische Struktur. Wir sagen, dass ein Eindeutigkeitssatz für das Lösen von Gleichungen gilt, falls

$$\forall a, b \in M : \forall x_1, x_2 \in M : a \circ x_1 = b \wedge a \circ x_2 = b \Rightarrow x_1 = x_2$$

$$(\forall a, b \in M : \forall x_1, x_2 \in M : x_1 \circ a = b \wedge x_2 \circ a = b \Rightarrow x_1 = x_2)$$

**Beispiel 6.1.7** In den algebraischen Strukturen aus den Beispielen gelten folgende Sätze:

- $((N), +)$  erfüllt den Eindeutigkeitssatz, nicht aber den Existenzsatz
- $((Z), +)$  erfüllt den Eindeutigkeitssatz und den Existenzsatz
- $((N), *)$  erfüllt den Eindeutigkeitssatz, nicht aber den Existenzsatz
- $((Z), *)$  erfüllt weder Eindeutigkeitssatz noch den Existenzsatz
- $((Q)_+, *)$  erfüllt sowohl den Eindeutigkeitssatz als den Existenzsatz
- $((Q)_+, /)$  erfüllt sowohl den Eindeutigkeitssatz als den Existenzsatz

Wenn eine algebraische Struktur durch eine Verknüpfungstafel gegeben ist, kann man die Existenz- und Eindeutigkeitssätze leicht erkennen:

**EXISTENZSATZ UND VERKNÜPFUNGSTAFEL:**

Sei  $(M, \circ)$  eine algebraische Struktur.

Der Existenzsatz

$$\forall a, b \in M : \exists x \in M : a \circ x = b$$

ist genau richtig, wenn jedes Element aus  $M$  in jeder Zeile der Verknüpfungstafel mindestens einmal vorkommt.

Der Existenzsatz

$$\forall a, b \in M : \exists x \in M : x \circ a = b$$

ist genau richtig, wenn jedes Element aus  $M$  in jeder Spalte der Verknüpfungstafel mindestens einmal vorkommt.

Prinzip :  
Existenzsatz und  
Ver-  
knüpfungstafel

In der verbalen Formulierung ist der Existenzquantor in dem Verb „vorkommt“ versteckt. Auch lässt die verbale Formulierung auf den ersten Blick kaum vermuten, dass in der Aussage drei Variablen benötigt werden.

**EINDEUTIGKEITSSATZ UND VERKNÜPFUNGSTAFEL:**

Sei  $(M, \circ)$  eine algebraische Struktur.

Der Eindeutigkeitssatz

$$\forall a, b \in M : \forall x_1, x_2 \in M : a \circ x_1 = b \wedge a \circ x_2 = b \Rightarrow x_1 = x_2$$

ist genau richtig, wenn jedes Element aus  $M$  in jeder Zeile der Verknüpfungstafel höchstens einmal vorkommt.

Der Eindeutigkeitssatz

$$\forall a, b \in M : \forall x_1, x_2 \in M : x_1 \circ a = b \wedge x_2 \circ a = b \Rightarrow x_1 = x_2$$

ist genau richtig, wenn jedes Element aus  $M$  in jeder Spalte der Verknüpfungstafel höchstens einmal vorkommt.

Prinzip :  
Eindeutigkeitssatz  
und Ver-  
knüpfungstafel

Kommt in einer Verknüpfungstafel ein Element in einer Zeile nicht vor, so muss ein anderes doppelt vorkommen, weil es genauso viele Spalten wie Elemente gibt. Aus demselben Grund muss auch ein Element fehlen, wenn ein anderes Element doppelt ist. Damit haben wir folgenden Satz bewiesen:

**EXISTENZ- UND EINDEUTIGKEITSSÄTZE IN ENDLICHEN ALGEBRAISCHEN STRUKTUREN:**

Sei  $(M, \circ)$  eine endliche algebraische Struktur. Dann sind gleichwertig

$$\forall a, b \in M : \exists x \in M : a \circ x = b$$

und

$$\forall a, b \in M : \forall x_1, x_2 \in M : a \circ x_1 = b \wedge a \circ x_2 = b \Rightarrow x_1 = x_2$$

**Satz 6.1.1**  
Existenz- und  
Eindeutig-  
keitssätze in  
endlichen  
Algebraischen  
Strukturen

Entsprechendes gilt, wenn die Unbekannte von links verknüpft wird.

**Aufgabe 6.1:**

Ist  $(\mathbb{Z}, \max)$  eine algebraische Struktur? Wenn ja, welche Eigenschaften erfüllt sie?

**Aufgabe 6.2:**

Ist  $(\mathbb{Q}, \text{mittelwert})$  eine algebraische Struktur? Wenn ja, welche Eigenschaften erfüllt sie?

**Aufgabe 6.3:**

Erfüllt die Menge der Bijektionen von  $\{1, 2, 3\}$  mit der Verkettung einen Existenz- und Eindeutigkeitssatz?

**Aufgabe 6.4:**

Geben Sie durch Angabe einer Verknüpfungstafel ein Beispiel für eine algebraische Struktur an, für die

$$\forall a, b \in M : \exists x \in M : a \circ x = b$$

wahr ist, aber

$$\forall a, b \in M : \exists x \in M : x \circ a = b$$

falsch.

**Aufgabe 6.5:**

Gegeben ist eine unvollständige Verknüpfungstafel. Ergänzen Sie die Verknüpfungstafel so, dass sowohl Existenz als auch der Eindeutigkeitssätze für die Zeilen und die Spalten gelten.



	a	b	c	d	e	f
a	e	c		f	a	d
b	d				b	
c				e		
d		f			d	a
e	a		c		e	f
f	c	d		b	f	

## 6.2 Restklassenoperationen

In Abschnitt 5.8.2 wurden die Restklassen eingeführt. Nun sollen die Restklassen als Rechenobjekte erschlossen werden. Das verwendete Konstruktionsprinzip ist ein sehr typisches Beispiel für die Thematik der Abstraktion. Abstraktionen machen nur dann Sinn, wenn die „Beziehungen“ unter den Objekten zu „Beziehungen“ zwischen den Äquivalenzklassen werden.

### RESTKLASSENADDITION:

Sei  $m \in \mathbb{N}$  ein fester Modulus. Für beliebige  $a, b \in \mathbb{Z}$  definieren wir:

$$[a]_m \oplus [b]_m = [a + b]_m$$

**Definition 6.2.1**  
Restklassenaddition

Es ist klar, dass die Restklassen, die addiert werden, denselben Modulus haben müssen. Andere Arten von Restklassenaddition sind nicht definiert.

Diese Definition hat eine Hürde: die Laufvariablen  $a$  und  $b$  durchlaufen eine unendliche Menge. Es gibt aber nur endlich viele Restklassen, die zu addieren sind. Für jedes Paar von Restklassen gibt es durch die Definition 6.2.1 unendlich viele Festlegungen für das Ergebnis. Damit wir eine Verknüpfung festlegen, müssen wir uns nun noch überlegen, dass alle diese Festlegungen dasselbe Ergebnis -im Sinne einer Restklasse - liefern. Man nennt diese Eigenschaft „Unabhängigkeit vom Repräsentanten“.

### UNABHÄNGIGKEIT VOM REPRÄSENTANTEN:

Legt man in einer Definition einer Eigenschaft von Äquivalenzklassen diese Eigenschaft durch den Rückgriff auf einen Repräsentanten fest, so muss man die Unabhängigkeit von diesem Repräsentanten beweisen.

Prinzip :  
Unabhängigkeit  
vom  
Repräsentanten

**Satz 6.2.1**

Restklassenaddition

**RESTKLASSENADDITION:**

Sei  $m \in \mathbb{N}$  ein fester Modulus. In der Menge  $\mathbb{Z}/m$  der Restklassen modulo  $m$  ist  $\oplus$  eine Verknüpfung. M.a.W.  $(\mathbb{Z}/m, \oplus)$  ist eine algebraische Struktur.

**Beweis:**

Um die Unabhängigkeit von den Repräsentanten zu beweisen, seien zwei ganze Zahlen  $a, a' \in \mathbb{Z}$  gegeben, die dieselbe Restklasse repräsentieren, also  $[a]_m = [a']_m$ . Ferner seien die Zahlen  $b, b' \in \mathbb{Z}$  so, dass  $[b]_m = [b']_m$ . Wir müssen beweisen, dass  $[a + b]_m = [a' + b']_m$  ist. Nach der Voraussetzung gibt es ganze Zahlen  $q_1, q_2 \in \mathbb{Z}$ , so dass  $a - a' = q_1 * m$  und  $b - b' = q_2 * m$ . Dann gilt:

$$a + b - (a' + b') = a - a' + (b - b') = q_1 * m + q_2 * m = (q_1 + q_2) * m$$

**q.e.d.****Beispiel 6.2.1** *Rechnen mit Vorteil*

Bei der Restklassenaddition hilft die geschickte Wahl eines Repräsentanten Berechnungen einfacher zu gestalten:

- $[683]_2 \oplus [281]_2 = [1]_2 \oplus [1]_2 = [0]_2$
- $[34]_{12} \oplus [17]_{12} = [-2]_{12} \oplus [5]_{12} = [3]_{12}$
- $[52]_{18} \oplus [52]_{18} = [-2]_{18} \oplus [-2]_{18} = [-4]_{18} = [14]_{18}$

Bemerkung 19: Wiederholtes Addieren schreibt man auch als Multiplikation mit dem Wiederholungsfaktor  $n \in \mathbb{N}$ :

$$\underbrace{[a]_m \oplus [a]_m \oplus \dots \oplus [a]_m}_{n\text{-mal}} = n * [a]_m$$

Um das wiederholte Addieren vereinfacht berechnen zu können, kann man feststellen:

$$n * [a]_m = [n * a]_m$$

**Beispiel 6.2.2**

- $13 * [57]_{12} = 13 * [-3]_{12} = [13 * (-3)]_{12} = [-39]_{12} = [9]_{12}$

Entsprechend der Restklassenaddition können wir auch die Multiplikation für Restklassen definieren.

**RESTKLASSENMULTIPLIKATION:**

Sei  $m \in \mathbb{N}$  ein fester Modulus. Für beliebige  $a, b \in \mathbb{Z}$  definieren wir:

$$[a]_m \otimes [b]_m = [a * b]_m$$

**Definition 6.2.2**  
Restklassenmultiplikation

**RESTKLASSEN- MULTIPLIKATION:**

Sei  $m \in \mathbb{N}$  ein fester Modulus. In der Menge  $\mathbb{Z}/m$  der Restklassen modulo  $m$  ist  $\otimes$  eine Verknüpfung. M.a.W.  $(\mathbb{Z}/m, \otimes)$  ist eine algebraische Struktur.

