Eine Einführung in die Mathematik für Informatiker

— WS 2011/2012 —

DHBW Stuttgart

Prof. Dr. Karl Stroetmann

27. Februar 2012

Inhaltsverzeichnis

Kapitel 1

Einführung

Das vorliegende Skript ist die Grundlage der Mathematik-Vorlesung des ersten Semesters. Gleich zu Beginn eine Warnung: Da ich diese Vorlesung in der vorliegenden Form zum ersten Mal halte, ist das Skript noch lückenhaft und unvollständig. Ich möchte daher als erstes auf die Literatur verweisen, die Sie neben der Vorlesung benutzen können:

1. Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra
   von Gerald Teschl und Susanne Teschl [TT08],
2. Mathematik für Informatiker: Ein praxisbezogenes Lehrbuch
   von Peter Hartmann [Har06],
3. Mathematik für Informatiker,
   von Matthias Schubert [Sch07],
4. Mathematische Grundlagen der Informatik: mathematisches Denken und Beweisen ; eine Einführung
   von Christoph Meinel und Martin Mundhenk [MM06].

Alle diese Bücher finden Sie in elektronischer Form auf der Webseite unserer Bibliothek:

`http://www.dhbw-stuttgart.de/`
`themen/service-einrichtungen/bibliothek/literatursuche-datenbankangebote.html`

Dort folgen Sie dem Link "`eBooks`". Der direkte Link zu den digitalen Büchern ist:

`https://milibib.missing-link.de/milibib.php`

Dieser Link funktioniert allerdings nur innerhalb des Intranets der DHBW, ein Zugang von außerhalb ist aus Gründen des Copyrights nicht möglich.

1.1 Motivation

Bevor wir uns in die Mathematik stürzen, sollten wir uns überlegen, warum wir als Informatiker überhaupt Mathematik brauchen.

1. Historisch sind Mathematik und Informatik eng miteinander verknüpft, so ist beispielsweise das Wort "*Informatik*" ein Kunstwort, das aus den beiden Wörtern "*Information*" und "*Mathematik*" gebildet worden ist, was ich durch die Gleichung

   $$\texttt{Informatik} = \texttt{Information} + \texttt{Mathematik}$$

symbolisieren möchte. Das hat zur Folge, dass sich die Informatik an vielen Stellen mathematischer Sprech- und Denkweisen bedient. Um diese verstehen zu können, ist eine gewisse Vertrautheit mit der Mathematik unabdingbar.

2. Mathematik schult das abstrakte Denken und genau das wird in der Informatik ebenfalls benötigt. Ein komplexes Sofware-System, dass von hunderten von Programmierern über Jahre hinweg entwickelt wird, ist nur durch die Einführung geeigneter Abstraktionen beherrschbar. Die Fähigkeit, abstrakt denken zu können, ist genau das, was einen Mathematiker auszeichnet. Eine Möglichkeit, diese Fähigkeit zu erwerben besteht darin, sich mit den abstrakten Gedankengebäuden, die in der Mathematik konstruiert werden, auseinander zu setzen.

3. Es gibt eine Vielzahl von mathematischen Methoden, die unmittelbar in der Informatik angewendet werden. In dieser Vorlesung behandeln wir unter anderem die folgenden Methoden:

   (a) *Rekurrenz-Gleichungen* sind Gleichungen, durch die Folgen definiert werden. Beispielsweise können die Fibonacci-Zahlen durch die Rekurrenz-Gleichung

   $$a_{n+2} = a_{n+1} + a_n \quad \text{und die Anfangs-Bedingungen } a_0 \text{ und } a_1 = 1$$

   definiert werden. Wir können mit der oberen Rekurrenz-Gleichung sukzessive die verschiedenen Werte der Folge $(a_n)_n$ berechnen und finden

   $$a_0 = 0,\ a_1 = 1,\ a_2 = 1,\ a_3 = 2,\ a_4 = 3,\ a_5 = 5,\ a_6 = 8,\ a_7 = 13,\ \cdots.$$

   Wir werden später sehen, dass es eine geschlossene Formel zur Berechnung der Fibonacci-Zahlen gibt, es gilt

   $$a_n = \tfrac{1}{\sqrt{5}} \cdot \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^n - \left(\tfrac{1-\sqrt{5}}{2} \right)^n \right).$$

   Wir werden verschiedene Verfahren angeben, mit denen sich für in der Praxis auftretende Rekurrenz-Gleichungen geschlossene Formeln finden lassen. Solche Verfahren sind wichtig bei der Analyse der Komplexität von Algorithmen, denn die Berechnung der Laufzeit rekursiver Algorithmen führt auf Rekurrenz-Gleichungen.

   (b) Elementare Zahlentheorie bildet die Grundlage moderner kryptografischer Verfahren. Konkret werden wir den RSA-Algorithmus zur asymetrischen Verschlüsselung besprechen und die dafür notwendige Zahlentheorie im Rahmen der Vorlesung einführen.

   Die Liste der mathematischen Algorithmen, die in der Praxis eingesetzt werden, könnte leicht über mehrere Seiten fortgesetzt werden. Natürlich können im Rahmen eines Bachelor-Studiums nicht alle mathematischen Verfahren, die in der Informatik eine Anwendung finden, auch tatsächlich diskutiert werden. Das Ziel kann nur sein, in ausreichend mathematische Fähigkeiten zu vermitteln so dass Sie später im Beruf in der Lage sind, sich die mathematischen Verfahren, die sie benötigen, selbstständig anzueignen.

4. Mathematik schult das *exakte Denken*. Wie wichtig dieses ist, möchte ich mit den folgenden Beispielen verdeutlichen:

   (a) Am 9. Juni 1996 stürzte die Rakete Ariane 5 auf ihrem Jungfernflug ab. Ursache war ein Kette von Software-Fehlern: Ein Sensor im Navigations-System der Ariane 5 misst die horizontale Neigung und speichert diese zunächst als Gleitkomma-Zahl mit einer Genauigkeit von 64 Bit ab. Später wird dieser Wert dann in eine 16 Bit Festkomma-Zahl konvertiert. Bei dieser Konvertierung trat ein Überlauf ein, da die zu konvertierende Zahl zu groß war, um als 16 Bit Festkomma-Zahl dargestellt werden zu können. In der Folge gab das Navigations-System auf dem Datenbus, der dieses System mit der Steuerungs-Einheit verbindet, eine Fehlermeldung aus. Die Daten dieser Fehlermeldung wurden von der Steuerungs-Einheit als Flugdaten interpretiert. Die Steuer-Einheit leitete daraufhin eine Korrektur des Fluges ein, die dazu führte, dass die Rakete auseinander

brach und die automatische Selbstzerstörung eingeleitet werden mußte. Die Rakete war mit 4 Satelliten beladen. Der wirtschaftliche Schaden, der durch den Verlust dieser Satelliten entstanden ist, lag bei mehreren 100 Millionen Dollar.

Ein vollständiger Bericht über die Ursache des Absturzes des Ariane 5 findet sich im Internet unter der Adresse

`http://www.ima.umn.edu/~arnold/disasters/ariane5rep.html`

(b) Die Therac 25 ist ein medizinisches Bestrahlungs-Gerät, das durch Software kontrolliert wird. Durch Fehler in dieser Software erhielten 1985 mindestens 6 Patienten eine Überdosis an Strahlung. Drei dieser Patienten sind an den Folgen dieser Überdosierung gestorben.

Einen detailierten Bericht über diese Unfälle finden Sie unter

`http://courses.cs.vt.edu/~cs3604/lib/Therac_25/Therac_1.html`

(c) Im ersten Golfkrieg konnte eine irakische *Scud* Rakete von dem *Patriot* Flugabwehrsystem aufgrund eines Programmier-Fehlers in der Kontrollsoftware des Flugabwehrsystems nicht abgefangen werden. 28 Soldaten verloren dadurch ihr Leben, 100 weitere wurden verletzt.

`http://www.ima.umn.edu/~arnold/disasters/patriot.html`

(d) Im Internet finden Sie unter

`http://www.cs.tau.ac.il/~nachumd/horror.html`

eine Auflistung von schweren Unfällen, die auf Software-Fehler zurückgeführt werden konnten.

Diese Beispiele zeigen, dass bei der Konstruktion von IT-Systemen mit großer Sorgfalt und Präzision gearbeitet werden sollte. Die Erstellung von IT-Systemen muß auf einer wissenschaftlich fundierten Basis erfolgen, denn nur dann ist es möglich, die Korrekheit solcher Systeme zu *verifizieren*, also mathematisch zu beweisen. Diese oben geforderte wissenschaftliche Basis für die Entwicklung von IT-Systemen ist die Informatik, und diese hat ihre Wurzeln sowohl in der Mengenlehre als auch in der mathematischen Logik. Diese beiden Gebiete werden uns daher im ersten Semester des Informatik-Studiums beschäftigen.

Aus meiner Erfahrung weiß ich, dass einige der Studenten sich unter dem Thema Informatik etwas Anderes vorgestellt haben als die Diskussion abstrakter Konzepte. Für diese Studenten ist die Beherrschung einer Programmiersprache und einer dazugehörigen Programmierumgebung das Wesentliche der Informatik. Natürlich ist die Beherrschung einer Programmiersprache für einen Informatiker unabdingbar. Sie sollten sich allerdings darüber im klaren sein, dass das damit verbundene Wissen sehr vergänglich ist, denn niemand kann heute sagen, in welcher Programmiersprache in 10 Jahren programmiert werden wird. Im Gegensatz dazu sind die mathematischen Grundlagen der Informatik wesentlich beständiger.

1.2 Überblick

Ich möchte Ihnen zum Abschluss dieser Einführung noch einen Überblick über all die Themen geben, die ich im Rahmen der Vorlesung behandeln werde. Da ich diese Vorlesung allerdings zum ersten Mal halte und noch nicht weiss, wieviel Zeit die einzelnen Themen benötigen, ist die folgende Themenliste mit einem hohen Unsicherheitsfaktor behaftet:

1. Mathematische Formeln dienen der Abkürzung. Sie werden aus den *Junktoren*
   (a) $\wedge$ (“*und*”),
   (b) $\vee$ (“*oder*”),
   (c) $\neg$ (“*nicht*”),

(d) $\rightarrow$ ("*wenn* $\cdots$*, dann*") und
(e) $\leftrightarrow$ ("*genau dann, wenn*")

sowie den *Quantoren*

(a) $\forall$ ("*für alle*") und
(b) $\exists$ ("*es gibt*")

aufgebaut. Wir werden Junktoren und Quantoren zunächst als reine Abkürzungen einführen. Im Rahmen der Informatik-Vorlesung werden wir die Bedeutung und Verwendung von Junktoren und Quantoren weiter untersuchen.

2. Mengenlehre

   Die Mengenlehre bildet die Grundlage der modernen Mathematik. Fast alle Lehrbücher und Veröffentlichungen bedienen sich der Begriffsbildungen der Mengenlehre. Daher ist eine solide Grundlage an dieser Stelle für das weitere Studium unabdingbar.

3. Beweis-Prinzipien

   In der Informatiker benötigen wir im wesentlichen drei Arten von Beweisen:

   (a) Ein *direkter Beweis* folgert eine zu beweisende Aussage mit Hilfe elementarer logischer Schlüsse und algebraischer Umformungen. Diese Art von Beweisen kennen Sie bereits aus der Schule.

   (b) Ein *indirekter Beweis* hat das Ziel zu zeigen, dass eine bestimmte Aussage A falsch ist. Bei einem indirekten Beweis nehmen wir an, dass A doch gilt und leiten aus dieser Annahme einen Widerspruch her. Dieser Widerspruch zeigt uns dann, dass die Annahme A nicht wahr sein kann.
   Beispielsweise werden wir mit Hilfe eines indirekten Beweises zeigen, dass $\sqrt{2}$ keine rationale Zahl ist.

   (c) Ein induktiver Beweis hat das Ziel, eine Aussage für alle natürliche Zahlen zu beweisen. Beispielsweise werden wir zeigen, dass die Summenformel

   $$\sum_{i=1}^{n} i = \tfrac{1}{2} \cdot n \cdot (n+1) \quad \text{für alle natürlichen Zahlen } n \in \mathbb{N} \text{ gilt.}$$

4. Zahlentheorie

   Wir werden uns zumindest soweit mit der elementaren Zahlentheorie auseinandersetzen, dass wir in der Lage sind, die Grundlagen moderner Verschlüsselungs-Algorithmen zu verstehen.

5. Komplexe Zahlen

   Aus der Schule wissen Sie, dass die Gleichung

   $$x^2 = -1$$

   für $x \in \mathbb{R}$ keine Lösung hat. Wir werden die Menge der reellen Zahlen $\mathbb{R}$ zur Menge der komplexen Zahlen $\mathbb{C}$ erweitern und zeigen, dass im Raum der komplexen Zahlen jede quadratische Gleichung eine Lösung hat.

6. Lineare Vektor-Räume

   Die Theorie der *linearen Vektor-Räume* ist unter anderem die Grundlage für das Lösen von linearen Gleichungs-Systemen, linearen Rekurrenz-Gleichungen und linearen Differential-Gleichungen. Bevor wir uns also mit konkreten Algorithmen zur Lösung von Gleichungs-Systemen beschäftigen können, gilt es die Theorie der linearen Vektor-Räume zu verstehen.

7. Lineare Gleichungs-Systeme

   Lineare Gleichungs-Systeme treten in der Informatik an vielen Stellen auf. Wir zeigen, wie sich solche Gleichungs-Systeme lösen lassen.

8. Eigenwerte und Eigenvektoren

   Ist A eine *Matrix*, ist $\vec{x}$ ein Vektor und gilt

   $$A\vec{x} = \lambda\vec{x}$$

   so ist $\vec{x}$ ein Eigenvektor von der Matrix A zum Eigenwert λ.

   Sie brauchen an dieser Stelle keine Angst haben: Im Laufe der Vorlesung werden den Begriff der *Matrix* definieren und die Frage, wie die Multiplikation $A\vec{x}$ der Matrix A mit dem Vektor $\vec{x}$ definiert ist, wird ebenfalls noch geklärt. Weiter werden wir sehen, wie Eigenvektoren berechnet werden können.

9. Rekurrenz-Gleichungen

   Die Analyse der Komplexität rekursiver Prozeduren führt auf Rekurrenz-Gleichungen. Wir werden Verfahren entwickeln, mit denen sich solche Rekurrenz-Gleichungen lösen lassen.

Bemerkung: Ich gehe davon aus, dass das Skript eine Reihe von Tippfehlern und auch anderen Fehlern enthalten wird. Ich möchte Sie darum bitten, mir solche Fehler per Email unter der Adresse

`stroetmann@dhbw-stuttgart.de`

mitzuteilen.

Kapitel 2

Prädikatenlogische Formeln

Der Begriff der *prädikatenlogischen Formel* wird in dieser Vorlesung eine zentrale Rolle spielen. Wir werden prädikatenlogische Formeln als *Abkürzungen* definieren. Zunächst motivieren wir die Verwendung solcher Formeln.

2.1 Warum Formeln

Betrachten wir einmal den folgenden mathematischen Text:

> *Addieren wir zwei Zahlen und bilden dann das Quadrat dieser Summe, so ist das Ergebnis das selbe, wie wenn wir zunächst beide Zahlen einzeln quadrieren, diese Quadrate aufsummieren und dazu noch das Produkt der beiden Zahlen zweifach hinzu addieren.*

Der mathematische Satz, der hier ausgedrückt wird, ist Ihnen aus der Schule bekannt, es handelt sich um den ersten Binomischen Satz. Um dies zu sehen, führen wir für die in dem Text genannten zwei Zahlen die Variablen a und b ein und übersetzen dann die in dem obigen Text auftretenden Teilsätze in Terme. Die folgende Tabelle zeigt diesen Prozeß:

Addieren wir zwei Zahlen	$a + b$
bilden das Quadrat dieser Summe	$(a + b)^2$
beide Zahlen einzeln quadrieren	a^2, b^2
diese Quadrate aufsummieren	$a^2 + b^2$
das Produkt der beiden Zahlen ...	$a \cdot b$
... zweifach hinzu addieren	$a^2 + b^2 + 2 \cdot a \cdot b$

Insgesamt finden wir so, dass der obige Text zu der folgenden Formel äquivalent ist:

$$(a + b)^2 = a^2 + b^2 + 2 \cdot a \cdot b.$$

Für den mathematisch Geübten ist diese Formel offensichtlich leichter zu verstehen ist als der oben angegebene Text. Aber die Darstellung von mathematischen Zusammenhängen durch Formeln bietet neben der verbesserten Lesbarkeit noch zwei weitere Vorteile:

1. Formeln sind *manipulierbar*, d. h. wir können mit Formeln *rechnen*. Außerdem lassen Formeln sich aufgrund ihrer vergleichsweise einfachen Struktur auch mit Hilfe von Programmen bearbeiten und analysieren. Beim heutigen Stand der Technik ist es hingegegen nicht möglich, natürlichsprachlichen Text mit dem Rechner vollständig zu analysieren und zu verstehen.

2. Darüber hinaus läßt sich die Bedeutung von Formeln mathematisch definieren und steht damit zweifelsfrei fest. Eine solche mathematische Definition der Bedeutung ist für natürlichsprachlichen Text so nicht möglich, da natürlichsprachlicher Text oft mehrdeutig ist und die genaue Bedeutung nur aus dem Zusammenhang hervorgeht.

2.2 Formeln als Kurzschreibweise

Nach dieser kurzen Motivation führen wir zunächst Formeln als Abkürzungen ein und stellen der Reihe nach die Ingredienzen vor, die wir zum Aufbau einer Formel benötigen.

1. *Variablen*

   Variablen dienen uns als Namen für verschieden Objekte. Oben haben wir beispielsweise für die beiden zu addierenden Zahlen die Variablen a und b eingeführt. Die Idee bei der Einführung einer Variable ist, dass diese ein Objekt bezeichnet, dessen Identität noch nicht feststeht.

2. *Konstanten*

   Konstanten bezeichnen Objekte, deren Identität schon feststeht. In der Mathematik werden beispielsweise Zahlen wie 1 oder π als Konstanten verwendet. Würden wir Aussagen über den biblischen Stammbaum als Formeln darstellen, so würden wir `Adam` und `Eva` als Konstanten verwenden.

   > Dieses letzte Beispiel mag Sie vielleicht verwundern, weil Sie davon ausgehen, dass Formeln nur dazu benutzt werden, mathematische oder allenfalls technische Zusammenhänge zu beschreiben. Der logische Apparat ist aber keineswegs auf eine Anwendung in diesen Bereichen beschränkt. Gerade auch Sachverhalte aus dem täglichen Leben lassen sich mit Hilfe von Formeln präzise beschreiben. Das ist auch notwendig, denn wir wollen ja später unsere Formeln zur Analyse von Programmen benutzen und diese Programme werden sich durchaus auch mit der Lösung von Problemen beschäftigen, die ihren Ursprung außerhalb der Technik haben.

   Variablen und Konstanten werden zusammenfassend auch als *atomare Terme* bezeichnet. Das Attribut *atomar* bezieht sich hierbei auf die Tatsache, dass diese Terme sich nicht weiter in Bestandteile zerlegen lassen. Im Gegensatz dazu stehen die *zusammengesetzten Terme*. Dies sind Terme, die mit Hilfe von Funktions-Zeichen aus anderen Termen aufgebaut werden.

3. *Funktions-Zeichen*

   Funktions-Zeichen benutzen wir, um aus Variablen und Konstanten neue Ausdrücke aufzubauen, die wiederum Objekte bezeichnen. In dem obigen Beispiel haben wir das Funktions-Zeichen "+" benutzt und mit diesem Funktions-Zeichen aus den Variablen a und b den Ausdruck $a + b$ gebildet. Allgemein nennen wir Ausdrücke, die sich aus Variablen, Konstanten und Funktions-Zeichen bilden lassen, *Terme*.

   Das Funktions-Zeichen "+" ist zweistellig, aber natürlich gibt es auch einstellige und mehrstellige Funktions-Zeichen. Ein Beispiel aus der Mathematik für ein einstelliges Funktions-Zeichen ist das Zeichen "$\sqrt{}$". Ein weiteres Beispiel ist durch das Zeichen "sin" gegeben, dass in der Mathematik für die Sinus-Funktion verwendet wird.

   Allgemein gilt: Ist f ein n-stelliges Funktions-Zeichen und sind $t_1, \cdots, t_n$ Terme, so kann mit Hilfe des Funktions-Zeichen f daraus der neue Term

   $$f(t_1, \cdots, t_n)$$

   gebildet werden. Diese Schreibweise, bei der zunächst das Funktions-Zeichen gefolgt von einer öffnenden Klammer angegeben wird und anschließend die Argumente der Funktion durch Kommata getrennt aufgelistet werden, gefolgt von einer schließenden Klammer, ist der "Normalfall". Diese Notation wird auch als *Präfix-Notation* bezeichnet. Bei einigen zweistelligen Funktions-Zeichen hat es sich aber eingebürgert, diese in einer *Infix-Notation* darzustellen, d. h. solche Funktions-Zeichen werden zwischen die Terme geschrieben. In der Mathematik liefern die Funktions-Zeichen "+", "−", "·" und "/" hierfür Beispiele. Schließlich gibt es noch Funktions-Zeichen, die auf ihr Argument folgen. Ein Beispiel dafür ist das Zeichen "`!`" zur Bezeichnung der Fakultät[1] denn für die Fakultät einer Zahl n hat sich in der Mathematik die Schreibweise "$n!$" eingebürgert. Eine solche Notation wird als *Postfix-Notation* bezeichnet.

[1] Für eine positive natürliche Zahl n ist die *Fakultät* von n als das Produkt aller natürlichen Zahlen von 1 bis n definiert. Die Fakultät von n wird mit $n!$ bezeichnet, es gilt also $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$.

4. *Prädikate*

   Prädikate stellen zwischen verschiedenen Objekten eine Beziehung her. Ein wichtiges Prädikat ist das Gleichheits-Prädikat, dass durch das Gleichheits-Zeichen "=" dargestellt wird. Setzen wir zwei Terme t_1 und t_2 durch das Gleichheits-Zeichen in Beziehung, so erhalten wir die *Formel* $t_1 = t_2$.

   Genau wie Funktions-Zeichen auch hat jedes Prädikat eine vorgegebene *Stelligkeit*. Diese gibt an, wie viele Objekte durch das Prädikat in Relation gesetzt werden. Im Falle des Gleichheits-Zeichens ist die Stelligkeit 2, aber es gibt auch Prädikate mit anderen Stelligkeiten. Zum Beispiel könnten wir ein Prädikat "`istQuadrat`" definieren, dass für natürliche Zahlen ausdrückt, dass diese Zahl eine Quadrat-Zahl ist. Ein solches Prädikat wäre dann einstellig.

   Ist allgemein p ein n-stelliges Prädikats-Zeichen und sind die Ausdrücke $t_1, \cdots, t_n$ Terme, so kann aus diesen Bestandteilen die *Formel*

   $$p(t_1, \cdots, t_n)$$

   gebildet werden. Formeln von dieser Bauart bezeichnen wir auch als *atomare Formel*, denn sie ist zwar aus Termen, nicht jedoch aus aus anderen Formeln zusammengesetzt.

   Genau wie bei zweistelligen Funktions-Zeichen hat sich auch bei zweistelligen Prädikats-Zeichen eine *Infix-Notation* eingebürgert. Das Prädikats-Zeichen "=" liefert ein Beispiel hierfür, denn wir schreiben "$a = b$" statt "$= (a, b)$". Andere Prädikats-Zeichen, für die sich eine Infix-Notation eingebürgert hat, sind die Prädikats-Zeichen "$<$", "$\leq$", "$>$" und "$\geq$", die zum Vergleich von Zahlen benutzt werden.

5. *Junktoren*

   Junktoren werden dazu benutzt, Formeln mit einander in Beziehung zu setzen. Der einfachste Junktor ist das "*und*". Haben wir zwei Formeln F_1 und F_2 und wollen ausdrücken, dass sowohl F_1 als auch F_2 gültig ist, so schreiben wir

   $$F_1 \wedge F_2$$

   und lesen dies als "F_1 *und* F_2". Die nachfolgende Tabelle listet alle Junktoren auf, die wir verwenden werden:

Junktor	Bedeutung
$\neg F$	nicht F
$F_1 \wedge F_2$	F_1 und F_2
$F_1 \vee F_2$	F_1 oder F_2
$F_1 \rightarrow F_2$	wenn F_1, dann F_2
$F_1 \leftrightarrow F_2$	F_1 genau dann, wenn F_2

   Hier ist noch zu bemerken, dass es bei komplexeren Formeln zur Vermeidung von Mehrdeutigkeiten notwendig ist, diese geeignet zu klammern. Bezeichnen beispielsweise P, Q und R atomare Formeln, so können wir unter Zuhilfenahme von Klammern daraus die folgenden Formeln bilden:

   $$P \rightarrow (Q \vee R) \quad \text{und} \quad (P \rightarrow Q) \vee R.$$

   Umgangssprachlich würden beide Formeln wie folgt interpretiert:

   Aus P folgt Q oder R.

   Die mathematische Schreibweise ist hier im Gegensatz zu der umgangssprachlichen Formulierung eindeutig.

   Die Verwendung von vielen Klammern vermindert die Lesbarkeit einer Formel. Um Klammern einsparen zu können, vereinbaren wir daher ähnliche Bindungsregeln, wie wir sie aus der Schulmathematik kennen. Dort wurde vereinbart, dass "+" und "−" schwächer binden als "$\cdot$" und "/" und damit ist gemeint, dass

$$x + y \cdot z \quad \text{als} \quad x + (y \cdot z)$$

interpretiert wird. Ähnlich vereinbaren wir hier, dass "$\neg$" stärker bindet als "$\wedge$" und "$\vee$" und dass diese beiden Operatoren stärker binden als "$\rightarrow$". Schließlich bindet der Operator "$\leftrightarrow$" schwächer als alle anderen Operatoren. Mit diesen Vereinbarungen lautet die Formel

$$P \wedge Q \rightarrow R \leftrightarrow \neg R \rightarrow \neg P \vee \neg Q$$

dann in einer vollständig geklammerten Schreibweise

$$\big((P \wedge Q) \rightarrow R\big) \leftrightarrow \big((\neg R) \rightarrow ((\neg P) \vee (\neg Q))\big).$$

6. *Quantoren* geben an, in welcher Weise eine Variable in einer Formel verwendet wird. Wir kennen zwei Quantoren, den All-Quantor "$\forall$" und den Existenz-Quantor "$\exists$". Eine Formel der Form

   $$\forall x : F$$

   lesen wir als "*für alle x gilt F*" und eine Formel der Form

   $$\exists x : F$$

   wird als "*es gibt ein x, so dass F gilt*" gelesen. In dieser Vorlesung werden wir üblicherweise *qualifizierte Quantoren* verwenden. Die Qualifizierung gibt dabei an, in welchem Bereich die durch die Variablen bezeichneten Objekte liegen müssen. Im Falle des All-Quantors schreiben wir dann

   $$\forall x \in M : F$$

   und lesen dies als "*für alle x aus M gilt F*". Hierbei bezeichnet M eine Menge. Dies ist nur eine abkürzende Schreibweise, die wir wie folgt definieren können:

   $$\forall x \in M : F \stackrel{def}{\Longleftrightarrow} \forall x \colon (x \in M \rightarrow F)$$

   Entsprechend lautet die Notation für den Existenz-Quantor

   $$\exists x \in M : F$$

   und das wird dann als "*es gibt ein x aus M, so dass F gilt*" gelesen. Formal läßt sich das als

   $$\exists x \in M : F \stackrel{def}{\Longleftrightarrow} \exists x \colon (x \in M \wedge F)$$

   definieren. Wir verdeutlichen die Schreibweisen durch eine Beispiel. Die Formel

   $$\forall x \in \mathbb{R} : \exists n \in \mathbb{N} : n > x$$

   lesen wir wie folgt:

   Für alle x aus $\mathbb{R}$ gilt: Es gibt ein n aus $\mathbb{N}$, so dass n größer als x ist.

   Hier steht $\mathbb{R}$ für die reellen Zahlen und $\mathbb{N}$ bezeichnet die natürlichen Zahlen. Die obige Formel drückt also aus, dass es zu jeder reellen Zahl x eine natürlich Zahl n gibt, so dass n größer als x ist.

   Treten in einer Formel Quantoren und Junktoren gemischt auf, so stellt sich die Frage, was stärker bindet. Wir vereinbaren, dass Quantoren stärker binden als Junktoren. In der folgenden Formel sind die Klammern also notwendig:

   $$\forall x \colon \big(p(x) \wedge q(x)\big).$$

2.3 Beispiele für Terme und Formeln

Um die Konzepte "Term" und "Formel" zu verdeutlichen, geben wir im folgenden einige Beispiele an. Wir wählen ein Beispiel aus dem täglichen Leben und geben Terme und Formeln an, die sich mit Verwandschaftsbeziehungen beschäftigen. Wir beginnen damit, dass wir die Konstanten, Variablen, Funktions-Zeichen und Prädikats-Zeichen festlegen.

1. Als *Konstanten* verwenden wir die Wörter
   “`adam`”, “`eva`”, “`kain`” und “`abel`”, “`lisa`”.

2. Als *Variablen* verwenden wir die Buchstaben
   “x”, “y” und “z”.

3. Als *Funktions-Zeichen* verwenden wir die Wörter
   “`vater`” und “`mutter`”.
   Diese beiden Funktions-Zeichen sind einstellig.

4. Als *Prädikats-Zeichen* verwenden wir die Wörter
   “`bruder`”, “`schwester`”, “`onkel`”, “`männlich`” und “`weiblich`”.
   Alle diese Prädikats-Zeichen sind zweistellig. Als weiteres zweisteliges Prädikats-Zeichen verwenden wir das Gleichheits-Zeichen “=”.

Eine solche Ansammlung von Konstanten, Variablen, Funktions-Zeichen und Prädikats-Zeichen bezeichen wir auch als *Signatur*. Wir geben zunächst einige Terme an, die sich mit dieser Signatur bilden lassen:

1. “`kain`” ist ein Term, denn “`kain`” ist eine Konstante.

2. “`vater`(`kain`)” ist ein Term, denn “`kain`” ist ein Term und “`vater`” ist ein einstelliges Funktions-Zeichen.

3. “$\texttt{mutter}\big(\texttt{vater}(\texttt{kain})\big)$” ist ein Term, denn “`vater`(`kain`)” ist ein Term und “`mutter`” ist ein einstelliges Funktions-Zeichen,

4. “`männlich`(`kain`)” ist eine Formel, denn “`kain`” ist ein Term und “`männlich`” ist ein einstelliges Prädikats-Zeichen.

5. “`männlich`(`lisa`)” ist ebenfalls eine Formel, denn “`lisa`” ist ein Term.
   Dieses Beispiel zeigt, dass Formeln durchaus auch falsch sein können. Die bisher gezeigten Formeln sind alle atomar. Wir geben nun Beispiele für zusammengesetzte Formeln.

6. “$\texttt{vater}(x) = \texttt{vater}(y) \wedge \texttt{mutter}(x) = \texttt{mutter}(y) \rightarrow \texttt{bruder}(x, y) \vee \texttt{schwester}(x, y)$”
   ist eine Formel, die aus den beiden Formeln
   “$\texttt{vater}(x) = \texttt{vater}(y) \wedge \texttt{mutter}(x) = \texttt{mutter}(y)$” und
   “$\texttt{bruder}(x, y) \vee \texttt{schwester}(x, y)$”
   aufgebaut ist.

7. “$\forall x\colon \forall y\colon \texttt{bruder}(x, y) \vee \texttt{schwester}(x, y)$” ist eine Formel.

Die Formel Nr. 7 ist intuitiv gesehen falsch. Auch die Formel Nr. 6 ist falsch, wenn wir davon ausgehen, dass niemand sein eigener Bruder ist. Um die Begriffe “*wahr*” und “*falsch*” für Formeln streng definieren zu können, ist es notwendig, die *Interpretation* der verwendeten Signatur festzulegen. Anschaulich gesehen definiert eine *Interpretation* die Bedeutung der *Symbole*, also der Konstanten, Funktions- und Prädikats-Zeichen, aus denen die Signatur besteht. Exakt kann der Begriff aber erst angegeben werden, wenn Hilfsmittel aus der Mengenlehre zur Verfügung stehen. Dieser wenden wir uns jetzt zu.

Kapitel 3

Mengen und Relationen

Die Mengenlehre ist gegen Ende des 19-ten Jahrhunderts aus dem Bestreben heraus entstanden, die Mathematik auf eine solide Grundlage zu stellen. Die Schaffung einer solchen Grundlage wurde als notwendig erachtet, da der Begriff der Unendlichkeit den Mathematikern zunehmends Kopfzerbrechen bereitete.

Begründet wurde die Mengenlehre in wesentlichen Teilen von Georg Cantor (1845 – 1918). Die erste Definition des Begriffs der Menge lautete etwa wie folgt [Can95]:

Eine Menge *ist eine* wohldefinierte *Ansammlung von* Elementen.

Das Attribut "*wohldefiniert*" drückt dabei aus, dass wir für eine vorgegebene Menge M und ein Objekt x stets klar sein muss, ob das Objekt x zu der Menge M gehört oder nicht. In diesem Fall schreiben wir

$$x \in M$$

und lesen diese Formel als "*x ist ein Element der Menge M*". Das Zeichen "$\in$" wird in der Mengenlehre also als zweisteliges Prädikats-Zeichen gebraucht, für das sich eine Infix-Notation eingebürgert hat. Um den Begriff der *wohldefinierten Ansammlung von Elementen* mathematisch zu präzisieren, führte Cantor das sogenannte *Komprehensions-Axiom* ein. Wir können dieses zunächst wie folgt formalisieren: Ist $p(x)$ eine Eigenschaft, die ein Objekt x entweder hat oder nicht, so können wir die Menge M aller Objekte, welche die Eigenschaft $p(x)$ haben, bilden. Wie schreiben dann

$$M = \{x \mid p(x)\}$$

und lesen dies als "M ist die Menge aller x, auf welche die Eigenschaft $p(x)$ zutrifft". Eine Eigenschaft $p(x)$ ist dabei nichts anderes als eine Formel, in der die Variable x vorkommt. Wir veranschaulichen das Komprehensions-Axiom durch ein Beispiel: Es sei $\mathbb{N}$ die Menge der natürlichen Zahlen. Ausgehend von der Menge $\mathbb{N}$ wollen wir die Menge der *geraden Zahlen* definieren. Zunächst müssen wir dazu die Eigenschaft einer Zahl x, *gerade* zu sein, durch eine Formel $p(x)$ mathematisch erfassen. Eine natürliche Zahl x ist genau dann gerade, wenn es eine natürliche Zahl y gibt, so dass x das Doppelte von y ist. Damit können wir die Eigenschaft $p(x)$ folgendermaßen definieren:

$$p(x) \;:=\; (\exists y \in \mathbb{N} : x = 2 \cdot y).$$

Also kann die Menge der geraden Zahlen als

$$\{x \mid \exists y \in \mathbb{N} : x = 2 \cdot y\}$$

geschrieben werden.