**Satz 6.2.2**  
Restklassen-  
multiplikation

**Beweis:**

Um die Unabhängigkeit von den Repräsentanten zu beweisen, seien zwei ganze Zahlen  $a, a' \in \mathbb{Z}$  gegeben, die dieselbe Restklasse repräsentieren, also  $[a]_m = [a']_m$ . Ferner seien die Zahlen  $b, b' \in \mathbb{Z}$  so, dass  $[b]_m = [b']_m$ . Wir müssen beweisen, dass  $[a * b]_m = [a' * b']_m$  ist. Nach der Voraussetzung gibt es ganze Zahlen  $q_1, q_2 \in \mathbb{Z}$ , so dass  $a - a' = q_1 * m$  und  $b - b' = q_2 * m$ . Dann gilt:

$$\begin{aligned} a * b - (a' * b') &= a * b - a' * b + a' * b - a' * b' = (a - a') * b + a' * (b - b') = \\ &= q_1 * m * b + a' * q_2 * m = (q_1 * b + a' * q_2) * m \end{aligned}$$

**q.e.d.**

**Beispiel 6.2.3** Rechnen mit Vorteil

Auch bei der Restklassenmultiplikation hilft die geschickte Wahl eines Repräsentanten Berechnungen zu vereinfachen:

- $[68]_{13} \otimes [28]_{13} = [3]_{13} \otimes [2]_{13} = [6]_{13}$
- $[34]_{12} \otimes [17]_{12} = [-2]_{12} \otimes [5]_{12} = [-10]_{12} = [2]_{12}$
- $[52]_{18} \otimes [52]_{18} = [-2]_{18} \otimes [-2]_{18} = [4]_{18}$

Bemerkung 20: Wiederholtes Multiplizieren schreibt man auch als Potenz mit dem Exponenten  $n \in \mathbb{N}$ :

$$\underbrace{[a]_m \otimes [a]_m \otimes \dots \otimes [a]_m}_{n\text{-mal}} = [a]_m^n$$

Um das wiederholte Multiplizieren vereinfacht berechnen zu können, kann man

feststellen:

$$[a]_m^n = [a^n]_m$$

**Beispiel 6.2.4** *Rechenbeispiel Multiplikation:*

$$[57]_{12} \otimes [57]_{12} \otimes [57]_{12} = [-3]_{12} \otimes [-3]_{12} \otimes [-3]_{12} = [(-3)]_{12}^3 = [(-3)^3]_{12} = [27]_{12}$$

Wenn die Unabhängigkeit vom Repräsentanten gezeigt ist, lassen sich sehr leicht Gesetze, die in den ganzen Zahlen gelten, auf die Restklassen übertragen:

**RECHENGESETZE RESTKLASSEN:**

Sei  $m \in \mathbb{Z}$  ein fester Modulus. Und  $a, b, c \in \mathbb{Z}$  beliebig. Dann gilt

- $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$
- $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$
- $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$
- $([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$

**Satz 6.2.3**  
Rechengesetze  
Restklassen

**Aufgabe 6.6:**

Erstellen Sie eine Verknüpfungstafel für  $((\mathbb{Z})/6, \oplus)$ . Gelten Existenz und Eindeutigkeitssätze?

**Aufgabe 6.7:**

Erstellen Sie eine Verknüpfungstafel für  $((\mathbb{Z})/7, \oplus)$ . Gelten Existenz und Eindeutigkeitssätze?

**Aufgabe 6.8:**

Zeigen Sie, dass Restklassenpotenzieren nicht unabhängig vom Repräsentanten definiert werden kann. M.a.W.

$$[a]_m^{[b]_m} = [a^b]_m$$

ist keine sinnvolle Definition.

**Aufgabe 6.9:**

Berechnen Sie folgende Restklassenausdrücke:

- $[57]_{13} \otimes [38]_{13}$
- $[23016]_{256} \otimes [1024]_{256}$
- $[26]_{57} \otimes [58]_{57}$
- $[58]_{57}^{12}$
- $[26]_{57} \otimes [58]_{57}$

**Aufgabe 6.10:**

- $[4]_{12}^2$
- $[10]_{15}^2$
- $[6]_{12}^2$
- $[10]_{12} \otimes [6]_{12}$
- $[9]_{15} \otimes [10]_{15}$
- $[5]_{12}^2$
- $[4]_{15}^2$
- $[8]_{15} \otimes [2]_{15}$

**Aufgabe 6.11:**

Erstellen Sie eine Verknüpfungstafel für  $((\mathbb{Z})/6, \otimes)$ . Welche der folgenden Gleichungen sind lösbar? Sind die Lösungen eindeutig?

- $[3]_6 \otimes [x]_6 = [2]_6$
- $[5]_6 \otimes [x]_6 = [1]_6$
- $[5]_6 \otimes [x]_6 = [3]_6$
- $[4]_6 \otimes [x]_6 = [1]_6$

- $[4]_6 \otimes [x]_6 = [2]_6$
- $[4]_6 \otimes [x]_6 = [3]_6$

**Aufgabe 6.12:**

Erstellen Sie eine Verknüpfungstafel für  $((\mathbb{Z})/6, \otimes)$ . Wenn Sie die  $[0]_6$  aus der Grundmenge herausnehmen, gelten dann die Existenz und Eindeutigkeitssätze?

**6.3 Gruppen**

Verweis auf Quelle: [theory.gsi.de/~vanhees/faq/dieder/node4.html](http://theory.gsi.de/~vanhees/faq/dieder/node4.html)

**GRUPPE:**

Eine algebraische Struktur  $(G, \circ)$  heißt Gruppe, wenn gilt:

1.  $(a \circ b) \circ c = a \circ (b \circ c)$  (Assoziativgesetz)
2. Es gibt ein  $e \in G$  (neutrales Element von  $G$ ) mit folgenden Eigenschaften:
  - (a)  $e \circ a = a$  für alle  $a \in G$ , (linksneutrales Element)
  - (b) Zu jedem  $a \in G$  gibt es ein  $a' \in G$  mit  $a' \circ a = e$ .

**Definition 6.3.1**  
Gruppe

Manche Mathematiker (und auch viele Physiker) stellen an eine Gruppe nicht nur diese Forderungen, sondern auch die Existenz eines rechtsneutralen Elementes und eines rechtsinversen Elementes, die den zugehörigen linksneutralen beziehungsweise linksinversen gleichen, also ein  $e$ , so dass  $e \circ a = a \circ e = a$  und nennen  $e$  dann einfach neutrales Element.

Im Folgenden werden wir jedoch erkennen, dass unsere Forderungen vollkommen ausreichen und wir die soeben angesprochenen weiteren Forderungen aus unseren bisherigen ableiten können.

Bemerkung 21: Die Eigenschaft 2 der Gruppensdefinition kann man leicht an der Verknüpfungstafel erkennen:

- Zunächst prüft man, ob es eine Zeile gibt, in die genau die Überschrift

enthält (also die Elemente in derselben Reihenfolge).

- Dann prüft man, ob dieses Element in jeder Spalte vorkommt.

**Beispiel 6.3.1** Gruppe der Bijektionen

Anhand der Gruppentafel kann man erkennen, dass die Menge der Bijektionen der Menge  $\{1, 2, 3\}$  die Forderungen der Definition 6.3.1 erfüllt. Das Assoziativgesetz für die Verkettung von Relationen wurde in Satz 5.2.1 bewiesen. Damit ist die Menge der Bijektionen der Menge  $\{1, 2, 3\}$  eine Gruppe.

Bemerkung 22: Wir werden in dieser Arbeit manchmal von den vier Gruppenaxiomen sprechen; dabei sehen wir die Abgeschlossenheit der Abbildung  $\circ$  bezüglich  $G$  als unser erstes Axiom, die Erfüllung des Assoziativgesetzes als zweites, die Existenz eines linksneutralen Elementes als drittes Axiom und die Existenz eines linksinversen als viertes Axiom an.

Bemerkung 23: Im Folgenden werden wir, solange keine Missverständnisse zu befürchten sind, für eine Gruppe  $(G, \circ)$  nur  $G$  schreiben.

**ABELSCHE GRUPPE:**

Ist  $G$  eine Gruppe und gilt ferner noch das Kommutativgesetz ( $a \circ b = b \circ a$  für alle  $a, b \in G$ ), so heißt  $G$  abelsche Gruppe. Anstatt von „ $\circ$ “ verwendet man dann meist „ $+$ “.

**Definition 6.3.2**  
abelsche Gruppe

Ist  $G$  abelsch, so verwendet man neben „ $\circ$ “ oft auch andere Symbole, wie zum Beispiel „ $+$ “ oder „ $\oplus$ “.

- Beispiel 6.3.2**
1.  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  sind abelsche Gruppen (neutrales Element der Addition ist 0, inverses Element zu  $a$  ist  $-a$ ),  $(\mathbb{N}, +)$  aber nicht, da es in  $\mathbb{N}$  keine inversen Elemente bezüglich der Addition in  $\mathbb{N}$  gibt.
  2.  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{C} \setminus \{0\}, \cdot)$  sind abelsche Gruppen (mit 1 als neutralem Element und  $\frac{1}{a}$  als inverse Element zu  $a$ ).
  3.  $(\{0\}, +)$  und  $(\{1\}, \cdot)$  sind (abelsche) Gruppen.

Bei Verknüpfungen auf „kleinen“ Mengen (wie etwa  $(\{0, 1, 2\}, \oplus)$ , wobei  $\oplus$  in diesem Fall der Addition modulo 3 entsprechen soll) erstellt man häufig Verknüpfungstafeln:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Diese Verknüpfungstafel verrät uns folgendes: 0, 1, 2 ist bezüglich  $\oplus$  abgeschlossen. 0 ist das neutrale Element, 1 das inverse Element zu 2, 2 das inverse Element zu 1 und 0 das inverse Element zu sich selbst.

Die Tatsache, dass die Verknüpfungstafel spiegelsymmetrisch zu ihrer Hauptdiagonalen ist, bedeutet nichts weiteres als  $a \circ b = b \circ a$  für alle  $a, b \in \{0, 1, 2\}$ , also dass das Kommutativgesetz gilt.

**Beispiel 6.3.3** Sei  $m \in \mathbb{Z}$  ein fester Modulus. Dann ist  $(\mathbb{Z}/m, \oplus)$  eine Gruppe. Das Assoziativgesetz „erbt“ man vom Assoziativgesetz der ganzen Zahlen, denn man rechnet:

$$\begin{aligned} ([a]_m \oplus [b]_m) \oplus [c]_m &= [a + b]_m \oplus [c]_m = [(a + b) + c]_m \\ &= [a + (b + c)]_m = [a]_m \oplus [b + c]_m = [a]_m \oplus ([b]_m \oplus [c]_m). \end{aligned}$$

Das neutrale Element ist  $[0]_m$  und das inverse Element zu einer Restklasse  $[a]_m$  ist die Restklasse  $[-a]_m$ .

Unmittelbar aus der Definition folgen für eine Gruppe  $G$  die Eigenschaften:

#### ELEMENTARE GRUPPENEIGENSCHAFTEN:

Sei  $(G, \circ)$  eine Gruppe

1. Sei  $e \in G$  linksneutrales Element und  $a, a' \in G$ , so dass  $a' \circ a = e$ . Dann gilt auch  $a \circ a' = e$ . Man nennt  $a'$  dann nur noch ein inverses Element zu  $a$ .
2. Sei  $e \in G$  linksneutrales Element. Dann gilt:  $a \circ e = a$  für alle  $a \in G$  und man nennt  $e$  dann ein neutrales Element.
3. Es gibt genau ein neutrales Element  $e \in G$ .
4. Zu jedem  $a \in G$  gibt es genau ein inverses Element  $a' \in G$  (oft mit  $a^{-1}$  bezeichnet).
5.  $(a^{-1})^{-1} = a$ .
6.  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ .

**Satz 6.3.1**  
elementare Gruppeneigenschaften



**Beweis:**

Zu 1.: Wählen wir  $a''$  mit  $a'' \circ a' = e$ . Dann gilt:  $a \circ a' = e \circ a \circ a' = a'' \circ a' \circ a \circ a' = a'' \circ e \circ a' = a'' \circ a' = e$

Zu 2.:  $a \circ e = a \circ (a' \circ a) = (a \circ a') \circ a = e \circ a = a$ .

Zu 3.: Wir nehmen an, es gäbe zwei neutrale Elemente von  $G$  ( $e, e^* \in G$ ). Dann ist jedoch  $e^* = e \circ e^* = e$ . Die beiden neutralen Elemente sind also zwangsläufig gleich.

Zu 4.: Wir nehmen an, es gäbe ein zweites inverses Element  $a^*$  neben  $a'$  zu  $a$  in  $G$ . Dann muss jedoch  $a^* = a'$  sein:  $a^* = a^* \circ e = a^* \circ (a \circ a') = (a^* \circ a) \circ a' = e \circ a' = a'$ .

Zu 5.: Es gilt  $(a^{-1})^{-1} \circ a^{-1} = e$ . Es gilt aber auch  $a \circ a^{-1} = e$ . Zu  $a^{-1}$  gibt es jedoch nur ein inverses Element ( $\leftarrow$  vierte Eigenschaft von Gruppen). Also ist  $(a^{-1})^{-1} = a$ .

Zu 6.: Es gilt  $(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ e \circ b = e$ . Somit ist  $(b^{-1} \circ a^{-1})$  das inverse Element zu  $(a \circ b)$ . Also ist  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ . **q.e.d.**

**CHARAKTERISIERUNG GRUPPE:**

Eine algebraische Struktur  $(G, \circ)$  ist genau dann eine Gruppe, wenn

1.  $(a \circ b) \circ c = a \circ (b \circ c)$  für alle  $a, b, c \in G$ . (Assoziativität)
2. Gleichungsvariante:
  - (a) die Gleichung  $a \circ c = b$  für jedes  $a, b \in G$  mit einem Element von  $G$  ( $c$ ) lösbar ist.
  - (b) die Gleichung  $d \circ a = b$  für jedes  $a, b \in G$  mit einem Element von  $G$  ( $d$ ) lösbar ist.

**Satz 6.3.2**  
Charakterisierung  
Gruppe

**Beweis:**

„ $\Rightarrow$ “

Sei  $G$  eine Gruppe. Dann ist  $G$  assoziativ. (1) gilt also. Zu zeigen ist also nur (2 Gleichungsvariante a) und (2 Gleichungsvariante b). Für (2 Gleichungsvariante a) setzen wir  $c = a^{-1} \circ b$ ; dann ist  $a \circ c = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$ . Für

(2 Gleichungsvariante b) setzen wir  $d = b \circ a^{-1}$ ; dann ist  $d \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$ .

„ $\Leftarrow$ “

Für  $G$  gelte also (1) und (2 Gleichungsvariante). Zu zeigen ist, dass  $G$  eine Gruppe ist, also dass  $G$  die Definition 1 erfüllt. (1) gilt zweifelsohne. Es bleibt also (2) zu zeigen. Wir wählen uns nun ein  $a_0$  ( $G$  darf also nicht leer sein). Dann gibt es ein  $e \in G$ , so dass die Gleichung  $e \circ a_0 = a_0$  erfüllt ist. Nun wählen wir uns ein beliebiges  $a \in G$  und dazu ein  $c$ , so dass  $a_0 \circ c = a$ . Dann ist  $e \circ a = e \circ a_0 \circ c = a_0 \circ c = a$ .

Nun beweisen wir (2b). Laut (2 Gleichungsvariante b) lässt sich zu jeder Gleichung  $d \circ a = b$  für zwei vorgegebene  $a, b$  ein  $d$  finden, so dass die Gleichung  $d \circ a = b$  erfüllt ist. Insbesondere lässt sich ein  $d$  zur Gleichung  $d \circ a = e$  finden (da ja  $e \in G$ ). Dieses  $d$  ist damit das verlangte linksinverse Element zu  $a$ . **q.e.d.**

#### EINDEUTIGKEIT DER LÖSBARKEIT VON GLEICHUNGEN:

Sei  $(G, \circ)$  eine beliebige Gruppe. Dann gilt:

1. Es gibt für jedes  $a, b \in G$  höchstens eine Lösung  $c \in G$  der Gleichung  $a \circ c = b$
2. Es gibt für jedes  $a, b \in G$  höchstens eine Lösung  $c \in G$  der Gleichung  $c \circ a = b$

**Satz 6.3.3**  
Eindeutigkeit der  
Lösbarkeit von  
Gleichungen

#### Beweis:

Im Folgenden werden wir uns darauf beschränken, dies für die erste Gleichung zu zeigen.

Gäbe es nun ein  $c_1$  und ein  $c_2$ , so dass 1 für  $c_1$  und  $c_2$  erfüllt ist, so haben wir  $a \circ c_1 = b$  und  $a \circ c_2 = b$ , also  $a \circ c_1 = a \circ c_2$ . Wir können uns nun ein inverses Element  $d$  zu  $a$  suchen (wie oben) und die Gleichung mit diesem von links durchmultiplizieren, womit wir bei  $c_1 = c_2$  angelangt sind: Die Gleichung hat also höchstens eine Lösung. **q.e.d.**

Bemerkung 24: Aus dem Satz 6.3.2 aber wissen wir bereits, dass jede Gleichung mindestens eine Lösung besitzt. Die Gleichung muss also genau eine Lösung haben.

Beim Beweis des vorhergehenden Satzes haben wir gesehen, welche Vorteile uns die bewusste Minimierung unserer Forderungen einbringt. Hätten wir zum

Beispiel nun auch noch die Existenz rechtsneutraler und rechtsinverser Elemente gefordert, so hätten wir zwar immer noch die gleiche Struktur, nämlich eine Gruppe, mit der wir uns befassen, jedoch müssten wir für manche Sätze, wie zum Beispiel diesen Satz, viel mehr beweisen.

Die Tatsache, dass  $(\mathbb{N}_0, +)$  keine Gruppe darstellt, spiegelt sich zum Beispiel in der Tatsache, dass kein  $x \in \mathbb{N}_0$ , welches die Gleichung  $1 + x = 0$  erfüllt, wider. Dies ist natürlich nichts anderes als das von uns schon angesprochene Fehlen inverser Elemente bezüglich der Addition in  $\mathbb{N}_0$ . Um jedoch jede Gleichung, die uns begegnen könnte, lösen zu können, haben wir unseren „Zahlenbegriff“ immer wieder erweitert: Von  $\mathbb{N}$  gelangten wir zunächst nach  $\mathbb{Q}^+$  (Multiplikation) und dann zu  $\mathbb{Z}$  (Addition).

#### ORDNUNG EINER GRUPPE:

Unter der Ordnung einer Gruppe versteht man die Anzahl ihrer Elemente. Für die Ordnung einer Gruppe  $G$  schreibt man oft  $|G|$  oder  $\text{ord}(G)$ .

**Definition 6.3.3**  
Ordnung einer Gruppe

**Beispiel 6.3.4** Die Gruppe der Bijektionen der Menge  $\{1, 2, 3\}$  hat die Ordnung 6. Die Gruppe  $(\mathbb{Z}/m, \oplus)$  hat die Ordnung  $m$ .

#### SYMMETRISCHE GRUPPEN:

Geben wir uns eine Menge  $X$  vor und betrachten die Menge aller bijektiven Abbildungen von  $X$  auf sich selbst. Wir schreiben  $S(X) = \{f : X \rightarrow X \mid f \text{ bijektiv}\}$ . Die Menge  $S(X)$  mit der Verkettung von Funktionen ist eine Gruppe.

**Satz 6.3.4**  
Symmetrische Gruppen

#### Beweis:

Da die Verkettung von Bijektionen wieder eine Bijektion ist, ist klar, dass wir eine algebraische Struktur haben. Das Assoziativgesetz wurde in Satz 5.2.1 bewiesen. Das neutrale Element der Verknüpfung ist die Identische Abbildung, d.h. die Abbildung die jedes Element auf sich abbildet. Das inverse Element zu  $f \in S(X)$  ist die Inverse Abbildung  $f^{-1}$ . **q.e.d.**

## 6.4 Restklassengruppen mit Multiplikation

Wenn wir die multiplikativen Restklassenstrukturen  $((\mathbb{Z})/m, \otimes)$  auf ihre Gruppeneigenschaften untersuchen, fällt zunächst auf, dass die Restklasse der 1 ein

prima Kandidat für ein neutrales Element ist. Leider muss dann die Restklasse der 0 auf jeden Fall ausgeschlossen werden, denn sie kann niemals ein inverses Element besitzen. Schauen wir uns nun zwei Beispiele an:

**Beispiel 6.4.1** Restklassenmultiplikation in  $\mathbb{Z}/5 \setminus \{[0]_5\}$ :

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Man kann an der Gruppentafel erkennen, dass die Existenzforderung eines linksneutralen und linksinversen Elements aus der Definition 6.3.1 erfüllt ist. Es handelt sich um eine Gruppe.

An dieser Stelle sollte man ruhig einmal innehalten und sich wundern. In den ganzen Zahlen  $\mathbb{Z}$  gibt es zu der Zahl 3 kein inverses Element, denn  $1/3$  ist keine ganze Zahl. Wenn man jedoch modulo 5 rechnet, findet man, dass  $[2]_5$  multiplikatives Inverses zu  $[3]_5$  ist, denn  $[2]_5 \otimes [3]_5 = [1]_5$ . In der Restklassenstruktur modulo 5 kann man ohne Probleme durch  $[3]_5$  dividieren.

**Beispiel 6.4.2** Restklassenmultiplikation in  $\mathbb{Z}/6 \setminus \{[0]_6\}$ :

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2

Man kann an der Gruppentafel erkennen, dass nicht einmal eine algebraische Struktur vorliegt, denn das Verknüpfungsergebnis von  $[2]_6$  und Restklasse  $[3]_6$  liegt nicht in der Menge  $\mathbb{Z}/6 \setminus \{[0]_6\}$ .

Wir werden sehen, dass die Gruppeneigenschaft damit zu tun haben wird, dass der Modulus eine Primzahl ist.

In diesem Kapitel soll beantwortet werden, wann eine Restklasse modulo  $m$  ein multiplikatives Inverses besitzt. Dieses Wissen greift auf die Grundfeste der Ma-

thematik, die von den griechischen Mathematikern vor mehr als 2000 Jahren gelegt wurden, zurück.

In der Schule benötigt man den ggT und den kgV zweier Zahlen, um Bruchrechnung zu erlernen. Man lernt, den ggT zweier Zahlen durch Primfaktorzerlegung zu ermitteln:

**Beispiel 6.4.3** *ggT durch Primfaktorzerlegung*

Es ist der ggT(240, 420) zu bestimmen. Dazu zerlegt man die Zahlen in Primfaktoren:

$$240 = 2^4 * 3 * 5$$

$$420 = 2^2 * 3 * 5 * 7$$

Der ggT wird durch die gemeinsamen Primfaktoren bestimmt:  $\text{ggT}(240, 140) = 2^2 * 3 * 5 = 60$ .

Leider ist aus Algorithmischer Sicht die Primfaktorzerlegung ein sehr schwieriges Problem. Werden die Zahlen größer, ist es sehr schwer, Primfaktoren zu finden. In der Tat beruhen manche kryptographische Verfahren darauf, dass es praktisch unmöglich ist (also viel zu lange dauert), eine große Zahl in ihre Primfaktoren zu zerlegen, wenn diese Primfaktoren selbst große Zahlen sind. Zum Glück gibt es zur Primfaktorzerlegung Alternativen, die algorithmisch sogar sehr leicht umzusetzen sind: den euklidischen Algorithmus. Dieser benutzt die Division mit Rest:

**DIVISION MIT REST:**

Gegeben seien zwei beliebige Zahlen  $a, b \in \mathbb{N}$ . Dann gibt es genau zwei Zahlen  $q, r \in \mathbb{N}_0$  ( $q$  steht für Quotient und  $r$  steht für Rest), so dass

$$a = q * b + r \text{ wobei } 0 \leq r < b$$

Man schreibt  $q = a \text{ div } b$  und  $r = a \text{ mod } b$ .