Leider führt die uneingeschränkte Anwendung des Komprehensions-Axiom schnell zu Problemen. Betrachten wir dazu die Eigenschaft einer Menge, sich selbst zu enthalten, wir setzen also $p(x) := \neg(x \in x)$ und definieren die Menge R als

$$R := \{x \mid \neg\, x \in x\}.$$

Intuitiv würden wir vielleicht erwarten, dass keine Menge sich selbst enthält. Wir wollen jetzt zunächst für die eben definierte Menge R überprüfen, wie die Dinge liegen. Es können zwei Fälle auftreten:

1. Fall: $\neg(R \in R)$. Also enthält die Menge R sich nicht selbst. Da die Menge R aber als die Menge der Mengen definiert ist, die sich nicht selber enthalten, müßte R eine Element von R sein, es müsste also $R \in R$ gelten im Widerspruch zur Voraussetzung $\neg\, R \in R$.

2. Fall: $R \in R$. Setzen wir hier die Definition von R ein, so haben wir

   $$R \in \{x \mid \neg(x \in x)\}.$$

   Dass heißt dann aber gerade $\neg\, R \in R$ und steht im Widerspruch zur Voraussetzung $R \in R$.

Wie wir es auch drehen und wenden, es kann weder $R \in R$ noch $\neg\, R \in R$ gelten. Als Ausweg können wir nur feststellen, dass das vermittels

$$\{x \mid \neg\, x \in x\}$$

definierte Objekt keine Menge ist. Das heißt dann aber, dass das Komprehensions-Axiom zu allgemein ist. Wir folgern, dass nicht jede in der Form

$$M = \{x \mid p(x)\}$$

angegebene Menge existiert. Die Konstruktion der "Menge" "$\{x \mid \neg\, x \in x\}$"stammt von dem britischen Logiker und Philosophen Bertrand Russell (1872 – 1970). Sie wird deswegen auch als *Russell'sche Antinomie* bezeichnet.

Um Paradoxien wie die Russell'sche Antinomie zu vermeiden, ist es erforderlich, bei der Konstruktion von Mengen vorsichtiger vorzugehen. Wir werden im folgenden Konstruktions-Prinzipien für Mengen vorstellen, die schwächer sind als das Komprehensions-Axiom, die aber für die Praxis der Informatik ausreichend sind. Wir wollen dabei die dem Komprehensions-Axiom zugrunde liegende Notation beibehalten und Mengendefinitionen in der Form

$$M = \{x \mid p(x)\}$$

angeben. Um Paradoxien zu vermeiden, werden wir nur bestimmte Sonderfälle dieser Mengendefinition zulassen. Diese Sonderfälle, sowie weitere Möglichkeiten Mengen zu konstruieren, stellen wir jetzt vor.

3.1 Erzeugung von Mengen durch explizites Auflisten

Die einfachste Möglichkeit, eine Menge festzulegen, besteht in der expliziten *Auflistung* aller ihrer Elemente. Diese Elemente werden in den geschweiften Klammern "{" und "}" eingefaßt und durch Kommas getrennt. Definieren wir beispielsweise

$$M := \{1, 2, 3\},$$

so haben wir damit festgelegt, dass die Menge M aus den Elementen 1, 2 und 3 besteht. In der Schreibweise des Komprehensions-Axioms können wir diese Menge als

$$M = \{x \mid x = 1 \vee x = 2 \vee x = 3\}$$

angeben. Als ein weiteres Beispiel für eine Menge, die durch explizite Aufzählung ihrer Elemente angegeben werden kannn, betrachten wir die Menge der kleinen Buchstaben, die wir wie folgt definieren:

$$\{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}, \mathtt{g}, \mathtt{h}, \mathtt{i}, \mathtt{j}, \mathtt{k}, \mathtt{l}, \mathtt{m}, \mathtt{n}, \mathtt{o}, \mathtt{p}, \mathtt{q}, \mathtt{r}, \mathtt{s}, \mathtt{t}, \mathtt{u}, \mathtt{v}, \mathtt{w}, \mathtt{x}, \mathtt{y}, \mathtt{z}\}.$$

Als letztes Beispiel betrachten wir die leere Menge $\emptyset$, die durch Aufzählung aller Ihrer Elemente definiert werden kann:

$$\emptyset := \{\}.$$

Die leere Menge enthält also überhaupt keine Elemente. Diese Menge ist genau so wichtig wie die Zahl 0

3.2 Die Menge der natürlichen Zahlen

Alle durch explizite Auflistung definierten Mengen haben offensichtlich nur endlich viele Elemente. Aus der mathematischen Praxis kennen wir aber auch Mengen mit unendlich vielen Elementen. Ein Beispiel ist die Menge der natürlichen Zahlen, die wir mit $\mathbb{N}$ bezeichnen. Im Gegensatz zu einigen anderen Autoren will ich dabei die Zahl 0 auch als natürliche Zahl auffassen. Mit den bisher behandelten Verfahren läßt sich die Menge $\mathbb{N}$ nicht definieren. Wir müssen daher die Existenz dieser Menge als Axiom fordern:

$$\mathbb{N} := \{0, 1, 2, 3, \cdots\}.$$

Neben der Menge $\mathbb{N}$ der natürlichen Zahlen verwenden wir noch die folgenden Mengen von Zahlen:

1. $\mathbb{Z}$: Menge der ganzen Zahlen.

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

2. $\mathbb{Q}$: Menge der rationalen Zahlen.

   $$\left\{ \tfrac{p}{q} \mid p \in \mathbb{Z} \wedge q \in \mathbb{N} \wedge q > 0 \right\}$$

3. $\mathbb{R}$: Menge der reellen Zahlen.

   Wie die reellen Zahlen tatsächlich konstruiert werden, kann ich Ihnen erst im zweiten Semester zeigen.

In der Mathematik wird gezeigt, wie sich diese Mengen aus der Menge der natürlichen Zahlen erzeugen lassen.

3.3 Das Auswahl-Prinzip

Das *Auswahl-Prinzip* ist eine Abschwächung des Komprehensions-Axiom. Die Idee ist, mit Hilfe einer Eigenschaft p aus einer schon vorhandenen Menge M die Menge N der Elemente x *auszuwählen*, die eine bestimmte Eigenschaft $p(x)$ besitzen:

$$N = \{x \in M \mid p(x)\}$$

In der Notation des Komprehensions-Axioms schreibt sich diese Menge als

$$N = \{x \mid x \in M \wedge p(x)\}.$$

Im Unterschied zu dem Komprehensions-Axiom können wir uns hier nur auf die Elemente einer bereits vorgegebenen Menge M beziehen und nicht auf völlig beliebige Objekte.

Beispiel: Die Menge der geraden Zahlen kann mit dem Auswahl-Prinzip wie folgt definiert werden:

$$\{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : x = 2 \cdot y\}.$$

3.4 Potenz-Mengen

Um den Begriff der *Potenz-Menge* einführen zu können, müssen wir zunächst *Teilmengen* definieren. Sind M und N zwei Mengen, so heißt M eine *Teilmenge* von N genau dann, wenn jedes Element der Menge M auch ein Element der Menge N ist. In diesem Fall schreiben wir $M \subseteq N$. Formal können wir den Begriff der Teilmenge also wie folgt einführen:

$$M \subseteq N \overset{def}{\iff} \forall x : (x \in M \rightarrow x \in N)$$

Beispiel: Es gilt

$$\{1, 3, 5\} \subseteq \{1, 2, 3, 4, 5\}$$

Weiter gilt für jede beliebige Menge M

$$\emptyset \subseteq M.$$

Unter der *Potenz-Menge* einer Menge M wollen wir nun die Menge aller Teilmengen von M verstehen. Wir schreiben 2^M für die Potenz-Menge von M. Dann gilt:

$$2^M = \{x \mid x \subseteq M\}.$$

Beispiel: Wir bilden die Potenz-Menge der Menge $\{1, 2, 3\}$. Es gilt:

$$2^{\{1,2,3\}} = \big\{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}.$$

Diese Menge hat $8 = 2^3$ Elemente. Allgemein kann durch Induktion über die Anzahl der Elemente der Menge M gezeigt werden, dass die Potenz-Menge einer Menge M, die aus m verschiedenen Elementen besteht, insgesamt 2^m Elemente enthält. Bezeichnen wir die Anzahl der Elemente einer endlichen Menge mit $card(M)$, so gilt also

$$card\left(2^M\right) = 2^{card(M)}.$$

Dies erklärt die Schreibweise 2^M für die Potenz-Menge von M.

3.5 Vereinigungs-Mengen

Sind zwei Mengen M und N gegeben, so enthält die Vereinigung von M und N alle Elemente, die in der Menge M oder in der Menge N liegen. Für diese Vereinigung schreiben wir $M \cup N$. Formal kann die Vereinigung wie folgt definiert werden:

$$M \cup N := \{x \mid x \in M \vee x \in N\}.$$

Beispiel: Ist $M = \{1, 2, 3\}$ und $N = \{2, 5\}$, so gilt:

$$\{1, 2, 3\} \cup \{2, 5\} = \{1, 2, 3, 5\}.$$

Der Begriff der Vereinigung von Mengen läßt sich verallgemeinern. Betrachten wir dazu eine Menge X, deren Elemente selbst wieder Mengen sind. Beispielsweise ist die Potenz-Menge einer Menge von dieser Art. Wir können dann die Vereinigung aller Mengen, die Elemente von der Menge X sind, bilden. Diese Vereinigung schreiben wir als $\bigcup X$. Formal kann das wie folgt definiert werden:

$$\bigcup X = \{y \mid \exists x \in X : y \in x\}.$$

Beispiel: Die Menge X sei wie folgt gegeben:

$$X = \big\{\{\}, \{1, 2\}, \{1, 3, 5\}, \{7, 4\}\big\}.$$

Dann gilt

$$\bigcup X = \{1, 2, 3, 4, 5, 7\}.$$

3.6 Schnitt-Menge

Sind zwei Mengen M und N gegeben, so definieren wir den *Schnitt* von M und N als die Menge aller Elemente, die sowohl in M als auch in N auftreten. Wir bezeichen den Schnitt von M und N mit $M \cap N$. Formal können wir $M \cap N$ wie folgt definieren:

$$M \cap N := \{x \mid x \in M \wedge x \in N\}.$$

Beispiel: Wir berechnen den Schnitt der Mengen $M = \{1, 3, 5\}$ und $N = \{2, 3, 5, 6\}$. Es gilt

$$M \cap N = \{3, 5\}$$

3.7 Differenz-Mengen

Sind zwei Mengen M und N gegeben, so bezeichen wir die *Differenz* von M und N als die Menge aller Elemente, die in M aber nicht N auftreten. Wir schreiben hierfür $M \backslash N$. Das wird als M *ohne* N gelesen und kann formal wie folgt definiert werden:

$$M \backslash N := \{x \mid x \in M \wedge x \notin N\}.$$

Beispiel: Wir berechnen die Differenz der Mengen $M = \{1, 3, 5, 7\}$ und $N = \{2, 3, 5, 6\}$. Es gilt

$$M \backslash N = \{1, 7\}.$$

3.8 Bild-Mengen

Es sei M eine Menge und f sei eine Funktion, die für alle x aus M definiert ist. Dann heißt die Menge aller Abbilder $f(x)$ von Elementen x aus der Menge M das *Bild* von M unter f. Wir schreiben $f(M)$ für dieses Bild. Formal kann $f(M)$ wie folgt definiert werden:

$$f(M) := \{y \mid \exists x \in M : y = f(x)\}.$$

In der Literatur findet sich für die obige Menge auch die Schreibweise

$$f(M) = \big\{f(x) \mid x \in M\big\}.$$

Beispiel: Die Menge Q aller Quadrat-Zahlen kann wie folgt definiert werden:

$$Q := \{y \mid \exists x \in \mathbb{N} : y = x^2\}.$$

Alternativ können wir auch schreiben

$$Q = \big\{x^2 \mid x \in \mathbb{N}\big\}.$$

3.9 Kartesische Produkte

Um den Begriff des kartesischen Produktes einführen zu können, benötigen wir zunächst den Begriff des geordneten Paares zweier Objekte x und y. Dieses wird als

$$\langle x, y \rangle$$

geschrieben. Wir sagen, dass x die *erste Komponente* des Paares $\langle x, y \rangle$ ist, und y ist die *zweite Komponente*. Zwei geordnete Paare $\langle x_1, y_1 \rangle$ und $\langle x_2, y_2 \rangle$ sind genau dann gleich, wenn sie komponentenweise gleich sind, d.h. es gilt

$$\langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle \Leftrightarrow x_1 = x_2 \wedge y_1 = y_2.$$

Das kartesische Produkt zweier Mengen M und N ist nun die Menge aller geordneten Paare, deren erste Komponente in M liegt und deren zweite Komponente in N liegt. Das kartesische Produkt von M und N wird als $M \times N$ geschrieben, formal gilt:

$$M \times N := \big\{z \mid \exists x \colon \exists y \colon z = \langle x, y \rangle \wedge x \in M \wedge y \in N\big\}.$$

Alternativ können wir auch schreiben

$$M \times N := \big\{\langle x, y \rangle \mid x \in M \wedge y \in N\big\}.$$

Beispiel: Wir setzen $M = \{1, 2, 3\}$ und $N = \{5, 7\}$. Dann gilt

$$M \times N = \big\{\langle 1, 5 \rangle, \langle 2, 5 \rangle, \langle 3, 5 \rangle, \langle 1, 7 \rangle, \langle 2, 7 \rangle, \langle 3, 7 \rangle\big\}.$$

Der Begriff des geordneten Paares läßt sich leicht zum Begriff des n-Tupels verallgemeinern: Ein n-Tupel hat die Form

$$\langle x_1, x_2, \cdots, x_n \rangle.$$

Analog kann auch der Begriff des kartesischen Produktes auf n Mengen $M_1, \cdots, M_n$ verallgemeinert werden. Das sieht dann so aus:

$$M_1 \times \cdots \times M_n = \big\{ z \mid \exists x_1 \colon \cdots \exists x_n \colon \; z = \langle x_1, x_2, \cdots, x_n \rangle \wedge x_1 \in M_1 \wedge \cdots \wedge x_n \in M_n \big\}.$$

Ist f eine Funktion, die auf $M_1 \times \cdots \times M_n$ definiert ist, so vereinbaren wir folgende Vereinfachung der Schreibweise:

$$f(x_1, \cdots, x_n) \text{ steht für } f(\langle x_1, \cdots, x_n \rangle).$$

Gelegentlich werden n-Tupel auch als *endliche Folgen* oder als *Listen* bezeichnet.

3.10 Gleichheit von Mengen

Wir haben nun alle Verfahren, die wir zur Konstruktion von Mengen benötigen, vorgestellt. Wir klären jetzt die Frage, wann zwei Mengen gleich sind. Dazu postulieren wir das folgende *Extensionalitäts-Axiom* für Mengen:

Zwei Mengen sind genau dann gleich, wenn sie die selben Elemente besitzen.

Mathematisch können wir diesen Sachverhalt wie folgt ausdrücken:

$$M = N \;\leftrightarrow\; \forall x : (x \in M \leftrightarrow x \in N)$$

Eine wichtige Konsequenz aus diesem Axiom ist die Tatsache, dass die Reihenfolge, mit der Elemente in einer Menge aufgelistet werden, keine Rolle spielt. Beispielsweise gilt

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

denn beide Mengen enthalten die selben Elemente.

Falls Mengen durch explizite Aufzählung ihrer Elemente definiert sind, ist die Frage nach der Gleichheit zweier Mengen trivial. Ist eine der Mengen mit Hilfe des Auswahl-Prinzips definiert, so kann es beliebig schwierig sein zu entscheiden, ob zwei Mengen gleich sind. Hierzu ein Beispiel: Es läßt sich zeigen, dass

$$\{n \in \mathbb{N} \mid \exists x, y, z \in \mathbb{N} : x > 0 \wedge y > 0 \wedge x^n + y^n = z^n\} = \{1, 2\}$$

gilt. Allerdings ist der Nachweis dieser Gleichheit sehr schwer, denn er ist äquivalent zum Beweis der *Fermat'schen Vermutung*. Diese Vermutung wurde 1637 von *Pierre de Fermat* aufgestellt und konnte erst 1995 von Andrew Wiles bewiesen werden. Es gibt andere, ähnlich aufgebaute Mengen, wo bis heute unklar ist, welche Elemente in der Menge liegen und welche nicht.

3.11 Rechenregeln für das Arbeiten mit Mengen

Vereinigungs-Menge, Schnitt-Menge und die Differenz zweier Mengen genügen Gesetzmäßigkeiten, die in den folgenden Gleichungen zusammengefaßt sind:

1.	$M \cup \emptyset = M$	$M \cap \emptyset = \emptyset$
2.	$M \cup M = M$	$M \cap M = M$
3.	$M \cup N = N \cup M$	$M \cap N = N \cap M$
4.	$(K \cup M) \cup N = K \cup (M \cup N)$	$(K \cap M) \cap N = K \cap (M \cap N)$
5.	$(K \cup M) \cap N = (K \cap N) \cup (M \cap N)$	$(K \cap M) \cup N = (K \cup N) \cap (M \cup N)$
6.	$M \backslash \emptyset = M$	$M \backslash M = \emptyset$
7.	$K \backslash (M \cup N) = (K \backslash M) \cap (K \backslash N)$	$K \backslash (M \cap N) = (K \backslash M) \cup (K \backslash N)$
8.	$(K \cup M) \backslash N = (K \backslash N) \cup (M \backslash N)$	$(K \cap M) \backslash N = (K \backslash N) \cap (M \backslash N)$
9.	$K \backslash (M \backslash N) = (K \backslash M) \cup (K \cap N)$	$(K \backslash M) \backslash N = K \backslash (M \cup N)$
10.	$M \cup (N \backslash M) = M \cup N$	$M \cap (N \backslash M) = \emptyset$
11.	$M \cup (M \cap N) = M$	$M \cap (M \cup N) = M$

Wir beweisen exemplarisch die Gleichung $K \backslash (M \cup N) = (K \backslash M) \cap (K \backslash N)$. Um die Gleichheit zweier Mengen zu zeigen ist nachzweisen, dass beide Mengen die selben Elemente enthalten. Wir haben die folgende Kette von Äquivalenzen:

$$
\begin{array}{ll}
 & x \in K \backslash (M \cup N) \\
\leftrightarrow & x \in K \ \wedge \ \neg\, x \in M \cup N \\
\leftrightarrow & x \in K \ \wedge \ \neg\, (x \in M \vee x \in N) \\
\leftrightarrow & x \in K \ \wedge \ (\neg\, x \in M) \wedge (\neg\, x \in N) \\
\leftrightarrow & (x \in K \wedge \neg\, x \in M) \ \wedge \ (x \in K \wedge \neg\, x \in N) \\
\leftrightarrow & (x \in K \backslash M) \ \wedge \ (x \in K \backslash N) \\
\leftrightarrow & x \in (K \backslash M) \cap (K \backslash N).
\end{array}
$$

Die übrigen Gleichungen können nach dem selben Schema hergeleitet werden.

Aufgabe 1: Beweisen Sie die Gleichung $K \backslash (M \cap N) = (K \backslash M) \cup (K \backslash N)$.

Zur Vereinfachung der Darstellung von Beweisen vereinbaren wir die folgende Schreibweise: Ist M eine Menge und x ein Objekt, so schreiben wir $x \notin M$ für die Formel $\neg\, x \in M$, formal:

$$x \notin M \ \stackrel{def}{\Longleftrightarrow} \ \neg\, x \in M.$$

Eine analoge Notation verwenden wir auch für das Gleichheitszeichen:

$$x \neq y \ \stackrel{def}{\Longleftrightarrow} \ \neg\, (x = y).$$

3.12 Binäre Relationen

Relationen treten in der Informatik an vielen Stellen auf. Die wichtigste Anwendung findet sich in der Theorie der relationalen Datenbanken. Wir betrachten im Folgenden den Spezialfall der *binären Relationen* und beleuchten das Verhältnis von binären Relationen und Funktionen. Wir werden sehen, dass wir Funktionen als spezielle binäre Relationen auffassen können. Damit stellt der Begriff der binären Relationen eine Verallgemeinerung des Funktions-Begriffs dar.

Zum Abschluß des Kapitels führen wir *transitive Relationen* und *Äquivalenz-Relationen* ein. Einerseits sind dies grundlegende Konzepte, die jeder Informatiker kennen muss, andererseits werden wir schon nächsten Kapitel mit Hilfe transitiver Ralationen interessante Suchprobleme lösen können.

3.13 Binäre Relationen und Funktionen

Ist eine Menge R als Teilmenge des kartesischen Produkts zweier Mengen M und N gegeben, gilt also

$$R \subseteq M \times N,$$

so bezeichnen wir R auch als *binäre Relation*. In diesem Fall definieren wir den *Definitions-Bereich*

von R als

$$\mathrm{dom}(R) := \{x \mid \exists y \in N : \langle x, y\rangle \in R\}.$$

Entsprechend wird der *Werte-Bereich* von R als

$$\mathrm{rng}(R) := \{y \mid \exists x \in M : \langle x, y\rangle \in R\}$$

definiert.

Beispiel: Es sei $R = \{\langle 1,1\rangle, \langle 2,4\rangle, \langle 3,9\rangle\}$. Dann gilt

$$\mathrm{dom}(R) = \{1,2,3\} \quad \text{und} \quad \mathrm{rng}(R) = \{1,4,9\}. \qquad \square$$

Das nächste, stark vereinfachte Beispiel gibt einen Vorgeschmack von der Bedeutung binärer Relationen in der Theorie der *relationalen Datenbanken*.

Beispiel: Ein Autoverkäufer speichert in seiner Datenbank, welcher Kunde welches Auto gekauft hat. Nehmen wir an, dass die Mengen $Auto$ und $Kunde$ wie folgt gegeben sind:

$$Kunde = \{\text{Bauer}, \text{Maier}, \text{Schmidt}\} \quad \text{und} \quad Auto = \{\text{Polo}, \text{Fox}, \text{Golf}\}.$$

Dann könnte die binäre Relation

$$Verkauf \subseteq Kunde \times Auto$$

beispielsweise durch die folgende Menge gegeben sein:

$$\{\langle \text{Bauer}, \text{Golf}\rangle, \langle \text{Bauer}, \text{Fox}\rangle, \langle \text{Schmidt}, \text{Polo}\rangle\}.$$

Diese Relation würde ausdrücken, dass der Kunde Bauer einen Golf und einen Fox erworben hat, der Kunde Schmidt hat einen Polo gekauft und Maier hat bisher noch kein Auto erworben. In der Theorie der Datenbanken werden Relationen üblicherweise in Form von Tabellen dargestellt. Die oben angegebene Relation hätte dann die folgende Form:

Kunde	*Auto*
Bauer	Golf
Bauer	Fox
Schmidt	Polo

Die oberste Zeile, in der wir die Spalten-Überschriften $Kunde$ und $Auto$ angeben, gehört selbst nicht zu der Relation, sondern wird als *Relationen-Schema* bezeichnet und die Relation zusammen mit ihrem Relationen-Schema nennen wir *Tabelle*.

3.13.1 Links- und Rechts-Eindeutige Relationen

Wir nennen eine Relation $R \subseteq M \times N$ *rechts-eindeutig*, wenn folgendes gilt:

$$\forall x \in M : \forall y_1, y_2 \in N : \big(\langle x, y_1\rangle \in R \wedge \langle x, y_2\rangle \in R \rightarrow y_1 = y_2\big).$$

Bei einer rechts-eindeutigen Relation $R \subseteq M \times N$ gibt es also zu jedem $x \in M$ höchstens ein $y \in N$ so, dass $\langle x, y\rangle \in R$ gilt. Entsprechend nennen wir eine Relation $R \subseteq M \times N$ *links-eindeutig*, wenn gilt:

$$\forall y \in N : \forall x_1, x_2 \in M : \big(\langle x_1, y\rangle \in R \wedge \langle x_2, y\rangle \in R \rightarrow x_1 = x_2\big).$$

Bei einer links-eindeutigen Relation $R \subseteq M \times N$ gibt es also zu jedem $y \in N$ höchstens ein $x \in M$ so, dass $\langle x, y\rangle \in R$ gilt.

Beispiele: Es sei $M = \{1,2,3\}$ und $N = \{4,5,6\}$.

1. Die Relation R_1 sei definiert durch

   $$R_1 = \{\langle 1,4\rangle, \langle 1,6\rangle\}.$$

Diese Relation ist nicht rechts-eindeutig, denn $4 \neq 6$. Die Relation ist links-eindeutig, denn die rechten Seiten aller in R_1 auftretenden Tupel sind verschieden.

2. Die Relation R_2 sei definiert durch

$$R_2 = \{\langle 1, 4\rangle, \langle 2, 6\rangle\}.$$

Diese Relation ist rechts-eindeutig, denn die linken Seiten aller in R_2 auftretenden Tupel sind verschieden. Sie ist auch links-eindeutig, denn die rechten Seiten aller in R_2 auftretenden Tupel sind verschieden.

3. Die Relation R_3 sei definiert durch

$$R_3 = \{\langle 1, 4\rangle, \langle 2, 6\rangle, \langle 3, 6\rangle\}.$$

Diese Relation ist rechts-eindeutig, denn die linken Seiten aller in R_2 auftretenden Tupel sind verschieden. Sie ist nicht links-eindeutig, denn es gilt $\langle 2, 6\rangle \in R$ und $\langle 3, 6\rangle \in R$, aber $2 \neq 3$.

3.13.2 Totale Relationen

Eine binäre Relation $R \subseteq M \times N$ heißt *links-total auf* M, wenn

$$\forall x \in M \colon \exists y \in N \colon \langle x, y\rangle \in R$$

gilt. Dann gibt es für alle x aus der Menge M ein y aus der Menge N, so dass $\langle x, y\rangle$ in der Menge R liegt. Die Relation R_3 aus dem obigen Beispiel ist links-total, denn jedem Element aus M wird durch R_3 ein Element aus N zugeordnet.

Analog nennen wir eine binäre Relation $R \subseteq M \times N$ *rechts-total auf* N, wenn

$$\forall y \in N \colon \exists x \in M \colon \langle x, y\rangle \in R$$

gilt. Dann gibt es für alle y aus der Menge N ein x aus der Menge M, so dass $\langle x, y\rangle$ in der Menge R liegt. Die Relation R_3 aus dem obigen Beispiel ist nicht rechts-total, denn dem Element 5 aus N wird durch R_3 kein Element aus M zugeordnet, denn für alle $\langle x, y\rangle \in R_3$ gilt $y \neq 5$.

3.13.3 Funktionale Relationen

Eine Relation $R \subseteq M \times N$, die sowohl links-total auf M als auch rechts-eindeutig ist, nennen wir eine *funktionale* Relation auf M. Ist $R \subseteq M \times N$ eine funktionale Relation, so können wir eine Funktion $f_R \colon M \to N$ wie folgt definieren:

$$f_R(x) := y \overset{def}{\iff} \langle x, y\rangle \in R.$$

Diese Definition funktioniert, denn aus der Links-Totalität von R folgt, dass es für jedes $x \in M$ auch ein $y \in N$ gibt, so dass $\langle x, y\rangle \in R$ ist. Aus der Rechts-Eindeutigkeit von R folgt dann, dass dieses y eindeutig bestimmt ist. Ist umgekehrt eine Funktion $f : M \to N$ gegeben, so können wir dieser Funktion eine Relation $\mathit{graph}(f) \subseteq M \times N$ zuordnen, indem wir definieren:

$$\mathit{graph}(f) := \big\{\langle x, f(x)\rangle \mid x \in M\big\}.$$

Die so definierte Relation $\mathit{graph}(f)$ ist links-total, denn die Funktion f berechnet ja für jedes $x \in M$ ein Ergebnis und die Relation ist rechts-eindeutig, denn die Funktion berechnet für jedes Argument immer nur ein Ergebnis.

Aufgrund der gerade diskutierten Korrespondenz zwischen Funktionen und Relationen werden wir daher im folgenden alle Funktionen als spezielle binäre Relationen auffassen. Für die Menge aller Funktionen von M nach N schreiben wir auch N^M, genauer definieren wir

$$N^M := \{R \subseteq M \times N \mid R \text{ funktional}\}.$$

Diese Schreibweise erklärt sich wie folgt: Sind M und N endliche Mengen mit m bzw. n Elementen, so gibt es genau n^m verschiedene Funktionen von M nach N, es gilt also

$$\mathit{card}\left(N^M\right) = \mathit{card}(N)^{\mathit{card}(M)}.$$

Wir werden daher funktionale Relationen und die entsprechenden Funktionen identifizieren. Damit ist dann für eine funktionale Relation $R \subseteq M \times N$ und ein $x \in M$ auch die Schreibweise $R(x)$ zulässig: Mit $R(x)$ bezeichnen wir das eindeutig bestimmte $y \in N$, für das $\langle x, y\rangle \in R$ gilt.

Beispiele:

1. Wir setzen $M = \{1, 2, 3\}$, $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und definieren

   $$R := \{\langle 1, 1\rangle, \langle 2, 4\rangle, \langle 3, 9\rangle\}.$$

   Dann ist R eine funktionale Relation auf M. Diese Relation berechnet gerade die Quadrat-Zahlen auf der Menge M.

2. Diesmal setzen wir $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und $N = \{1, 2, 3\}$ und definieren

   $$R := \{\langle 1, 1\rangle, \langle 4, 2\rangle, \langle 9, 3\rangle\}.$$

   Dann ist R keine funktionale Relation auf M, denn R ist nicht links-total auf M. Beispielsweise wird das Element 2 von der Relation R auf kein Element aus N abgebildet.

3. Wir setzen nun $M = \{1, 2, 3\}$, $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und definieren

   $$R := \{\langle 1, 1\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle, \langle 3, 9\rangle\}$$

   Dann ist R keine funktionale Relation auf M, denn R ist nicht rechts-eindeutig auf M. Beispielsweise wird das Element 2 von der Relation R sowohl auf 3 als auch auf 4 abgebildet.

Ist $R \subseteq M \times N$ eine binäre Relation und ist weiter $X \subseteq M$, so definieren wir das *Bild von X unter R* als

$$R(X) := \{y \mid \exists x \in X \colon \langle x, y\rangle \in R\}.$$

3.13.4 Inverse Relation

Zu einer Relation $R \subseteq M \times N$ definieren wir die *inverse* Relation $R^{-1} \subseteq N \times M$ wie folgt:

$$R^{-1} := \big\{\langle y, x\rangle \mid \langle x, y\rangle \in R\big\}.$$

Aus dieser Definition folgt sofort, dass R^{-1} rechts-eindeutig ist genau dann, wenn R links-eindeutig ist. Außerdem ist R^{-1} links-total genau dann, wenn R rechts-total ist. Ist eine Relation sowohl links-eindeutig als auch rechts-eindeutig und außerdem sowohl links-total als auch rechts-total, so nennen wir sie auch *bijektiv*. In diesem Fall läßt sich neben der Funktion f_R auch eine Funktion $f_{R^{-1}}$ definieren. Die Definition der letzten Funktion lautet ausgeschrieben:

$$f_{R^{-1}}(y) := x \overset{def}{\iff} \langle y, x\rangle \in R^{-1} \iff \langle x, y\rangle \in R.$$

Diese Funktion ist dann aber genau die Umkehr-Funktion von f_R, es gilt

$$\forall y \in N \colon f_R\big(f_{R^{-1}}(y)\big) = y \quad \text{und} \quad \forall x \in M \colon f_{R^{-1}}\big(f_R(x)\big) = x.$$

Dieser Umstand rechtfertigt im nachhinein die Schreibweise R^{-1}.

3.13.5 Komposition von Relationen

Ähnlich wie wir Funktionen verknüpfen können, können auch Relationen verknüpft werden. Wir betrachten zunächst Mengen L, M und N. Sind dort zwei Relationen $R \subseteq L \times M$ und $Q \subseteq M \times N$ definiert, so ist das *relationale Produkt* $R \circ Q$ wie folgt definiert:

$$R \circ Q := \big\{\langle x, z\rangle \mid \exists y \in M \colon (\langle x, y\rangle \in R \wedge \langle y, z\rangle \in Q)\big\}$$

Offenbar gilt $R \circ Q \subseteq L \times N$. Das relationale Produkt von Q und R wird gelegentlich auch als die *Komposition* von Q und R bezeichnet. In der Theorie der Datenbanken werden Sie dem relationalen Produkt wiederbegegnen.

Beispiel: Es sei $L = \{1, 2, 3\}$, $M = \{4, 5, 6\}$ und $N = \{7, 8, 9\}$. Weiter seien die Relationen Q und R wie folgt gegeben:

$$R = \{\langle 1, 4\rangle, \langle 1, 6\rangle, \langle 3, 5\rangle\} \quad \text{und} \quad Q = \{\langle 4, 7\rangle, \langle 6, 8\rangle, \langle 6, 9\rangle\}.$$

Dann gilt

$$R \circ Q = \{\langle 1, 7\rangle, \langle 1, 8\rangle, \langle 1, 9\rangle\}.$$

Ist $R \subseteq L \times M$ eine funktionale Relation auf L und ist $Q \subseteq M \times N$ eine funktionale Relation auf M, so ist auch $R \circ Q$ eine funktionale Relation auf L und die Funktion $f_{R \circ Q}$ kann wie folgt aus den Funktionen f_R und f_Q berechnet werden:

$$f_{R \circ Q}(x) = f_Q\big(f_R(x)\big).$$

Bemerkung: In einigen Lehrbüchern wird das relationale Produkt, das wir als $R \circ Q$ definiert haben, mit $Q \circ R$ bezeichnet. Damit lautet die Definition von $R \circ Q$ dann wie folgt: Ist $R \subseteq M \times N$ und $Q \subseteq L \times M$, dann ist

$$R \circ Q := \big\{\langle x, z\rangle \mid \exists y \in M \colon (\langle x, y\rangle \in Q \wedge \langle y, z\rangle \in R)\big\}.$$

Diese Definition hat den folgenden Vorteil: Falls R und Q funktionale Relationen sind und wenn dann weiter f und g die diesen Relationen zugeordneten Funktionen sind, wenn also

$$Q = \mathit{graph}(f) \quad \text{und} \quad R = \mathit{graph}(g)$$

gilt, dann haben wir für die Komposition der Funktionen f und g, die durch $(g \circ f)(x) = g\big(f(x)\big)$ definiert ist, die Gleichung

$$\mathit{graph}(g \circ f) = R \circ Q = \mathit{graph}(g) \circ \mathit{graph}(f).$$

Die von uns verwendete Definition hat den Vorteil, dass später die Berechnung des transitiven Abschlusses einer Relation intuitiver wird. □

Beispiel: Das nächste Beispiel zeigt die Verwendung des relationale Produkts im Kontext einer Datenbank. Wir nehmen an, dass die Datenbank eines Autohändler unter anderem die folgenden beiden Tabellen enthält.