**Satz 6.4.1**  
Division mit Rest

Dieser Satz soll hier nicht bewiesen werden. Sollten Sie Schwierigkeiten haben, den Inhalt des Satzes zu verstehen, so empfehle ich Ihnen einfach ein paar Beispiele durchzurechnen.

**Beispiel 6.4.4** *Division mit Rest.*

$a = 67$  und  $b = 17$ . Dann ist  $67 = 3 * 17 + 16$ .

$a = 17$  und  $b = 67$ . Dann ist  $17 = 0 * 67 + 17$ .

Die Division mit Rest erlaubt es, die Aufgabe, gemeinsame Teiler von zwei Zahlen zu finden, etwas zu vereinfachen. Betrachten Sie dazu den folgenden Satz:

**GEMEINSAME TEILER UND DIVISION MIT REST:**

Seien  $a, b \in \mathbb{N}$  zwei beliebige natürliche Zahlen und  $q, r \in \mathbb{N}_0$  so dass

$$(*) \quad a = q * b + r, (0 \leq r < b).$$

Dann ist die Menge  $gT(a, b)$  der gemeinsamen Teiler von  $a$  und  $b$  gleich der Menge  $gT(b, r)$  der gemeinsamen Teiler von  $b$  und  $r$ .

**Satz 6.4.2**

Gemeinsame  
Teiler und  
Division mit Rest

**Beweis:**

Wir teilen den Beweis in zwei Schritte:

1. Sei  $t$  ein gemeinsamer Teiler von  $a$  und  $b$ . Wir zeigen:  $t$  ist gemeinsamer Teiler von  $b$  und  $r$ .
2. Sei  $t$  ein gemeinsamer Teiler von  $r$  und  $b$ . Wir zeigen:  $t$  ist gemeinsamer Teiler von  $a$  und  $b$ .

Zu 1)

Sei  $t$  ein gemeinsamer Teiler von  $a$  und  $b$ . Das heißt, dass Zahlen  $a_1, b_1 \in \mathbb{N}_0$  existieren, so dass  $a = a_1 * t$  und  $b = b_1 * t$ . Da  $t$  dann schon Teiler von  $b$  ist, brauchen wir nur zu zeigen, dass  $t$  auch Teiler von  $r$  ist. Es gilt aber wegen (\*):

$$r = a - q * b = (a_1 - q * b_1) * t,$$

was zeigt, dass  $t$  Teiler von  $r$  ist.

Zu 2)

Sei  $t$  ein gemeinsamer Teiler von  $b$  und  $r$ . Das heißt, dass Zahlen  $b_1, r_1 \in \mathbb{N}_0$  existieren, so dass  $b = b_1 * t$  und  $r = r_1 * t$ . Da  $t$  dann schon Teiler von  $b$  ist, brauchen wir nur zu zeigen, dass  $t$  auch Teiler von  $a$  ist. Es gilt aber wegen (\*):

$$a = q * b + r = (qb_1 + r_1) * t$$

, was zeigt, dass  $t$  Teiler von  $a$  ist. **q.e.d.**

Wieso hilft uns der obige Satz beim Finden des ggT? Nun, die Antwort ist: Die Menge der gemeinsamen Teiler von  $r$  und  $b$  zu bestimmen, ist deshalb leichter als die gemeinsamen Teiler von  $a$  und  $b$  zu bestimmen, weil die Zahlen  $b$  und  $r$  kleiner sind als die Zahlen  $a$  und  $b$ . Vielleicht scheint nicht besonders viel gewonnen, aber man kann dieses Verfahren mehrfach anwenden. Dabei werden immer wieder Reste entstehen, die immer kleiner werden müssen, bis sie schließlich 0 sind. Und dann haben wir nun wirklich gewonnen. Denn die gemeinsamen Teiler einer Zahl und 0 sind einfach die Teiler der ersten Zahl, denn alle Zahlen sind Teiler der 0. Und natürlich hat die Menge aller Teiler einer Zahl ein größtes Element, nämlich die Zahl selbst.

Der euklidische Algorithmus ist nichts anderes als das wiederholte Anwenden von Satz 6.4.2. Er wird durch folgendes Schema beschrieben:

#### Algorithmus 1: Euklidischer Algorithmus

Der euklidische Algorithmus berechnet den größten gemeinsamen Teiler (ggT) zweier positiver ganzer Zahlen  $a$  und  $b$

(1)	$r_1$	$=$	$q_1 * r_2 + r_3$	$0 < r_3 < r_2$	Wir nennen $a = r_1$ und $b = r_2$
(2)	$r_2$	$=$	$q_2 * r_3 + r_4$	$0 < r_4 < r_3$	Dividiere $r_2$ durch $r_3$ mit Rest
	$\dots$	$=$	$\dots$	$\dots$	
(i)	$r_i$	$=$	$q_i * r_{i+1} + r_{i+2}$	$0 < r_{i+2} < r_{i+1}$	Dividiere $r_i$ durch $r_{i+1}$ mit Rest
	$\dots$	$=$	$\dots$	$\dots$	
$(n-3)$	$r_{n-3}$	$=$	$q_{n-3} * r_{n-2} + r_{n-1}$	$0 < r_{n-1} < r_{n-2}$	
$(n-2)$	$r_{n-2}$	$=$	$q_{n-2} * r_{n-1} + r_n$	$0 = r_n < r_{n-1}$	Der letzte auftretende Rest $r_n$ ist 0.

In Form der Programmiersprache Java würde dies wie folgt aussehen:

```
int euclid(int a, int b){
    int r;
    while (b!=0){
        r= a%b;
        a=b;
        b=r;
    }
    return a;
}
```

Wie Sie erkennen, wird der Divisor und der Rest einer vorhergehenden Zeile der Dividend und der Divisor der Folgezeile. Die dabei entstehenden Reste werden

immer kleiner. Deshalb muss das Verfahren schließlich mit einem Rest  $r_n = 0$  abbrechen.  $r_{n-1}$  ist dann der gesuchte ggT.

**Beispiel 6.4.5** Euklids Algorithmus

Wir wollen den  $\text{ggT}(1547, 560)$  bestimmen. Dazu rechnen wir:

$$\begin{aligned} 1547 &= 2 * 560 + 427 \\ 560 &= 1 * 427 + 133 \\ 427 &= 3 * 133 + 28 \\ 133 &= 4 * 28 + 21 \\ 28 &= 1 * 21 + 7 \\ 21 &= 3 * 7 + 0 \end{aligned}$$

Damit ist klar:  $\text{ggT}(1547, 560) = 7$ .

Die Aussage dieses Satzes erscheint zunächst verwirrend. Er enthält aber genau die Aussage, die erforderlich ist, um in multiplikativen Restklassenstrukturen zu invertieren. Es erfordert etwas Nachdenken, um diesen Satz zu verstehen.

**SATZ VON BÉZOUT:**

Seien  $a, b \in \mathbb{N}$  gegeben. Dann gibt es  $a^* \in \mathbb{N}$  und  $b^* \in \mathbb{Z}$ , so dass

$$a^*a + b^*b = \text{ggT}(a, b)$$

**Satz 6.4.3** Satz  
von Bézout

Bemerkung 25:

Wenn wir eine beliebige „Kombination“  $pa + qb$ ;  $p, q \in \mathbb{Z}$  bilden, gilt immer  $\text{ggT}(a, b) | pa + qb$ , denn  $\text{ggT}(a, b)$  teilt mit  $a$  auch  $pa$  und mit  $b$  auch  $qb$ . Deshalb teilt  $\text{ggT}(a, b)$  auch  $pa + qb$ .  $\text{ggT}(a, b)$  ist damit untere Schranke (bzgl. —) der Menge  $\{pa + qb | p, q \in \mathbb{Z}\}$ . Der Satz von Bézout sagt aus, dass  $\text{ggT}(a, b)$  kleinstes Element dieser Menge ist.

**Beweis:**

Wenn man den euklidischen Algorithmus durchrechnet, ist der Beweis des Satzes von Bézout sehr einfach: Man muss den euklidischen Algorithmus einfach von hinten her aufrollen: **q.e.d.**

Einfacher ist der Satz von Bézout an einem Beispiel zu erklären.



**Beispiel 6.4.6** Satz von Bézout

Nach dem letzten Beispiel wissen wir, dass  $\text{ggT}(1547, 560) = 7$  ist. Der Satz von Bézout sagt, dass sich 7 in der Form  $p * 1547 + q * 560$  schreiben lässt.

Wie findet man  $p$  und  $q$ ? Man rechnet den euklidischen Algorithmus rückwärts!

$$\begin{aligned}
 7 &= 28 - 1 * 21 &= 28 - 1 * (133 - 4 * 28) &= \\
 &5 * 28 - 1 * 133 &= 5 * (427 - 3 * 133) - 1 * 133 &= \\
 &5 * 427 - 16 * 133 &= 5 * 427 - 16 * (560 - 1 * 427) &= \\
 &21 * 427 - 16 * 560 &= 21 * (1547 - 2 * 560) - 16 * 560 &= \\
 &21 * 1547 - 58 * 560
 \end{aligned}$$

Mittels der Zahlen aus dem Satz von Bézout kann man nun das inverse Element einer Restklasse modulo  $m$  bestimmen:

**EXISTENZSATZ MULTIPLIKATIVE INVERSE RESTKLASSEN:**

Sei  $m \in \mathbb{N}$  ein fester Modulus und  $a \in \mathbb{Z}$ . Die Restklasse  $[a]_m$  hat genau dann ein inverses Element, wenn  $\text{ggT}(a, m) = 1$ .

**Satz 6.4.4**  
Existenzsatz  
multiplikative  
inverse  
Restklassen

**Beweis:**

Seien  $a, m$  wie im Satz mit  $\text{ggT}(a, m) = 1$ . Dann gibt es nach dem Satz von Bézout Zahlen  $a^*, m^*$ , so dass

$$1 = a^*a + m^*m$$

Wenn wir zu Restklassen modulo  $m$  übergehen, erhalten wir:

$$[1]_m = [a^*a + m^*m]_m = [a^*]_m \otimes [a]_m \oplus [m^*]_m \otimes [m]_m = [a^*]_m \otimes [a]_m$$

Dabei gilt die letzte Gleichheit, da  $[m]_m = [0]_m$ . Die obige Gleichung zeigt, dass das gesuchte inverse Element genau die Restklasse von  $[a^*]_m$  ist.

Seien  $a, m$  wie im Satz und  $[a]_m$  habe ein multiplikatives Inverses  $[a^*]_m$ . Dann gilt:  $[a^*]_m \otimes [a]_m = [1]_m$ . Dann unterscheiden sich  $a^*a$  und 1 nur um ein Vielfaches von  $m$ . Es gibt also ein  $m^*$ , so dass  $a^*a - 1 = m^*m$ . Stellt man die Summanden um, so erhält man:

$$a^*a + (-m^*)m = 1$$

Nach der Bemerkung zum Satz von Bézout ist der  $\text{ggT}(a, m)$  ein Teiler von 1. Das geht aber nur, wenn  $\text{ggT}(a, m) = 1$ . **q.e.d.**

Wenn der Modulus eine Primzahl ist, ist der  $\text{ggT}$  immer dann 1, wenn  $a$  nicht Vielfaches von  $m$  ist.

**Satz 6.4.5**

Multiplikative  
Restklassengrup-  
pen

**MULTIPLIKATIVE RESTKLASSENGRUPPEN:**

Sei  $p \in \mathbb{N}$  eine Primzahl. Dann ist  $(\mathbb{Z}/p \setminus \{[0]_p\})$  eine Gruppe.