Kauf:

Kunde	*Auto*
Bauer	Golf
Bauer	Fox
Schmidt	Polo

Preis:

Auto	*Betrag*
Golf	20 000
Fox	10 000
Polo	13 000

Dann ist das relationale Produkt der in den Tabellen *Kauf* und *Preis* dargestellten Relationen durch die in der folgenden Tabelle dargestellten Relation gegeben:

Kunde	*Betrag*
Bauer	20 000
Bauer	10 000
Schmidt	13 000

Diese Relation könnte dann zur Rechnungsstellung weiter verwendet werden. □

Bemerkung: In der Theorie der Datenbanken wird der Begriff der Komposition zweier Relationen zu dem Begriff des *Joins* verallgemeinert.

3.13.6 Eigenschaften des relationalen Produkts

Die Komposition von Relationen ist *assoziativ*: Sind

$$R \subseteq K \times L, \quad Q \subseteq L \times M \quad \text{und} \quad P \subseteq M \times N$$

binäre Relationen, so gilt

$$(R \circ Q) \circ P = R \circ (Q \circ P).$$

Beweis: Wir zeigen

$$\langle x, u\rangle \in (R \circ Q) \circ P \leftrightarrow \langle x, u\rangle \in R \circ (Q \circ P) \tag{3.1}$$

Wir formen zunächst die linke Seite $\langle x, u\rangle \in (R \circ Q) \circ P$ der Äquivalenz 3.1 um. Es gilt

$$\begin{array}{lll}
 & \langle x, u\rangle \in (R \circ Q) \circ P & \\
\leftrightarrow & \exists z : \big(\langle x, z\rangle \in R \circ Q \wedge \langle z, u\rangle \in P\big) & \text{nach Def. von } (R \circ Q) \circ P \\
\leftrightarrow & \exists z : \big(\big(\exists y : \langle x, y\rangle \in R \wedge \langle y, z\rangle \in Q\big) \wedge \langle z, u\rangle \in P\big) & \text{nach Def. von } R \circ Q
\end{array}$$

Da die Variable y in der Formel $\langle z, u\rangle \in P$ nicht auftritt, können wir den Existenz-Quantor über y auch herausziehen, so dass wir die obige Kette von Äquivalenzen zu

$$\leftrightarrow \quad \exists z : \exists y : \big(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in Q \wedge \langle z, u\rangle \in P\big) \tag{3.2}$$

fortsetzen können. Wir formen nun die rechte Seite der Äquivalenz 3.1 um:

$$\begin{array}{lll}
 & \langle x, u\rangle \in R \circ (Q \circ P) & \\
\leftrightarrow & \exists y : \big(\langle x, y\rangle \in R \wedge \langle y, u\rangle \in Q \circ P\big) & \text{nach Def. von } R \circ (Q \circ P) \\
\leftrightarrow & \exists y : \big(\langle x, y\rangle \in R \wedge \exists z : \big(\langle y, z\rangle \in Q \wedge \langle z, u\rangle \in P\big)\big) & \text{nach Def. von } Q \circ P
\end{array}$$

Da die Variable z in der Formel $\langle x, y\rangle \in R$ nicht vorkommt, können wir den Existenz-Quantor über z auch vorziehen und können daher diese Kette von Äquivalenzen als

$$\leftrightarrow \quad \exists z : \exists y : \big(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in Q \wedge \langle z, u\rangle \in P\big) \tag{3.3}$$

fortsetzen. Die Formeln (3.2) und (3.3) sind identisch. Damit ist die Äquivalenz (3.1) nachgewiesen und der Beweis der Assoziativität des Kompositions-Operators ist erbracht. □

Eine weitere wichtige Eigenschaft des relationalen Produkts ist die folgende: Sind zwei Relationen $R \subseteq L \times M$ und $Q \subseteq M \times N$ gegeben, so gilt

$$(R \circ Q)^{-1} = Q^{-1} \circ R^{-1}.$$

Beachten Sie, dass sich die Reihenfolgen von Q und R hier vertauschen. Zum Beweis ist zu zeigen, dass für alle Paare $\langle z, x\rangle \in N \times L$ die Äquivalenz

$$\langle z, x\rangle \in (Q \circ R)^{-1} \quad \leftrightarrow \quad \langle z, x\rangle \in R^{-1} \circ Q^{-1}$$

gilt. Den Nachweis erbringen wir durch die folgende Kette von Äquivalenz-Umformungen:

$$\begin{array}{ll}
 & \langle z, x\rangle \in (R \circ Q)^{-1} \\
\leftrightarrow & \langle x, z\rangle \in R \circ Q \\
\leftrightarrow & \exists y \in M\big(: \langle x, y\rangle \in R \wedge \langle y, z\rangle \in Q\big) \\
\leftrightarrow & \exists y \in M : \big(\langle y, z\rangle \in Q \wedge \langle x, y\rangle \in R\big) \\
\leftrightarrow & \exists y \in M : \big(\langle z, y\rangle \in Q^{-1} \wedge \langle y, x\rangle \in R^{-1}\big) \\
\leftrightarrow & \langle z, x\rangle \in Q^{-1} \circ R^{-1} \qquad \square
\end{array}$$

Wir bemerken noch, dass das folgende Distributivgesetz gilt: Sind R_1 und R_2 Relationen auf $L \times M$ und ist Q eine Relation auf $M \times N$, so gilt

$$(R_1 \cup R_2) \circ Q = (R_1 \circ Q) \cup (R_2 \circ Q).$$

Analog gilt ebenfalls

$$R \circ (Q_1 \cup Q_2) = (R \circ Q_1) \cup (R \circ Q_2),$$

falls R eine Relation auf $L \times M$ und Q_1 und Q_2 Relationen auf $M \times N$ sind. Um Gleichungen der obigen Art kürzer schreiben zu können vereinbaren wir, dass der Kompositions-Operator $\circ$ stärker bindet als $\cup$ und $\cap$. Wir beweisen nun das erste Distributivgesetz, indem wir

$$\langle x, z \rangle \in (R_1 \cup R_2) \circ Q \;\leftrightarrow\; \langle x, z \rangle \in R_1 \circ Q \cup R_2 \circ Q \tag{3.4}$$

zeigen. Wir formen zunächst den Ausdruck $\langle x, z \rangle \in (R_1 \cup R_2) \circ Q$ um:

$$\begin{array}{lll}
 & \langle x, z \rangle \in (R_1 \cup R_2) \circ Q & \\
\leftrightarrow & \exists y : \big(\langle x, y \rangle \in R_1 \cup R_2 \wedge \langle y, z \rangle \in Q\big) & \text{nach Def. von } (R_1 \cup R_2) \circ Q \\
\leftrightarrow & \exists y : \big(\big(\langle x, y \rangle \in R_1 \vee \langle x, y \rangle \in R_2\big) \wedge \langle y, z \rangle \in Q\big) & \text{nach Def. von } R_1 \cup R_2
\end{array}$$

Diese Formel stellen wir mit Hilfe des Distributiv-Gesetzes der Aussagen-Logik um. In der Aussagenlogik werden wir im Rahmen der Informatik-Vorlesung sehen, dass für beliebige Formeln F_1, F_2 und G die Äquivalenz

$$(F_1 \vee F_2) \wedge G \;\leftrightarrow\; (F_1 \wedge G) \vee (F_2 \wedge G)$$

gilt. Die Anwendung dieses Gesetzes liefert:

$$\begin{array}{rl}
 & \exists y : \big(\big(\underbrace{\langle x, y \rangle \in R_1}_{F_1} \vee \underbrace{\langle x, y \rangle \in R_2}_{F_2}\big) \wedge \underbrace{\langle y, z \rangle \in Q}_{G}\big) \\
\leftrightarrow & \exists y : \big(\big(\underbrace{\langle x, y \rangle \in R_1}_{F_1} \wedge \underbrace{\langle y, z \rangle \in Q}_{G}\big) \vee \big(\underbrace{\langle x, y \rangle \in R_2}_{F_2} \wedge \underbrace{\langle y, z \rangle \in Q}_{G}\big)\big)
\end{array} \tag{3.5}$$

Wir formen nun den Ausdruck $\langle x, z \rangle \in R_1 \circ Q \cup R_2 \circ Q$ um:

$$\begin{array}{lll}
 & \langle x, z \rangle \in R_1 \circ Q \cup R_2 \circ Q & \\
\leftrightarrow & \langle x, z \rangle \in R_1 \circ Q \;\vee\; \langle x, z \rangle \in R_2 \circ Q & \text{nach Def. von } \cup \\
\leftrightarrow & \big(\exists y : (\langle x, y \rangle \in R_1 \wedge \langle y, z \rangle \in Q)\big) \;\vee\; \big(\exists y : (\langle x, y \rangle \in R_2 \wedge \langle y, z \rangle \in Q)\big) & \\
 & \text{nach Def. von } R_1 \circ Q \text{ und } R_2 \circ Q &
\end{array}$$

Diese letzte Formel stellen wir mit Hilfe eines Distributiv-Gesetzes für die Prädikaten-Logik um. In der Prädikaten-Logik werden wir später sehen, dass für beliebige Formeln F_1 und F_2 die Äquivalenz

$$\exists y : \big(F_1 \vee F_2\big) \;\leftrightarrow\; \big(\exists y : F_1\big) \vee \big(\exists y : F_2\big)$$

gültig ist. Damit folgt dann

$$\begin{array}{rl}
 & \exists y : \big(\underbrace{\langle x, y \rangle \in R_1 \wedge \langle y, z \rangle \in Q}_{F_1}\big) \;\vee\; \exists y : \big(\underbrace{\langle x, y \rangle \in R_2 \wedge \langle y, z \rangle \in Q}_{F_2}\big) \\
\leftrightarrow & \exists y : \Big(\big(\underbrace{\langle x, y \rangle \in R_1 \wedge \langle y, z \rangle \in Q}_{F_1}\big) \;\vee\; \big(\underbrace{\langle x, y \rangle \in R_2 \wedge \langle y, z \rangle \in Q}_{F_2}\big)\Big)
\end{array} \tag{3.6}$$

Da die Formeln 3.5 und 3.6 identisch sind, ist der Beweis des Distributiv-Gesetzes

$$(R_1 \cup R_2) \circ Q = R_1 \circ Q \cup R_2 \circ Q$$

erbracht. □

Interessant ist noch zu bemerken, dass für den Schnitt von Relationen und dem Kompositions-Operator kein Distributivgesetz gilt, die Gleichung

$$(R_1 \cap R_2) \circ Q = R_1 \circ Q \cap R_2 \circ Q$$

ist im Allgemeinen falsch. Um diese Behauptung zu belegen, benötigen wir ein Gegenbeispiel. Dazu definieren wir die Relationen R_1, R_2 und Q wie folgt:

$$R_1 := \{\langle 1, 2\rangle\}, \quad R_2 := \{\langle 1, 3\rangle\} \quad \text{und} \quad Q = \{\langle 2, 4\rangle, \langle 3, 4\rangle\}.$$

Dann gilt

$$R_1 \circ Q = \{\langle 1, 4\rangle\}, \quad R_2 \circ Q = \{\langle 1, 4\rangle\}, \quad \text{also } R_1 \circ Q \cap R_2 \circ Q = \{\langle 1, 4\rangle\},$$

aber andererseits haben wir

$$(R_1 \cap R_2) \circ Q = \emptyset \circ Q = \emptyset \neq \{\langle 1, 4\rangle\} = R_1 \circ Q \cap R_2 \circ Q.$$

3.13.7 Identische Relation

Ist M eine Menge, so definieren wir die *identische Relation* $\mathrm{id}_M \subseteq M \times M$ wie folgt:

$$\mathrm{id}_M := \big\{\langle x, x\rangle \mid x \in M\big\}.$$

Beispiel: Es sei $M = \{1, 2, 3\}$. Dann gilt

$$\mathrm{id}_M := \big\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\big\}.$$

Aus der Definition folgt sofort

$$\mathrm{id}_M^{-1} = \mathrm{id}_M.$$

Sei weiterhin $R \subseteq M \times N$ und eine binäre Relation, so gilt

$$R \circ \mathrm{id}_N = R \quad \text{und} \quad \mathrm{id}_M \circ R = R.$$

Wir weisen die zweite Gleichung nach. Nach Definition des relationalen Produkts gilt

$$\mathrm{id}_M \circ R = \big\{\langle x, z\rangle \mid \exists y : \langle x, y\rangle \in \mathrm{id}_M \wedge \langle y, z\rangle \in R\big\}.$$

Nun ist $\langle x, y\rangle \in \mathrm{id}_M$ genau dann, wenn $x = y$ ist, also gilt

$$\mathrm{id}_M \circ R = \big\{\langle x, z\rangle \mid \exists y : x = y \wedge \langle y, z\rangle \in R\big\}.$$

Es gilt die folgende Äquivalenz

$$\big(\exists y : x = y \wedge \langle y, z\rangle \in R\big) \leftrightarrow \langle x, z\rangle \in R.$$

Diese Äquivalenz ist leicht einzusehen: Falls $\exists y : x = y \wedge \langle y, z\rangle \in R$ gilt, so muß dass y dessen Existenz gefordert wird, den Wert x haben und dann gilt natürlich auch $\langle x, z\rangle \in R$. Gilt andererseits $\langle x, z\rangle \in R$, so definieren wir $y := x$. Für das so definierte y gilt offensichtlich $x = y \wedge \langle y, z\rangle \in R$. Unter Verwendung der oberen Äquivalenz haben wir

$$\mathrm{id}_M \circ R = \big\{\langle x, z\rangle \mid \langle x, z\rangle \in R\big\}.$$

Wegen $R \subseteq M \times N$ besteht R nur aus geordneten Paaren und daher gilt

$$R = \big\{\langle x, z\rangle \mid \langle x, z\rangle \in R\big\}.$$

Damit ist $\mathrm{id}_M \circ R = R$ gezeigt. □

Aufgabe 2: Es sei $R \subseteq M \times N$. Unter welchen Bedingungen gilt

$$R \circ R^{-1} = \mathrm{id}_M?$$

Unter welchen Bedingungen gilt

$$R^{-1} \circ R = \mathrm{id}_M?$$ □

3.14 Binäre Relationen auf einer Menge

Wir betrachten im Folgenden den Spezialfall von Relationen $R \subseteq M \times N$, für den $M = N$ gilt. Wir definieren: Eine Relation $R \subseteq M \times M$ heißt eine Relation *auf* der Menge M. Im Rest dieses Abschnittes betrachten wir nur noch solche Relationen. Statt $M \times M$ schreiben wir kürzer M^2.

Ist R eine Relation auf M und sind $x, y \in M$, so verwenden wir gelegentlich die Infix-Schreibweise und schreiben statt $\langle x, y\rangle \in R$ auch $x\,R\,y$. Beispielsweise läßt sich die Relation $\leq$ auf $\mathbb{N}$ wie folgt definieren:

$$\leq := \{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid \exists z \in \mathbb{N}\colon x + z = y\}.$$

Statt $\langle x, y\rangle \in \leq$ hat sich in der Mathematik die Schreibweise $x \leq y$ eingebürgert.

Definition 1 Eine Relation $R \subseteq M \times M$ ist *reflexiv* auf der Menge M falls gilt:

$$\forall x \in M\colon \langle x, x\rangle \in R.$$

Satz 2 Eine Relation $R \subseteq M \times M$ ist genau dann reflexiv, wenn $\mathrm{id}_M \subseteq R$ gilt.

Beweis: Es gilt

	$\mathrm{id}_M \subseteq R$
g.d.w.	$\{\langle x, x\rangle \mid x \in M\} \subseteq R$
g.d.w.	$\forall x \in M : \langle x, x\rangle \in R$
g.d.w.	R reflexiv

□

Definition 3 Eine Relation $R \subseteq M \times M$ ist *symmetrisch* falls gilt:

$$\forall x, y \in M\colon \big(\langle x, y\rangle \in R \rightarrow \langle y, x\rangle \in R\big).$$

Satz 4 Eine Relation $R \subseteq M \times M$ ist genau dann symmetrisch, wenn $R^{-1} \subseteq R$ gilt.

Beweis: Die Äquivalenz der beiden Bedingungen wird offensichtlich, wenn wir die Inklusions-Bedingung $R^{-1} \subseteq R$ expandieren, indem wir die Gleichungen

$$R^{-1} = \big\{\langle y, x\rangle \mid \langle x, y\rangle \in R\big\} \quad \text{und} \quad R = \big\{\langle x, y\rangle \mid \langle x, y\rangle \in R\big\}$$

berücksichtigen, denn dann hat die Inklusions-Bedingung die Form

$$\big\{\langle y, x\rangle \mid \langle x, y\rangle \in R\big\} \subseteq \big\{\langle x, y\rangle \mid \langle x, y\rangle \in R\big\}.$$

Nach der Definition der Teilmengen-Beziehung ist diese Bedingung gleichwertig zu der Formel

$$\forall x, y \in M\colon \big(\langle x, y\rangle \in R \rightarrow \langle y, x\rangle \in R\big).$$ □

Definition 5 Eine Relation $R \subseteq M \times M$ ist *anti-symmetrisch* falls gilt:

$$\forall x, y \in M\colon \big(\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \rightarrow x = y\big).$$

Satz 6 Eine Relation $R \subseteq M \times M$ ist genau dann anti-symmetrisch, wenn $R \cap R^{-1} \subseteq \mathrm{id}_M$ gilt.

Beweis: Wir nehmen zunächst an, dass R anti-symmetrisch ist und folglich

$$\forall x, y \in M : \langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \rightarrow x = y$$

gilt und zeigen, dass aus dieser Voraussetzung die Inklusions-Beziehung $R \cap R^{-1} \subseteq \mathrm{id}_M$ folgt. Sei also $\langle x, y\rangle \in R \cap R^{-1}$. Dann gilt einerseits $\langle x, y\rangle \in R$ und andererseits folgt aus $\langle x, y\rangle \in R^{-1}$, dass auch $\langle y, x\rangle \in R$ ist. Dann folgt aber aus der Voraussetzung sofort $x = y$ und das impliziert $\langle x, y\rangle \in \mathrm{id}_M$, womit $R \cap R^{-1} \subseteq \mathrm{id}_M$ gezeigt ist.

Wir nehmen nun an, dass $R \cap R^{-1} \subseteq \mathrm{id}_M$ gilt und zeigen, dass daraus die Gültigkeit von

$$\forall x, y \in M : \langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \rightarrow x = y$$

folgt. Seien also $x, y \in M$ und es gelte $\langle x, y\rangle \in R$ und $\langle y, x\rangle \in R$. Wir müssen zeigen, dass daraus $x = y$ folgt. Aus $\langle y, x\rangle \in R$ folgt $\langle x, y\rangle \in R^{-1}$. Also gilt $\langle x, y\rangle \in R \cap R^{-1}$. Aus der Inklusions-Beziehung $R \cap R^{-1} \subseteq \mathrm{id}_M$ folgt dann $\langle x, y\rangle \in \mathrm{id}_M$ und daraus folgt sofort $x = y$. □

Definition 7 Eine Relation $R \subseteq M \times M$ ist *transitiv* falls gilt:

$$\forall x, y, z \in M : \langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \in R.$$

Satz 8 Eine Relation $R \subseteq M \times M$ ist genau dann transitiv, wenn $R \circ R \subseteq R$ ist.

Beweis: Wir nehmen zunächst an, dass

$$\forall x, y, z \in M : \langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \in R$$

gilt und zeigen, dass daraus $R \circ R \subseteq R$ folgt. Sei also $\langle x, z\rangle \in R \circ R$. Nach Definition des relationalen Produkts gibt es dann ein y, so dass $\langle x, y\rangle \in R$ und $\langle y, z\rangle \in R$ gilt. Nach Voraussetzung gilt jetzt $\langle x, z\rangle \in R$ und das war zu zeigen.

Wir nehmen nun an, dass die Inklusion $R \circ R \subseteq R$ gilt und zeigen, dass daraus

$$\forall x, y, z \in M : \langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \in R$$

folgt. Seien also $x, y, z \in M$ mit $\langle x, y\rangle \in R$ und $\langle y, z\rangle \in R$ gegeben. Nach Definition des relationalen Produkts gilt dann $\langle x, z\rangle \in R \circ R$ und aus der Voraussetzung $R \circ R \subseteq R$ folgt $\langle x, z\rangle \in R$. □

Beispiele: In den ersten beiden Beispielen sei $M = \{1, 2, 3\}$.

1. $R_1 = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$.

   R_1 ist reflexiv, symmetrisch, anti-symmetrisch und transitiv.

2. $R_2 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle\}$.

   R_2 ist nicht reflexiv, da $\langle 1, 1\rangle \notin R_2$. R_2 ist symmetrisch. R_2 ist nicht anti-symmetrisch, denn aus $\langle 1, 2\rangle \in R_2$ und $\langle 2, 1\rangle \in R_2$ müßte $2 = 1$ folgen. Schließlich ist R_2 auch nicht transitiv, denn aus $\langle 1, 2\rangle \in R_2$ und $\langle 2, 1\rangle \in R_2$ müßte $\langle 1, 1\rangle \in R_2$ folgen.

   In den beiden folgenden Beispielen sei $M = \mathbb{N}$.

3. $R_3 := \{\langle n, m\rangle \in \mathbb{N}^2 \mid n \leq m\}$.

   R_3 ist reflexiv, denn für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt $n \leq n$. R_3 ist nicht symmetrisch, denn beispielsweise gilt $1 \leq 2$, aber es gilt nicht $2 \leq 1$. Allerdings ist R_3 anti-symmetrisch, denn wenn $n \leq m$ und $m \leq n$ gilt, so muß schon $m = n$ gelten. Schließlich ist R_3 auch transitiv, denn aus $k \leq m$ und $m \leq n$ folgt natürlich $k \leq n$.

4. $R_4 := \{\langle m, n\rangle \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} : m \cdot k = n\}$

   Für zwei positive Zahlen m und n gilt $\langle m, n\rangle \in R_4$ genau dann, wenn m ein Teiler von n ist. Damit ist klar, dass R_4 reflexiv ist, denn jede Zahl teilt sich selbst. Natürlich ist R_4 nicht symmetrisch, denn 1 ist ein Teiler von 2 aber nicht umgekehrt. Dafür ist R_4 aber antisymmetrisch, denn wenn sowohl m ein Teiler von n ist und auch n ein Teiler vom m, so muß $m = n$ gelten. Schließlich ist R_4 auch transitiv: Ist m ein Teiler von n und n ein Teiler von o, so ist natürlich m ebenfalls ein Teiler von o.

Ist R eine Relation auf M, die nicht transitiv ist, so können wir R zu einer transitiven Relation erweitern. Dazu definieren wir für alle $n \in \mathbb{N}$ die Potenzen R^n durch Induktion über n.

1. Induktions-Anfang: $n = 0$. Wir setzen
   $$R^0 := \mathrm{id}_M$$
2. Induktions-Schritt: $n \to n+1$. Nach Induktions-Voraussetzung ist R^n bereits definiert. Daher können wir R^{n+1} definieren als
   $$R^{n+1} = R \circ R^n.$$

Wir benötigen später das folgende Potenz-Gesetz: Für beliebige natürliche Zahlen $k, l \in \mathbb{N}$ gilt:

$$R^k \circ R^l = R^{k+l}.$$

Beweis: Wir führen den Beweis durch Induktion nach k.

I.A.: $k = 0$. Es gilt

$$R^0 \circ R^l = id_M \circ R^l = R^l = R^{0+l}.$$

I.S.: $k \mapsto k + 1$. Es gilt

$$\begin{array}{lcll} R^{k+1} \circ R^l & = & (R \circ R^k) \circ R^l & \text{nach Def. von } R^{n+1} \\ & = & R \circ (R^k \circ R^l) & \text{aufgrund des Assoziativ-Gesetzes für } \circ \\ & = & R \circ R^{k+l} & \text{nach Induktions-Voraussetzung} \\ & = & R^{(k+l)+1} & \text{nach Def. von } R^{n+1} \\ & = & R^{(k+1)+l}. & \end{array}$$

□

Wir definieren den *transitiven Abschluß* von R als die Menge

$$R^+ := \bigcup_{n=1}^{\infty} R^n.$$

Dabei ist für eine Folge $(A_n)_n$ von Mengen der Ausdruck $\bigcup_{i=1}^{\infty} A_n$ wie folgt definiert:

$$\bigcup_{i=1}^{\infty} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots.$$

Satz 9 Es sei M eine Menge und $R \subseteq M \times M$ eine binäre Relation auf M. Dann hat die oben definierte Relation R^+ die folgenden Eigenschaften:

1. R^+ ist transitiv.
2. R^+ ist die bezüglich der Inklusions-Ordnung $\subseteq$ kleinste Relation T auf M, die einerseits transitiv ist und andererseits die Relation R enthält. Anders ausgedrückt: Ist T ein transitive Relation auf M mit $R \subseteq T$, so muß $R^+ \subseteq T$ gelten.

Beweis:

1. Wir zeigen zunächst, dass R^+ transitiv ist. Dazu müssen wir die Gültigkeit der Formel

   $$\forall x, y, z : \langle x, y\rangle \in R^+ \wedge \langle y, z\rangle \in R^+ \rightarrow \langle x, z\rangle \in R^+$$

   nachweisen. Wir nehmen also an, dass $\langle x, y\rangle \in R^+$ und $\langle y, z\rangle \in R^+$ gilt und zeigen, dass aus dieser Voraussetzung auf $\langle x, z\rangle \in R^+$ geschlossen werden kann. Nach Definition von R^+ haben wir

   $$\langle x, y\rangle \in \bigcup_{n=1}^{\infty} R^n \quad \text{und} \quad \langle y, z\rangle \in \bigcup_{n=1}^{\infty} R^n.$$

   Nach der Definition der Menge $\bigcup_{n=1}^{\infty} R^n$ gibt es dann natürliche Zahlen $k, l \in \mathbb{N}$, so dass

   $$\langle x, y\rangle \in R^k \quad \text{und} \quad \langle y, z\rangle \in R^l$$

   gilt. Aus der Definition des relationalen Produktes folgt nun

   $$\langle x, z\rangle \in R^k \circ R^l.$$

   Aufgrund des Potenz-Gesetzes für das relationale Produkt gilt

   $$R^k \circ R^l = R^{k+l}.$$

   Also haben wir $\langle x, z\rangle \in R^{k+l}$ und daraus folgt sofort

   $$\langle x, z\rangle \in \bigcup_{n=1}^{\infty} R^n.$$

   Damit gilt $\langle x, z\rangle \in R^+$ und das war zu zeigen. □

2. Um zu zeigen, dass R^+ die kleinste Relation ist, die einerseits transitiv ist und andererseits R enthält, nehmen wir an, dass T eine transitive Relation ist, für die $R \subseteq T$ gilt. Wir müssen dann zeigen, dass $R^+ \subseteq T$ gilt. Wir zeigen zunächst durch vollständige Induktion über $n \in \mathbb{N}$, dass für alle positiven natürlichen Zahlen $n \in \mathbb{N}$ die folgende Inklusion gilt:

   $$R^n \subseteq T.$$

   I.A.: $n = 1$. Dann ist $R^1 \subseteq T$ zu zeigen. Wegen $R^1 = R \circ R^0 = R \circ \mathrm{id}_M = R$ folgt dies aber unmittelbar aus der Voraussetzung $R \subseteq T$.

   I.S.: $n \mapsto n + 1$. Nach Induktions-Voraussetzung wissen wir

   $$R^n \subseteq T.$$

   Wir multiplizieren diese Inklusion auf beiden Seiten von links relational mit R und haben dann

   $$R^{n+1} = R \circ R^n \subseteq R \circ T.$$

   Multiplizieren wir die Voraussetzung $R \subseteq T$ von rechts relational mit T, so finden wir

   $$R \circ T \subseteq T \circ T.$$

   Weil T transitiv ist, gilt

   $$T \circ T \subseteq T.$$

Insgesamt haben wir also die folgende Kette von Inklusionen

$$R^{n+1} \subseteq R \circ T \subseteq T \circ T \subseteq T.$$

Damit folgt $R^{n+1} \subseteq T$ und der Induktions-Beweis ist abgeschlossen.

Wir zeigen nun, dass $R^+ \subseteq T$ ist. Sei $\langle x, y\rangle \in R^+$. Nach Definition von R^+ muss es dann eine positive natürliche Zahl n geben, so dass $\langle x, y\rangle \in R^n$ ist. Wegen $R^n \subseteq T$ folgt daraus aber $\langle x, y\rangle \in T$ und damit ist auch der zweite Teil des Beweises abgeschlossen. □

Beispiel: Es sei *Mensch* die Menge alle Menschen, die jemals gelebt haben. Wir definieren die Relation *Eltern* auf M indem wir setzen

$$\mathit{Eltern} := \{\langle x, y\rangle \in \mathit{Mensch}^2 \mid x \text{ ist Vater von } y \text{ oder } x \text{ ist Mutter von } y\}$$

Dann besteht der transitive Abschluß der Relation *Eltern* aus allen Paaren $\langle x, y\rangle$, für die x ein Vorfahre von y ist:

$$\mathit{Eltern}^+ = \{\langle x, y\rangle \in \mathit{Mensch}^2 \mid x \text{ ist Vorfahre von } y\}.$$

Beispiel: Es sei F die Menge aller Flughäfen. Wir definieren auf der Menge F eine Relation D durch

$$D := \{\langle x, y\rangle \in F \times F \mid \text{Es gibt einen Direktflug von } x \text{ nach } y\}.$$

D bezeichnet also die direkten Verbindungen. Die Relation D^2 ist dann definiert als

$$D^2 = \{\langle x, z\rangle \in F \times F \mid \exists z \in F : \langle x, y\rangle \in D \wedge \langle y, z\rangle \in D\}.$$

Das sind aber gerade die Paare $\langle x, z\rangle$, für die es einen Luftweg von x nach z gibt, der genau einen Zwischenstop enthält. Entsprechend enthält D^3 die Paare $\langle x, z\rangle$, für die man mit zwei Zwischenstops von x nach y kommt und allgemein enthält D^k die Paare $\langle x, z\rangle$, für die man mit $k-1$ Zwischenstops von dem Flughafen x zu dem Flughafen z kommt. Der transitive Abschluß von D enthält dann alle Paare $\langle x, y\rangle$, für die es überhaupt eine Möglichkeit gibt, auf dem Luftweg von x nach y zu kommen.

Aufgabe 3: Auf der Menge $\mathbb{N}$ der natürlichen Zahlen wird die Relation R wie folgt definiert:

$$R = \{\langle k, k+1\rangle \mid k \in \mathbb{N}\}.$$

Berechnen Sie die folgenden Relationen:

1. R^2,
2. R^3,
3. R^n für beliebige $n \in \mathbb{N}$ mit $n \geq 1$,
4. R^+.

3.15 Äquivalenz-Relationen

Definition 10 Eine Relation $R \subseteq M \times M$ ist eine *Äquivalenz-Relation* auf M genau dann, wenn folgende Bedingungen erfüllt sind:

1. R ist reflexiv auf M,
2. R ist symmetrisch und
3. R ist transitiv.

Der Begriff der Äquivalenz-Relationen verallgemeinert den Begriff der Gleichheit, denn ein triviales Beispiel für eine Äquivalenz-Relation auf M ist die Relation id_M. Als nicht-triviales Beispiel betrachten wir die Menge $\mathbb{Z}$ der ganzen Zahlen zusammen mit der Relation $\approx_n$, die wir für natürliche Zahlen $n \neq 0$ wie folgt definieren:

$$\approx_n := \{\langle x, y\rangle \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}\colon k \cdot n = x - y\}$$

Für zwei Zahlen $x, y \in \mathbb{Z}$ gilt also $x \approx_n y$ genau dann, wenn x und y beim Teilen durch n den gleichen Rest ergeben. Wir zeigen, dass die Relation $\approx_n$ für $n \neq 0$ eine Äquivalenz-Relation auf $\mathbb{Z}$ definiert.

1. Um zu zeigen, dass $\approx_n$ reflexiv ist müssen wir nachweisen, dass für alle $x \in \mathbb{Z}$ gilt $\langle x, x\rangle \in \approx_n$. Nach Definition von $\approx_n$ ist dies äquivalent zu

   $$\langle x, x\rangle \in \big\{\langle x, y\rangle \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z} : k \cdot n = x - y\big\}.$$

   Dies ist offenbar gleichbedeutend mit

   $$\exists k \in \mathbb{Z} : k \cdot n = x - x.$$

   Offenbar erfüllt $k = 0$ diese Gleichung, denn es gilt:

   $$0 \cdot n = 0 = x - x.$$

   Damit ist die Reflexivität nachgewiesen.

2. Um die Symmetrie von $\approx_n$ nachzuweisen nehmen wir an, dass $\langle x, y\rangle \in \approx_n$ ist. Dann gibt es also ein $k \in \mathbb{Z}$, so dass

   $$k \cdot n = x - y$$

   gilt. Daraus folgt sofort

   $$(-k) \cdot n = y - x.$$

   Das zeigt aber, dass $\langle y, x\rangle \in \approx_n$ ist und damit ist die Symmetrie nachgewiesen.