**Beweis:**

Wenn  $p$  eine Primzahl ist, dann ist für alle  $a$  mit  $1 < a < p$   $\text{ggT}(a, p) = 1$ . Daher haben alle Restklassen  $[a]_p$  ein inverses Element. **q.e.d.**

Eine Verallgemeinerung des Satzes 6.4.4 ist der folgende Satz:

**Satz 6.4.6**

Existenzsatz  
Restklassenglei-  
chungen

**EXISTENZSATZ RESTKLASSENGLEICHUNGEN:**

Sei  $m \in \mathbb{N}$  ein fester Modulus. Dann hat für gegebene  $a, b \in \mathbb{Z}$  die Restklassengleichung:

$$[a]_m \otimes [x]_m = [b]_m$$

genau dann eine Lösung, wenn  $\text{ggT}(a, m) | b$ .

**Beispiel 6.4.7** *Lösungen Restklassengleichung*

Hat die Gleichung  $[12]_{15} \otimes [x]_{15} = [7]_{15}$  eine Lösung?

Nein, denn 7 ist nicht Vielfaches von  $\text{ggT}(12, 15) = 3$ .

**Beispiel 6.4.8** *Lösungen Restklassengleichung*

Hat die Gleichung  $[11]_{15} \otimes [x]_{15} = [7]_{15}$  eine Lösung?

Ja, denn 7 ist Vielfaches von  $\text{ggT}(11, 15) = 1$ .

Wir können eine Lösung berechnen:

$$15 = 1 \cdot 11 + 4$$

$$11 = 2 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

Rechnen wir den euklidischen Algorithmus rückwärts:

$$1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = 3 \cdot (15 - 11) - 11 = 3 \cdot 15 - 4 \cdot 11$$

Daher ist das multiplikative Inverse von  $[11]_{15}$  die Restklasse  $[-4]_{15} = [11]_{15}$ . Daher ist die gesuchte Lösung  $x = 7 \cdot 11 \bmod 15 = 2$ .

**Aufgabe 6.13:**

Welche der folgenden Restklassengleichungen hat eine Lösung? Geben Sie eine Lösung an, wenn eine existiert.

1.  $[45]_{81} \otimes [x]_{81} = [21]_{81}$
2.  $[17]_{25} \otimes [x]_{25} = [7]_{25}$
3.  $[45]_{81} \otimes [x]_{81} = [20]_{81}$
4.  $[44]_{81} \otimes [x]_{81} = [20]_{81}$

**Aufgabe 6.14:**

Beweisen Sie Satz 6.4.6.

**Aufgabe 6.15:**

Programmieren Sie den euklidischen Algorithmus.

**Aufgabe 6.16:**

Erstellen Sie ein Programm, dass in der Lage ist Restklassengleichungen zu lösen.

**Aufgabe 6.17:**

Aufgrund der vielen Studenten soll die Nordakademie in Elmshorn an die U Bahn angeschlossen werden. Zwei Linien, die  $U_{15}$  und die  $U_{21}$  fahren im 15 bzw. 21 Minuten Takt. Leider hat der Bahnhof nur einen Bahnsteig, so dass in einer Minute immer nur ein Zug in Elmshorn halten kann. Ist es möglich, einen Fahrplan zu erstellen, so dass die angegebene Taktung eingehalten werden kann.

Wie verhält es sich mit den Linien  $U_{15}$  und  $U_{22}$ ?

## 6.5 Untergruppen

**UNTERGRUPPE:**

Sei  $(G, \circ)$  eine Gruppe und  $U \subseteq G$  eine nichtleere Teilmenge von  $G$ .  $U$  heißt Untergruppe von  $G$ , wenn sie selbst eine Gruppe mit  $\circ$  bildet.

**Definition 6.5.1**  
Untergruppe

Bemerkung 26:  $U$  ist genau dann eine Untergruppe von  $G$ , wenn die Gruppenaxiome 1,2a und 2b für  $U$  erfüllt sind, da das Assoziativgesetz ja aufgrund seiner Gültigkeit für  $G$  auch für alle Elemente aus  $U$  gilt. Man kann an eine Untergruppe also folgende Forderungen stellen:

1.  $a \circ b \in U$  für alle  $a, b \in U$ .
2.  $a^{-1} \in U$  für alle  $a \in U$ .

Bemerkung 27:  $\{e\}$  und  $G$  selbst sind offensichtlich immer Untergruppen einer Gruppe  $G$ . Deshalb bezeichnet man sie als triviale Untergruppen.

**Beispiel 6.5.1** Wir betrachten wieder die Gruppe der Bijektionen der Menge  $\{1, 2, 3\}$  auf sich selbst. In dieser Gruppe gibt es folgende nichttriviale Untergruppen:

- $H_1 = \{R_1, R_5\}$
- $H_2 = \{R_2, R_5\}$
- $H_3 = \{R_6, R_5\}$
- $H_4 = \{R_3, R_4, R_5\}$

Eine Untergruppe einer Gruppe kann man finden, indem man ausgehend von einem  $g \in G$  alle die Elemente der Gruppe hinzunimmt, die erforderlich sind, um die Abgeschlossenheit bezüglich der Verknüpfung und der Inversenbildung zu erhalten.

**GRUPPENELEMENT ERZEUGT UNTERGRUPPE:**

Sei  $(G, \circ)$  eine endliche Gruppe und  $g \in G$  ein beliebiges Element. Dann

1. gibt es ein  $k \in \mathbb{N} \leq \text{ord}(g)$ , so dass

$$\underbrace{g \circ \dots \circ g}_{k\text{-mal}} = e$$

2. ist die Menge  $\{\underbrace{g \circ \dots \circ g}_{k\text{-mal}} \mid k \in \mathbb{N}\}$  eine Untergruppe von  $G$ .

**Satz 6.5.1**  
Gruppenelement  
erzeugt  
Untergruppe

**Beweis:**

Sei  $(G, \circ)$  eine endliche Gruppe und  $g \in G$  ein beliebiges Element, sowie  $\text{ord}(G) = n \in \mathbb{N}$  die Anzahl der Elemente von  $G$ .

Zur ersten Teilaussage: Wir betrachten die  $n + 1$  lange Folge von Elementen aus  $G$ :

$$g, g \circ g, g \circ g \circ g, \dots, \underbrace{g \circ \dots \circ g}_{n+1\text{-mal}}$$

Da die Gruppe nur  $n$  Elemente hat, müssen wenigstens zwei der Elemente der Folge gleich sein. Das erste dieser Elemente sei  $\underbrace{g \circ \dots \circ g}_{i\text{-mal}}$  und das zweite  $\underbrace{g \circ \dots \circ g}_{j\text{-mal}}$ , wobei  $i$  und  $j$  natürliche Zahlen mit  $1 \leq i, j \leq n + 1 \wedge i < j$ . Das bedeutet:

$$\underbrace{g \circ \dots \circ g}_{i\text{-mal}} = \underbrace{g \circ \dots \circ g}_{j\text{-mal}} = \underbrace{g \circ \dots \circ g}_{i\text{-mal}} \circ \underbrace{g \circ \dots \circ g}_{j-i\text{-mal}}$$

Dabei haben wir in der letzten Gleichung die  $j$  Verknüpfungselemente  $g$  in einmal  $i$  und einmal  $j-i$  Elemente aufgespalten. Das dürfen wir, weil das Assoziativgesetz gilt.

Da die Gleichung  $\underbrace{g \circ \dots \circ g}_{i\text{-mal}} = \underbrace{g \circ \dots \circ g}_{i\text{-mal}} \circ x$  genau eine Lösung hat und  $e$  eine Lösung ist, muss  $\underbrace{g \circ \dots \circ g}_{j-i\text{-mal}} = e$  sein.  $j-i$  muss  $\leq n$  und  $\geq 1$  sein. Die kleinste Zahl  $n \in \mathbb{N}$ , für die  $\underbrace{g \circ \dots \circ g}_{n\text{-mal}} = e$  gilt, wird Ordnung von  $g$  oder  $\text{ord}(g)$  genannt.

Zur zweiten Teilaussage: Wir müssen zeigen, dass die Menge  $H$  bezüglich der Verknüpfung  $\circ$  und der Inversenbildung abgeschlossen ist. Dass  $H$  bezüglich  $\circ$  abgeschlossen ist, ergibt sich direkt aus der Definition von  $H$ . **q.e.d.**

#### VON $g$ ERZEUGTE UNTERGRUPPE:

Sei  $(G, \circ)$  eine endliche Gruppe und  $g \in G$  ein beliebiges Element. Die Menge  $\{\underbrace{g \circ \dots \circ g}_{k\text{-mal}} \mid k \in \mathbb{N}\}$  wird die von  $g$  erzeugte Untergruppe genannt. Wir schreiben für diese Untergruppe  $\langle g \rangle$ .

**Definition 6.5.2**  
Von  $g$  erzeugte Untergruppe

Wenn wir uns unter einer typischen Gruppe die Bewegungen des Zauberwürfels vorstellen, dann kann man sich unter dem Ausdruck  $\underbrace{g \circ \dots \circ g}_{k\text{-mal}}$  die  $k$ -fache Wiederholung der Bewegung  $g$  vorstellen. Es macht Sinn, für diesen „länglichen“ Ausdruck eine abkürzende Schreibweise einzuführen:

**WIEDERHOLUNGEN VON GRUPPENELEMENTEN:**

Sei  $(G, \circ)$  eine beliebige Gruppe sowie  $g \in G$  und  $k \in \mathbb{Z}$  beliebig. Dann definieren wir:

$$g^k = \begin{cases} \underbrace{g \circ \dots \circ g}_{k\text{-mal}} & \text{falls } k > 0 \\ e & \text{falls } k = 0 \\ \underbrace{g^{-1} \circ \dots \circ g^{-1}}_{-k\text{-mal}} & \text{falls } k < 0 \end{cases}$$

**Definition 6.5.3**  
Wiederholungen  
von Gruppenele-  
menten

Man beachte, dass für negative Werte von  $k$  Wiederholungen als Wiederholungen des inversen Elements definiert sind.

Da man Wiederholungen eines Elements beliebig aneinanderhängen kann, ergibt sich folgender kleiner Satz, dessen Beweis sich sofort aus der Definition der Wiederholung von Gruppenelementen ergibt:

**WIEDERHOLUNG VON GRUPPENELEMENTEN:**

Sei  $(G, \circ)$  eine beliebige Gruppe sowie  $g \in G$  und  $k, l \in \mathbb{Z}$  beliebig. Dann gilt:

$$g^k \circ g^l = g^{k+l}$$

**Satz 6.5.2**  
Wiederholung  
von Gruppenele-  
menten

Bitte beachten Sie, dass es Sinn macht, sich für einen Beweis noch einmal die Fälle, in denen einer der Werte  $k$  und  $l$  0 ist, sowie die Fälle, in denen  $k$  und  $l$  unterschiedliches Vorzeichen haben, getrennt zu überlegen.

**ORDNUNG EINES GRUPPENELEMENTS:**

Sei  $(G, \circ)$  eine beliebige Gruppe sowie  $g \in G$  beliebig.

Wenn es eine endliche Wiederholungsanzahl  $k \in \mathbb{N}$  gibt, so dass  $g^k = e$  ist, dann bezeichnen wir die kleinste solche Zahl als Ordnung des Elements  $g$  und schreiben dafür  $\text{ord}(g)$ .

Gibt es keine natürliche Zahl  $k$ , so dass  $g^k = e$  ist, so sagen wir, dass  $g$  die Ordnung  $\infty$  hat.