3. Zum Nachweis der Transitivität von $\approx$ nehmen wir an, dass sowohl $\langle x, y\rangle \in \approx_n$ als auch $\langle y, z\rangle \in \approx_n$ gelten. Dann gibt es also $k_1, k_2 \in \mathbb{Z}$ so dass

   $$k_1 \cdot n = x - y \quad \text{und} \quad k_2 \cdot n = y - z$$

   gelten. Addieren wir diese beiden Gleichungen, so sehen wir

   $$(k_1 + k_2) \cdot n = x - z.$$

   Mit $k_3 := k_1 + k_2$ gilt also $k_3 \cdot n = x - z$ und damit haben wir $\langle x, z\rangle \in \approx_n$ nachgewiesen und die Transitivität von $\approx_n$ gezeigt. □

Aufgabe 4: Beweisen Sie, dass für alle ganzen Zahlen x und y

$$x \approx_n y \;\leftrightarrow\; x \,\%\, n = y \,\%\, n$$

gilt.

Satz 11 Es seien M und N Mengen und

$$f : M \to N$$

sei eine Funktion. Definieren wir die Relation $R_f \subseteq M \times M$ als

$$R_f := \big\{\langle x, y\rangle \in M \times M \mid f(x) = f(y)\big\},$$

so ist R_f eine Äquivalenz-Relation.

Beweis: Wir weisen Reflexivität, Symmetrie und Transitivität von R_f nach:

1. R_f ist reflexiv, denn es gilt

   $$\forall x \in M : f(x) = f(x).$$

   Daraus folgt sofort

   $$\forall x \in M : \langle x, x \rangle \in R_f.$$

2. Um die Symmetrie von R_f nachzuweisen, müssen wir

   $$\forall x, y \in M : (\langle x, y \rangle \in R_f \rightarrow \langle y, x \rangle \in R_f)$$

   zeigen. Sei also $\langle x, y \rangle \in R_f$. Dann gilt nach Definition von R_f

   $$f(x) = f(y).$$

   Daraus folgt sofort

   $$f(y) = f(x)$$

   und nach Definition von R_f ist das äquivalent zu

   $$\langle y, x \rangle \in R_f.$$

3. Um die Transitivität von R_f nachzuweisen, müssen wir

   $$\forall x, y, z \in M : \big(\langle x, y \rangle \in R_f \wedge \langle y, z \rangle \in R_f \rightarrow \langle x, z \rangle \in R_f\big)$$

   zeigen. Gelte also

   $$\langle x, y \rangle \in R_f \wedge \langle y, z \rangle \in R_f.$$

   Nach Definition von R_f heißt das

   $$f(x) = f(y) \wedge f(y) = f(z).$$

   Daraus folgt sofort

   $$f(x) = f(z).$$

   Nach Definition der Relation R_f haben wir also

   $$\langle x, z \rangle \in R_f.$$ □

Bemerkung: Ist $f : M \rightarrow N$ eine Funktion und gilt

$$R_f = \big\{\langle x, y \rangle \in M \times M \mid f(x) = f(y)\big\}$$

so sagen wir, dass R_f die von f *auf* M *erzeugte* Äquivalenz-Relation ist. Wir werden später sehen, dass es zu jeder Äquivalenz-Relation eine Funktion gibt, die diese Äquivalenz-Relation erzeugt.

Beispiel: Die Äquivalenz-Relation $\approx_n$ wird von der Funktion

$$x \mapsto x \,\%\, n$$

erzeugt, denn wir haben gezeigt, dass für alle $x, y \in \mathbb{Z}$ gilt:

$$x \approx_n y \;\leftrightarrow\; x \,\%\, n = y \,\%\, n.$$

Beispiel: Es sei M die Menge aller Menschen und S sei die Menge aller Staaten. Nehmen wir zur Vereinfachung an, dass jeder Mensch genau eine Staatsbürgerschaft hat, so können wir eine Funktion

$$sb : M \to S$$

defineren, die jedem Menschen x seine Staatsbürgerschaft $sb(x)$ zuordnet. Bei der durch diese Funktion definierten Äquivalenz-Relation sind dann alle die Menschen äquivalent, welche die selbe Staatsbürgerschaft haben.

Definition 12 (Äquivalenz-Klasse) Ist R eine Äquivalenz-Relation auf M, so definieren wir für alle $x \in M$ die Menge $[x]_R$ durch

$$[x]_R := \big\{y \in M \mid x\,R\,y\big\}. \qquad \text{(Wir schreiben hier } xRy \text{ als Abkürzung für } \langle x, y\rangle \in R.\text{)}$$

Die Menge $[x]_R$ bezeichnen wir als die von x erzeugte *Äquivalenz-Klasse*.

Satz 13 (Charakterisierung der Äquivalenz-Klassen) Ist $R \subseteq M \times M$ eine Äquivalenz-Relation, so gilt:

1. $\forall x \in M : x \in [x]_R$,
2. $\forall x, y \in M : \big(x\,R\,y \to [x]_R = [y]_R\big)$,
3. $\forall x, y \in M : \big(\neg x\,R\,y \to [x]_R \cap [y]_R = \emptyset\big)$.

Bemerkung: Da für $x, y \in M$ entweder $x\,R\,y$ oder $\neg(x\,R\,y)$ gilt, zeigen die letzten beiden Eigenschaften, dass zwei Äquivalenz-Klassen entweder gleich oder disjunkt sind:

$$\forall x, y \in M : \big([x]_R = [y]_R \vee [x]_R \cap [y]_R = \emptyset\big).$$

Beweis: Wir beweisen die Behauptungen in der selben Reihenefolge wie oben angegeben.

1. Wir haben $x \in [x]_R$ genau dann, wenn $x \in \big\{y \in M \mid x\,R\,y\big\}$ gilt und letzteres ist äquivalent zu $x\,R\,x$. Nun folgt $x\,R\,x$ unmittelbar aus der Reflexivität der Äquivalenz-Relation.

2. Sei $x\,R\,y$. Um $[x]_R = [y]_R$ nachzuweisen zeigen wir $[x]_R \subseteq [y]_R$ und $[y]_R \subseteq [x]_R$.

   (a) Zeige $[x]_R \subseteq [y]_R$:
   Sei $u \in [x]_R$. Dann gilt $x\,R\,u$. Aus der Voraussetzung $x\,R\,y$ folgt wegen der Symmetrie der Relation R, dass auch $y\,R\,x$ gilt. Aus $y\,R\,x$ und $x\,R\,u$ folgt wegen der Transitivität der Relation R, dass $y\,R\,u$ gilt. Nach der Definition der Menge $[y]_R$ folgt damit $u \in [y]_R$. Damit ist $[x]_R \subseteq [y]_R$ nachgewiesen.

   (b) Zeige $[y]_R \subseteq [x]_R$:
   Um $[y]_R \subseteq [x]_R$ zu zeigen nehmen wir $u \in [y]_R$ an. Dann gilt $y\,R\,u$. Aus der Voraussetzung $x\,R\,y$ und $y\,R\,u$ folgt wegen der Transitivität der Relation R sofort $x\,R\,u$. Dann gilt aber $u \in [x]_R$ und damit ist auch die Inklusion $[y]_R \subseteq [x]_R$ nachgewiesen.

3. Sei nun $\neg(x\,R\,y)$ vorausgesetzt. Um nachzuweisen, dass $[x]_R \cap [y]_R = \emptyset$ ist nehmen wir an, dass es ein $z \in [x]_R \cap [y]_R$ gibt. Aus dieser Annahme werden wir einen Widerspruch zu der Voraussetzung $\neg(x\,R\,y)$ herleiten. Sei also $z \in [x]_R$ und $z \in [y]_R$. Nach Definition der Äquivalenz-Klassen $[x]_R$ und $[y]_R$ gilt dann

   $$x\,R\,z \quad \text{und} \quad y\,R\,z.$$

   Aufgrund der Symmetrie von R können wir $y\,R\,z$ umdrehen und haben dann

   $$x\,R\,z \quad \text{und} \quad z\,R\,y.$$

Aus der Transitivität der Äquivalenz-Relation R folgt jetzt $x\,R\,y$. Dies steht aber im Widerspruch zu der Voraussetzung $\neg(x\,R\,y)$. Damit ist die Annahme, dass es ein $z \in [x]_R \cap [y]_R$ gibt, widerlegt. Folglich ist die Menge $[x]_R \cap [y]_R$ leer. □

Bemerkung: Die Aussagen 2. und 3. lassen sich prägnant zu einer Aussage zusammen fassen: Falls $R \subseteq M \times M$ eine Äquivalenz-Relation ist, dann gilt

$$\langle x, y\rangle \in R \;\leftrightarrow\; [x]_R = [y]_R.$$

Bemerkung: Ist $R \subseteq M \times M$ eine Äquivalenz-Relation auf M, so können wir eine Funktion

$$f_R : M \to 2^M$$

durch die Festlegung

$$f_R(x) := [x]_R = \big\{y \in M | xRy\big\}$$

definieren. Der letzte Satz zeigt dann, dass die Funktion f_R die Äquivalenz-Relation R erzeugt, denn es gilt

$$\begin{aligned} R_{f_R} &= \big\{\langle x, y\rangle \in M \times M \mid f_R(x) = f_R(y)\big\} \\ &= \big\{\langle x, y\rangle \in M \times M \mid [x]_R = [y]_R\big\} \\ &= \big\{\langle x, y\rangle \in M \times M \mid \langle x, y\rangle \in R\big\} \\ &= R, \end{aligned}$$

denn wir haben gerade gesehen, dass $\langle x, y\rangle \in R$ genau dann gilt, wenn $[x]_R = [y]_R$ gilt.

Definition 14 (Quotienten-Raum) Ist M eine Menge und R eine Äquivalenz-Relation auf M so definieren wir die Menge M/R (lese: M *modulo* R) als die Menge der von R auf M erzeugten Äquivalenz-Klassen:

$$M/R := \big\{[x]_R \mid x \in M\big\}.$$

Die Menge M/R der von R erzeugten Äquivalenz-Klassen nennen wir den *Quotienten-Raum* vom M über R.

Beispiel: Setzen wir das letzte Beispiel fort, in dem alle die Menschen äquivalent waren, die die selbe Staatsbürgerschaft haben, so finden wir, dass die Äquivalenz-Klassen, die von dieser Äquivalenz-Relation erzeugt werden, gerade aus den Menschen besteht, die die selbe Staatsbürgerschaft besitzen.

Definition 15 (Partition) Ist $\mathcal{P} \subseteq 2^M$ eine Menge von Teilmengen von M, so sagen wir, dass $\mathcal{P}$ eine *Partition* von M ist, falls $\mathcal{P}$ folgende Eigenschaften hat:

1. *Vollständigkeits-Eigenschaft*

   $$\forall x \in M : \exists K \in \mathcal{P} : x \in K,$$

   jedes Element aus M findet sich in einer Menge aus $\mathcal{P}$ wieder.

2. *Separations-Eigenschaft*

   $$\forall K, L \in \mathcal{P} : K \cap L = \emptyset \vee K = L,$$

   zwei Mengen aus $\mathcal{P}$ sind entweder disjunkt oder identisch.

Gelegentlich wird eine Partition einer Menge M auch als *Zerlegung* von M bezeichnet.

Bemerkung: Der letzte Satz hat gezeigt, dass für jede Äquivalenz-Relation R auf einer Menge M der Quotienten-Raum

$$M/R = \big\{[x]_R \mid x \in M\big\}$$

eine Partition der Menge M darstellt. Der nächste Satz zeigt, dass auch die Umkehrung gilt, denn aus jeder Partition einer Menge läßt sich eine Äquivalenz-Relation erzeugen.

Satz 16 Es sei M eine Menge und $\mathcal{P} \subseteq 2^M$ eine Partition von M. Definieren wir die Relation R durch

$$R := \big\{ \langle x, y \rangle \in M \times M \mid \exists K \in \mathcal{P} : \big(x \in K \wedge y \in K\big) \big\},$$

so ist R eine Äquivalenz-Relation auf M.

Beweis: Wir haben zu zeigen dass die Relation R reflexiv, symmetrisch und transitiv ist.

1. Reflexivität: Zu zeigen ist

   $$\forall x \in M : x \mathrel{R} x.$$

   Das ist nach Definition der Relation R äquivalent zu der Formel

   $$\forall x \in M : \exists K \in \mathcal{P} : \big(x \in K \wedge x \in K\big)$$

   Das können wir sofort zu der Formel

   $$\forall x \in M : \exists K \in \mathcal{P} : x \in K$$

   vereinfachen. Diese Formel ist nichts anderes als die Vollständigkeit der Partition $\mathcal{P}$.

2. Symmetrie: Zu zeigen ist

   $$\forall x, y \in M : \big(x \mathrel{R} y \rightarrow y \mathrel{R} x\big).$$

   Wir nehmen also an, dass

   $$x \mathrel{R} y$$

   gilt. Nach Definition der Relation R ist das äquivalent zu

   $$\exists K \in \mathcal{P} : \big(x \in K \wedge y \in K\big).$$

   Diese Formel ist offenbar äquivalent zu

   $$\exists K \in \mathcal{P} : \big(y \in K \wedge x \in K\big)$$

   und nach Definition der Relation R folgt nun

   $$y \mathrel{R} x.$$

3. Transitivität: Zu zeigen ist

   $$\forall x, y, z \in M : \big(x \mathrel{R} y \wedge y \mathrel{R} z \rightarrow x \mathrel{R} z\big).$$

   Wir nehmen also an, dass

   $$x \mathrel{R} y \wedge y \mathrel{R} z$$

   gilt. Das ist nach Definition der Relation R äquivalent zu

   $$\exists K \in \mathcal{P} : \big(x \in K \wedge y \in K\big) \wedge \exists L \in \mathcal{P} : \big(y \in L \wedge z \in L\big).$$

   Dann gibt es aber offenbar zwei Mengen $K, L \in \mathcal{P}$, so dass

   $$x \in K \wedge y \in K \cap L \wedge z \in L$$

   gilt. Damit ist $K \cap L \neq \emptyset$ und aus der Separations-Eigenschaft der Partition $\mathcal{P}$ folgt

   $$K = L.$$

   Damit haben wir

   $$\exists K \in \mathcal{P} : \big(x \in K \wedge z \in K\big)$$

   gezeigt und nach Definition der Relation R heißt das

$x \, R \, z$. □

3.16 Partielle Ordnung, Totale Ordnung

Eine Relation $R \subseteq M \times M$ ist eine *partielle Ordnung (im Sinne von $\leq$) auf M* genau dann, wenn R

1. reflexiv,
2. anti-symmetrisch und
3. transitiv ist.

Die Relation ist darüber hinaus eine *totale Ordnung auf M*, wenn gilt:

$$\forall x \in M : \forall y \in M : \big(x \, R \, y \vee y \, R \, x\big).$$

Beispiel: Die Teilbarkeitsrelation `div` kann auf den natürlichen Zahlen wie folgt definiert werden

$$\texttt{div} := \big\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : k \cdot x = y\big\}.$$

Wir zeigen dass diese Relation eine partielle Ordnung auf $\mathbb{N}$ ist und weisen dazu Reflexivität, Anti-Symmetrie und Transitivität nach.

1. Reflexivität: Zu zeigen ist

   $$\forall x \in \mathbb{N} : x \, \texttt{div} \, x.$$

   Nach Definition der Relation `div` ist das äquivalent zu

   $$\exists k \in \mathbb{N} : k \cdot x = x$$

   Setzen wir $k = 1$, so gilt sicher $k \cdot x = x$ und damit ist die Reflexivität gezeigt.

2. Anti-Symmetrie: Zu zeigen ist

   $$\forall x, y \in \mathbb{N} : \big(x \, \texttt{div} \, y \wedge y \, \texttt{div} \, x \rightarrow x = y\big)$$

   Wir nehmen also an, dass

   $$x \, \texttt{div} \, y \wedge y \, \texttt{div} \, x$$

   gilt (und werden $x = y$ zeigen). Nach Definition der Relation `div` ist die Annahme äquivalent zu

   $$\big(\exists k_1 \in \mathbb{N} : k_1 \cdot x = y\big) \wedge \big(\exists k_2 \in \mathbb{N} : k_2 \cdot y = x\big)$$

   Also gibt es natürliche Zahlen k_1 und k_2, so dass

   $$k_1 \cdot x = y \wedge k_2 \cdot y = x$$

   gilt. Setzen wir diese Gleichungen ineinander ein, so erhalten wir

   $$k_1 \cdot k_2 \cdot y = y \quad \text{und} \quad k_2 \cdot k_1 \cdot x = x.$$

   Dann muss aber

   $$k_1 \cdot k_2 = 1 \ \vee \ (x = 0 \wedge y = 0)$$

   gelten. Da aus $k_1 \cdot k_2 = 1$ sofort $k_1 = 1$ und $k_2 = 1$ folgt, haben wir wegen der ursprünglichen Gleichungen $k_1 \cdot x = y$ und $k_2 \cdot y = x$ in jedem Fall $x = y$.

3. Transitivität: Zu zeigen ist

   $$\forall x, y, z \in \mathbb{N} : \big(x \, \texttt{div} \, y \wedge y \, \texttt{div} \, z \rightarrow x \, \texttt{div} \, z\big)$$

   Wir nehmen also an, dass

$$x \,\texttt{div}\, y \wedge y \,\texttt{div}\, z$$

gilt (und werden $x \,\texttt{div}\, z$ zeigen). Nach Definition der Relation `div` ist die Annahme äquivalent zu

$$\big(\exists k_1 \in \mathbb{N} : k_1 \cdot x = y\big) \wedge \big(\exists k_2 \in \mathbb{N} : k_2 \cdot y = z\big)$$

Also gibt es natürliche Zahlen k_1 und k_2, so dass

$$k_1 \cdot x = y \wedge k_2 \cdot y = z$$

gilt. Setzen wir die erste Gleichung in die zweite ein, so erhalten wir

$$k_2 \cdot k_1 \cdot x = z.$$

Setzen wir $k_3 := k_2 \cdot k_1$, so haben wir also $k_3 \cdot x = z$ und das zeigt

$$x \,\texttt{div}\, z.$$

Die Relation `div` ist keine totale Ordnung, denn beispielsweise gilt weder $2 \,\texttt{div}\, 3$ noch $3 \,\texttt{div}\, 2$. ◇

Aufgabe 5: Auf der Menge der ganzen Zahlen $\mathbb{N}$ definieren wir die Relation $\leq$ wie folgt:

$$\leq := \big\{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : x + k = y\big\}.$$

Zeigen Sie, dass die Relation $\leq$ eine totale Ordnung auf $\mathbb{N}$ ist. ◇

Aufgabe 6: Auf der Potenz-Menge der natürlichen Zahlen definieren wir die Relation $\subseteq$ als

$$\subseteq := \big\{\langle A, B\rangle \in 2^{\mathbb{N}} \times 2^{\mathbb{N}} \mid \exists C \in 2^{\mathbb{N}} : A \cup C = B\big\}$$

Zeigen Sie, dass die Relation $\subseteq$ auf $2^{\mathbb{N}}$ zwar eine partielle, aber keine totale Ordnung ist. ◇

Wir schließen damit den theoretischen Teil unseres Ausflugs in die Mengenlehre und verweisen für weitere Details auf die Literatur [Lip98].

Kapitel 4

Mathematische Beweise

Mathematik ist eine exakte Wissenschaft. Diese Exaktheit verdankt die Mathematik der Tatsache, dass Behauptungen *bewiesen* werden können. Der Begriff des *Beweises* ist daher für die Mathematik zentral. In diesem Abschnitt gehen wir auf den mathematischen Beweisbegriff ein. Wir beleuchten dabei nur die praktische Seite und stellen verschiedene Methoden des Beweisens vor. Für eine theoretische Analyse des Beweis-Begriffs ist die *Logik* zuständig, die ein Teil der Informatik-Vorlesung ist, wir wenden uns hier den praktischen Beweis-Verfahren zu. Grob können wir zwischen drei Arten von Beweisen unterscheiden:

1. direkten Beweisen,
2. indirekten Beweisen,
3. Beweisen durch vollständige Induktion.

4.1 Direkte Beweise

Direkte Beweise sind die Beweise, die Sie bereits aus der Schule kennen. Die wesentlichen Hilfsmittel eines direkten Beweises sind algebraische Umformungen und Fallunterscheidungen. Wir geben ein einfaches Beispiel für einen direkten Beweis, benötigen dafür aber zunächst noch eine Definition.

Definition 17 ($\mathbb{N}^+$) Die Menge der positiven natürlichen Zahlen wird im Rest dieses Skripts mit $\mathbb{N}^+$ bezeichnet, es gilt also

$$\mathbb{N}^+ := \big\{n \in \mathbb{N} \mid n > 0\big\}.$$

Definition 18 (Pythagoräische Tripel)
Ein Tripel $\langle x, y, z\rangle \in \mathbb{N}^+ \times \mathbb{N}^+ \times \mathbb{N}^+$ heißt *Pythagoräisches Tripel*, falls

$$x^2 + y^2 = z^2$$

gilt. In diesem Fall sind die Zahlen x, y und z nach dem Satz des Pythagoras die Längen eines rechtwinkligen Dreiecks: x und y sind die Längen der Katheten, während z die Länge der Hypothenuse ist.

Beispiel: Das Tripel $\langle 3, 4, 5\rangle$ ist ein pythagoräisches Tripel, denn es gilt

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2.$$

Satz 19 Es seien u und v positive natürliche Zahlen mit $u > v$. Dann ist

$$\big\langle u^2 - v^2,\ 2 \cdot u \cdot v,\ u^2 + v^2\big\rangle$$

ein pythagoräisches Tripel.

Beweis: Wir müssen zeigen, dass

$$\left(u^2 - v^2\right)^2 + \left(2 \cdot u \cdot v\right)^2 = \left(u^2 + v^2\right)^2 \tag{4.1}$$

gilt. Dazu vereinfachen wir die beiden Seiten dieser Gleichung auf algebraischem Wege. Wir benutzen dabei lediglich die beiden binomischen Formeln $(a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2$ und $(a - b)^2 = a^2 - 2 \cdot a \cdot b + b^2$. Die Rechnung verläuft wie folgt:

$$\begin{aligned}
& \left(u^2 - v^2\right)^2 + \left(2 \cdot u \cdot v\right)^2 \\
= \;& u^4 - 2 \cdot u^2 \cdot v^2 + v^4 + 4 \cdot u^2 \cdot v^2 \\
= \;& u^4 + 2 \cdot u^2 \cdot v^2 + v^4 \\
= \;& \left(u^2 + v^2\right)^2
\end{aligned}$$

Damit haben wir die linke Seite der Gleichung (4.1) in die rechte Seite umgeformt. □

Wir haben in dem Kapitel über Mengenlehre bereits eine ganze Reihe direkter Beweise gesehen. Während der letzte Beweis rein algebraisch war, ist es oft auch nötig, eine Fall-Unterscheidung durchzuführen. Um beispielsweise die Gleichheit zweier Mengen A und B zu zeigen, zeigen wir zunächst, dass $A \subseteq B$ ist und zeigen dann, dass auch $B \subseteq A$ gilt. So hatten beispielsweise wir im letzten Kapitel nachgewiesen, dass für eine Äquivalenz-Relation R aus der Beziehung $\langle x, y \rangle \in R$ die Gleichung $[x]_R = [y]_R$ gefolgert werden kann.

4.2 Indirekte Beweise

Wollen wir eine Aussage A auf indirektem Wege nachweisen, so nehmen wir an, dass A nicht gilt, wir nehmen also an, dass die Aussage $\neg A$ richtig ist. Wir versuchen dann weiter, aus dieser Annahme eine offensichtlich falsche Aussage herzuleiten, beispielsweise die Aussage, dass $1 = 2$ gilt. Wenn dies gelingt, dann können wir rückwärts schließen, dass die Annahme $\neg A$ falsch sein muss und dass folglich die Aussage A wahr ist. Wir geben einige Beispiele für indirekte Beweise.

Bevor wir das erste Beispiel präsentieren können, wiederholen wir den Begriff der *geraden* und *ungeraden* Zahlen. Eine natürliche Zahl n ist gerade, wenn Sie durch 2 teilbar ist. Eine solche Zahl läßt sich also immer in der Form $n = 2 \cdot k$ mit $k \in \mathbb{N}$ schreiben. Eine natürliche Zahl n ist ungerade, wenn sie nicht durch 2 teilbar ist. Eine ungerade Zahl hat bei Division durch 2 also den Rest 1 und läßt sich damit immer in der Form $2 \cdot k + 1$ darstellen.

Lemma 20 Es seien $p \in \mathbb{N}$ und das Quadrat p^2 sei eine gerade Zahl. Dann ist p eine gerade Zahl.

Beweis: Wir nehmen an, dass p ungerade ist. Damit läßt sich p in der Form

$$p = 2 \cdot q + 1 \quad \text{mit} \quad q \in \mathbb{N}$$

schreiben. Bilden wir das Produkt $p^2 = p \cdot p$, so finden wir

$$\begin{aligned}
p \cdot p &= (2 \cdot q + 1) \cdot (2 \cdot q + 1) \\
&= 4 \cdot q^2 + 4 \cdot q + 1 \\
&= 2 \cdot (2 \cdot q^2 + 2 \cdot q) + 1
\end{aligned}$$

Da die Zahl $2 \cdot (2 \cdot q^2 + 2 \cdot q) + 1$ die Form $2 \cdot s + 1$ mit $s = (2 \cdot q^2 + 2 \cdot q)$ hat, handelt es sich um eine ungerade Zahl. Diese Zahl ist aber gleich p^2 und damit haben wir einen Widerspruch zur Voraussetzung erhalten. Dieser Widerspruch zeigt, dass die Annahme, dass p ungerade ist, falsch sein muss. Folglich ist p gerade. □

Satz 21 Die Quadratwurzel aus 2 ist irrational, es gilt $\sqrt{2} \notin \mathbb{Q}$.

Beweis: Wir führen den Beweis indirekt und machen die Annahme, dass $\sqrt{2} \in \mathbb{Q}$ ist. Jede positive rationale Zahl läßt sich in der Form $\frac{p}{q}$ mit $p, q \in \mathbb{Q}$ schreiben. Dabei können wir zusätzlich annehmen, dass p und q keinen von 1 verschiedenen gemeinsamen Teiler haben, denn wenn p und q einen gemeinsamen Teiler $r > 1$ hätten, könnten wir durch r kürzen. Nach unserer Annahme gilt also

$$\sqrt{2} = \frac{p}{q} \quad \text{mit } ggt(p, q) = 1. \tag{4.2}$$

Die Funktion $ggt(p, q)$ berechnet hier den größten gemeinsamen Teiler von p und q. Da p und q keinen echten gemeinsamen Teiler mehr haben, einen eventuellen gemeinsamen Teiler haben wir ja gekürzt, gilt $ggt(p, q) = 1$. Quadrieren wir Gleichung (4.2), so verschwindet die Quadratwurzel auf der linken Seite der Gleichung und wir erhalten die Gleichung

$$2 = \frac{p^2}{q^2}. \tag{4.3}$$

Diese Gleichung multiplizieren wir mit q^2. Das ergibt

$$2 \cdot q^2 = p^2. \tag{4.4}$$

Damit sehen wir, dass 2 ein Teiler von p^2 ist. Damit ist die Zahl $p^2 = p \cdot p$ also eine gerade Zahl. Nach dem eben bewiesenen Lemma muss dann auch die Zahl p gerade sein. Also ist 2 auch ein Teiler von p und damit schreibt sich p in der Form $p = 2 \cdot s$ mit $s \in \mathbb{N}$. Setzen wir die Gleichung $p = 2 \cdot s$ in Gleichung (4.4) ein, so erhalten wir

$$2 \cdot q^2 = (2 \cdot s)^2 = 4 \cdot s^2. \tag{4.5}$$

Diese Gleichung teilen wir durch 2 und haben

$$q^2 = (2 \cdot s)^2 = 2 \cdot s^2. \tag{4.6}$$

Gleichung (4.6) zeigt nun, dass q^2 eine gerade Zahl ist und wieder nach dem Lemma 20 können wir folgern, dass auch q gerade ist. Folglich ist q durch 2 teilbar. Damit sind dann aber p und q nicht teilerfremd und wir haben einen Widerspruch zu der Annahme, dass $\sqrt{2}$ sich als Bruch $\frac{p}{q}$ zweier natürlicher Zahlen p und q darstellen läßt, denn einen solchen Bruch können wir immer so kürzen, dass p und q teilerfremd sind. □

Ein anderes typisches Beispiel für einen indirekten Beweis ist der Nachweis der Nicht-Abzählbarkeit der Menge Potenz-Menge der natürlichen Zahlen.

Definition 22 (Abzählbar) Eine unendliche Menge M heißt *abzählbar unendlich*, wenn eine surjektive Funktion

$$f : \mathbb{N} \to M$$

existiert.

Die Idee bei dieser Definition ist, dass die Menge M in einem gewissen Sinne nicht mehr Elemente hat als die Menge der natürlichen Zahlen, denn die Elemente können ja über die Funktion f aufgezählt werden, wobei wir eventuelle Wiederholung eines Elements zulassen wollen.

Beispiel: Die Menge $\mathbb{Z}$ der ganzen Zahlen ist abzählbar, denn die Funktion

$$f : \mathbb{N} \to \mathbb{Z},$$

die durch die Fallunterscheidung

$$f(n) := \begin{cases} (n-1)/2+1 & \text{falls } n \,\%\, 2 = 1 \\ -n/2 & \text{falls } n \,\%\, 2 = 0 \end{cases}$$

definiert ist, ist surjektiv. Um dies einzusehen, zeigen wir zunächst, dass f wohldefiniert ist. Dazu ist zu zeigen, dass $f(n)$ tatsächlich in jedem Fall eine ganze Zahl ist.

1. $n \,\%\, 2 = 1$: Dann ist n ungerade, also ist $(n-1)$ gerade und die Division $(n-1)/2$ liefert eine ganze Zahl.
2. $n \,\%\, 2 = 0$: In diesem Fall ist n gerade und daher liefert jetzt die Division $n/2$ eine ganze Zahl.

Es bleibt zu zeigen, dass f surjektiv ist. Wir müssen also zeigen, dass es für jedes $z \in \mathbb{Z}$ eine natürliche Zahl n gibt, so dass $f(n) = z$ ist. Wir führen diesen Nachweis mittels einer Fall-Unterscheidung:

1. Fall: $z > 0$.

   Wir definieren $n := 2 \cdot (z-1) + 1$. Wegen $z > 0$ gilt $n \geq 0$ und damit ist n tatsächlich eine natürliche Zahl. Außerdem ist klar, dass n ungerade ist. Daher gilt

   $$f(n) = (n-1)/2 + 1 = \big(\big(2 \cdot (z-1) + 1\big) - 1\big)/2 + 1 = \big(2 \cdot (z-1)/2\big) + 1 = z - 1 + 1 = z.$$

   Also gilt $f(n) = z$.

2. Fall: $z \leq 0$.

   Wir definieren $n := -2 \cdot z$. Wegen $z \leq 0$ ist klar, dass n eine gerade natürliche Zahl ist. Damit haben wir

   $$f(n) = -\big(-2 \cdot z\big)/2 = z.$$

   Also gilt ebenfalls $f(n) = z$.

Damit ist die Sujektivität von f gezeigt und somit ist $\mathbb{Z}$ abzählbar. □

Den Beweis des letzten Satzes haben wir direkt geführt, aber zum Nachweis des nächsten Satzes werden wir einen indirekten Beweis benötigen. Vorab noch eine Definition.

Definition 23 (Überabzählbar)
Eine unendliche Menge heißt *überabzählbar*, wenn sie nicht abzählbar ist.

Satz 24 Die Potenzmenge der Menge der natürlichen Zahlen ist überabzählbar.

Beweis: Wir führen den Beweis indirekt und nehmen an, dass $2^{\mathbb{N}}$ abzählbar ist. Dann gibt es also eine Funktion

$$f : \mathbb{N} \to 2^{\mathbb{N}},$$

die surjektiv ist. Wir definieren nun die Menge C wie folgt:

$$C := \big\{ n \in \mathbb{N} \;\big|\; n \notin f(n) \big\}.$$

Offenbar ist C eine Teilmenge der Menge der natürlichen Zahlen und damit gilt $C \in 2^{\mathbb{N}}$. Da die Funktion f surjektiv ist, gibt es also eine natürliche Zahl n_0, so dass

$$C = f(n_0)$$

gilt. Wir untersuchen nun, ob $n_0 \in C$ gilt. Dazu betrachten wir die folgende Kette von Äquivalenzen:

$$
\begin{aligned}
& n_0 \in C \\
\leftrightarrow \quad & n_0 \in \big\{ n \in \mathbb{N} \;\big|\; n \notin f(n) \big\} \\
\leftrightarrow \quad & n_0 \notin f(n_0) \\
\leftrightarrow \quad & n_0 \notin C
\end{aligned}
$$

Wir haben also

$$n_0 \in C \;\leftrightarrow\; n_0 \notin C \qquad \lightning$$

gezeigt und das ist ein offensichtlicher Widerspruch. □

Bemerkung: Wir haben soeben gezeigt, dass es in gewisser Weise mehr Mengen von natürlichen Zahlen gibt, als es natürliche Zahlen gibt. In ähnlicher Weise kann gezeigt werden, dass die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist.

Aufgabe 7: Zeigen Sie, dass das Intervall

$$[0,1] := \{x \in \mathbb{R} \mid 0 \leq x \wedge x \leq 1\}$$

überabzählbar ist. Nehmen Sie dazu an, dass die Zahlen $x \in [0,1]$ in der Form

$$x = 0, d_1 d_2 d_3 \cdots \qquad \text{mit } d_i \in \{0, \cdots, 9\} \text{ für alle } i \in \mathbb{N}$$

dargestellt sind, es gilt dann also

$$x = \sum_{i=1}^{\infty} d_i \cdot \big(\tfrac{1}{10}\big)^i.$$

Führen Sie den Beweis indirekt und nehmen Sie an, dass es eine surjektive Funktion

$$f : \mathbb{N} \to [0,1]$$

gibt, die die Menge $[0,1]$ aufzählt. Dann gibt es auch eine Funktion

$$g : \mathbb{N} \times \mathbb{N} \to \{0, \cdots, 9\}$$

so dass $g(n,i)$ die i-te Nachkommastelle von $f(n)$ berechnet:

$$f(n) = 0, g(n,1)g(n,2)g(n,3) \cdots.$$

Konstruieren Sie nun mit Hilfe dieser Funktion g eine Zahl $c \in [0,1]$ in der Form

$$c = 0, c_1 c_2 c_3 \cdots$$

so, dass sich ein Widerspruch ergibt. Orientieren Sie sich dabei an der Konstruktion der Menge C im Beweis der Überabzählbarkeit von $2^{\mathbb{N}}$.