**Definition 6.5.4**  
Ordnung eines  
Gruppenele-  
ments

Satz 6.5.1 besagt, dass in endlichen Gruppen jedes Element eine endliche Ordnung hat.

**Beispiel 6.5.2** In der Gruppe der Bijektionen der Menge  $\{1, 2, 3\}$  auf sich selbst haben die Elemente folgende Ordnungen:

$g$	$\text{ord}(g)$	$\langle g \rangle$
$R_1$	2	$\{R_1, R_5\}$
$R_2$	2	$\{R_2, R_5\}$
$R_3$	3	$\{R_3, R_4, R_5\}$
$R_4$	3	$\{R_4, R_3, R_5\}$
$R_5$	1	$\{R_5\}$
$R_6$	2	$\{R_6, R_5\}$

**Beispiel 6.5.3** Wenn wir die Gruppe der Bewegungen des Zauberwürfels betrachten, können wir durch Ausprobieren für die aneinandergrenzenden weißen und grünen Seiten folgende Ordnungen feststellen:

$$\begin{aligned}\text{ord}(w^+) &= \text{ord}(g^-) = 4 \\ \text{ord}(w^+ g^-) &= 63\end{aligned}$$

Wie man an dem Beispiel des Zauberwürfels sehen kann, kann durch Verknüpfung von zwei Elementen in einer nicht kommutativen Gruppe eine anscheinend willkürliche Ordnung entstehen. Dies zeigt die Komplexität, die in nicht kommutative Gruppen stecken kann.

**Beispiel 6.5.4** Wenn wir die Gruppe  $(\mathbb{Z}/5, \oplus)$  betrachten, erhalten wir folgende Ordnungen:

$g$	$\text{ord}(g)$	$\langle g \rangle$
0	1	$\{0\}$
1	5	$\{1, 2, 3, 4, 0\}$
2	5	$\{2, 4, 1, 3, 0\}$
3	5	$\{3, 1, 4, 2, 0\}$
4	5	$\{4, 3, 2, 1, 0\}$

In diesem Beispiel sind der besseren Übersichtlichkeit halber nicht Restklassen, sondern ihre Repräsentanten angegeben.

**Beispiel 6.5.5** Wenn wir die Gruppe  $(\mathbb{Z}/6, \oplus)$  betrachten, erhalten wir folgende Ordnungen:

$g$	$\text{ord}(g)$	$\langle g \rangle$
0	1	$\{0\}$
1	6	$\{1, 2, 3, 4, 5, 0\}$
2	3	$\{2, 4, 0\}$
3	2	$\{3, 0\}$
4	3	$\{4, 2, 0\}$
5	6	$\{5, 4, 3, 2, 1, 0\}$

**Beispiel 6.5.6** Wenn wir die Gruppe  $(\mathbb{Z}/5 \setminus \{[0]_5\}, \otimes)$  betrachten, erhalten wir folgende Ordnungen:

$g$	$\text{ord}(g)$	$\langle g \rangle$
1	1	$\{1\}$
2	4	$\{2, 4, 3, 1\}$
3	4	$\{3, 4, 2, 1\}$
4	2	$\{4, 1\}$

Wie man in den Beispielen sieht, ist die Ordnung einer Untergruppe immer ein Teiler der Ordnung der Gruppe. Das ist nicht nur in diesen Beispielen so, sondern dahinter steckt ein allgemeiner Satz:

**Satz 6.5.3**  
Ordnung einer  
Untergruppe

**ORDNUNG EINER UNTERGRUPPE:**

Sei  $(G, \circ)$  eine beliebige endliche Gruppe sowie  $H$  eine beliebige Untergruppe. Dann gilt:

$$\text{ord}(H) \mid \text{ord}(G)$$

**Bemerkung:** Da die Ordnung eines Gruppenelements  $g$  genau die Ordnung der von ihm erzeugten Untergruppe ist, folgt natürlich sofort:

$$\forall g \in G : \text{ord}(g) \mid \text{ord}(G)$$

Der Beweis beruht auf einer geschickt gewählten Äquivalenzrelation  $\equiv_H$ , die wir Kongruenz modulo  $H$  nennen. Sie ist eine Art Verallgemeinerung der Kongruenz modulo  $m$ , die wir in der Untersuchung der Restklassen definiert haben.



**KONGRUENZ MODULO EINER UNTERGRUPPE:**

Sei  $(G, \circ)$  eine beliebige Gruppe sowie  $H$  eine beliebige Untergruppe. Wir definieren:

$$\forall g_1, g_2 \in G : g_1 \equiv_H g_2 \Leftrightarrow g_1 \circ g_2^{-1} \in H$$

**Definition 6.5.5**

Kongruenz modulo einer Untergruppe

Bemerkung 28: Würden wir von der Addition als Gruppenoperation sprechen, so besagt dies: die Differenz zweier Elemente  $g_1$  und  $g_2$  ist in der Untergruppe.

Bei der Kongruenz modulo einer Untergruppe handelt es sich genau wie bei der Äquivalenz modulo  $m$  um eine Äquivalenzrelation.

**KONGRUENZ IST ÄQUIVALENZRELATION:**

Sei  $(G, \circ)$  eine beliebige Gruppe sowie  $H$  eine beliebige Untergruppe. Dann ist  $\equiv_H$  eine Äquivalenzrelation.

Für die Äquivalenzklassen bezüglich dieser Äquivalenzrelation gilt:

$$\forall g \in G : [g]_{\equiv_H} = \{h \circ g \mid h \in H\}$$

**Satz 6.5.4**

Kongruenz ist Äquivalenzrelation

**Beweis:**

Wir müssen die Eigenschaften einer Äquivalenzrelation nachweisen:

- Reflexivität ( $\forall g \in G : g \equiv_H g$ ):

Sei  $g \in G$  beliebig. Dann gilt:  $g \circ g^{-1} = e$ . Da das neutrale Element in jeder Untergruppe liegt, folgt:  $g \equiv_H g$ .

- Symmetrie ( $\forall g_1, g_2 \in G : g_1 \equiv_H g_2 \Rightarrow g_2 \equiv_H g_1$ ):

Seien  $g_1, g_2 \in G$  beliebig mit  $g_1 \equiv_H g_2$ . Nach der Definition von  $\equiv_H$  folgt  $g_1 \circ g_2^{-1} \in H$ . Nach dem Satz 6.3.1 über elementare Gruppeneigenschaften folgt:

$$g_2 \circ g_1^{-1} = (g_2^{-1})^{-1} \circ g_1^{-1} = (g_1 \circ g_2^{-1})^{-1} \in H$$

Dabei wird im letzten Schritt ausgenutzt, dass  $H$  abgeschlossen bezüglich der Inversenbildung ist.

- Transitivität ( $\forall g_1, g_2, g_3 \in G : g_1 \equiv_H g_2 \wedge g_2 \equiv_H g_3 \Rightarrow g_1 \equiv_H g_3$ ):

Seien  $g_1, g_2, g_3 \in G$  beliebig mit  $g_1 \equiv_H g_2$  und  $g_2 \equiv_H g_3$ . Nach der Definition von  $\equiv_H$  folgt:  $g_1 \circ g_2^{-1} \in H$  und  $g_2 \circ g_3^{-1} \in H$ . Da  $H$  bezüglich der Gruppenoperation  $\circ$  abgeschlossen ist, folgt:

$$g_1 \circ g_3^{-1} = \underbrace{g_1 \circ g_2^{-1}}_{\in H} \circ \underbrace{g_2 \circ g_3^{-1}}_{\in H} \in H$$

Um den zweiten Teil zu beweisen, notieren wir folgende gleichwertige Aussagen:

Seien  $a, g \in G$  beliebige Elemente. Dann gilt:

$$\begin{aligned} a \in [g]_{\equiv_H} & \Leftrightarrow \\ a \equiv_H g & \Leftrightarrow \\ a \circ g^{-1} \in H & \Leftrightarrow \\ \exists h \in H : h = a \circ g^{-1} & \Leftrightarrow \\ \exists h \in H : h \circ g = a & \Leftrightarrow \\ a \in \{h \circ g \mid h \in H\} & \end{aligned}$$

**q.e.d.**

Damit können wir nun Satz 6.5.3 beweisen:

**Beweis:**

Sei  $(G, \circ)$  eine beliebige Gruppe und  $H$  eine beliebige Untergruppe. Wir wissen, dass die Äquivalenzklassen von  $\equiv_H$  eine disjunkte Zerlegung der Menge  $G$  bilden: Es gibt also  $g_1, \dots, g_k \in G$ , so dass:

$$G = [g_1]_{\equiv_H} \dot{\cup} \dots \dot{\cup} [g_k]_{\equiv_H}$$

Dabei steht  $\dot{\cup}$  für die Vereinigung von elementfremden Mengen. Deshalb gilt:

$$|G| = |[g_1]_{\equiv_H}| + \dots + |[g_k]_{\equiv_H}| = |\{h \circ g_1 \mid h \in H\}| + \dots + |\{h \circ g_k \mid h \in H\}|$$

.

Jede der Äquivalenzklassen  $\{h \circ g \mid h \in H\}$  hat aber genauso viel Elemente wie  $H$ , denn wenn  $h$  alle Elemente von  $H$  durchläuft, durchläuft  $h \circ g$  alle Elemente  $\{h \circ g \mid h \in H\}$  genau einmal. Deshalb können wir die obige Gleichungskette fortführen:

$$= \underbrace{|H| + \dots + |H|}_{k\text{-mal}} = k|H|$$

**q.e.d.**

**SATZ VON EULER:**

Sei  $(G, \circ)$  eine beliebige endliche Gruppe und  $g \in G$  beliebig. Dann gilt:

$$g^{\text{ord}(G)} = e$$

**Satz 6.5.5** Satz von Euler

**Beweis:**

Nach dem Satz 6.5.3 ist die Ordnung von  $G$  ein  $k$ -faches der Ordnung von  $G$ . Deshalb gilt:

$$g^{\text{ord}(G)} = g^{k \times \text{ord}(g)} = (g^{\text{ord}(g)})^k = e^k = e$$

**q.e.d.**

Der berühmte Mathematiker Pierre Fermat hat einen Spezialfall dieser Aussage bewiesen, der für die moderne Verschlüsselungstechnik (Rivest Shamir Adelman Verfahren) eine zentrale Rolle spielt:

**KLEINER FERMAT:**

Sei  $p \in \mathbb{N}$  eine Primzahl. Dann gilt:

$$\forall a \in \mathbb{N}, 1 < a < p : a^{p-1} \equiv_p 1$$

**Satz 6.5.6** kleiner Fermat

Bemerkung 29: In der Notation der Restklassen bedeutet die Formel aus dem kleinen Fermat, dass für jede Primzahl  $p$  und jede Restklasse  $[a]_p \neq [0]_p$  gilt:

$$[a]_p^{p-1} = [1]_p$$

**Beweis:**

Diese Aussage ist eine Anwendung des Satzes 6.5.5 auf die Gruppe  $(\mathbb{Z}/p, \otimes)$ . Die Ordnung dieser Gruppe ist  $p - 1$ . Deshalb gilt für alle  $a \in \mathbb{Z}$ , die nicht die Restklasse  $[0]_p$  repräsentieren:

$$[a^{p-1}]_p = [a]_p^{p-1} = [1]_p$$

. Das ist aber nichts anderes als die Aussage von Satz 6.5.6.

**q.e.d.**

**Aufgabe 6.18:**

Verwenden Sie Excel, um die Ordnungen der Elemente in den Gruppen  $(\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$  für  $p = 7, 19$  und  $139$  zu bestimmen.

**Aufgabe 6.19:**

Bestimmen Sie alle Untergruppen der Gruppe  $(\mathbb{Z}/9, \oplus)$ .

**Aufgabe 6.20:**

Bestimmen Sie alle Untergruppen der Gruppe  $(\mathbb{Z}/7 \setminus \{[0]_p\}, \otimes)$ .

**Aufgabe 6.21:**

Bestimmen Sie alle Untergruppen der Gruppe  $(\mathbb{Z}/9 \setminus \{[0]_p, [3]_p, [6]_p\}, \otimes)$ .

**Aufgabe 6.22:**

Sei  $(G, \circ)$  eine kommutative (abelsche) Gruppe. Dann können wir eine Verknüpfung auf den Äquivalenzklassen bezüglich  $\equiv_H$  definieren:

$$[g_1]_{\equiv_H} \circ [g_2]_{\equiv_H} = [g_1 \circ g_2]_{\equiv_H}$$

Zeigen Sie, dass diese Definition unabhängig von der Wahl der Repräsentanten ist.

## 6.6 Isomorphismen

Unter einem Isomorphismus einer Gruppe versteht man eine Umbenennung der Gruppenelemente. Wendet man die Umbenennung in der Gruppentafel konsistent an, entsteht eine neue Gruppentafel, die ganz anders als die alte aussehen kann: Wir werden in diesem Kapitel sehen, dass für Primzahlen  $p \in \mathbb{Z}$  die Gruppen  $(\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$  und  $((\mathbb{Z})/p - 1, \oplus)$  durch Umbenennungen auseinander hervorgehen. Das ist ein Ergebnis, das alles andere als intuitiv klar ist.

**GRUPPENISOMORPHISMUS:**

Seien  $(G, \circ)$  und  $(H, \otimes)$  beliebige Gruppen. Ein Isomorphismus ist eine Abbildung

$$\phi : G \rightarrow H$$

die

1. bijektiv
2. strukturerhaltend ist, d.h. es gilt:

$$\forall g_1, g_2 \in G : \phi(g_1 \circ g_2) = \phi(g_1) \otimes \phi(g_2)$$

Wenn es einen Isomorphismus zwischen  $G$  und  $H$  gibt, heißen die beiden Gruppen isomorph.

**Definition 6.6.1**  
Gruppenisomorphismus

Bemerkung 30: Wörtlich übersetzt bedeutet isomorph gleich(iso)gestaltet(morph).

Bemerkung 31: Zwei isomorphe Gruppen haben dieselbe Anzahl von Elementen.

Bemerkung 32: Wenn  $\phi : G \rightarrow H$  eine bijektive Abbildung ist, dann ist  $\phi^{-1} : H \rightarrow G$  ebenfalls eine bijektive Abbildung. Wendet man auf beiden Seiten der obigen Gleichung  $\phi^{-1}$  an, erhält man die folgende Gleichung:

$$g_1 \circ g_2 = \phi^{-1}(\phi(g_1 \circ g_2)) = \phi^{-1}(\phi(g_1) \otimes \phi(g_2))$$

Es ist aber  $g_1 = \phi^{-1}(\phi(g_1))$  und  $g_2 = \phi^{-1}(\phi(g_2))$ . Wenn  $g_1$  und  $g_2$  unabhängig voneinander die Gruppe  $G$  durchlaufen, durchlaufen  $h_1 = \phi(g_1)$  und  $h_2 = \phi(g_2)$  unabhängig voneinander die Gruppe  $H$ . Insofern gilt:

$$\forall h_1, h_2 \in H : \phi^{-1}(h_1) \circ \phi^{-1}(h_2) = \phi^{-1}(h_1 \otimes h_2)$$

Also ist  $\phi^{-1}$  auch ein Isomorphismus.

Bemerkung 33: Man kann die strukturerhaltende Eigenschaft auch folgendermaßen schreiben:

$$\forall g_1, g_2 \in G : g_1 \circ g_2 = \phi^{-1}(\phi(g_1) \otimes \phi(g_2))$$

$$\forall h_1, h_2 \in H : h_1 \otimes h_2 = \phi(\phi^{-1}(h_1) \circ \phi^{-1}(h_2))$$

Das bedeutet, dass man bei bekannter Umbenennung  $\phi, \phi^{-1}$  berechnen kann, wenn man  $\otimes$  kennt, und dass man  $\otimes$  berechnen kann, wenn man  $\circ$  kennt.

**Beispiel 6.6.1** Sei  $p$  eine Primzahl  $G = (\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$  und  $[g]_p \in G$  ein Element der Ordnung  $p - 1$ . Dann ist die Abbildung:

$$\phi : (\mathbb{Z}/p - 1, \oplus) \rightarrow (\mathbb{Z}/p \setminus \{[0]_p\}, \otimes); \phi([a]_{p-1}) = [g]_p^a$$

ein Isomorphismus.

Es ist zunächst zu überlegen, dass diese Abbildung überhaupt sinnvoll ist, denn man muss die Unabhängigkeit vom Repräsentanten einsehen. Die ergibt sich aber sofort aus dem kleinen Satz von Fermat, denn zwei unterschiedliche Repräsentanten  $a, a'$  derselben Restklasse modulo  $p - 1$  unterscheiden sich um ein Vielfaches - sagen wir das  $k$ -fache - von  $p - 1$ . Dann gilt nach dem kleinen Fermat

$$[g]_p^a = [g]_p^{a' + k \cdot (p-1)} = [g]_p^{a'} \otimes [g]_p^{k \cdot (p-1)} = [g]_p^{a'} \otimes ([g]_p^{p-1})^k = [g]_p^{a'} \otimes ([1]_p)^k = [g]_p^{a'}$$

$\phi$  ist bijektiv, das die Ordnung von  $[g]_p$  als  $p - 1$  vorausgesetzt war.

Die strukturerhaltende Eigenschaft ist genau die Aussage des Satzes refWiederholungGruppenelemente über die Wiederholung von Gruppenelementen.

**Beispiel 6.6.2** Rechenschieber für Multiplikation modulo 19...

#### GRUPPENISOMORPHISMEN ERHALTEN DIE GRUPPENSTRUKTUR:

Seien  $(G, \circ)$  und  $(H, \otimes)$  beliebige Gruppen und  $\phi : G \rightarrow H$  ein Isomorphismus. Dann gilt:

#### Satz 6.6.1

Gruppenisomorphismen erhalten die Gruppenstruktur

- $\phi(e_G) = e_H$
- $\forall g \in G : \text{ord}(g) = \text{ord}(\phi(g))$
- $\forall g \in G : \phi(g^{-1}) = \phi(g)^{-1}$

#### Aufgabe 6.23:

Benutzen Sie Excel, um ein Element der Ordnung 22 in der Gruppe  $G = (\mathbb{Z}/23 \setminus \{[0]_{23}\}, \otimes)$  zu finden. Berechnen Sie folgende Produkte und Quotienten mit dem Rechenschieber:

- $[17]_{23} \otimes [7]_{23}$
- $[21]_{23} \otimes [19]_{23}$

- $[22]_{23} \otimes [11]_{23}$
- $[16]_{23} \otimes [11]_{23}^{-1}$
- $[6]_{23} \otimes [17]_{23}^{-1}$
- $[16]_{23} \otimes [21]_{23}^{-1}$

**Aufgabe 6.24:**

Sind die beiden folgenden Gruppen isomorph?

$\nabla$	00	10	20	01	11	21		$\circ$	0	1	2	3	4	5
00	00	10	20	01	11	21		0	0	1	2	3	4	5
10	10	20	00	11	21	01		1	1	2	3	4	5	0
20	20	00	10	21	01	11	und	2	2	3	4	5	0	1
01	01	11	21	00	10	20		3	3	4	5	0	1	2
11	11	21	01	10	20	00		4	4	5	0	1	2	3
21	21	01	11	20	00	10		5	5	0	1	2	3	4

**Aufgabe 6.25:**

Sind die beiden folgenden Gruppen isomorph?

$\oplus$	0	1	2	3		$\square$	1	2	3	4
0	0	1	2	3		1	1	2	3	4
1	1	2	3	0	und	2	2	1	4	3
2	2	3	0	1		3	3	4	1	2
3	3	0	1	2		4	4	3	2	1

## 6.7 Eine Anwendung aus der Kryptographie

### 6.7.1 Grundlagen der Kryptographie

In manchen Computer Bulletin Boards ist es üblich, Nachrichten, die die Gefühle anderer Personen verletzen könnten, (z.B. ein schmutziger Witz) zu verschlüsseln. Man verwendet dann absichtlich einfach zu entschlüsselnde Codes. Beliebte sind dabei Translationscodes (Caesars Chiffren), die jeden Buchstaben durch einen im Alphabet verschobenen ersetzen. Die Formel hierfür lautet:  $C = P + b \bmod 26$ . Dann ist es sehr einfach, die Texte zu entziffern, aber niemand ist wirklich gezwungen, das zu tun.

**Beispiel 6.7.1** Caesar Chiffre

Auf einem internationalen Chirurgenkongress wetteifern die Vertreter der unterschiedlichen Nationen, wer die größten Fortschritte in der Wiederherstellung abgetrennter Körperteile gemacht hat. Die Franzosen, die Amerikaner und die Russen treten besonders selbstbewusst auf. Der französische Chirurg erzählt: „Wir haben einem Läufer ein abgetrenntes Bein wieder angenäht, und ein Jahr später konnte er einen nationalen 1000 m Lauf gewinnen“.

„Durch Nutzung modernster chirurgischer Techniken“ entgegnet darauf der russische Chirurg, „haben wir einem Athleten einen ganzen Arm wieder angenäht, und ein Jahr später konnte er mit eben jenem Arm einen neuen Weltrekord im Hammerwerfen erzielen.“

Alle fielen in stilles Schweigen, als der Amerikaner erzählt: „Jr frjrq n fzvyr ba n ube-fr'f nff, naq n lrne yngre vg jnfryrpgrq cerfoqrag!“ . (Bemerkung der Text ist Englisch, Satzzeichen und Leerzeichen wurden zur besseren Lesbarkeit übernommen.)

Es gibt symmetrische und asymmetrische Verschlüsselungsverfahren:

- Symmetrische Verschlüsselungsverfahren:

Absender und Empfänger nutzen denselben Schlüssel zum Ver- und Entschlüsseln. Vorteile: Diese Verfahren sind deshalb effizient und schnell. Nachteile: Der Schlüssel muss auf einem zweiten geheimen Weg ausgetauscht werden, starker Zuwachs der Schlüsselmenge:  $n^2$  Schlüssel sind nötig bei  $n$  Kommunikationsteilnehmern- für jedes Kommunikationspaar einer.

- Asymmetrische Verschlüsselungsverfahren:

Jeder Kommunikationsteilnehmer nutzt ein Schlüsselpaar: geheimer Schlüssel (private), öffentlicher Schlüssel (public), nicht einmal der Absender kann die von ihm verschlüsselte Nachricht entschlüsseln. Vorteile: Keine geheime Schlüsselweitergabe nötig, Anzahl der Schlüssel nur  $2 \cdot n$  bei  $n$  Teilnehmern. Nachteile: Öffentliche Schlüssel müssen authentisch sein (Authentisierung = Nachweis der Datenquelle und des unverschlüsselten Inhalts), Vergleichsweise langsame Abarbeitung.

## 6.7.2 Diffie Hellman Key Exchange

Das Diffie Hellman Key Exchange Verfahren ist ein weit verbreitetes asymmetrisches Verfahren zum Schlüsselaustausch, das es erlaubt, einen geheimen Schlüssel über ein unsicheres Medium zu übertragen, da es bei Verwendung



von genügend langen Schlüsseln (entsprechend guter Generator vorausgesetzt) als sicher bezeichnet wird. Die Sicherheit beruht auf dem diskreten Logarithmus Problem, welches als äquivalent zum Faktorisierungsproblem von ganzen Zahlen angesehen wird. Dies war das erste Public Key Verfahren (1976). Es wurde 1980 in den USA patentiert.