4.3 Induktions-Beweise

Die wichtigste Beweismethode in der Informatik ist der Beweis durch vollständige Induktion. Es sei $F(n)$ eine Formel, in der die Variable n vorkommt. Um eine Aussage der Form

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

zu beweisen, können wir wie folgt vorgehen.

1. Zunächst zeigen wir, dass die Aussage für $n = 0$ richtig ist, wir weisen also die Gültigkeit der Formel $F(0)$ nach.

   Dieser Schritt wird als *Induktions-Anfang* bezeichnet.

2. Dann zeigen wir, dass die Formel

   $$\forall n \in \mathbb{N} : \big(F(n) \to F(n+1)\big)$$

gilt, wir zeigen also, dass jedesmal, wenn $F(n)$ gilt, auch $F(n+1)$ richtig sein muss.

Dieser Schritt wird als *Induktions-Schritt* bezeichnet.

Insgesamt können wir dann schließen, dass die Formel $F(n)$ für alle natürlichen Zahlen gilt, denn zunächst wissen wir, dass $F(0)$ gilt, nach dem Induktions-Schritt gilt dann auch $F(1)$, daraus folgt dass auch $F(2)$ gilt, woraus wir auf die Gültigkeit von $F(3)$ schließen können. Durch Fortführung dieser Argumentation schließen wir insgesamt, dass $F(n)$ für jede beliebige Zahl richtig ist. Diese Argumentation ist zunächst informal. Ein exakter Beweis folgt.

Satz 25 Es sei $F(x)$ eine Formel. Dann gilt

$$F(0) \wedge \big(\forall n \in \mathbb{N} : F(n) \to F(n+1)\big) \to \forall n \in \mathbb{N} : F(n).$$

Beweis: Wir nehmen an, dass

$$F(0) \wedge \big(\forall n \in \mathbb{N} : F(n) \to F(n+1)\big)$$

richtig ist und zeigen, dass dann

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

gilt. Den Nachweis dieser Behauptung führen wir indirekt und nehmen an, dass

$$\neg\big(\forall n \in \mathbb{N} : F(n)\big)$$

gilt. Das ist aber äquivalent zu

$$\exists n \in \mathbb{N} : \neg F(n).$$

Wir definieren eine Menge M als die Menge aller der Zahlen, für die $F(n)$ falsch ist:

$$M := \big\{n \in \mathbb{N} \;\big|\; \neg F(n)\big\}.$$

Nach unserer Annahme ist M nicht leer. Dann muss aber M ein kleinstes Element haben. Wir definieren n_0 als das Minimum von M.

$$n_0 := \min(M) = \min\big(\big\{n \in \mathbb{N} \;\big|\; \neg F(n)\big\}\big).$$

Also haben wir $\neg F(n_0)$ und wissen außerdem, dass für alle $n < n_0$ die Formel $F(n)$ gilt, denn sonst wäre n_0 ja nicht das Minimum der Menge M.

Weiter schließen wir dann aus der Tatsache, dass $F(0)$ gilt, dass $n_0 \neq 0$ ist. Aus $n_0 - 1 < n_0$ folgt nun

$$F(n_0 - 1).$$

Wegen $\forall n \in \mathbb{N} : F(n) \to F(n+1)$ können wir dann folgern, dass

$$F((n_0 - 1) + 1)$$

gilt. Also gilt $F(n_0)$ und das ist ein Widerspruch zur Definition von n_0. □

Wir geben nun einige typische Beispiele für Induktions-Beweise.

Satz 26 Es gilt

$$\sum_{i=0}^{n} i = \tfrac{1}{2} \cdot n \cdot (n+1) \quad \text{für alle } n \in \mathbb{N}.$$

Beweis: Wir führen den Beweis durch Induktion nach n.

1. Induktions-Anfang: $n = 0$.

   Wir haben einerseits

   $$\sum_{i=0}^{0} i = 0$$

und andererseits gilt auch

$$\tfrac{1}{2} \cdot 0 \cdot (0+1) = 0.$$

Damit ist die Behauptung für $n = 0$ richtig.

2. Induktions-Schritt: $n \mapsto n+1$.

   Wir können nun voraussetzen, dass

   $$\sum_{i=0}^{n} i = \tfrac{1}{2} \cdot n \cdot (n+1)$$

   für ein gegebenes festes n gilt. Diese Voraussetzung wird als *Induktions-Voraussetzung* bezeichnet. Wir müssen dann nachweisen, dass die Behauptung auch für $n+1$ gilt, zu zeigen ist also

   $$\sum_{i=0}^{n+1} i = \tfrac{1}{2} \cdot (n+1) \cdot \big((n+1)+1\big).$$

   Wir formen beide Seiten dieser Gleichung getrennt um und beginnen mit der linken Seite.

   $$\begin{array}{lll}
   & \sum\limits_{i=0}^{n+1} i & \\
   = & \sum\limits_{i=0}^{n} i + (n+1) & \text{nach Definition der Summe} \\
   = & \tfrac{1}{2} \cdot n \cdot (n+1) + (n+1) & \text{nach Induktions-Voraussetzung} \\
   = & \tfrac{1}{2} \cdot \big(n^2 + n + 2 \cdot (n+1)\big) & \text{Hauptnenner} \\
   = & \tfrac{1}{2} \cdot \big(n^2 + 3 \cdot n + 2\big) &
   \end{array}$$

   Nun formen wir die rechte Seite um:

   $$\begin{array}{ll}
   & \tfrac{1}{2} \cdot (n+1) \cdot \big((n+1)+1\big) \\
   = & \tfrac{1}{2} \cdot (n+1) \cdot (n+2) \\
   = & \tfrac{1}{2} \cdot (n^2 + 2 \cdot n + n + 2) \\
   = & \tfrac{1}{2} \cdot (n^2 + 3 \cdot n + 2)
   \end{array}$$

   Da beide Seiten identisch sind, ist der Beweis erbracht. □

Aufgabe 8: Zeigen Sie, dass

$$\sum_{i=1}^{n} i^2 = \tfrac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1) \quad \text{für alle } n \in \mathbb{N}$$

gilt.

Satz 27 (Mächtigkeit der Potenz-Menge) Es sei M eine endliche Menge. Dann gilt

$$\mathit{card}\big(2^M\big) = 2^{\mathit{card}(M)}.$$

Beweis: Es sei $n := \mathit{card}(M)$. Dann hat M die Form

$$M = \{x_1, x_2, \cdots, x_n\}.$$

Wir zeigen durch Induktion nach n, dass Folgendes gilt:

$$\mathit{card}\big(2^M\big) = 2^n.$$

1. Induktions-Anfang: $n = 0$.

   Dann gilt $M = \{\}$ und für die Potenz-Menge 2^M finden wir

$$2^M = 2^{\{\}} = \big\{\{\}\big\}.$$

Die Potenz-Menge der leeren Menge hat also genau ein Element. Daher gilt

$$\mathit{card}\big(2^{\{\}}\big) = \mathit{card}\big(\big\{\{\}\big\}\big) = 1.$$

Auf der anderen Seite haben wir

$$2^{\mathit{card}(\{\})} = 2^0 = 1.$$

2. Induktions-Schritt: $n \mapsto n+1$.

   Wenn $\mathit{card}(M) = n+1$ ist, dann hat M die Form

   $$M = \{x_1, x_2, \cdots x_n, x_{n+1}\}.$$

   Es gibt zwei verschiedene Arten von Teilmengen von M: Solche, die x_{n+1} enthalten und solche, die x_{n+1} nicht enthalten. Dementsprechend können wir die Potenz-Menge 2^M wie folgt aufteilen:

   $$2^M = \big\{K \in 2^M \;\big|\; x_{n+1} \in K\big\} \cup \big\{K \in 2^M \;\big|\; x_{n+1} \notin K\big\}$$

   Wir bezeichnen die erste dieser Mengen mit A, die zweite nennen wir B:

   $$A := \big\{K \in 2^M \;\big|\; x_{n+1} \in K\big\}, \quad B := \big\{K \in 2^M \;\big|\; x_{n+1} \notin K\big\}.$$

   Offenbar sind die Mengen A und B disjunkt: $A \cap B = \emptyset$. Daher folgt aus der Gleichung

   $$2^M = A \cup B,$$

   dass die Anzahl der Elemente von 2^M gleich der Summe der Anzahl der Elemente in A und der Anzahl der Elemente in B ist:

   $$\mathit{card}\big(2^M\big) = \mathit{card}(A) + \mathit{card}(B).$$

   Die Menge B enthält genau die Teilmengen von M, die x_{n+1} nicht enthalten. Das sind dann aber genau die Teilmengen der Menge $\{x_1, \cdots, x_n\}$, es gilt also

   $$B = 2^{\{x_1, \cdots, x_n\}}.$$

   Nach Induktions-Voraussetzung wissen wir daher, dass

   $$\mathit{card}(B) = \mathit{card}\big(2^{\{x_1, \cdots, x_n\}}\big) \stackrel{IV}{=} 2^{\mathit{card}(\{x_1, \cdots, x_n\})} = 2^n$$

   gilt. Als nächstes zeigen wir, dass die Menge A genau so viele Elemente hat, wie die Menge B. Zu diesem Zweck konstruieren wir eine bijektive Funktion f, die jedem $K \in B$ eindeutig eine Menge $f(K) \in A$ zuordnet:

   $$f : B \to A \quad \text{ist definiert durch} \quad f(K) := K \cup \{x_{n+1}\}.$$

   Die Umkehrfunktion $f^{-1} : A \to B$ kann offenbar durch die Formel

   $$f^{-1}(K) := K \backslash \{x_{n+1}\}$$

   definiert werden. Damit ist aber klar, dass die Mengen A und B gleich viele Elemente haben:

   $$\mathit{card}(A) = \mathit{card}(B).$$

   Insgesamt haben wir jetzt

   $$\begin{aligned}
   \mathit{card}\big(2^M\big) &= \mathit{card}(A) + \mathit{card}(B) \\
   &= \mathit{card}(B) + \mathit{card}(B) \\
   &= 2 \cdot \mathit{card}(B) \\
   &= 2 \cdot 2^n \\
   &= 2^{n+1}.
   \end{aligned}$$

Wir haben also $card\big(2^M\big) = 2^{n+1}$ bewiesen. Damit ist der Induktions-Schritt abgeschlossen und der Beweis der Behauptung ist erbracht. $\square$

Kapitel 5

Gruppen

In diesem Kapitel und dem nächsten Kapitel untersuchen wir algebraische Strukturen wie Gruppen, Ringe und Körper, wobei wir in diesem Kapitel mit den Gruppen beginnen.

5.1 Gruppen

Definition 28 (Gruppe) Ein Tripel $\langle G, e, \circ \rangle$ heißt *Gruppe* falls folgendes gilt:

1. G ist eine Menge.
2. $e \in G$ ist ein Element der Menge G.
3. $\circ$ ist eine binäre Funktion auf der Menge G, es gilt also
   $$\circ : G \times G \to G.$$
   Wir schreiben den Funktions-Wert $\circ(x, y)$ als $x \circ y$ und benutzen $\circ$ also als Infix-Operator.
4. Es gilt
   $$e \circ x = x \quad \text{für alle } x \in G,$$
   das Element e ist also bezüglich der Operation $\circ$ ein *links-neutrales* Element.
5. Für alle $x \in G$ gibt es ein $y \in G$, so dass
   $$y \circ x = e$$
   gilt. Wir sagen, dass y ein zu x bezüglich der Operation $\circ$ *links-inverses* Element ist.
6. Es gilt das folgende *Assoziativ-Gesetz*:
   $$(x \circ y) \circ z = x \circ (y \circ z) \quad \text{für alle } x, y, z \in G.$$

Falls zusätzlich das Kommutativ-Gesetz

$$\forall x, y \in G : x \circ y = y \circ x$$

gilt, dann sagen wir, dass $\langle G, e, \circ \rangle$ eine *kommutative Gruppe* ist.

Beispiele: Bevor wir Sätze über Gruppen beweisen, präsentieren wir zunächst einige Beispiele, an Hand derer klar wird, worum es bei Gruppen überhaupt geht.

1. $\langle \mathbb{Z}, 0, + \rangle$ ist eine kommutative Gruppe, denn es gilt:
   (a) $0 + x = x \quad$ für alle $x \in \mathbb{Z}$.
   (b) $-x + x = 0 \quad$ für alle $x \in \mathbb{Z}$,
   und damit ist die Zahl $-x$ das *Links-Inverse* der Zahl x bezüglich der Addition.

(c) $(x + y) + z = x + (y + z)$ für alle $x, y, z \in \mathbb{Z}$.

(d) $x + y = y + x$ für alle $x, y \in \mathbb{Z}$.

Dieses Beispiel zeigt, dass der Begriff der Gruppe versucht, die Eigenschaften der Addition auf den natürlichen Zahlen zu verallgemeinern.

2. Definieren wir $\mathbb{Q}^+$ als die Menge der positiven rationalen Zahlen, also als

$$\mathbb{Q}^+ := \{q \in \mathbb{Q} \mid q > 0\}$$

und bezeichnen wir mit

$$\cdot : \mathbb{Q}^+ \times \mathbb{Q}^+ \to \mathbb{Q}^+$$

die Multiplikation, so ist die Struktur $\langle \mathbb{Q}, 1, \cdot \rangle$ eine kommutative Gruppe, denn es gilt:

(a) $1 \cdot q = q$ für alle $q \in \mathbb{Q}^+$.

(b) $\frac{1}{q} \cdot q = 1$ für alle $q \in \mathbb{Q}^+$,
und damit ist die Zahl $\frac{1}{q}$ das *Links-Inverse* der Zahl x bezüglich der Multiplikation.

(c) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in \mathbb{Q}^+$.

(d) $x \cdot y = y \cdot x$ für alle $x, y \in \mathbb{Q}^+$.

3. In den letzten beiden Beispielen war die der Gruppe zu Grunde liegende Menge G jedesmal unendlich. Das dies keineswegs immer so ist, zeigt das nächste Beispiel.

Wir definieren die Menge G als

$$G := \{e, a\}$$

und definieren nun auf der Menge G eine Verknüfung

$$\circ : G \times G \to G$$

indem wir definieren:

$$\begin{array}{ll} e \circ e := e, & e \circ a := a, \\ a \circ e := a, & a \circ a := e. \end{array}$$

Dann ist $\langle G, e, \circ \rangle$ eine kommutative Gruppe, denn offenbar gilt für alle $x \in G$, dass $e \circ x = x$ ist und wir finden auch für jedes der beiden Elemente ein links-inverses Element: Das Links-Inverse zu e ist e und das Links-Inverse zu a ist a. Es bleibt das Assoziativ-Gesetz nachzuweisen. Dazu müssen wir die Gleichung

$$(x \circ y) \circ z = x \circ (y \circ z)$$

für alle Werte $x, y, z \in G$ prüfen. Es gibt insgesamt 8 Fälle:

(a) $(e \circ e) \circ e = e \circ e = e$ und $e \circ (e \circ e) = e \circ e = e$. ✓

(b) $(e \circ e) \circ a = e \circ a = a$ und $e \circ (e \circ a) = e \circ a = a$. ✓

(c) $(e \circ a) \circ e = a \circ e = a$ und $e \circ (a \circ e) = e \circ a = a$. ✓

(d) $(e \circ a) \circ a = a \circ a = e$ und $e \circ (a \circ a) = e \circ e = e$. ✓

(e) $(a \circ e) \circ e = a \circ e = a$ und $a \circ (e \circ e) = a \circ e = a$. ✓

(f) $(a \circ e) \circ a = a \circ a = e$ und $a \circ (e \circ a) = a \circ a = e$. ✓

(g) $(a \circ a) \circ e = e \circ e = e$ und $a \circ (a \circ e) = a \circ a = e$. ✓

(h) $(a \circ a) \circ a = e \circ a = a$ und $a \circ (a \circ a) = a \circ e = a$. ✓

Die Tatsache, dass die Verknüfung $\circ$ kommutativ ist, folgt unmittelbar aus der Definition. Wir werden uns im Rahmen der Zahlentheorie noch näher mit endlichen Gruppen auseinander setzen.

Bevor wir weitere Beispiele von Gruppen präsentieren, beweisen wir einige Sätze, die unmittelbar aus der Definition der Gruppen folgen.

Satz 29 (Links-Inverses ist auch Rechts-Inverses)
Ist $\langle G, e, \circ \rangle$ eine Gruppe, ist $a \in G$ ein beliebiges Element aus G und ist b ein Links-Inverses zu a, gilt also

$$b \circ a = e,$$

dann ist b auch ein Rechts-Inverses zu a, es gilt folglich

$$a \circ b = e.$$

Beweis: Zunächst bemerken wir, dass das Element b ebenfalls ein Links-Inverses haben muss. Es gibt also ein $c \in G$, so dass

$$c \circ b = e$$

gilt. Nun haben wir die folgende Kette von Gleichungen:

$$\begin{array}{rcll}
a \circ b & = & e \circ (a \circ b) & \text{denn } e \text{ ist links-neutral,} \\
& = & (c \circ b) \circ (a \circ b) & \text{denn } c \text{ ist links-invers zu } b\text{, also gilt } c \circ b = e, \\
& = & c \circ \big(b \circ (a \circ b)\big) & \text{Assoziativ-Gesetz} \\
& = & c \circ \big((b \circ a) \circ b\big) & \text{Assoziativ-Gesetz} \\
& = & c \circ \big(e \circ b\big) & \text{denn } b \text{ ist links-invers zu } a\text{, also gilt } b \circ a = e, \\
& = & c \circ b & \text{denn } e \text{ ist links-neutral} \\
& = & e & \text{denn } c \text{ ist links-invers zu } b.
\end{array}$$

Insgesamt haben wir also $a \circ b = e$ bewiesen. □

Bemerkung: Da jedes zu einem Element a links-inverse Element b auch rechts-invers ist, sprechen wir im folgenden immer nur noch von einem inversen Element und lassen den Zusatz "*links*" bzw. "*rechts*" weg.

Satz 30 (Links-neutrales Element ist auch rechts-neutrales Element)
Ist $\langle G, e, \circ \rangle$ eine Gruppe, so gilt

$$a \circ e = a \quad \text{für alle } a \in G.$$

Beweis: Es sei $a \in G$ beliebig und b das zu a inverse Element. Dann haben wir die folgende Kette von Gleichungen:

$$\begin{array}{rcll}
a \circ e & = & a \circ (b \circ a) & \text{denn } b \text{ ist invers zu } a, \\
& = & (a \circ b) \circ a & \text{Assoziativ-Gesetz} \\
& = & e \circ a & \text{denn } b \text{ ist invers zu } a, \\
& = & a & \text{denn } e \text{ ist links-neutral.}
\end{array}$$

Wir haben also $a \circ e = a$ gezeigt. □

Bemerkung: Da das links-neutrale Element e einer Gruppe $\langle G, e, \circ \rangle$ auch rechts-neutral ist, sprechen wir im folgenden immer nur noch von einem neutralen Element und lassen den Zusatz "links" bzw. "*recht*" weg.

Satz 31 (Eindeutigkeit des neutralen Elements)
Ist $\langle G, e, \circ \rangle$ eine Gruppe und ist $f \in G$ ein weiteres Element, so dass

$$f \circ x = x \quad \text{für alle } x \in G \text{ gilt,}$$

so folgt schon $f = e$.

Beweis: Wir haben die folgende Kette von Gleichungen:

$$\begin{array}{rcll} f & = & f \circ e & \text{denn } e \text{ ist neutrales Element und damit auch rechts-neutral,} \\ & = & e & \text{denn } f \circ x = x \text{ für alle } x \in G, \text{ also auch für } x = e. \end{array}$$

Also gilt $f = e$ gezeigt. □

Bemerkung: Der letzte Satz zeigt, dass das neutrale Element eindeutig bestimmt ist. Wir sprechen daher in Zukunft immer von *dem* neutralen Element anstatt von *einem* neutralen Element.

Satz 32 (Eindeutigkeit des inversen Elements)
Ist $\langle G, e, \circ \rangle$ eine Gruppe, ist $a \in G$ und sind b, c beide invers zu a, so folgt $b = c$:

$$b \circ a = e \ \wedge \ c \circ a = e \ \rightarrow \ b = c.$$

Beweis: Wir haben die folgende Kette von Gleichungen:

$$\begin{array}{rcll} c & = & c \circ e & \text{denn } e \text{ ist neutrales Element,} \\ & = & c \circ (a \circ b) & \text{denn } b \text{ ist invers zu } a, \\ & = & (c \circ a) \circ b & \text{Assoziativ-Gesetz} \\ & = & e \circ b & \text{denn } c \text{ ist invers zu } a, \\ & = & b & \text{denn } e \text{ ist neutrales Element.} \end{array}$$

Also ist $c = b$ gezeigt. □

Bemerkung: Der letzte Satz zeigt, dass in einer Gruppe $\langle G, e, \circ \rangle$ für ein gegebenes Element a das zugehörige inverse Element eindeutig bestimmt ist. Damit können wir eine Funktion

$$^{-1} : G \rightarrow G$$

definieren, die für alle $a \in G$ das zu a inverse Element berechnet: Es gilt also

$$a^{-1} \circ a = e \quad \text{und} \quad a \circ a^{-1} \quad \text{für alle } a \in G.$$

Bemerkung: Ist $\langle G, e, \circ \rangle$ eine Gruppe und sind die Operation $\circ$ und das neutrale Element e aus dem Zusammenhang klar, so sprechen wir einfach von der Gruppe G, obwohl wir formal korrekt eigentlich von der Gruppe $\langle G, e, \circ \rangle$ sprechen müssten.

Satz 33 ($(a \circ b)^{-1} = b^{-1} \circ a^{-1}$)
Ist $\langle G, e, \circ \rangle$ eine Gruppe und bezeichnen wir das zu x inverse Element mit x^{-1}, so gilt

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad \text{für alle } a, b \in G.$$

Beweis: Wir haben

$$\begin{array}{rcll} (b^{-1} \circ a^{-1}) \circ (a \circ b) & = & b^{-1} \circ \big(a^{-1} \circ (a \circ b)\big) & \text{Assoziativ-Gesetz} \\ & = & b^{-1} \circ \big((a^{-1} \circ a) \circ b\big) & \text{Assoziativ-Gesetz} \\ & = & b^{-1} \circ (e \circ b) & \\ & = & b^{-1} \circ b & \\ & = & e & \end{array}$$

Also gilt $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$ und damit ist gezeigt, dass das Element $(b^{-1} \circ a^{-1})$ zu $a \circ b$ invers ist. Da das inverse Element eindeutig bestimmt ist, folgt

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}. \qquad \square$$

Satz 34 ($(a^{-1})^{-1} = a$) Ist $\langle G, e, \circ \rangle$ eine Gruppe und bezeichnen wir das zu x inverse Element mit x^{-1}, so gilt

$$(a^{-1})^{-1} = a \quad \text{für alle } a \in G.$$

Das inverse Element des zu a inversen Elements ist also wieder a.

Beweis: Wir haben

$$\begin{array}{lcll}
(a^{-1})^{-1} & = & (a^{-1})^{-1} \circ e & e \text{ ist auch rechts-neutral} \\
& = & (a^{-1})^{-1} \circ (a^{-1} \circ a) & \text{denn } a^{-1} \circ a = e \\
& = & \big((a^{-1})^{-1} \circ a^{-1}\big) \circ a & \text{Assoziativ-Gesetz} \\
& = & e \circ a & \text{denn } (a^{-1})^{-1} \text{ ist das Inverse zu } a^{-1} \\
& = & a &
\end{array}$$

Also gilt $(a^{-1})^{-1} = a$. $\square$

Definition 35 (Halb-Gruppe) Eine Paar $\langle G, \circ \rangle$ ist eine *Halb-Gruppe*, falls gilt:

1. G ist eine Menge,
2. $\circ$ ist eine binäre Funktion auf G, es gilt also

   $$\circ : G \times G \to G.$$

   Genau wie bei Gruppen schreiben wir $\circ$ als Infix-Operator.
3. Für den Operator $\circ$ gilt das Assoziativ-Gesetz

   $$(x \circ y) \circ z = x \circ (y \circ z).$$

Ist der Operator $\circ$ aus dem Zusammenhang klar, so sagen wir oft auch, dass G eine Halb-Gruppe ist.

Beispiele:

1. Das Paar $\langle \mathbb{N}, + \rangle$ ist eine Halb-Gruppe.
2. Das Paar $\langle \mathbb{Z}, \cdot \rangle$ ist eine Halb-Gruppe.

Falls G eine Gruppe ist, so lassen sich die Gleichungen

$$a \circ x = b \quad \text{und} \quad y \circ a = b$$

für alle $a, b \in G$ lösen: Durch Einsetzen verifzieren Sie sofort, dass $x := a^{-1} \circ b$ eine Lösung der ersten Gleichung ist, während $y := b \circ a^{-1}$ die zweite Gleichung löst. Interessant ist nun, dass sich dies auch umkehren läßt, denn es gilt der folgende Satz.

Satz 36 Ist $\langle G, \circ \rangle$ eine Halb-Gruppe, in der für alle Werte $a, b \in G$ die beiden Gleichungen

$$a \circ x = b \quad \text{und} \quad y \circ a = b$$

für die Variablen x und y eine Lösung in G haben, dann gibt es ein neutrales Element $e \in G$, so dass $\langle G, e, \circ \rangle$ eine Gruppe ist.

Beweis: Es sei b ein beliebiges Element von G. Nach Voraussetzung hat die Gleichung

$$x \circ b = b$$

eine Lösung, die wir mit e bezeichnen. Für dieses e gilt also

$$e \circ b = b.$$

Es sei nun a ein weiteres beliebiges Element von G. Dann hat die Gleichung

$$b \circ y = a$$

nach Voraussetzung ebenfalls eine Lösung, die wir mit c bezeichnen. Es gilt dann

$$b \circ c = a.$$

Dann haben wir folgende Gleichungs-Kette

$$\begin{array}{rcll} e \circ a & = & e \circ (b \circ c) & \text{wegen } b \circ c = a \\ & = & (e \circ b) \circ c & \text{Assoziativ-Gesetz} \\ & = & b \circ c & \text{wegen } e \circ b = b \\ & = & a & \text{wegen } b \circ c = a. \end{array}$$

Wir haben also insgesamt für jedes $a \in G$ gezeigt, dass $e \circ a = a$ ist und damit ist e ein links-neutrales Element bezüglich der Operation $\circ$. Nach Voraussetzung hat nun die Gleichung

$$x \circ a = e$$

für jedes a eine Lösung, nennen wir diese d. Dann gilt

$$d \circ a = e$$

und wir sehen, dass zu jedem $a \in G$ ein links-inverses Element existiert. Da das Assoziativ-Gesetz ebenfalls gültig ist, denn $\langle G, \circ \rangle$ ist eine Halb-Gruppe, ist $\langle G, e, \circ \rangle$ eine Gruppe. □

Bemerkung: Es sei $\langle G, e, \circ \rangle$ eine Gruppe, weiter sei $a, b, c \in G$ und es gelte

$$a \circ c = b \circ c.$$

Multiplizieren wir diese Gleichung auf beiden Seiten mit c^{-1}, so sehen wir, dass dann $a = b$ gelten muss. Ähnlich folgt aus

$$c \circ a = c \circ b$$

die Gleichung $a = b$. In einer Gruppe gelten also die beiden folgenden Kürzungs-Regeln:

$$a \circ c = b \circ c \rightarrow a = b \quad \text{und} \quad c \circ a = c \circ b \rightarrow a = b.$$

Interessant ist nun die Beobachtung, dass im Falle einer endlichen Halb-Gruppe $\langle G, \circ \rangle$ aus der Gültigkeit der Kürzungs-Regeln geschlossen werden kann, dass G eine Gruppe ist. Um dies zu sehen, brauchen wir drei Definitionen und einen Satz.

Definition 37 (injektiv) Eine Funktion $f : M \rightarrow N$ ist *injektiv* genau dann, wenn

$$f(x) = f(y) \rightarrow x = y \quad \text{für alle } x, y \in M$$

gilt. Diese Forderung ist logisch äquivalent zu der Formel

$$x \neq y \rightarrow f(x) \neq f(y),$$

verschiedene Argumente werden also auf verschiedene Werte abgebildet.

Definition 38 (surjektiv) Eine Funktion $f : M \rightarrow N$ ist *surjektiv* genau dann, wenn

$$\forall y \in N : \exists x \in M : f(x) = y$$

gilt. Jedes Element y aus N tritt also als Funktionswert auf.

Definition 39 (bijektiv)
Eine Funktion $f : M \to N$ ist *bijektiv* genau dann, wenn f sowohl injektiv als auch surjektiv ist.

Satz 40 Es sei M eine endliche Menge und die Funktion

$$f : M \to M$$

sei injektiv. Dann ist f auch surjektiv.

Beweis: Da f injektiv ist, werden verschiedene Argumente auch auf verschiedene Werte abgebildet. Damit hat die Funktion f genau so viele Werte, wie sie Argumente hat, es gilt

$$card\big(f(M)\big) = card(M).$$

Hierbei steht $f(M)$ für das Bild der Menge M, es gilt also

$$f(M) = \big\{f(x) \mid x \in M\big\}.$$

Nun gilt aber $f(M) \subseteq M$ und wenn die Mengen M und $f(M)$ die gleiche Anzahl Elemente haben, dann kann das bei einer endlichen Menge nur dann gehen, wenn

$$f(M) = M$$

gilt. Setzen wir hier die Definition von $f(M)$ ein, so haben wir

$$\big\{f(x) \mid x \in M\big\} = M.$$

Damit gibt es also für jedes $y \in M$ ein $x \in M$, so dass $y = f(x)$ gilt und folglich ist f surjektiv. □

Aufgabe 9: Es sei M eine endliche Menge und die Funktion

$$f : M \to M$$

sei surjektiv. Zeigen Sie, dass f dann auch injektiv ist.

Satz 41 Es sei $\langle G, \circ\rangle$ eine endliche Halb-Gruppe, in der die beiden Kürzungs-Regeln

$$a \circ c = b \circ c \to a = b \quad \text{und} \quad c \circ a = c \circ b \to a = b$$

für alle $a, b, c \in G$ gelten. Dann ist G bereits eine Gruppe.

Beweis: Wir beweisen die Behauptung in dem wir zeigen, dass für alle $a, b \in G$ die beiden Gleichungen

$$a \circ x = b \quad \text{und} \quad a \circ y = b$$

Lösungen haben, denn dann folgt die Behauptung aus Satz 36. Zunächst definieren wir für jedes $a \in G$ eine Funktion

$$f_a : G \to G \quad \text{durch} \quad f_a(x) := a \circ x.$$

Diese Funktionen $f_a(x)$ sind alle injektiv, denn aus

$$f_a(x) = f_a(y)$$

folgt nach Definition der Funktion f_a zunächst

$$a \circ x = a \circ y$$

und aus der Gültigkeit der ersten Kürzungs-Regel folgt nun $x = y$. Nach dem letzten Satz ist f_a dann auch surjektiv. Es gibt also zu jedem $b \in G$ ein $x \in G$ mit

$$f_a(x) = b \quad \text{beziehungsweise} \quad a \circ x = b.$$

Damit haben wir gesehen, dass für beliebige $a, b \in G$ die Gleichung $a \circ x = b$ immer eine Lösung hat. Genauso läßt sich zeigen, dass für beliebige $a, b \in G$ die Gleichung

$$y \circ a = b$$

eine Lösung hat. Nach dem letzten Satz ist G damit eine Gruppe.

5.2 Die Permutations-Gruppe S_n

Bisher waren alle Gruppen, die wir kennengelernt haben, kommutativ. Das ändert sich jetzt, denn wir werden gleich eine Gruppe kennen lernen, die nicht kommutativ ist. Zunächst definieren wir für alle positiven natürlichen Zahlen $n \in \mathbb{N}$ die Menge $\mathbb{Z}_n^+$ als die Menge aller natürlichen Zahlen von 1 bis n:

$$\mathbb{Z}_n^+ := \{i \in \mathbb{N} \mid 1 \leq i \wedge i \leq n\}.$$

Eine Relation $R \subseteq \mathbb{Z}_n^+ \times \mathbb{Z}_n^+$ heißt eine *Permutation* genau dann, wenn R auf $\mathbb{Z}_n^+$ als bijektive Funktion aufgefasst werden kann und dass ist genau dann der Fall, wenn folgendes gilt:

1. Die Relation R ist links-total auf $\mathbb{Z}_n^+$:

   $$\forall x \in \mathbb{Z}_n^+ : \exists y \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R.$$

2. Die Relation R ist rechts-total auf $\mathbb{Z}_n^+$:

   $$\forall y \in \mathbb{Z}_n^+ : \exists x \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R.$$

3. Die Relation R ist rechts-eindeutig:

   $$\forall x, y_1, y_2 \in \mathbb{Z}_n^+ : \langle x, y_1\rangle \in R \wedge \langle x, y_2\rangle \in R \rightarrow y_1 = y_2.$$

Aus der ersten und der dritten Forderung folgt, dass die Relation R als Funktion

$$R : \mathbb{Z}_n^+ \rightarrow \mathbb{Z}_n^+$$

aufgefasst werden kann. Aus der zweiten Forderung folgt, dass diese Funktion surjektiv ist. Da die Menge $\mathbb{Z}_n^+$ endlich ist, ist die Funktion R damit auch injektiv, denn wenn es ein $x_1, x_2, y \in \mathbb{Z}_n^+$ gäbe, so dass

$$\langle x_1, y\rangle \in R, \quad \langle x_2, y\rangle \in R, \quad \text{und} \quad x_1 \neq x_2$$

gelten würde, dann könnte R nicht mehr surjektiv sein. Wir definieren nun S_n als die Menge aller Permutationen auf der Menge $\mathbb{Z}_n^+$:

$$S_n := \{R \subseteq \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid R \text{ ist Permutation auf } \mathbb{Z}_n^+\}.$$

Weiter definieren wir die identische Permutation E_n auf $\mathbb{Z}_n^+$ als

$$E_n := \{\langle x, x\rangle \mid \langle x, x\rangle \in \mathbb{Z}_n^+\}.$$

Wir erinnern an die Definition des relationalen Produkts, es gilt:

$$R_1 \circ R_2 := \{\langle x, z\rangle \mid \exists y \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R \wedge \langle y, z\rangle \in R\}.$$

Die entscheidende Beobachtung ist nun, dass $R_1 \circ R_2$ eine Permutation ist, wenn R_1 und R_2 bereits Permutationen sind.