Nehmen Sie an, Alice möchte Bob eine Nachricht über ein öffentliches Medium, wie z.B. das Internet zukommen lassen. Sie müssen damit rechnen, dass Eve (eine Eavesdropper, also ein Lauscher) die Kommunikation mit verfolgt. Deshalb vereinbaren Sie, die Nachricht zu verschlüsseln. Dazu müssen sie sich auf einen gemeinsamen Schlüssel einigen. Das Problem besteht nun darin, dass auch der Austausch des Schlüssels von Eve belauscht wird. Das Diffie Hellman Key Exchange Protokoll stellt sicher, dass Alice und Bob ihre „Teile“ vom Schlüssel übertragen können, und nur diese beiden in der Lage sind, aus den Teilen den eigentlichen Schlüssel zu konstruieren. Eve kennt zwar die Teile, kann aber nicht (in vertretbarer Zeit, also z.B. der Lebensdauer eines Menschen oder des Universums) den eigentlichen Schlüssel rekonstruieren.

#### Algorithmus 1: Diffie Hellman Key Exchange

Der Diffie Hellman Schlüsselaustausch bedient sich einer öffentlichen großen Primzahl  $p$  und eines Elements  $g$ , das Generator genannt wird. Man wählt üblicherweise  $g$  so, dass

$$\text{ord}(g) = p - 1 \text{ in der Gruppe } (\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$$

$p$  und  $g$  können von einer Vielzahl von Anwendern genutzt werden, d.h. es ist nicht erforderlich, dass unterschiedliche Personen unterschiedliches  $p$  und  $g$  verwenden. In der Praxis sind  $p$  und  $g$  etwa 500 stellige Dualzahlen.

1. Alice wählt zufällig ein beliebiges  $1 < r < p$ . Dieses  $r$  behält sie für sich. Sie überträgt  $a = g^r \bmod p$  an Bob.
2. Bob wählt sich ein beliebiges  $1 < s < p$ . Dieses  $s$  behält er für sich. Er überträgt  $b = g^s \bmod p$  an Alice.
3. Der gemeinsame private Schlüssel ist:  $k = g^{rs} \bmod p$ . Alice und Bob können diese Zahl jeder für sich ohne Probleme berechnen:

$$\text{Alice: } k = b^r \bmod p = (g^s)^r \bmod p = g^{sr} \bmod p \text{ (denn Alice kennt } b \text{ und } r)$$

$$\text{Bob: } k = a^s \bmod p = (g^r)^s \bmod p = g^{rs} \bmod p \text{ (denn Bob kennt } a \text{ und } s)$$

$k$  kann von beiden als Schlüssel für eine symmetrische Verschlüsselung verwendet werden.

Warum hat Eve so schlechte Karten, den gemeinsamen Schlüssel zu errechnen? Sie kennt  $p, g, a, b$ . Sie kennt nicht  $r$  und  $s$ . Einer der beiden Exponenten ist aber erforderlich, um  $k$  zu berechnen.

#### DISKRETER LOGARITHMUS:

Sei  $p$  eine Primzahl und  $g$  ein Generator modulo  $p$ . Dann ist die Abbildung

$$\phi : (\mathbb{Z}/(p-1), \oplus) \rightarrow (\mathbb{Z}/p \setminus \{[0]_p\}, \otimes); \phi([n]) = [g]_p^n$$

ein Isomorphismus (d.h. eine eindeutige Abbildung, bei der alle Beziehungen zwischen den Elementen erhalten bleiben) der additiven Gruppe  $(\mathbb{Z}/(p-1), \oplus)$  auf die multiplikative Gruppe  $(\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$ .

Die Umkehrabbildung  $\phi$  von  $\phi$

$$\text{Ind}_g : (\mathbb{Z}/p \setminus \{[0]_p\}, \otimes) \rightarrow (\mathbb{Z}/(p-1), \oplus)$$

ist deshalb ebenfalls ein Isomorphismus und heißt der Index oder diskreter Logarithmus zur Basis  $g$ . Es gelten analoge Rechenregeln wie für den gewöhnlichen Logarithmus, d. h. man kann die Multiplikation auf die Addition und die Potenzierung auf die Multiplikation zurück führen.

**Definition 6.7.1**  
Diskreter  
Logarithmus

#### DISKRETES LOGARITHMUS PROBLEM:

Seien  $p$  eine Primzahl und  $g$  ein Generator, d.h. ein Element mit  $\text{ord}(g) = p-1$  in  $(\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$ .

Es ist rechentechnisch sehr aufwendig, zu einem gegebenen  $1 \leq a \leq p$  einen Exponenten  $1 \leq r \leq p-1$  zu finden, so dass  $g^r \bmod p = a$ .

Prinzip :  
Diskretes  
Logarithmus  
Problem

**Beispiel 6.7.2** Nehmen wir an, Alice und Bob einigen sich auf  $p=139$  und  $g = 12$ . Alice wählt als privaten Schlüssel  $r=7$ . Damit überträgt Alice an Bob  $R = 12^7 \bmod 139 = 110$  an Bob.

Bob wählt als privaten Schlüssel  $s=15$ . Damit überträgt Bob an Alice;  $S = 12^{15} \bmod 139 = 84$ .

Der gemeinsame private Schlüssel ist  $gps = 84^7 \bmod 139 = 110^{15} \bmod 139 = 94$

- Öffentlich bekannt sind:  $p=139, g=12, R=110, S=84$ .
- Nur Alice kennt:  $r = 7$ .
- Nur Bob kennt:  $s = 15$
- Alice und Bob kennen:  $gps = 94$

#### Algorithmus 2: Ausprobieren aller Möglichkeiten

Seien  $p$  eine Primzahl und  $g$  ein Generator. Um den diskreten Logarithmus einer Zahl  $a$  zu bestimmen, berechne man Potenzen  $g^j$  wobei  $1 \leq j \leq p-1$ . Sobald der gesuchte Wert auftritt, breche man die Suche ab.

Bemerkung 1: Natürlich ist das Ausprobieren zwar eine Lösung des diskreten Logarithmus Problems, jedoch wenn  $p$  eine große Zahl ist (sagen wir mehr als 200 Dezimalstellen), dürfte der Algorithmus länger als die Lebensdauer des Universums brauchen.

Bemerkung 2: Silver, Pohligman und Hellman geben einen Algorithmus an, der das diskrete Logarithmus Problem in der Gruppe  $(\mathbb{Z}/p \setminus \{[0]_p\}, \otimes)$  auf das Problem in einer Gruppe der Ordnung  $q$  zurückführt, wobei  $q$  ein Primteiler von  $p-1$  ist. Dieser Algorithmus löst das diskrete Logarithmus Problem unter der Annahme, dass alle Primfaktoren von  $(p-1)$  klein sind. Wenn man  $p$  so wählt, dass  $p-1$  auch große Primfaktoren hat (etwa 20 Dezimalstellen werden in der Literatur als ausreichend angegeben), so ist kein effizienter Algorithmus bekannt. Das ist natürlich kein Beweis, jedoch würde ein anders lautendes Ergebnis die gesamte mathematische Welt sehr überraschen.

#### 6.7.3 Exponentieren durch wiederholtes Quadrieren

Eine der wesentlichen Rechnenvorgänge des Diffie Hellman Algorithmus ist die Exponentiation einer Zahl modulo  $p$ . Wenn diese Zahl sehr groß wird, und das ist in der Praxis in der Tat der Fall, kann Exponentieren als wiederholtes multi-

plizieren eine sehr aufwendige Sache werden. Zum Beispiel um 2 hoch einer 500stelligen Zahl modulo einer anderen 500stelligen Zahl zu bilden würde man, wenn man immer nur mit 2 multipliziert, wesentlich länger als die Lebensdauer des Universums brauchen, selbst wenn man annimmt, dass eine einzige Multiplikation nur  $10^{-32}s$  dauert. Man braucht einen effizienteren Algorithmus.

**Beispiel 6.7.3** Wir bestimmen  $12^{61} \bmod 139$ . Dafür bestimmen wir  $12^r$  für jede Zweierpotenz  $r = 2^t$ .

$t$	0	1	2	3	4	5
$2^t$	1	2	4	8	16	32
$12^{2^t}$	12	5	25	69	35	113

In der dritten Zeile ergibt sich jede Zelle als Quadrat der vorhergehenden, wegen der üblichen Potenzrechengesetze:  $12^{2^t} * 12^{2^t} = 12^{2^t+2^t} = 12^{2^{t+1}}$ .

Das gewünschte Endergebnis berechnet man: Da  $61 = 32+16+8+4+1$  ist ergibt sich wieder wegen der Potenzrechengesetze:  $12^{61} \bmod 139 = 12 * 25 * 69 * 35 * 113 \bmod 139 = 2$ .

Algorithmus 1: Gegeben sei eine Zahl  $a$ , ein Modulus  $m$  und ein Exponent  $r$ . Um  $a^r \bmod m$  zu berechnen geht man folgendermaßen vor:

Man berechnet als Zwischenergebnis zunächst nur solche Potenzen, in denen Zweierpotenzen  $2^t$  im Exponenten stehen. Dann berechnet man  $a^r$  dann durch weitere Multiplikation, indem der Exponent  $r$  als Summe von Zweierpotenzen dargestellt wird.

In einem Algorithmus sieht das wie folgt aus:

```
void powermod(BigInteger a, BigInteger r, BigInteger m) {
    BigInteger power = a mod m; BigInteger result;
    Integer counter = 1;
    while (power < r) do {
        if (testbit(r, counter)) result = result * power mod m;
        power = power * power mod m;
        counter++;
    }
    return result;
}
```

Bemerkung 1: Wie Sie erkennen, benötigt man zum Erheben der  $r$ -ten Potenz, wo  $r$  eine  $n$ -stellige Dualzahl ist, höchstens  $2n + 1$  Multiplikationen. Das sind wesentlich weniger als  $r+1$ .

**Aufgabe 6.26:**

Finden Sie den Logarithmus zur Basis 12 der folgenden 131 stelligen Dezimalzahl:

3 81005 08485 36404 27148 20015 04667 86861 89921 30505 62546 64059 11470  
15405 79559 31742 72455 49185 97722 41486 03248 86786 36622 87893 77852 89534  
34112.

dass heißt lösen Sie  $12^x = \text{obige Zahl}$ .

Tipp: Betrachten Sie zum Finden einer Lösung nur die Anzahl der Dezimalstellen. Wenn Sie die richtig hin bekommen, haben Sie gewonnen.  $12^2$  hat 3 Stellen,  $12^3$  hat 4 Stellen usw.  $12^x$  hat 131 Stellen, wie groß könnte  $x$  dann sein? Benutzen Sie z.B. Smalltalk, um zu überprüfen, ob das geratene  $x$  zu groß oder zu klein ist. Korrigieren Sie Ihre Schätzung.

**Aufgabe 6.27:**

Finden Sie den Logarithmus zur Basis 12 in  $\mathbb{Z}/139 \setminus \{[0]_{139}\}$  von 2.

Tipp: Vielleicht ist Teamarbeit angesagt?

**Aufgabe 6.28:**

Berechnen Sie  $17^{113} \bmod 19$ .

Tipp: Beachten Sie Satz 6.5.6.

**Aufgabe 6.29:**

Berechnen Sie  $12^{97} \bmod 139$  durch wiederholtes Quadrieren. Wieviele Multiplikationen benötigen Sie?