Aufgabe 10: Beweisen Sie

$$\forall R_1, R_2 \in S_n : R_1 \circ R_2 \in S_n. \qquad \square$$

Bemerkung: Wir hatten früher bereits gezeigt, dass für das relationale Produkt das Assoziativ-Gesetz gilt und wir haben ebenfalls gesehen, dass für die identische Permutation E_n die Beziehung

$$E_n \circ R = R \quad \text{für alle } R \in S_n$$

gilt. Weiter sehen wir: Ist $R \in S_n$, so haben wir

$$\begin{aligned}
& R^{-1} \circ R \\
= \; & \{\langle x, z\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid \exists y : \langle x, y\rangle \in R^{-1} \wedge \langle y, z\rangle \in R\} \\
= \; & \{\langle x, z\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid \exists y : \langle y, x\rangle \in R \wedge \langle y, z\rangle \in R\} \\
= \; & \{\langle x, z\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid \exists y : x = z\} && \text{denn } R \text{ ist rechts-eindeutig} \\
= \; & \{\langle x, z\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid x = z\} \\
= \; & E_n.
\end{aligned}$$

Folglich ist für eine Permutation R der Ausdruck R^{-1} tatsächlich das Inverse bezüglich des relationalen Produkts $\circ$. Damit ist klar, dass die Struktur $\langle S_n, E_n, \circ\rangle$ eine Gruppe ist. Diese Gruppe trägt den Namen *Permutations-Gruppe*.

Aufgabe 11: Zeigen Sie, dass S_3 keine kommutative Gruppe ist. Schreiben Sie dazu eine *SetlX*-Programm, dass zunächst die Menge S_3 berechnet und anschließend überprüft, ob in dieser Menge das Kommutativ-Gesetz gilt.

5.3 Untergruppen, Normalteiler und Faktor-Gruppen

Definition 42 (Untergruppe) Es sei $\langle G, e, \circ\rangle$ eine Gruppe und es sei $U \subseteq G$. Dann ist U eine *Untergruppe* von G, geschrieben $U \leq G$, falls folgendes gilt:

1. $\forall x, y \in U : x \circ y \in U$,

   die Menge U ist also unter der Operation $\circ$ abgeschlossen.

2. $e \in U$,

   das neutrale Element der Gruppe G ist also auch ein Element der Menge U.

3. Bezeichnen wir das zu $x \in G$ bezüglich der Operation $\circ$ inverse Element mit x^{-1}, so gilt

   $$\forall x \in U : u^{-1} \in U,$$

   die Menge U ist also unter der Operation $\cdot^{-1} : x \mapsto x^{-1}$ abgeschlossen.

Bemerkung: Falls U eine Untergruppe der Gruppe $\langle G, e, \circ\rangle$ ist, dann ist $\langle U, e, \circ_{|U}\rangle$ offenbar eine Gruppe. Hierbei bezeichnet $\circ_{|U}$ die Einschränkung der Funktion $\circ$ auf U, es gilt also

$$\circ_{|U} : U \times U \to U \quad \text{mit } \circ_{|U}(x, y) := \circ(x, y) \text{ für alle } x, y \in U.$$

Beispiele:

1. In der Gruppe $\langle \mathbb{Z}, 0, +\rangle$ ist die Menge

   $$2\mathbb{Z} := \{2 \cdot x \mid x \in \mathbb{Z}\}$$

   der geraden Zahlen eine Untergruppe, denn wir haben:

   (a) Die Addition zweier gerader Zahlen liefert wieder eine gerade Zahl:

   $$2 \cdot x + 2 \cdot y = 2 \cdot (x + y) \in 2\mathbb{Z}.$$

   (b) $0 \in 2\mathbb{Z}$, denn $0 = 2 \cdot 0 \in \mathbb{Z}$.

   (c) Das bezüglich der Addition inverse Element einer geraden Zahl ist offenbar wieder gerade, denn es gilt

   $$-(2 \cdot x) = 2 \cdot (-x) \in 2\mathbb{Z}.$$

2. Das letzte Beispiel läßt sich verallgemeinern: Ist $k \in \mathbb{N}$ und definieren wir

   $$k\mathbb{Z} := \{k \cdot x \mid x \in \mathbb{Z}\}$$

   als die Menge der Vielfachen von k, so läßt sich genau wie in dem letzten Beispiel zeigen, dass die Menge $k\mathbb{Z}$ eine Untergruppe der Gruppe $\langle \mathbb{Z}, 0, + \rangle$ ist.

3. Wir definieren die Menge G als

   $$G := \{e, a, b, c\}$$

   und definieren auf der Menge G eine Funktion $\circ : G \times G \to G$ durch die folgende Verknüfungs-Tafel:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   Wollen wir zu gegeben $x, y \in G$ den Wert $x \circ y$ mit Hilfe dieser Tabelle finden, so können wir den Wert $x \circ y$ in der Zeile, die mit x beschriftet ist und der Spalte, die mit y beschriftet ist, finden. Beispielsweise gilt $a \circ b = c$. Es läßt sich zeigen, dass $\langle G, e, \circ \rangle$ eine Gruppe ist. Definieren wir die Mengen

   $$U := \{e, a\}, \quad V := \{e, b\}, \quad \text{und} \quad W := \{e, c\},$$

   so können Sie leicht nachrechen, dass $U \leq G$, $V \leq G$ und $W \leq G$ gilt.

Untergruppen sind interessant, weil sich mit ihrer Hilfe unter bestimmten Umständen neue Gruppen bilden lassen, sogenannte *Faktor-Gruppen*.

Definition 43 (Faktor-Gruppe) Es sei $\langle G, 0, + \rangle$ eine kommutative Gruppe und $U \leq G$. Dann definieren wir für jedes $a \in G$ die Menge $a + U$ als

$$a + U := \{a + x \mid x \in U\}.$$

Wir bezeichnen die Mengen $a + U$ als *Nebenklassen von G bezüglich U*. Nun definieren wir die Menge G/U (gelesen: G modulo U) als

$$G/U := \big\{a + U \mid a \in G\big\}.$$

G/U ist also die Menge der Nebenklassen von G bezüglich U. Weiter definieren wir ein Operation $+ : G/U \times G/U \to G/U$ durch

$$(a + U) + (b + U) := (a + b) + U.$$

Bemerkung: Zunächst ist gar nicht klar, dass die Definition

$$(a + U) + (b + U) := (a + b) + U$$

überhaupt Sinn macht. Wir müssen zeigen, dass für alle $a_1, a_2, b_1, b_2 \in G$

$$a_1 + U = a_2 + U \;\wedge\; b_1 + U = b_2 + U \;\Rightarrow\; (a_1 + b_1) + U = (a_2 + b_2) + U$$

gilt, denn sonst ist die Operation $+$ auf den Nebenklassen von G bezüglich U nicht eindeutig definiert. Um diesen Nachweis führen zu können, zeigen wir zunächst einen Hilfssatz, der uns darüber Aufschluss gibt, wann zwei Nebenklassen $a + U$ und $b + U$ gleich sind.

Lemma 44 Es sei $\langle G, 0, + \rangle$ eine kommutative Gruppe und $U \leq G$. Weiter seien $a, b \in G$. Dann gilt:

$$a + U = b + U \quad \text{g.d.w.} \quad a - b \in U.$$

Beweis: Wir zerlegen den Beweis in zwei Teile:

"⇒" : Gelte $a + U = b + U$. Wegen $0 \in U$ haben wir

$$a = a + 0 \in a + U$$

und wegen der Voraussetzung $a + U = b + U$ folgt daraus

$$a \in b + U.$$

Also gibt es ein $u \in U$, so dass

$$a = b + u$$

gilt. Daraus folgt $a - b = u$ und weil $u \in U$ ist, haben wir also

$$a - b \in U. \checkmark$$

"⇐" : Gelte nun $a - b \in U$. Weil U eine Untergruppe ist und Untergruppen zu jedem Element auch das Inverse enthalten, gilt dann auch $-(a - b) \in U$, also $b - a \in U$. Wir zeigen nun, dass sowohl

$$a + U \subseteq b + U \quad \text{als auch} \quad b + U \subseteq a + U$$

gilt.

(a) Sei $x \in a + U$. Dann gibt es ein $u \in U$, so dass

$$x = a + u$$

gilt. Daraus folgt

$$x = b + \big((a - b) + u\big).$$

Nun ist aber nach Voraussetzung $a - b \in U$ und da auch $u \in U$ ist, folgt damit, dass auch

$$v := (a - b) + u \in U$$

ist, denn die Untergruppe ist bezüglich der Addition abgeschlossen. Damit haben wir

$$x = b + v \text{ mit } v \in U$$

und nach Definition von $b + U$ folgt dann $x \in b + U$.

(b) Sei nun $x \in b + U$. Dann gibt es ein $u \in U$, so dass

$$x = b + u$$

gilt. Durch elementare Umformung sehen wir, dass

$$x = a + \big((b - a) + u\big)$$

gilt. Nun ist aber, wie oben gezeigt, $b - a \in U$ und da auch $u \in U$ ist, folgt damit, dass auch

$$v := (b - a) + u \in U$$

ist. Damit haben wir

$$x = a + v \text{ mit } v \in U$$

und nach Definition von $a + U$ folgt nun $x \in a + U$. □

Aufgabe 12: Es sei $\langle G, 0, + \rangle$ eine kommutative Gruppe und $U \leq G$ sei eine Untergruppe von G. Wir definieren auf der Menge G eine Relation $\approx_U$ wie folgt:

$$x \approx_U y \iff^{\text{def}} x - y \in U.$$

Zeigen Sie, dass $\approx_U$ eine Äquivalenz-Relation auf G ist.

Lemma 45 Es sei $\langle G, 0, + \rangle$ eine kommutative Gruppe und $U \leq G$. Weiter seien $a, b \in G$. Dann ist

$$(a + U) + (b + U) := (a + b) + U.$$

wohldefiniert.

Beweis: Wir haben zu zeigen, dass für alle $a_1, a_2, b_1, b_2 \in G$ die Formel

$$a_1 + U = a_2 + U \;\wedge\; b_1 + U = b_2 + U \;\Rightarrow\; (a_1 + b_1) + U = (a_2 + b_2) + U$$

gilt. Sei also $a_1 + U = a_2 + U$ und $b_1 + U = b_2 + U$ vorausgesetzt. Zu zeigen ist dann

$$(a_1 + b_1) + U = (a_2 + b_2) + U.$$

Aus $a_1 + U = a_2 + U$ folgt nach dem letzten Lemma $a_1 - a_2 \in U$ und aus $b_1 + U = b_2 + U$ folgt $b_1 - b_2 \in U$. Da U unter der Operation $+$ abgeschlossen ist, folgt

$$(a_1 - a_2) + (b_1 - b_2) \in U$$

und das ist äquivalent zu

$$(a_1 + b_1) - (a_2 + b_2) \in U.$$

Aus der Rückrichtung des letzten Lemmas folgt nun

$$(a_1 + b_1) + U = (a_2 + b_2) + U.$$

Damit ist gezeigt, dass die Addition auf den Nebenklassen von U wohldefiniert ist. □

Satz 46 Es sei $\langle G, 0, + \rangle$ eine kommutative Gruppe und $U \leq G$. Dann ist $\langle G/U, 0 + U, + \rangle$ mit der oben definierten Addition von Nebenklassen eine Gruppe.

Beweis: Der Beweis zerfällt in drei Teile.

1. $0 + U$ ist das links-neutrale Element, denn wir haben

   $$(0 + U) + (a + U) = (0 + a) + U = a + U \quad \text{für alle } a \in G.$$

2. $-a + U$ ist das links-inverse Element zu $a + U$, denn wir haben

   $$(-a + U) + (a + U) = (-a + a) + U = 0 + U \quad \text{für alle } a \in G.$$

3. Es gilt das Assoziativ-Gesetz, denn

   $$\begin{array}{ll} & \big((a + U) + (b + U)\big) + (c + U) \\ = & \big((a + b) + U\big) + (c + U) \\ = & \big((a + b) + c\big) + U \\ = & \big(a + (b + c)\big) + U \\ = & (a + U) + \big((b + c) + U\big) \\ = & (a + U) + \big((b + U) + (c + U)\big) \end{array}$$

   Damit ist alles gezeigt. □

Beispiel: Wir haben früher bereits gesehen, dass die Mengen

$$k\mathbb{Z} := \big\{k \cdot x \mid x \in \mathbb{Z}\big\}$$

Untergruppen der Gruppe $\langle \mathbb{Z}, 0, + \rangle$ sind. Der letzte Satz zeigt nun, dass die Menge

$$\mathbb{Z}_k := \mathbb{Z}/(k\mathbb{Z}) = \big\{l + k\mathbb{Z} \mid l \in \mathbb{Z}\big\}$$

zusammen mit der durch

$$(l_1 + k\mathbb{Z}) + (l_2 + k\mathbb{Z}) = (l_1 + l_2) + k\mathbb{Z}$$

definierten Addition eine Gruppe ist, deren neutrales Element die Menge $0 + k\mathbb{Z} = k\mathbb{Z}$ ist. Es gilt

$$l_1 + k\mathbb{Z} = l_2 + k\mathbb{Z}$$

genau dann, wenn

$$l_1 - l_2 \in k\mathbb{Z}$$

ist, und dass ist genau dann der Fall, wenn $l_1 - l_2$ ein Vielfaches von k ist, wenn also $l_1 \approx_k l_2$ gilt. Wie wir bereits früher gezeigt haben, ist dies genau dann der Fall, wenn

$$l_1 \,\%\, k = l_2 \,\%\, k$$

ist. Damit sehen wir, dass die Menge $\mathbb{Z}/(k\mathbb{Z})$ aus genau k verschiedenen Nebenklassen besteht, denn es gilt

$$\mathbb{Z}_k = \big\{ l + k\mathbb{Z} \mid l \in \{0, \cdots, k-1\} \big\}.$$

Kapitel 6

Ringe und Körper

In diesem Abschnitt behandeln wir *Ringe* und *Körper*. Diese Begriffe werde ich gleich erklären. Im Folgenden möchte ich einen kurzen Überblick über den Aufbau dieses Kapitels geben. Da Sie Ringe und Körper noch nicht kennen, wird dieser Überblick notwendigerweise informal und unpräzise sein. Es geht mir hier nur darum, dass Sie eine, zunächst sicher noch verschwommene, Vorstellung von dem, was Sie in diesem Kapitel erwartet, bekommen.

Ringe sind Strukturen, in denen sowohl eine Addition, eine Subtraktion und als auch eine Multiplikation vorhanden ist und außerdem für diese Operationen ein Distributiv-Gesetz gilt. Bezüglich der Addition muss die Struktur dabei eine kommutative Gruppe sein. Ein typisches Beispiel für einen Ring ist die Struktur der ganzen Zahlen. Ein Ring ist ein Körper, wenn zusätzlich auch noch eine Division möglich ist. Ein typisches Beispiel ist die Struktur der rationalen Zahlen.

Es gibt zwei wichtige Methoden um mit Hilfe eines Rings einen Körper zu konstruieren. Die erste Methode funktioniert in sogenanten Integritäts-Ringen, dass sind solche Ringe, in denen sich das neutrale Element der Addition, also die 0, nicht als Produkt zweier von 0 verschiedenener Elemente darstellen läßt. Dann läßt sich nämlich aus einem Integritäts-Ring, der bezüglich der Multiplikation ein neutrales Element enthält, ein sogenannter Quotienten-Körper erzeugen. Die Konstruktion dieses Körpers verläuft analog zu der Konstruktion der rationalen Zahlen aus den reellen Zahlen.

Die zweite Methode funktioniert mit Hilfe sogenannter *maximaler Ideale*. Wir werden in Ringen zunächst *Ideale* definieren. Dabei sind Ideale das Analogon zu Untergruppen in der Gruppen-Theorie. Anschließend zeigen wir, wie sich mit Hilfe eines Ideals I auf einem Ring R eine Kongruenz-Relation erzeugen läßt. Die Konstruktion ist dabei analog zur Konstruktion der Faktor-Gruppe aus dem letzten Abschnitt. Für *maximale Ideale* werden wir schließlich zeigen, dass der so erzeugte Faktor-Ring sogar ein Körper ist.

6.1 Definition und Beispiele

Definition 47 (Ring) Ein 4-Tupel $\mathcal{R} = \langle R, 0, +, \cdot \rangle$ ist ein *Ring*, falls gilt:

1. $\langle R, 0, + \rangle$ ist eine kommutative Gruppe,
2. $\cdot : R \times R \to R$ ist eine Funktion für welche die folgenden Gesetze gelten:
   (a) Assoziativ-Gesetz: Für alle $x, y, z \in R$ gilt
   $$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$
   (b) Distributiv-Gesetze: Für alle $x, y, z \in R$ gilt
   $$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Die Operation "+" nennen wir die Addition auf dem Ring $\mathcal{R}$, die Operation "$\cdot$" bezeichnen wir als Multiplikation. $\mathcal{R}$ ist ein *kommutativer Ring* falls zusätzlich für die Multiplikation das Kommutativ-Gesetz

$$x \cdot y = y \cdot x \quad \text{für alle } x, y \in R$$

gilt. Wir sagen, dass R eine *Eins* hat, wenn es für die Multiplikation ein Element e gibt, so dass

$$e \cdot x = x \cdot e = x \quad \text{für alle } x \in R$$

gilt. Dieses Element e heißt dann die *Eins* des Rings. In diesem Fall schreiben wir $\mathcal{R} = \langle R, 0, e, + \rangle$, wir geben die Eins also explizit in der Struktur an.

Bemerkung: Bevor wir Beispiele betrachten, bemerken wir einige unmittelbare Konsequenzen der obigen Definition.

1. In jedem Ring $\mathcal{R} = \langle R, 0, +, \cdot \rangle$ gilt

   $$0 \cdot x = 0,$$

   denn wir haben die Gleichung

   $$\begin{array}{rcll} 0 \cdot x & = & (0 + 0) \cdot x & \text{denn } 0 + 0 = 0 \\ & = & 0 \cdot x + 0 \cdot x & \text{Distributiv-Gesetz} \end{array}$$

   Wenn wir nun auf beiden Seiten der eben gezeigten Gleichung $0 \cdot x = 0 \cdot x + 0 \cdot x$ abziehen, dann erhalten wir die Gleichung

   $0 = 0 \cdot x$. Genauso gilt natürlich auch $x \cdot 0 = 0$.

2. Bezeichnen wir das bezüglich der Addition $+$ zu einem Element x inverse Element mit $-x$, so gilt

   $$-(x \cdot y) = (-x) \cdot y = x \cdot (-y).$$

   Wir zeigen die erste dieser beiden Gleichungen, die zweite läßt sich analog nachweisen. Um zu zeigen, dass $-(x \cdot y) = (-x) \cdot y$ reicht es nachzuweisen, dass

   $$x \cdot y + (-x) \cdot y = 0$$

   ist, denn das Inverse ist in einer Gruppe eindeutig bestimmt. Die letzte Gleichung folgt aber sofort aus dem Distributiv-Gesetz, denn wir haben

   $$\begin{array}{rcl} x \cdot y + (-x) \cdot y & = & (x + -x) \cdot y \\ & = & 0 \cdot y \\ & = & 0. \end{array}$$

Beispiele:

1. Die Struktur $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ ist ein kommutativer Ring mit Eins.
2. Die Struktur $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ ist ebenfalls ein kommutativer Ring mit Eins.

In dieser Vorlesung werden wir nur kommutative Ringe betrachten, die eine Eins haben. Ein wichtiger Spezialfall ist der Fall eines kommutativen Rings $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ mit Eins, für dass die Struktur $\langle R \backslash \{0\}, 1, \cdot \rangle$ eine Gruppe ist. Dieser Spezialfall liegt beispielsweise bei dem Ring $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ vor. In einem solchen Fall sprechen wir von einem *Körper*. Die formale Definition folgt.

Definition 48 (Körper) Ein 5-Tupel $\mathcal{K} = \langle K, 0, 1, +, \cdot \rangle$ ist ein *Körper*, falls gilt:

1. $\langle K, 0, + \rangle$ ist eine kommutative Gruppe,

2. $\langle K \backslash \{0\}, 1, \cdot \rangle$ ist ebenfalls eine kommutative Gruppe,

3. Es gelten die Distributiv-Gesetze: Für alle $x, y, z \in R$ haben wir

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Wieder nennen wir die Operation "$+$" die *Addition*, während wir die Operation "$\cdot$" als die *Multiplikation* bezeichnen.

Unser Ziel ist es später, Ringe zu Körpern zu erweitern. Es gibt bestimmte Ringe, in denen dies auf keinen Fall möglich ist. Betrachten wir als Beispiel den Ring $\mathcal{R} := \langle \{0, 1, 2, 3\}, 0, 1, +_4, \cdot_4 \rangle$, bei dem die Operationen "$+_4$" und "$\cdot_4$" wie folgt definiert sind:

$$x +_4 y := (x + y) \,\%\, 4 \quad \text{und} \quad x \cdot_4 y := (x \cdot y) \,\%\, 4.$$

Es läßt sich zeigen, dass die so definierte Struktur $\mathcal{R}$ ein Ring ist. In diesem Ring gilt

$$2 \cdot_4 2 = 4 \,\%\, 4 = 0.$$

Falls es uns gelingen würde, den Ring $\mathcal{R}$ zu einem Körper $\mathcal{K} = \langle K, 0, 1, +_4, \cdot_4 \rangle$ so zu erweitern, dass $\{0, 1, 2, 3\} \subseteq K$ gelten würde, so müsste die Zahl Zahl 2 in diesem Körper ein Inverses 2^{-1} haben. Wenn wir dann die Gleichung

$$2 \cdot_4 2 = 0$$

auf beiden Seiten mit 2^{-1} multiplizieren würden, hätten wir die Gleichung

$$2 = 0$$

hergeleitet. Dieser Wiederspruch zeigt, dass sich der Ring $\mathcal{R}$ sicher nicht zu einem Körper erweitern läßt.

Definition 49 (Integritäts-Ring) Ein Ring $\mathcal{R} = \langle R, 0, +, \cdot \rangle$ heißt *nullteilerfrei*, wenn

$$\forall a, b \in R : \big(a \cdot b = 0 \rightarrow a = 0 \vee b = 0\big)$$

gilt, die Zahl 0 läßt sich in einem nullteilerfreien Ring also nur als triviales Produkt darstellen. Ein nullteilerfreier, kommutativer Ring, der eine Eins hat, wird als *Integritäts-Ring* bezeichnet.

Bemerkung: In einem nullteilerfreien Ring $\mathcal{R} = \langle R, 0, +, \cdot \rangle$ gilt die folgende *Streichungs-Regel*:

$$\forall a, b, c \in R : \big(a \cdot c = b \cdot c \wedge c \neq 0 \rightarrow a = b\big).$$

Beweis: Wir nehmen an, dass $c \neq 0$ ist und dass $a \cdot c = b \cdot c$ gilt. Es ist dann $a = b$ zu zeigen. Wir formen die Voraussetzung $a \cdot c = b \cdot c$ wie folgt um

$$\begin{array}{lll}
 & a \cdot c = b \cdot c & \mid -b \cdot c \\
\Rightarrow & a \cdot c - b \cdot c = 0 & \\
\Rightarrow & (a - b) \cdot c = 0 & \\
\Rightarrow & (a - b) = 0 & \text{denn } \mathcal{R} \text{ ist nullteilerfreier und } c \neq 0 \\
\Rightarrow & a = b. &
\end{array}$$

Damit ist der Beweis abgeschlossen. □

Ist R ein Ring und ist $\sim$ eine Äquivalenz-Relationen auf R, so läßt sich auf dem Quotienten-Raum $R/\sim$ unter bestimmten Umständen ebenfalls eine Ring-Struktur definieren. Das funktioniert aber nur, wenn die Addition und die Multiplikation des Rings in gewisser Weise mit der Äquivalenz-Relationen *verträglich* sind. In diesem Fall nenne wir dann $\sim$ eine *Kongruenz-Relation* auf R. Die formale Definition folgt.

Definition 50 (Kongruenz-Relation) Es sei $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins und $\sim \subseteq R \times R$ sei eine Äquivalenz-Relation auf R. Wir nennen $\sim$ eine *Kongruenz-Relation* falls zusätzlich die folgenden beiden Bedingungen erfüllt sind:

1. $\forall a_1, a_2, b_1, b_2 \in R : \big(a_1 \sim a_2 \wedge b_1 \sim b_2 \rightarrow a_1 + b_1 \sim a_2 + b_2\big)$,
   die Relation $\sim$ ist also *verträglich* mit der Addition auf R.
2. $\forall a_1, a_2, b_1, b_2 \in R : \big(a_1 \sim a_2 \wedge b_1 \sim b_2 \rightarrow a_1 \cdot b_1 \sim a_2 \cdot b_2\big)$,
   die Relation $\sim$ ist also auch mit der Multiplikation auf R *verträglich*.

Falls $\sim$ eine Kongruenz-Relation auf einem Ring $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ist, lassen sich die Operationen "+" und "$\cdot$" auf die Menge $R/\sim$ der von $\sim$ erzeugten Äquivalenz-Klassen fortsetzen, denn in diesem Fall können wir für $a, b \in R$ definieren:

$$[a]_\sim + [b]_\sim := [a + b]_\sim \quad \text{und} \quad [a]_\sim \cdot [b]_\sim := [a \cdot b]_\sim.$$

Um nachzuweisen, dass diese Definitionen tatsächlich Sinn machen, betrachten wir vier Elemente $[a_1]_\sim, [a_2]_\sim, [b_1]_\sim, [b_2]_\sim \in R/\sim$, für die

$$[a_1]_\sim = [a_2]_\sim \quad \text{und} \quad [b_1]_\sim = [b_2]_\sim$$

gilt. Wir müssen zeigen, dass dann auch

$$[a_1 + b_1]_\sim = [a_2 + b_2]_\sim$$

gilt. An dieser Stelle erinnern wir daran, dass nach Satz 13 allgemein für eine beliebige Äquivalenz-Relation R auf einer Menge M die Beziehung

$$[a]_R = [b]_R \;\leftrightarrow\; a \,R\, b$$

gilt. Damit folgt aus den Voraussetzungen $[a_1]_\sim = [a_2]_\sim$ und $[b_1]_\sim = [b_2]_\sim$, dass

$$a_1 \sim a_2 \quad \text{und} \quad b_1 \sim b_2$$

gilt. Da die Äquivalenz-Relation $\sim$ mit der Operation "+" verträglich ist, folgt daraus

$$a_1 + b_1 \sim a_2 + b_2$$

und damit gilt wieder nach Satz 13

$$[a_1 + b_1]_\sim = [a_2 + b_2]_\sim.$$

Genauso läßt sich zeigen, dass auch die Multiplikation $\cdot$ auf $R/\sim$ wohldefiniert ist. Mit den obigen Definitionen von $+$ und $\cdot$ haben wir nun eine Struktur $\mathcal{R}/\sim = \langle R/\sim, [0]_\sim, [1]_\sim, +, \cdot \rangle$ geschaffen, die als der *Faktor-Ring* $\mathcal{R}$ modulo $\sim$ bezeichnet wird. Der nächste Satz zeigt, dass es sich bei dieser Struktur tatsächlich um einen Ring handelt.

Satz 51 (Faktor-Ring)
Die oben definierte Struktur $\mathcal{R}/\sim = \langle R/\sim, [0]_\sim, [1]_\sim, +, \cdot \rangle$ ist ein kommutativer Ring mit Eins.

Beweis: Wir weisen die Eigenschaften, die einen Ring auszeichnen, einzeln nach.

1. Für die Operation "+" gilt das Assoziativ-Gesetz, denn für alle $[a]_\sim, [b]_\sim, [c]_\sim \in R/\sim$ gilt

$$\begin{aligned}
[a]_\sim + \big([b]_\sim + [c]_\sim\big) &= [a]_\sim + [b + c]_\sim \\
&= [a + (b + c)]_\sim \\
&= [(a + b) + c]_\sim \\
&= [a + b]_\sim + [c]_\sim \\
&= \big([a]_\sim + [b]_\sim\big) + [c]_\sim.
\end{aligned}$$

2. Für die Operation "+" gilt das Kommutativ-Gesetz, denn für alle $[a]_\sim, [b]_\sim \in R/\sim$ gilt

$$[a]_\sim + [b]_\sim = [a + b]_\sim = [b + a]_\sim = [b]_\sim + [a]_\sim.$$

3. $[0]_\sim$ ist das neutrale Element bezüglich der Addition, denn für alle $[a]_\sim \in R/\sim$ gilt

$$[a]_\sim + [0]_\sim = [a + 0]_\sim = [a]_\sim.$$

4. Ist $[a]_\sim \in R/\sim$ und bezeichnet $-a$ das additive Inverse von a in R, so ist das additive Inverse von $[a]_\sim$ durch die Äquivalenz-Klasse $[-a]_\sim$ gegeben, denn wir haben

$$[a]_\sim + [-a]_\sim = [a + -a]_\sim = [0]_\sim.$$

5. Die Nachweise, dass auch für den Operator "$\cdot$" dass Assoziativ- und das Kommutativ-Gesetz sind völlig analog zu den entsprechenden Beweisen für den Operator "+". Ebenso ist der Nachweis, dass die Äquivalenz-Klasse $[1]_\sim$ das neutrale Element bezüglich des Operators "$\cdot$" ist, analog zu dem Nachweis, dass die Äquivalenz-Klasse $[0]_\sim$ das neutrale Element bezüglich des Operators "+" ist.

6. Als letztes weisen wir die Gültigkeit des Distributiv-Gesetzes nach. Es seien $[a]_\sim, [b]_\sim, [c]_\sim$ beliebige Äquivalenz-Klassen aus $R/\sim$. Dann gilt

$$\begin{aligned}
[a]_\sim \cdot \big([b]_\sim + [c]_\sim\big) &= [a]_\sim \cdot [b + c]_\sim \\
&= [a \cdot (b + c)]_\sim \\
&= [a \cdot b + a \cdot c]_\sim \\
&= [a \cdot b]_\sim + [a \cdot c]_\sim \\
&= [a]_\sim \cdot [b]_\sim + [a]_\sim \cdot [c]_\sim.
\end{aligned}$$

Damit ist gezeigt, dass $\mathcal{R}/\sim$ ein kommutativer Ring mit Eins ist. □

6.2 Konstruktion des Quotienten-Körpers

Betrachten wir einen Integritäts-Ring $\mathcal{R} = \langle R, 0, 1, +, \cdot\rangle$, der selbst noch kein Körper ist, so können wir uns fragen, in welchen Fällen es möglich ist, aus diesem Ring einen Körper zu konstruieren. Wir versuchen bei einer solchen Konstruktion ähnlich vorzugehen wie bei der Konstruktion der rationalen Zahlen $\mathbb{Q}$ aus den ganzen Zahlen $\mathbb{Z}$. Es sei also ein Integritäts-Ring $\mathcal{R} = \langle R, 0, 1, +, \cdot\rangle$ gegeben. Dann definieren wir zunächst die Menge

$$Q := \big\{\langle x, y\rangle \in R \times R \mid y \neq 0\big\}$$

der formalen Brüche. Weiter definieren wir eine Relation

$$\sim \subseteq Q \times Q$$

auf Q indem wir festsetzen, dass für alle $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in Q$ das Folgende gilt:

$$\langle x_1, y_1\rangle \;\sim\; \langle x_2, y_2\rangle \stackrel{\text{def}}{\iff} x_1 \cdot y_2 = x_2 \cdot y_1.$$

Satz 52 Die oben definierte Relation $\sim$ ist eine Äquivalenz-Relation auf der Menge Q.

Beweis: Wir müssen zeigen, dass die Relation reflexiv, symmetrisch und transitiv ist.

1. Reflexivität: Für alle Paare $\langle x, y\rangle \in Q$ gilt nach Definition der Relation $\sim$:

$$\begin{aligned}
&\langle x, y\rangle \sim \langle x, y\rangle \\
\Leftrightarrow\quad & x \cdot y = x \cdot y.
\end{aligned}$$

   Da die letzte Gleichung offensichtlich wahr ist, ist die Reflexivität nachgewiesen. ✓

2. Symmetrie: Wir müssen zeigen, dass

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle \rightarrow \langle x_2, y_2 \rangle \sim \langle x_1, y_1 \rangle$$

gilt. Wir nehmem also an, dass $\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle$ gilt, und zeigen, dass daraus

$$\langle x_2, y_2 \rangle \sim \langle x_1, y_1 \rangle$$

folgt. Die Annahme

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle$$

ist nach Definition von $\sim$ äquivalent zu der Gleichung

$$x_1 \cdot y_2 = x_2 \cdot y_1.$$

Diese Gleichung drehen wir um und erhalten

$$x_2 \cdot y_1 = x_1 \cdot y_2.$$

Nach Definition der Relation $\sim$ gilt dann

$$\langle x_2, y_2 \rangle \sim \langle x_1, y_1 \rangle$$

und das war zu zeigen. ✓

3. Transitivität: Wir müssen zeigen, dass

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle \ \wedge \ \langle x_2, y_2 \rangle \sim \langle x_3, y_3 \rangle \ \rightarrow \ \langle x_1, y_1 \rangle \sim \langle x_3, y_3 \rangle$$

gilt. Wir nehmen also an, dass

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle \quad \text{und} \quad \langle x_2, y_2 \rangle \sim \langle x_3, y_3 \rangle$$

gilt und zeigen, dass daraus $\langle x_1, y_1 \rangle \sim \langle x_3, y_3 \rangle$ folgt. Nach Definition von $\sim$ folgt aus unserer Annahme, dass

$$x_1 \cdot y_2 = x_2 \cdot y_1 \quad \text{und} \quad x_2 \cdot y_3 = x_3 \cdot y_2$$

gilt. Wir multiplizieren die erste dieser beiden Gleichungen mit y_3 und die zweite Gleichung mit y_1. Dann erhalten wir die Gleichungen

$$x_1 \cdot y_2 \cdot y_3 = x_2 \cdot y_1 \cdot y_3 \quad \text{und} \quad x_2 \cdot y_3 \cdot y_1 = x_3 \cdot y_2 \cdot y_1$$

Da für den Operator "$\cdot$" das Kommutativ-Gesetzes gilt, können wir diese Gleichungen auch in der Form

$$x_1 \cdot y_3 \cdot y_2 = x_2 \cdot y_3 \cdot y_1 \quad \text{und} \quad x_2 \cdot y_3 \cdot y_1 = x_3 \cdot y_1 \cdot y_2$$

schreiben. Setzen wir diese Gleichungen zusammen, so sehen wir, dass

$$x_1 \cdot y_3 \cdot y_2 = x_3 \cdot y_1 \cdot y_2$$

gilt. Da der betrachtete Ring nullteilerfrei ist und wir nach Definition von Q wissen, dass $y_2 \neq 0$ ist, können wir hier die Streichungs-Regel benutzen und y_2 aus der letzten Gleichung herauskürzen. Dann erhalten wir

$$x_1 \cdot y_3 = x_3 \cdot y_1.$$

Nach Definition der Relation $\sim$ haben wir jetzt

$$\langle x_1, y_1 \rangle \sim \langle x_3, y_3 \rangle$$

und das war zu zeigen. ✓ □

Bemerkung: Würden wir in der Definition $Q := \big\{ \langle x, y \rangle \in R \times R \mid y \neq 0 \big\}$ die Bedingung $y \neq 0$ weglassen, so würde

$$\langle x, y \rangle \sim \langle 0, 0 \rangle \quad \text{für alle } x, y \in R$$

gelten und damit wäre dann die Relation $\sim$ nicht mehr transitiv.

Auf der Menge Q definieren wir jetzt Operatoren "+" und "$\cdot$". Den Operator $+ : Q \times Q \to Q$ definieren wir durch die Festlegung

$$\langle x, y\rangle + \langle u, v\rangle := \langle x \cdot v + u \cdot y, y \cdot v\rangle.$$

Motiviert ist diese Definition durch die Addition von Brüchen, bei der wir die beteiligten Brüche zunächst auf den Hauptnenner bringen:

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}.$$

Die Äquivalenz-Relation $\sim$ erzeugt auf der Menge Q der formalen Brüche den Quotienten-Raum $Q/\sim$. Unser Ziel ist es, auf diesem Quotienten-Raum eine Ringstruktur zu definieren. Damit dies möglich ist zeigen wir, dass die oben definierte Funktion $+$ mit der auf Q definierten Äquivalenz-Relationen $\sim$ verträglich ist. Es gelte also

$$\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle \quad \text{und} \quad \langle u_1, v_1\rangle \sim \langle u_2, v_2\rangle.$$

Nach Definition der Äquivalenz-Relation $\sim$ heißt das

$$x_1 \cdot y_2 = x_2 \cdot y_1 \quad \text{und} \quad u_1 \cdot v_2 = u_2 \cdot v_1.$$

Zu zeigen ist dann

$$\langle x_1 \cdot v_1 + u_1 \cdot y_1,\, y_1 \cdot v_1\rangle \sim \langle x_2 \cdot v_2 + u_2 \cdot y_2,\, y_2 \cdot v_2\rangle.$$

Nach Definition der Äquivalenz-Relation $\sim$ ist dies äquivalent zu der Gleichung

$$(x_1 \cdot v_1 + u_1 \cdot y_1) \cdot y_2 \cdot v_2 = (x_2 \cdot v_2 + u_2 \cdot y_2) \cdot y_1 \cdot v_1.$$

Multiplizieren wir dies mittels des Distributiv-Gesetzes aus und benutzen wir weiter das Kommutativ-Gesetz für die Multiplikation, so ist die letzte Gleichung äquivalent zu

$$x_1 \cdot y_2 \cdot v_1 \cdot v_2 + u_1 \cdot v_2 \cdot y_1 \cdot y_2 = x_2 \cdot y_1 \cdot v_1 \cdot v_2 + u_2 \cdot v_1 \cdot y_1 \cdot y_2.$$

Formen wir die linke Seite dieser Gleichung durch Verwendung der Voraussetzungen $x_1 \cdot y_2 = x_2 \cdot y_1$ und $u_1 \cdot v_2 = u_2 \cdot v_1$ um, so erhalten wir die offensichtlich wahre Gleichung

$$x_2 \cdot y_1 \cdot v_1 \cdot v_2 + u_2 \cdot v_1 \cdot y_1 \cdot y_2 = x_2 \cdot y_1 \cdot v_1 \cdot v_2 + u_2 \cdot v_1 \cdot y_1 \cdot y_2.$$

Damit haben wir die Verträglichkeit des oben definierten Operators "+" nachgewiesen. Folglich kann die oben definierte Funktion $+$ auf den Quotienten-Raum $Q/\sim$ durch die Festlegung

$$\big[\langle x, y\rangle\big]_\sim + \big[\langle u, v\rangle\big]_\sim := \big[\langle x \cdot v + u \cdot y, y \cdot v\rangle\big]_\sim$$

fortgesetzt werden. Die Äquivalenz-Klasse $\big[\langle 0, 1\rangle\big]_\sim$ ist bezüglich der Operation "+" das neutrale Element, denn es gilt

$$\big[\langle 0, 1\rangle\big]_\sim + \big[\langle x, y\rangle\big]_\sim = \big[\langle 0 \cdot y + x \cdot 1, 1 \cdot y\rangle\big]_\sim = \big[\langle x, y\rangle\big]_\sim.$$

Es gilt weiter

$$\big[\langle 0, 1\rangle\big]_\sim = \big[\langle 0, y\rangle\big]_\sim \quad \text{für alle } y \neq 0,$$

denn wir haben

$$0 \cdot y = 0 \cdot 1.$$

Das bezüglich der Operation "+" zu $\big[\langle x, y\rangle\big]_\sim$ inverse Element ist $\big[\langle -x, y\rangle\big]_\sim$, denn es gilt

$$\begin{aligned}
\big[\langle -x, y\rangle\big]_\sim + \big[\langle x, y\rangle\big]_\sim &= \big[\langle -x \cdot y + x \cdot y,\, y \cdot y\rangle\big]_\sim \\
&= \big[\langle (-x + x) \cdot y,\, y \cdot y\rangle\big]_\sim \\
&= \big[\langle 0,\, y \cdot y\rangle\big]_\sim \\
&= \big[\langle 0,\, 1\rangle\big]_\sim.
\end{aligned}$$

Als nächstes definieren wir auf der Menge Q den Operator $\cdot : Q \times Q \to Q$ wie folgt:

$$\langle x, y\rangle \cdot \langle u, v\rangle := \langle x \cdot u, y \cdot v\rangle.$$

Auch dies wird durch die Analogie für Brüche motiviert, denn für Brüche gilt

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Nun zeigen wir, dass die Operation "$\cdot$" mit der Äquivalenz-Relation $\sim$ verträglich ist. Es gelte also

$$\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle \quad \text{und} \quad \langle u_1, v_1\rangle \sim \langle u_2, v_2\rangle.$$

Nach Definition der Äquivalenz-Relation $\sim$ folgt daraus

$$x_1 \cdot y_2 = x_2 \cdot y_1 \quad \text{und} \quad u_1 \cdot v_2 = u_2 \cdot v_1.$$

Zu zeigen ist

$$\langle x_1 \cdot u_1,\, y_1 \cdot v_1\rangle \sim \langle x_2 \cdot u_2,\, y_2 \cdot v_2\rangle.$$

Dies ist nach Definition der Relation $\sim$ äquivalent zu

$$x_1 \cdot u_1 \cdot y_2 \cdot v_2 = x_2 \cdot u_2 \cdot y_1 \cdot v_1.$$

Diese Gleichung erhalten wir aber sofort, wenn wir die beiden Gleichungen $x_1 \cdot y_2 = x_2 \cdot y_1$ und $u_1 \cdot v_2 = u_2 \cdot v_1$ mit einander multiplizieren. Folglich kann der Operator "$\cdot$" durch die Definition

$$\big[\langle x, y\rangle\big]_\sim \cdot \big[\langle u, v\rangle\big]_\sim := \big[\langle x \cdot u, y \cdot v\rangle\big]_\sim$$

auf den Quotienten-Raum $Q/\sim$ fortgesetzt werden. Das bezüglich der Operation "$\cdot$" neutrale Element ist $\big[\langle 1, 1\rangle\big]_\sim$, denn es gilt

$$\begin{aligned}
\big[\langle 1, 1\rangle\big]_\sim \cdot \big[\langle x, y\rangle\big]_\sim &= \big[\langle 1 \cdot x,\, 1 \cdot y\rangle\big]_\sim \\
&= \big[\langle x, y\rangle\big]_\sim.
\end{aligned}$$

Das bezüglich der Operation "$\cdot$" zu $\big[\langle x, y\rangle\big]_\sim$ inverse Element ist nur definiert, falls

$$\big[\langle x, y\rangle\big]_\sim \neq \big[\langle 0, 1\rangle\big]_\sim$$

ist. Wir formen diese Ungleichung um:

$$\begin{aligned}
& \big[\langle x, y\rangle\big]_\sim && \neq && \big[\langle 0, 1\rangle\big]_\sim \\
\Leftrightarrow \quad & \langle x, y\rangle && \not\sim && \langle 0, 1\rangle \\
\Leftrightarrow \quad & x \cdot 1 && \neq && 0 \cdot y \\
\Leftrightarrow \quad & x && \neq && 0.
\end{aligned}$$

Damit sehen wir, dass wir zu dem Ausdruck $\big[\langle x, y\rangle\big]_\sim$ nur dann ein bezüglich der Operation "$\cdot$" inverses Element angeben müssen, wenn $x \neq 0$ ist. Wir behaupten, dass für $x \neq 0$ das Element

$$\big[\langle y, x\rangle\big]_\sim$$

zu $\big[\langle x, y\rangle\big]_\sim$ invers ist, denn es gilt:

$$\begin{aligned}\big[\langle y,x\rangle\big]_\sim \cdot \big[\langle x,y\rangle\big]_\sim &= \big[\langle y\cdot x, x\cdot y\rangle\big]_\sim \\ &= \big[\langle x\cdot y, x\cdot y\rangle\big]_\sim \\ &= \big[\langle 1,1\rangle\big]_\sim\end{aligned}$$

denn offenbar gilt $\langle x\cdot y, x\cdot y\rangle \sim \langle 1,1\rangle$.

Um zu zeigen, dass die Struktur

$$\mathcal{R}/\!\sim := \Big\langle Q/\!\sim, \big[\langle 0,1\rangle\big]_\sim, \big[\langle 1,1\rangle\big]_\sim, +, \cdot \Big\rangle$$

mit den oben definierten Operationen "+" und "$\cdot$" ein Körper ist, bleibt nachzuweisen, dass für die Operatoren "+" und "$\cdot$" jeweils das Assoziativ-Gesetz und das Kommutativ-Gesetz gilt. Zusätzlich muss das Distributiv-Gesetz nachgewiesen werden.

1. Der Operator "+" ist in Q assoziativ, denn für beliebige Paare $\langle x_1,y_1\rangle, \langle x_2,y_2\rangle, \langle x_3,y_3\rangle \in Q$ gilt:

   $$\begin{aligned}&\big(\langle x_1,y_1\rangle + \langle x_2,y_2\rangle\big) + \langle x_3,y_3\rangle \\ = \;& \big(\langle x_1\cdot y_2 + x_2\cdot y_1, y_1\cdot y_2\rangle\big) + \langle x_3,y_3\rangle \\ = \;& \langle (x_1\cdot y_2 + x_2\cdot y_1)\cdot y_3 + x_3\cdot y_1\cdot y_2,\; y_1\cdot y_2\cdot y_3\rangle \\ = \;& \langle x_1\cdot y_2\cdot y_3 + x_2\cdot y_1\cdot y_3 + x_3\cdot y_1\cdot y_2,\; y_1\cdot y_2\cdot y_3\rangle\end{aligned}$$

   Auf der anderen Seite haben wir

   $$\begin{aligned}&\langle x_1,y_1\rangle + \big(\langle x_2,y_2\rangle + \langle x_3,y_3\rangle\big) \\ = \;& \langle x_1,y_1\rangle + \big(\langle x_2\cdot y_3 + x_3\cdot y_2,\; y_2\cdot y_3\rangle\big) \\ = \;& \langle x_1\cdot y_2\cdot y_3 + (x_2\cdot y_3 + x_3\cdot y_2)\cdot y_1,\; y_1\cdot y_2\cdot y_3\rangle \\ = \;& \langle x_1\cdot y_2\cdot y_3 + x_2\cdot y_1\cdot y_3 + x_3\cdot y_1\cdot y_2,\; y_1\cdot y_2\cdot y_3\rangle\end{aligned}$$

   Da dies mit dem oben abgeleiteten Ergebnis übereinstimmt, haben wir die Gültigkeit des Assoziativ-Gesetzes nachgewiesen.

2. Der Operator "+" ist in Q kommutativ, denn für beliebige Paare $\langle x_1,y_1\rangle, \langle x_2,y_2\rangle \in Q$ gilt:

   $$\begin{aligned}&\langle x_1,y_1\rangle + \langle x_2,y_2\rangle\big) \\ = \;& \langle x_1\cdot y_2 + x_2\cdot y_1, y_1\cdot y_2\rangle \\ = \;& \langle x_2\cdot y_1 + x_1\cdot y_2, y_2\cdot y_1\rangle \\ = \;& \langle x_2,y_2\rangle + \langle x_1,y_1\rangle\big).\end{aligned}$$

   Genau wie oben folgt nun, dass das Kommutativ-Gesetz auch in $Q/\!\sim$ gilt.

3. Den Nachweis der Assoziativität und der Kommutativität des Multiplikations-Operators überlasse ich Ihnen zur Übung.

4. Zum Nachweis des Distributiv-Gesetzes in $Q/\!\sim$ zeigen wir, dass für alle Paare $\langle x_1,y_1\rangle$, $\langle x_2,y_2\rangle$, $\langle x_3,y_3\rangle \in Q$ folgendes gilt:

   $$\big[\langle x_1,y_1\rangle\big]_\sim \cdot \Big(\big[\langle x_2,y_2\rangle\big]_\sim + \big[\langle x_3,y_3\rangle\big]_\sim\Big) = \big[\langle x_1,y_1\rangle\big]_\sim \cdot \big[\langle x_2,y_2\rangle\big]_\sim + \big[\langle x_1,y_1\rangle\big]_\sim \cdot \big[\langle x_3,y_3\rangle\big]_\sim.$$

   Wir werten die linke und rechte Seite dieser Gleichung getrennt aus und beginnen mit der linken Seite.

$$
\begin{aligned}
& \big[\langle x_1, y_1\rangle\big]_\sim \cdot \Big(\big[\langle x_2, y_2\rangle\big]_\sim + \big[\langle x_3, y_3\rangle\big]_\sim\Big) \\
= \;& \big[\langle x_1, y_1\rangle\big]_\sim \cdot \big[\langle x_2 \cdot y_3 + x_3 \cdot y_2,\, y_2 \cdot y_3\rangle\big]_\sim \\
= \;& \big[\langle x_1 \cdot (x_2 \cdot y_3 + x_3 \cdot y_2),\, y_1 \cdot y_2 \cdot y_3\rangle\big]_\sim \\
= \;& \big[\langle x_1 \cdot x_2 \cdot y_3 + x_1 \cdot x_3 \cdot y_2,\, y_1 \cdot y_2 \cdot y_3\rangle\big]_\sim
\end{aligned}
$$

Wir werten nun die rechte Seite aus.

$$
\begin{aligned}
& \big[\langle x_1, y_1\rangle\big]_\sim \cdot \big[\langle x_2, y_2\rangle\big]_\sim + \big[\langle x_1, y_1\rangle\big]_\sim \cdot \big[\langle x_3, y_3\rangle\big]_\sim \\
= \;& \big[\langle x_1 \cdot x_2,\, y_1 \cdot y_2\rangle\big]_\sim + \big[\langle x_1 \cdot x_3,\, y_1 \cdot y_3\rangle\big]_\sim \\
= \;& \big[\langle x_1 \cdot x_2 \cdot y_1 \cdot y_3 + x_1 \cdot x_3 \cdot y_1 \cdot y_2,\, y_1 \cdot y_2 \cdot y_1 \cdot y_3\rangle\big]_\sim .
\end{aligned}
$$

Allgemein haben wir bereits gesehen, dass für $c \neq 0$, $c \in R$ und beliebige $a, b \in R$ die Gleichung

$$\big[\langle a, b\rangle\big]_\sim = \big[\langle a \cdot c,\, b \cdot c\rangle\big]_\sim$$

gilt. Wenden wir diese Gleichung auf die oben für die linke und rechte Seite des Distributiv-Gesetzes erzielten Ergebnisse an, so sehen wir, dass beide Seiten gleich sind. Damit ist die Gültigkeit des Distributiv-Gesetzes in $Q/\sim$ nachgewiesen.

Damit haben wir nun gezeigt, dass die Struktur

$$Quot(\mathcal{R}) := \langle Q/\sim, \big[\langle 0, 1\rangle\big]_\sim, \big[\langle 1, 1\rangle\big]_\sim, +, \cdot\rangle$$

ein Körper ist. Dieser Körper wird als der von R erzeugte *Quotienten-Körper* bezeichnet.

6.3 Ideale und Faktor-Ringe

Der im Folgenden definierte Begriff des *Ideals* hat in der Theorie der Ringe eine ähnliche Stellung wie der Begriff der Untergruppe in der Theorie der Gruppen.

Definition 53 (Ideal) Es sei $\mathcal{R} = \langle R, 0, 1, +, \cdot\rangle$ ein kommutatives Ring mit Eins. Eine Teilmenge $I \subseteq R$ ist ein *Ideal in* $\mathcal{R}$ falls folgendes gilt:

1. $\langle I, 0, +\rangle \leq \langle R, 0, +\rangle$,

   die Struktur $\langle I, 0, +\rangle$ ist also eine Untergruppe der Gruppe $\langle R, 0, +\rangle$.

2. $\forall a \in I : \forall b \in R : b \cdot a \in I$,

   für alle Elemente a aus dem Ideal I ist das Produkt mit einem beliebigen Element b aus dem Ring R wieder ein Element aus dem Ideal.

Bemerkung: An dieser Stelle sollten Sie sich noch einmal die Definition einer Untergruppe ins Gedächtnis rufen: Es gilt $\langle I, 0, +\rangle \leq \langle R, 0, +\rangle$ genau dann, wenn folgende Bedingungen erfüllt sind:

1. $0 \in I$,
2. $a, b \in I \rightarrow a + b \in I$,
3. $a \in I \rightarrow -a \in I$.

Beachten Sie außerdem, dass in der Formel

$$\forall a \in I : \forall b \in R : b \cdot a \in I,$$

der zweite All-Quantor nicht nur über die Elemente aus I läuft, sondern über alle Elemente von R.

Beispiele:

1. Die Menge alle geraden Zahlen

   $$2\mathbb{Z} = \{2 \cdot x \mid x \in \mathbb{Z}\}$$

   ist ein Ideal in dem Ring $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ der ganzen Zahlen, denn wir haben

   (a) $0 \in 2\mathbb{Z}$, da $0 = 2 \cdot 0$ ist und somit ist 0 eine gerade Zahl.

   (b) Sind a, b gerade Zahlen, so gibt es $x, y \in \mathbb{Z}$ mit $a = 2 \cdot x$ und $b = 2 \cdot y$. Daraus folgt

   $$a + b = 2 \cdot x + 2 \cdot y = 2 \cdot (x + y)$$

   und damit ist auch $a + b$ eine gerade Zahl.

   (c) Ist $a \in 2\mathbb{Z}$, so gibt es $x \in \mathbb{Z}$ mit $a = 2 \cdot x$. Dann gilt

   $$-a = -2 \cdot x = 2 \cdot (-x)$$

   und damit ist auch $-a$ eine gerade Zahl.

   (d) Ist a eine gerade Zahl und ist $b \in \mathbb{Z}$, so gibt es zunächst eine Zahl $x \in \mathbb{Z}$ mit $a = 2 \cdot x$. Daraus folgt

   $$a \cdot b = (2 \cdot x) \cdot b = 2 \cdot (x \cdot b)$$

   und das ist offenbar wieder eine gerade Zahl.

2. Das letzte Beispiel läßt sich verallgemeinern: Es sei $k \in \mathbb{Z}$. Dann ist die Menge

   $$k\mathbb{Z} := \{a \cdot k \mid a \in \mathbb{Z}\}$$

   der Vielfachen von k ein Ideal in dem Ring $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$. Der Nachweis ist anlog zu dem oben geführten Nachweis, dass $2\mathbb{Z}$ ein Ideal in dem Ring der ganzen Zahlen ist.

3. Wir verallgemeinern das letzte Beispiel für beliebige kommutative Ringe mit Eins. Es sei also $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins und es sei $a \in R$. Dann definieren wir die Menge

   $$\mathit{gen}(k) := \{k \cdot x \mid x \in R\}$$

   aller Vielfachen von k in R. Wir zeigen, dass diese Menge ein Ideal in $\mathcal{R}$ ist.

   (a) $0 \in \mathit{gen}(k)$, da $0 = k \cdot 0$ gilt.

   (b) Sind $a, b \in \mathit{gen}(k)$, so gibt es $x, y \in R$ mit $a = k \cdot x$ und $b = k \cdot y$. Daraus folgt

   $$a + b = k \cdot x + k \cdot y = k \cdot (x + y)$$

   und folglich gilt $a + b \in \mathit{gen}(k)$.

   (c) Ist $a \in \mathit{gen}(k)$, so gibt es ein $x \in R$ mit $a = k \cdot x$. Dann gilt

   $$-a = -(k \cdot x) = k \cdot (-x) \in \mathit{gen}(a).$$

   (d) Ist $a \in \mathit{gen}(k)$ und ist $b \in \mathbb{Z}$, so gibt es zunächst ein $x \in R$ mit $a = k \cdot x$. Daraus folgt

   $$a \cdot b = (k \cdot x) \cdot b = k \cdot (x \cdot b) \in \mathit{gen}(k).$$

   Die Menge $\mathit{gen}(a)$ wird das von a *erzeugte Ideal* genannt. Ideale dieser Form werden in der Literatur als *Haupt-Ideale* bezeichnet.

4. Wieder sei $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins. Dann sind die Mengen $\{0\}$ und R offenbar wieder Ideale von R. Wir nennen die Menge $\{0\}$ das Null-Ideal und R das Eins-Ideal. Diese beiden Ideale werden auch als die *trivialen* Ideale bezeichnet.

Mit Hilfe von Idealen läßt sich auf einem Ring eine Kongruenz-Relation erzeugen. Ist I ein Ideal auf dem kommutativen Ring mit Eins $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$, so definieren wir eine Relation $\sim_I$ auf R durch die Forderung

$$a \sim_I b \iff^{\text{def}} a - b \in I.$$

Wir zeigen, dass die Relation $\sim_I$ eine Kongruenz-Relation auf R ist.

1. $\sim_I$ ist reflexiv auf R, denn für alle $x \in R$ gilt

   $$\begin{aligned} & x \sim_I x \\ \Leftrightarrow \quad & x - x \in I \\ \Leftrightarrow \quad & 0 \in I \end{aligned}$$

   Da ein Ideal insbesondere eine Untergruppe ist, gilt $0 \in I$ und damit ist $x \sim_I x$ gezeigt. ✓

2. Wir zeigen: $\sim_I$ ist symmetrisch. Sei $x \sim_I y$ gegeben. Nach Definition der Relation $\sim_I$ folgt

   $$x - y \in I.$$

   Da eine Untergruppe bezüglich der Bildung des additiven Inversen abgeschlossen ist, gilt dann auch

   $$-(x - y) = y - x \in I.$$

   Wieder nach Definition der Relation $\sim_I$ heißt das

   $$y \sim_I x. \checkmark$$

3. Wir zeigen: $\sim_I$ ist transitiv. Es gelte

   $$x \sim_I y \quad \text{und} \quad y \sim_I z.$$

   Nach Definition der Relation $\sim_I$ folgt daraus

   $$x - y \in I \quad \text{und} \quad y - z \in I.$$

   Da Ideale unter Addition abgeschlossen sind, folgt daraus

   $$x - z = (x - y) + (y - z) \in I.$$

   Nach Definition der Relation $\sim_I$ heißt das

   $$x \sim_I z. \checkmark$$

4. Wir zeigen: $\sim_I$ ist mit der Addition auf dem Ring $\mathcal{R}$ verträglich. Es sei also

   $$x_1 \sim_I x_2 \quad \text{und} \quad y_1 \sim_I y_2$$

   gegeben. Zu zeigen ist, dass dann auch

   $$x_1 + y_1 \sim_I x_2 + y_2$$

   gilt. Aus den Voraussetzungen $x_1 \sim_I x_2$ und $y_1 \sim_I y_2$ folgt nach Definition der Relation $\sim_I$, dass

   $$x_1 - x_2 \in I \quad \text{und} \quad y_1 - y_2 \in I$$

   gilt. Addieren wir diese Gleichungen und berücksichtigen, dass das Ideal I unter Addition abgeschlossen ist, so erhalten wir

   $$(x_1 - x_2) + (y_1 - y_2) \in I.$$

   Wegen $(x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2)$ folgt daraus

   $$(x_1 + y_1) - (x_2 + y_2) \in I$$

   und nach Definition der Relation $\sim_I$ heißt das

   $$x_1 + y_1 \sim_I x_2 + y_2. \checkmark$$

5. Wir zeigen: $\sim_I$ ist mit der Multiplikation auf dem Ring $\mathcal{R}$ verträglich. Es sei also wieder

   $$x_1 \sim_I x_2 \quad \text{und} \quad y_1 \sim_I y_2$$

gegeben. Diesmal ist zu zeigen, dass daraus

$$x_1 \cdot y_1 \sim_I x_2 \cdot y_2$$

folgt. Aus den Voraussetzungen $x_1 \sim_I x_2$ und $y_1 \sim_I y_2$ folgt nach Definition der Relation $\sim_I$ zunächst, dass

$$x_1 - x_2 \in I \quad \text{und} \quad y_1 - y_2 \in I$$

gilt. Da ein Ideal unter Multiplikation mit beliebigen Elementen des Rings abgeschlossen ist, folgt daraus, dass auch

$$(x_1 - x_2) \cdot y_2 \in I \quad \text{und} \quad x_1 \cdot (y_1 - y_2) \in I$$

gilt. Addieren wir diese Gleichungen und berücksichtigen, dass das Ideal I unter Addition abgeschlossen ist, so erhalten wir

$$(x_1 - x_2) \cdot y_2 + x_1 \cdot (y_1 - y_2) \in I.$$

Nun gilt

$$\begin{aligned}(x_1 - x_2) \cdot y_2 + x_1 \cdot (y_1 - y_2) &= x_1 \cdot y_2 - x_2 \cdot y_2 + x_1 \cdot y_1 - x_1 \cdot y_2 \\ &= x_1 \cdot y_1 - x_2 \cdot y_2\end{aligned}$$

Also haben wir

$$x_1 \cdot y_1 - x_2 \cdot y_2 \in I$$

gezeigt. Nach Definition der Relation $\sim_I$ ist das äquivalent zu

$$x_1 \cdot y_1 \sim_I x_2 \cdot y_2.$$

und das war zu zeigen. ✓

Ist $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins und ist I ein Ideal dieses Rings, so haben wir gerade gezeigt, dass die von diesem Ideal erzeugte Relation $\sim_I$ eine Kongruenz-Relation auf $\mathcal{R}$ ist. Nach dem Satz über Faktor-Ringe (das war Satz 51 auf Seite 64) folgt nun, dass die Struktur

$$\mathcal{R}/I := \langle R/\sim_I, [0]_{\sim_I}, [1]_{\sim_I}, +, \cdot \rangle$$

ein Ring ist. In bestimmten Fällen ist diese Struktur sogar ein Körper. Das werden wir jetzt näher untersuchen.

Definition 54 (maximales Ideal) Es sei $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins. Ein Ideal I von $\mathcal{R}$ mit $I \neq R$ ist ein *maximales Ideal* genau dann, wenn für jedes andere Ideal J von $\mathcal{R}$ gilt:

$$I \subseteq J \rightarrow J = I \vee J = R.$$

Das Ideal ist also maximal, wenn es zwischen dem Ideal I und dem Eins-Ideal R keine weiteren Ideale gibt.

Der nächste Satz zeigt uns, in welchen Fällen wir mit Hilfe eines Ideals einen Körper konstruieren können.

Satz 55 (Faktor-Ringe maximaler Ideale sind Körper)
Es $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins und I sei ein maximales Ideal in $\mathcal{R}$. Dann ist der Faktor-Ring

$$\mathcal{R}/I := \langle R/\sim_I, [0]_{\sim_I}, [1]_{\sim_I}, +, \cdot \rangle$$

ein Körper.

Beweis: Es ist zu zeigen, dass es für jede Äquivalenz-Klasse $[a]_{\sim_I} \neq [0]_{\sim_I}$ ein multiplikatives Inverses, also eine Äquivalenz-Klasse $[b]_{\sim_I}$ existiert, so dass

$$[a]_{\sim_I} \cdot [b]_{\sim_I} = [1]_{\sim_I}$$

gilt. Nach unserer Definition des Multiplikations-Operators "$\cdot$" auf $R/\sim_I$ ist diese Gleichung äquivalent zu

$$[a \cdot b]_{\sim_I} = [1]_{\sim_I}$$

und nach dem Satz über die Charakterisierung der Äquivalenz-Klassen (13 auf Seite 34) ist diese Gleichung genau dann erfüllt, wenn

$$a \cdot b \sim_I 1$$

gilt. Nach Definition der Aquivalenz-Relation $\sim_I$ können wir diese Bedingung als

$$a \cdot b - 1 \in I$$

schreiben. Genauso sehen wir, dass die Bedingung $[a]_{\sim_I} \neq [0]_{\sim_I}$ zu $a - 0 \notin I$ äquivalent ist. Wir müssen also für alle $a \in R$ mit $a \notin I$ ein $b \in R$ finden, so dass $a \cdot b - 1 \in I$ gilt.

$$\text{zu zeigen:} \quad \forall a \in R : \big(a \notin I \rightarrow \exists b \in R : a \cdot b - 1 \in I\big) \tag{$*$}$$

Wir definieren eine Menge J als

$$J := \big\{a \cdot x + y \mid x \in R \wedge y \in I\big\}.$$

Wir zeigen, dass J ein Ideal des Rings $\mathcal{R}$ ist.

1. Wir zeigen, dass $0 \in J$ ist.

   Da I eine Ideal ist, gilt $0 \in I$. Setzen wir in der Definition von $x := 0$ und $y := 0$, was wegen $0 \in I$ möglich ist, so erhalten wir

   $$a \cdot 0 + 0 \in J, \quad \text{also} \quad 0 \in J. \;\checkmark$$

2. Wir zeigen, dass J abgeschlossen ist unter Addition.

   Es gelte $a \cdot x_1 + y_1 \in J$ und $a \cdot x_2 + y_2 \in J$ und es seien $x_1, x_2 \in R$ und $y_1, y_2 \in I$. Ofensichtlich ist dann auch $x_1 + x_2 \in R$ und da I unter Addition abgeschlossen ist, folgt $y_1 + y_2 \in I$. Dann haben wir

   $$(a \cdot x_1 + y_1) + (a \cdot x_2 + y_2) = a \cdot (x_1 + x_2) + (y_1 + y_2) \in J. \;\checkmark$$

3. Wir zeigen, dass J mit jeder Zahl z auch das zugehörige additive Inverse $-z$ enthält.

   Es gelte $a \cdot x + y \in J$, wobei $x \in R$ und $y \in I$ gelte. Offensichtlich ist dann auch $-x \in R$ und da mit y auch $-y$ ein Element von I ist, haben wir

   $$-(a \cdot x + y) = a \cdot (-x) + (-y) \in J. \;\checkmark$$

4. Wir zeigen, dass J unter Multiplikation mit beliebigen Elementen des Rings abgeschlossen ist.

   Es gelte $a \cdot x + y \in J$ mit $x \in R$ und $y \in J$. Weiter sei $k \in R$. Dann gilt auch $k \cdot y \in I$, denn I ist ja ein Ideal. Offensichtlich gilt $k \cdot x \in R$. Also haben wir

   $$k \cdot (a \cdot x + y) = a \cdot (k \cdot x) + (k \cdot y) \in J. \;\checkmark$$

Damit ist gezeigt, dass J ein Ideal des Rings $\mathcal{R}$ ist. Offenbar ist J eine Obermenge von I, denn für alle $y \in I$ gilt

$$y = a \cdot 0 + y \in J, \quad \text{also } I \subseteq J.$$

Als nächstes bemerken wir, dass das Ideal J von dem Ideal I verschieden ist, denn es gilt

$$a = a \cdot 1 + 0 \in J, \quad \text{aber} \quad a \notin I.$$

Nun ist die Voraussetzung, dass das Ideal I maximal ist. Da $J \neq I$ aber $I \subseteq J$ ist, kann jetzt nur noch $J = R$ gelten. Wegen $1 \in R$ folgt also $1 \in J$. Damit gibt es ein $x \in R$ und ein $y \in I$, so dass

$$1 = a \cdot x + y$$

gilt. Aus $y \in I$ folgt $-y \in I$ und damit haben wir

$$a \cdot x - 1 = -y \in I.$$

Setzen wir $b := x$, so haben wir damit die Formel $(*)$ nachgewiesen. □

Bemerkung: Wir werden später sehen, dass für eine Primzahl p das Ideal $p\mathbb{Z}$ ein maximales Ideal ist. Dann zeigt der letzte Satz, dass der Faktor-Ring $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper ist.

Kapitel 7

Zahlentheorie

In diesem Kapitel beschäftigen wir uns mit den ganzen Zahlen. Am Ende des Kapitels werden wir ausreichend Theorie entwickelt haben, um die Funktionsweise des RSA-Verschlüsselungs-Algorithmus verstehen zu können. Wir beginnen unsere Überlegungen damit, dass wir den Begriff der Teilbarkeit von Zahlen analysieren und uns ein wenig mit modularer Arithmetik beschäftigen.

7.1 Teilbarkeit und modulare Arithmetik

Definition 56 (Teiler) Es seien a und b natürlichen Zahlen. Dann ist a ein Teiler von b, wenn es eine natürliche Zahl c gibt, so dass $a \cdot c = b$ gilt. In diesem Fall schreiben wir $a \,|\, b$. Formal können wir die Teilbarkeitsrelation also wie folgt definieren:

$$a \,|\, b \iff^{\text{def}} \exists c \in \mathbb{N} : b = a \cdot c.$$

Bemerkung: Offenbar gilt $1 \,|\, n$ für alle natürlichen Zahlen n, denn für alle $n \in \mathbb{N}$ gilt $n = 1 \cdot n$. Aus der Gleichung $0 = n \cdot 0$ folgt analog, dass $n \,|\, 0$ für alle $n \in \mathbb{N}$ gilt. Schließlich zeigt die Gleichung $n = n \cdot 1$, dass $n \,|\, n$ für alle natürlichen Zahlen n gilt.

Für eine positive natürliche Zahl a bezeichnen wir die Menge aller Teiler von a mit $\texttt{teiler}(a)$. Es gilt also

$$\texttt{teiler}(a) = \{q \in \mathbb{N} \mid \exists k \in \mathbb{N} : k \cdot q = a\}.$$

Die Menge aller gemeinsamen Teiler zweier positiver natürlicher Zahlen a und b bezeichnen wir mit `gt(a,b)`. Es gilt

$$\texttt{gt}(a, b) = \texttt{teiler}(a) \cap \texttt{teiler}(b).$$

Der größte gemeinsame Teiler von a und b ist als das Maximum dieser Menge definiert, es gilt also

$$\texttt{ggt}(a, b) = \max\big(\texttt{gt}(a, b)\big).$$

Satz 57 (Divison mit Rest) Sind a und b natürliche Zahlen mit $b \neq 0$, so gibt es eindeutig bestimmte natürliche Zahlen q und r, so dass

$$a = q \cdot b + r \quad \text{mit } r < b$$

gilt. Wir nennen dann q den *Ganzzahl-Quotienten* und r den *Rest* der ganzzahligen Divison von a durch b. Als Operator für die Ganzzahl-Divison verwenden wir "$\div$" und für die Bildung des Rests verwenden wir den Operator "%". Damit gilt

$$q = a \div b \quad \text{und} \quad r = a \,\%\, b.$$

Beweis: Zunächst zeigen wir die Existenz der Zahlen q und r mit den oben behaupteten Eigenschaften. Dazu definieren wir eine Menge M von natürlichen Zahlen wie folgt:

$$M := \{p \in \mathbb{N} \mid p \cdot b \leq a\}.$$

Diese Menge ist nicht leer, es gilt $0 \in M$, da $0 \cdot b \leq a$ ist. Außerdem können wir sehen, dass $(a+1) \notin M$ ist, denn

$$(a+1) \cdot b = a \cdot b + b > a \cdot b \geq a, \quad \text{denn } b \geq 1.$$

Damit ist auch klar, dass alle Zahlen, die größer als a sind, keine Elemente von M sein können. Insgesamt wissen wir jetzt, dass die Menge nicht leer ist und dass alle Elemente von M kleinergleich a sind. Folglich muss die Menge M eine Maximum haben. Wir definieren

$$q := \max(M) \quad \text{und} \quad r := a - q \cdot b.$$

Wegen $q \in M$ wissen wir, dass

$$a \geq q \cdot b$$

gilt, woraus wir $r \geq 0$ schließen können und damit ist $r \in \mathbb{N}$.

Da wir q als Maximum der Menge M definiert haben, wissen wir weiter, dass die Zahl $q+1$ kein Element der Menge M sein kann, denn sonst wäre q nicht das Maximum. Also muss

$$(q+1) \cdot b > a$$

gelten. Wir formen diese Ungleichung wie folgt um:

$$\begin{array}{rrcll} & (q+1) \cdot b & > & a & \\ \Leftrightarrow & q \cdot b + b & > & a & \\ \Leftrightarrow & b & > & a - q \cdot b & \\ \Leftrightarrow & b & > & r & \text{nach Definition von } r. \end{array}$$

Also haben wir jetzt die zweite Behauptung $r < b$ gezeigt. Aus der Definition von r als $r = a - q \cdot b$ folgt sofort, dass

$$a = q \cdot b + r$$

gilt. Damit haben q und r die behaupteten Eigenschaften.

Als nächstes zeigen wir, dass q und r eindeutig bestimmt sind. Dazu nehmen wir an, dass zu den gegebenen Werten von a und b vier Zahlen q_1, q_2, r_1 und r_2 mit den Eigenschaften

$$a = q_1 \cdot b + r_1, \quad a = q_2 \cdot b + r_2, \quad r_1 < b, \quad \text{und} \quad r_2 < b$$

existieren. Wir müssen zeigen, dass dann $q_1 = q_2$ und $r_1 = r_2$ folgt. Aus den beiden Gleichungen folgt zunächst

$$q_1 \cdot b + r_1 = q_2 \cdot b + r_2.$$

und diese Gleichung können wir umstellen zu

$$(q_1 - q_2) \cdot b = r_2 - r_1 \tag{7.1}$$

Wir können ohne Beschränkung der Allgemeinheit annehmen, dass $r_2 \geq r_1$ ist, denn andernfalls können wir die Zahlen r_1 und q_1 mit den Zahlen r_2 und q_2 vertauschen. Dann zeigt Gleichung (7.1), dass b ein Teiler von $r_2 - r_1$ ist. Wegen $b > r_2 \geq r_1$ wissen wir, dass

$$0 \leq r_2 - r_1 < b$$

gilt. Soll nun b ein Teiler von $r_2 - r_1$ sein, so muss $r_2 - r_1 = 0$ also $r_2 = r_1$ gelten. Daraus folgt dann

$$(q_1 - q_2) \cdot b = 0$$

und wegen $b \neq 0$ muss auch $q_1 = q_2$ gelten. $\square$

Aufgabe 13: Wie müssen wir den obigen Satz ändern, damit er auch dann noch gilt, wenn $a \in \mathbb{Z}$ ist? Formulieren Sie die geänderte Version des Satzes und beweisen Sie Ihre Version des Satzes!

Bemerkung: In den meisten Programmier-Sprachen ist die ganzzahlige Division so implementiert, dass die Gleichung

$$(a \div q) \cdot q + a \,\%\, q = a$$

für $a < 0$ im Allgemeinen nicht gilt!

Mit dem letzten Satz können wir die Menge der Teiler einer natürlichen Zahl a auch wie folgt definieren:

$$\texttt{teiler}(a) = \{q \in \mathbb{N} \mid a \,\%\, q = 0\}.$$

Wir erinnern an dieser Stelle an die Definition der Äquivalenz-Relationen $\approx_n$, die wir für $n > 0$ im Abschnitt 3.15 durch die Formel

$$\approx_n := \{\langle x, y\rangle \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}\colon k \cdot n = x - y\}$$

definiert hatten. Der nächste Satz zeigt, dass sich diese Relation auch etwas anders charakterisieren läßt.

Satz 58 Für $a, b \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $n > 0$ gilt

$$a \approx_n b \;\leftrightarrow\; a \,\%\, n = b \,\%\, n.$$

Beweis: Wir zerlegen den Beweis in zwei Teile:

1. "$\Rightarrow$": Aus $a \approx_n b$ folgt nach Definition der Relation $\approx_n$, dass es ein $h \in \mathbb{Z}$ gibt mit

   $$a - b = h \cdot n.$$

   Definieren wir $l := b \div n$, so ist $l \in \mathbb{Z}$ und es gilt

   $$b = l \cdot n + b \,\%\, n.$$

   Setzen wir dies in die Gleichung für $a - b$ ein, so erhalten wir

   $$a - (l \cdot n + b \,\%\, n) = h \cdot n,$$

   was wir zu

   $$a = (h + l) \cdot l + b \,\%\, n,$$

   umstellen können. Aus dieser Gleichung folgt wegen der im Satz von der Divison mit Rest (Satz 57) gemachten Eindeutigkeits-Aussage, dass

   $$a \,\%\, n = b \,\%\, n$$

   gilt. ✓

2. "$\Leftarrow$": Es sei nun

   $$a \,\%\, n = b \,\%\, n$$

   vorausgesetzt. Nach Definition des Modulo-Operators gibt es ganze Zahlen $k, l \in \mathbb{Z}$, so dass

   $$a \,\%\, n = a - k \cdot n \quad \text{und} \quad b \,\%\, n = b - l \cdot n$$

   gilt, so dass wir insgesamt

   $$a - k \cdot n = b - l \cdot n$$

   haben. Daraus folgt

$$a - b = (k - l) \cdot n,$$

so dass n ein Teiler von $(a - b)$ ist und dass heißt $a \approx_n b$. ✓ □

Satz 59 Die Relation $\approx_n$ ist eine Kongruenz-Relation.

Beweis: Es gilt

$$\begin{array}{ll} & x \approx_n y \\ \Leftrightarrow & \exists k \in \mathbb{Z} : x - y = k \cdot n \\ \Leftrightarrow & x - y \in n\mathbb{Z} \\ \Leftrightarrow & x \sim_{n\mathbb{Z}} y \end{array}$$

Damit sehen wir, dass die Relation $\approx_n$ mit der von dem Ideal $n\mathbb{Z}$ erzeugten Kongruenz-Relation $\sim_{n\mathbb{Z}}$ übereinstimmt und folglich eine Kongruenz-Relation ist. □

Wir erinnern an dieser Stelle daran, dass wir im letzten Kapitel für natürliche Zahlen k die Menge $k\mathbb{Z}$ aller Vielfachen von k als

$$k\mathbb{Z} = \{k \cdot z \mid z \in \mathbb{Z}\}$$

definiert haben. Außerdem hatten wir gezeigt, dass diese Mengen Ideale sind. Der nächste Satz zeigt, dass alle Ideale in dem Ring $\mathbb{Z}$ der ganzen Zahlen diese Form haben.

Satz 60 ($\mathbb{Z}$ ist ein Haupt-Ideal-Ring)
Ist $I \subseteq \mathbb{Z}$ ein Ideal, so gibt es eine natürliche Zahl k, so dass $I = k\mathbb{Z}$ gilt.

Beweis: Wir betrachten zwei Fälle: Entweder ist $I = \{0\}$ oder nicht.

1. Fall: $I = \{0\}$.

   Wegen $\{0\} = 0\mathbb{Z}$ ist die Behauptung in diesem Fall offensichtlich wahr.

2. Fall: $I \neq \{0\}$.

   Dann gibt es ein $l \in I$ mit $l \neq 0$. Da I ein Ideal ist, liegt mit l auch $-l$ in dem Ideal I. Eine dieser beiden Zahlen ist positiv. Daher ist die Menge

   $$M := \{x \in I \mid x > 0\}$$

   nicht leer und hat folglich ein Minimum $k = \min(M)$, für welches offenbar

   $$k \in I \quad \text{und} \quad k > 0$$

   gilt. Wir behaupten, dass

   $$I = k\mathbb{Z}$$

   gilt. Sei also $y \in I$. Wir teilen y durch k und nach dem Satz über ganzzahlige Division mit Rest finden wir dann Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit

   $$y = q \cdot k + r \quad \text{und} \quad 0 \leq r < k.$$

   Aus der ersten Gleichung folgt

   $$r = y + (-q) \cdot k.$$

   Da nun sowohl $y \in I$ als auch $k \in I$ gilt und Ideale sowohl unter Multiplikation mit beliebigen Ring-Elementen als auch unter Addition abgeschlossen sind, folgt

   $$r \in I.$$

   Nun ist einerseits $k = \min\big(\{x \in I \mid x > 0\}\big)$, andererseits ist $r < k$. Das geht beides zusammen nur, wenn

$$r = 0$$

ist. Damit haben wir dann aber

$$y = q \cdot k$$

gezeigt, woraus sofort

$$y \in k\mathbb{Z}$$

folgt. Da y bei diesen Betrachtungen ein beliebiges Element der Menge I war, zeigt diese Überlegungen insgesamt, dass $I \subseteq k\mathbb{Z}$ gilt. Aus der Tatsache, dass $k \in I$ ist, folgt andererseits, dass $k\mathbb{Z} \subseteq I$ gilt, so dass wir insgesamt

$$I = k\mathbb{Z}$$

gezeigt haben. □

Bemerkung: Wir erinnern an dieser Stelle daran, dass wir für einen Ring $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ und ein Ring-Element $k \in R$ die Ideale der Form

$$gen(k) = \{k \cdot x \mid x \in R\}$$

als *Haupt-Ideale* bezeichnet haben. Der letzte Satz zeigt also, dass alle Ideale des Rings der ganzen Zahlen Haupt-Ideale sind. Einen Ring mit der Eigenschaft, dass alle Ideale bereits Haupt-Ideale sind, bezeichnen wir als *Haupt-Ideal-Ring*. Der letzte Satz zeigt daher, dass der Ring der ganzen Zahlen ein Haupt-Ideal-Ring ist.

Lemma 61 Für $u, v \in \mathbb{N}$ gilt

$$u\mathbb{Z} \subseteq v\mathbb{Z} \;\Leftrightarrow\; v \mid u.$$

Beweis: Wir zerlegen den Beweis der Äquivalenz der beiden Aussagen in den Beweis der beiden Implikationen.

1. "⇒": Wegen $u = u \cdot 1$ gilt

   $$u \in u\mathbb{Z}$$

   und aus der Voraussetzung $u\mathbb{Z} \subseteq v\mathbb{Z}$ folgt dann

   $$u \in v\mathbb{Z}.$$

   Nach Definition der Menge $v\mathbb{Z}$ gibt es nun ein $k \in \mathbb{Z}$, so dass

   $$u = v \cdot k$$

   gilt. Nach der Definition der Teilbarkeit haben wir also

   $$v \mid u.$$

2. "⇐": Es sei jetzt $v \mid u$ vorausgesetzt. Dann gibt es ein $k \in \mathbb{N}$ mit

   $$u = v \cdot k.$$

   Sei weiter $a \in u\mathbb{Z}$ beliebig. Nach Definition der Menge $u\mathbb{Z}$ gibt es also ein $x \in \mathbb{Z}$ mit

   $$a = u \cdot x.$$

   Ersetzen wir in dieser Gleichung u durch $v \cdot k$, so erhalten wir

   $$a = v \cdot (k \cdot x)$$

   und daraus folgt sofort

   $$a \in v\mathbb{Z},$$

   so dass wir insgesamt $u\mathbb{Z} \subseteq v\mathbb{Z}$ gezeigt haben.

Satz 62 Es sei p eine Primzahl. Dann ist das Ideal $p\mathbb{Z}$ ein maximales Ideal.

Beweis: Es sei $J \subseteq \mathbb{Z}$ ein Ideal, für das

$$p\mathbb{Z} \subseteq J$$

gilt. Wir müssen zeigen, dass dann $J = p\mathbb{Z}$ oder $J = \mathbb{Z}$ gilt. Da $\mathbb{Z}$ ein Haupt-Ideal-Ring ist, gibt es ein $q \in \mathbb{Z}$ mit

$$J = q\mathbb{Z}.$$

Damit haben wir

$$p\mathbb{Z} \subseteq q\mathbb{Z}$$

und nach dem letzten Lemma folgt daraus

$$q \,|\, p.$$

Da p eine Primzahl ist, gibt es nur zwei Zahlen, die Teiler von p sind: Die Zahl 1 und die Zahl p. Wir haben also

$$q = 1 \quad \text{oder} \quad q = p,$$

woraus

$$J = 1\mathbb{Z} = \mathbb{Z} \quad \text{oder} \quad J = p\mathbb{Z}$$

folgt und damit ist das Ideal $p\mathbb{Z}$ ein maximales Ideal. □

Korollar 63 Falls p eine Primzahl ist, dann ist $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper.

Beweis: Im letzten Kapitel haben wir gezeigt, dass für einen Ring R und ein maximales Ideal $I \subseteq R$ der Faktor-Ring R/I ein Körper ist. Wir haben gerade gesehen, dass für eine Primzahl p das Ideal $p\mathbb{Z}$ maximal ist. Diese beiden Tatsachen ergeben zusammen die Behauptung. □

Bemerkung: Bisher hatten alle Körper, die wir kennengelernt haben, unendlich viele Elemente. Der letzte Satz zeigt uns, dass es auch endliche Körper gibt.

Satz 64 (Lemma von Bézout) Es seien $a, b \in \mathbb{N}$. Dann existieren $x, y \in \mathbb{Z}$, so dass

$$ggt(a, b) = x \cdot a + y \cdot b$$

gilt. Der größte gemeinsame Teiler zweier natürlicher Zahlen a und b läßt sich also immer als ganzzahlige Linear-Kombination von a und b schreiben.

Beweis: Wir definieren die Menge I wie folgt:

$$I := \big\{ x \cdot a + y \cdot b \mid x, y \in \mathbb{Z} \big\}.$$

Wir zeigen, dass I ein Ideal ist:

1. $0 = 0 \cdot a + 0 \cdot b \in I$.
2. I ist abgeschlossen unter Bildung des additiven Inversen: Sei $u = x \cdot a + y \cdot b \in I$. Dann folgt sofort
$$-u = (-x) \cdot a + (-y) \cdot b \in I.$$
3. I ist abgeschlossen unter Addition: Seien $u = x_1 \cdot a + y_1 \cdot b \in I$ und $v = x_2 \cdot a + y_2 \cdot b \in I$. dann folgt
$$u + v = (x_1 + x_2) \cdot a + (y_1 + y_2) \cdot b \in I.$$

4. I ist abgeschlossen unter Multiplikation mit beliebigen ganzen Zahlen. Sei $u = x \cdot a + y \cdot b \in I$ und $z \in \mathbb{Z}$. Dann gilt

$$z \cdot u = (z \cdot x) \cdot a + (z \cdot y) \cdot b \in I.$$

Da der Ring der ganzen Zahlen ein Haupt-Ideal-Ring ist, gibt es also eine Zahl $d \in \mathbb{N}$, so dass

$$I = d\mathbb{Z}$$

gilt. Setzen wir in der Definition von I wahlweise $y = 0$ oder $x = 0$ ein, so sehen wir, dass

$$a\mathbb{Z} \subseteq I \quad \text{und} \quad b\mathbb{Z} \subseteq I$$

gilt, woraus nun

$$a\mathbb{Z} \subseteq d\mathbb{Z} \quad \text{und} \quad b\mathbb{Z} \subseteq d\mathbb{Z},$$

folgt. Nach dem Lemma, das wir gerade bewiesen haben, folgt daraus

$$d \mid a \quad \text{und} \quad d \mid b.$$

Damit ist d ein gemeinsamer Teiler von a und b. Wir zeigen, dass d sogar der größte gemeinsame Teiler von a und b ist. Dazu betrachten wir einen beliebigen anderen gemeinsamen Teiler e von a und b:

$$e \mid a \quad \text{und} \quad e \mid b.$$

Nach dem letzten Lemma folgt daraus

$$a\mathbb{Z} \subseteq e\mathbb{Z} \quad \text{und} \quad b\mathbb{Z} \subseteq e\mathbb{Z}.$$

Da wir das Ideal I als $\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}$ definiert hatten, können wir nun sehen, dass

$$I \subseteq e\mathbb{Z}$$

gilt, denn für $x, y \in \mathbb{Z}$ haben wir einerseits $x \cdot a \in a\mathbb{Z} \subseteq e\mathbb{Z}$ und andererseits $y \cdot b \in b\mathbb{Z} \subseteq e\mathbb{Z}$, so dass aufgrund der Abgeschlossenheit des Ideals $e\mathbb{Z}$ unter Addition insgesamt

$$a \cdot x + b \cdot y \in e\mathbb{Z}$$

gilt. Setzen wir in der Beziehung $I \subseteq e\mathbb{Z}$ für I den Ausdruck $d\mathbb{Z}$ ein, haben wir also

$$d\mathbb{Z} \subseteq e\mathbb{Z}$$

gezeigt, was nach dem letzten Lemma zu

$$e \mid d$$

äquivalent ist. Damit haben wir insgesamt gezeigt, dass

$$d = ggt(a, b)$$

gilt. Wegen $I = d\mathbb{Z}$ und $d \in d\mathbb{Z}$ folgt also

$$ggt(a, b) \in \{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}.$$

Damit gibt es dann $x, y \in \mathbb{Z}$, so dass

$$ggt(a, b) = x \cdot a + y \cdot b$$

gilt. □

Bemerkung: Der Beweis des letzten Satzes war nicht konstruktiv. Wir werden im nächsten Abschnitt ein Verfahren angeben, mit dessen Hilfe wir die Zahlen x und y, für $x \cdot a + y \cdot b = ggt(a, b)$ gilt, auch tatsächlich berechnen können.

7.2 Der Euklidische Algorithmus

Wir präsentieren nun einen Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier natürlicher Zahlen x und y. Abbildung 7.1 auf Seite 83 zeigt eine *SetlX*-Funktion, die für gegebene positive natürliche Zahlen x und y den größten gemeinsamen Teiler $ggt(x, y)$ berechnet. Diese Funktion implementiert den *Euklid'schen Algorithmus* zur Berechnung des größten gemeinsamen Teilers.

```
1  // Precondition: x > 0 and y > 0.
2  ggtS := procedure(x, y) {
3      if (x < y) {
4          return ggt(x, y - x);
5      }
6      if (y < x) {
7          return ggt(x - y, y);
8      }
9      // We must have x = y at this point.
10     return x;
11 };
```

Abbildung 7.1: Der Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers.

Um die Korrektheit des Euklidischen Algorithmus zu beweisen, benötigen wir das folgende Lemma.

Lemma 65 Sind $x, y \in \mathbb{Z}$, so gilt für alle $n \in \mathbb{N}^+$

$$x \,\%\, n = 0 \wedge y \,\%\, n = 0 \;\leftrightarrow\; (x + y) \,\%\, n = 0 \wedge y \,\%\, n = 0.$$

Beweis: Die Formel

$$p \wedge q \;\leftrightarrow\; r \wedge q$$

ist aussagenlogisch äquivalent zu der Formel

$$q \rightarrow (p \leftrightarrow r)$$

Daher reicht es, wenn wir

$$y \,\%\, n = 0 \rightarrow \big(x \,\%\, n = 0 \;\leftrightarrow\; (x + y) \,\%\, n = 0\big)$$

nachweisen. Unter Benutzung der Relation $\approx_n$ und bei weiterer Berücksichtigung der Tatsache, dass

$$a \approx_n b \;\leftrightarrow\; a \,\%\, n = b \,\%\, n$$

gilt, können wir diese Formel auch als

$$y \approx_n 0 \rightarrow \big(x \approx_n 0 \;\leftrightarrow\; (x + y) \approx_n 0\big)$$

schreiben. Diese Formel folgt aber aus der schon früher bewiesenen Tatsache, dass $\approx_n$ eine Kongruenz-Relation ist. Für die Richtung "$\rightarrow$" ist das unmittelbar klar und für die Richtung "$\leftarrow$" ist nur zu bemerken, dass aus

$$(x + y) \approx_n 0 \quad \text{und} \quad y \approx_n 0,$$

aus der Verträglichkeit der Relation $\approx_n$ mit der Addition selbstverständlich auch die Verträglichkeit mit der Subtraktion folgt, so dass

$$x = (x + y) - y \approx_n 0 - 0 = 0, \quad \text{also } x \approx_n 0$$

folgt. □

Korollar 66 Sind x und y positive natürliche Zahlen, so gilt

$$\texttt{ggt}(x+y,y) = \texttt{ggt}(x,y).$$

Beweis: Das vorige Lemma zeigt, dass die Menge der gemeinsamen Teiler der beiden Paare $\langle x, y\rangle$ und $\langle x+y, y\rangle$ identisch sind, dass also

$$\texttt{gt}(x,y) = \texttt{gt}(x+y,y)$$

gilt. Wegen

$$\texttt{ggt}(x,y) = \max\big(\texttt{gt}(x,y)\big) = \max\big(\texttt{gt}(x+y,y)\big) = \texttt{ggt}(x+y,y)$$

folgt die Behauptung. □

Satz 67 (Korrektheit des Euklidischen Algorithmus) Der Aufruf $\texttt{ggtS}(x,y)$ des in Abbildung 7.1 gezeigten Algorithmus berechnet für zwei positive natürliche Zahlen x und y den größten gemeinsamen Teiler von x und y:

$$\forall x, y \in \mathbb{N} : \texttt{ggtS}(x,y) = \mathit{ggt}(x,y).$$

Beweis: Wir führen den Beweis der Behauptung durch *Wertverlaufs-Induktion*.

1. Induktions-Anfang:

   Die Berechnung bricht genau dann ab, wenn $x = y$ ist. In diesem Fall wird als Ergebnis x zurückgegeben, wir haben also

   $$\texttt{ggtS}(x,y) = x$$

   Andererseits gilt dann

   $$\mathit{ggt}(x,y) = \mathit{ggt}(x,x) = x,$$

   denn x ist offenbar der größte gemeinsame Teiler von x und x.

2. Induktions-Schritt: Hier gibt es zwei Fälle zu betrachten, $x < y$ und $y < x$.

   (a) $x < y$: In diesem Fall sagt die Induktions-Voraussetzung, dass das Ergebnis des rekursiven Aufrufs der Funktion ggtS() korrekt ist, wir dürfen also voraussetzen, dass

   $$\texttt{ggtS}(x, y-x) = \mathit{ggt}(x, y-x)$$

   gilt. Zu zeigen ist

   $$\texttt{ggtS}(x,y) = \mathit{ggt}(x,y).$$

   Der Nachweis verläuft wie folgt:

   $$\begin{array}{rcll}
   \texttt{ggtS}(x,y) & = & \texttt{ggtS}(x,y-x) & \text{(nach Definition von } \texttt{ggtS}(x,y)) \\
   & \overset{IV}{=} & \mathit{ggt}(x,y-x) & \\
   & = & \mathit{ggt}(y-x,x) & \text{(denn } \mathit{ggt}(a,b) = \mathit{ggt}(b,a)) \\
   & = & \mathit{ggt}\big((y-x)+x,x\big) & \text{(nach Korollar 66)} \\
   & = & \mathit{ggt}(y,x) & \\
   & = & \mathit{ggt}(x,y) &
   \end{array}$$

   und das war zu zeigen.

   (b) $y < x$: Dieser Fall ist analog zu dem vorhergehenden Fall und wird daher nicht weiter ausgeführt.

Um nachzuweisen, dass das in Abbildung 7.1 gezeigte Programm tatsächlich funktioniert, müssen wir noch zeigen, dass es in jedem Fall terminiert. Dies folgt aber sofort daraus, dass die Summe der Argumente $x + y$ bei jedem rekursiven Aufruf kleiner wird:

1. Falls $x < y$ ist, haben wir für die Summe der Argument des rekursiven Aufrufs

   $$x + (y - x) = y < x + y \quad \text{falls } x > 0 \text{ ist.}$$

2. Falls $y < x$ ist, haben wir für die Summe der Argument des rekursiven Aufrufs

   $$(x - y) + y = x < x + y \quad \text{falls } y > 0 \text{ ist.}$$

Falls nun x und y beim ersten Aufruf von 0 verschieden sind, so werden die Summen bei jedem Aufruf kleiner, denn es ist auch sichergestellt, dass bei keinem rekursiven Aufruf eines der Argumente von *ggt*() den Wert 0 annimmt: Falls $x < y$ ist, ist $y - x > 0$ und wenn $y < x$ ist, dann ist $x - y > 0$ und im Fall $x = y$ bricht die Rekursion ab. □

```
1  ggtS2 := procedure(x, y) {
2      if (y == 0) {
3          return x;
4      }
5      return ggt(y, x % y);
6  };
```

Abbildung 7.2: Der verbesserte Euklidische Algorithmus.

Der in Abbildung 7.1 gezeigte Algorithmus ist nicht sehr effizient. Abbildung 7.2 zeigt eine verbesserte Version. Um die Korrektheit der verbesserten Version beweisen zu können, benötigen wir einen weiteren Hilfssatz.

Lemma 68 Für $x, y \in \mathbb{Z}$, $n \in \mathbb{N}^+$ und $k \in \mathbb{N}$ gilt

$$x \,\%\, n = 0 \wedge y \,\%\, n = 0 \;\leftrightarrow\; (x - k \cdot y) \,\%\, n = 0 \wedge y \,\%\, n = 0.$$

Beweis: Berücksichtigen wir, dass beispielsweise die Gleichung $x \,\%\, n = 0$ äquivalent zu $x \approx_n 0$ ist, so können wir die obige Behauptung auch in der Form

$$y \approx_n 0 \rightarrow \big(x \approx_n 0 \leftrightarrow (x - k \cdot y) \approx_n 0\big)$$

schreiben. Diese Behauptung folgt aber aus der Tatsache, dass die Relation $\approx_n$ eine Kongruenz-Relation ist. □

Korollar 69 Für $x, y \in \mathbb{Z}$ und $y \neq 0$ gilt

$$\mathit{ggt}(x, y) = \mathit{ggt}(y, x \,\%\, y).$$

Beweis: Nach dem Satz über die Divison mit Rest gibt es eine Zahl $k \in \mathbb{Z}$, so dass

$$x = k \cdot y + x \,\%\, y$$

gilt. Diese Gleichung formen wir zu

$$x \,\%\, y = x - k \cdot y$$

um. Dann haben wir für beliebige $n \in \mathbb{N}$ die folgende Kette von Äquivalenzen:

$$
\begin{array}{lll}
 & (x \,\%\, y) \,\%\, n = 0 \wedge y \,\%\, n = 0 & \\
\Leftrightarrow & (x - k \cdot y) \,\%\, n = 0 \wedge y \,\%\, n = 0 & \\
\Leftrightarrow & x \,\%\, n = 0 \wedge y \,\%\, n = 0 & \text{nach der letzten Aufgabe}
\end{array}
$$

Damit sehen wir aber, dass die Zahlen $x \,\%\, n$ und y die selben gemeinsamen Teiler haben wie die Zahlen x und y

$$gt(x \,\%\, n, y) = gt(x, y).$$

Daraus folgt sofort

$$ggt(x \,\%\, n, y) = ggt(x, y)$$

und wegen $ggt(a, b) = ggt(b, a)$ ist das die Behauptung. □

Satz 70 (Korrektheit des verbesserten Euklidischen Algorithmus)
Für die in Abbildung 7.2 gezeigte Funktion *ggtS2*() gilt

$$\texttt{ggtS2}(x, y) = ggt(x, y) \quad \text{für } x, y \in \mathbb{N}.$$

Beweis: Wir führen den Beweis wieder durch eine Wertverlaufs-Induktion.

1. Induktions-Anfang: $y = 0$. In diesem Fall gilt

   $$\texttt{ggtS2}(x, 0) = x = ggt(x, 0).$$

2. Induktions-Schritt: Falls $y \neq 0$ ist, haben wir

   $$
   \begin{array}{rcl}
   \texttt{ggtS2}(x, y) & = & \texttt{ggtS2}(y, x \,\%\, y) \\
   & \overset{IV}{=} & ggt(y, x \,\%\, y) \\
   & = & ggt(x, y),
   \end{array}
   $$

   wobei wir im letzten Schritt das Korollar 69 benutzt haben.

Es ist noch zu zeigen, dass ein Aufruf der Prozedur $\texttt{ggtS2}(x, y)$ für beliebige $x, y \in \mathbb{N}$ terminiert. Wir können ohne Beschränkung der Allgemeinheit anehmen, dass $x \geq y$ ist, denn falls $x < y$ ist, dann gilt $x \,\%\, y = x$ und damit werden dann bei dem ersten rekursiven Aufruf $\texttt{ggt}(y, x \,\%\, y)$ die Argumente x und y vertauscht.

Sei also jetzt $y \leq x$. Wir zeigen, dass diese Ungleichung dann auch bei jedem rekursiven Aufruf bestehen bleibt, denn es gilt

$$x \,\%\, y < y.$$

Weiter sehen wir, dass unter der Voraussetzung $y \leq x$ die Summe der Argumente bei jedem rekursiven Aufruf kleiner wird, denn wenn $y \leq x$ ist, haben wir

$$y + x \,\%\, y < y + x, \quad \text{da } x \,\%\, y < y \leq x \text{ ist.}$$

Da die Summe zweier natürlicher Zahlen nur endlich oft verkleinert werden kann, terminiert der Algorithmus. □

Der Euklidische Algorithmus kann so erweitert werden, dass für gegebene Zahlen $x, y \in \mathbb{N}$ zwei Zahlen $\alpha, \beta \in \mathbb{Z}$ berechnet werden, so dass

$$\alpha \cdot x + \beta \cdot y = ggt(x, y)$$

gilt. Abbildung 7.3 zeigt eine entsprechende Erweiterung.

Satz 71 (Korrektheit des erweiterten Euklidischen Algorithmus)
Die in Abbildung 7.3 gezeigte Funktion eggt() erfüllt folgende Spezifikation:

$$\forall x, y \in \mathbb{N} : \big(\texttt{eggt}(x, y) = [\alpha, \beta] \;\Rightarrow\; \alpha \cdot x + \beta \cdot y = ggt(x, y)\big).$$

```
1  eggt := procedure(x, y) {
2      if (y == 0) {
3          return [ 1, 0 ];
4      }
5      q := x / y;
6      r := x % y;
7      [ s, t ] := eggt(y, r);
8      return [ t, s - q * t ];
9  };
```

Abbildung 7.3: Der erweiterte Euklidische Algorithmus.

Beweis: Wir führen den Beweis durch Wertverlaufs-Induktion.

1. Induktions-Anfang: $y = 0$.

   Es gilt $\texttt{eggt}(x, 0) = [1, 0]$. Also haben wir $\alpha = 1$ und $\beta = 0$. Offensichtlich gilt

   $$\alpha \cdot x + \beta \cdot y = 1 \cdot x + 0 \cdot y = x = ggt(x, 0).$$

   und damit ist die Behauptung in diesem Fall gezeigt.

2. Induktions-Schritt: $y \neq 0$.

   Nach Induktions-Voraussetzung wissen wir, dass für den rekursiven Aufruf $eggt(y, r)$ die Gleichung

   $$s \cdot y + t \cdot r = ggt(y, r) \tag{7.2}$$

   richtig ist. Nach dem Programm gilt $r = x \,\%\, y$ und nach der Definition des Modulo-Operators ist $x \,\%\, y = x - (x \div y) \cdot y$. Setzen wir dies in Gleichung (7.2) ein, so erhalten wir

   $$s \cdot y + t \cdot \big(x - (x \div y) \cdot y\big) = ggt(y, x \,\%\, y). \tag{7.3}$$

   Stellen wir die linke Seite dieser Gleichung um und berücksichtigen weiter, dass nach Korollar 69 $ggt(y, x \,\%\, y) = ggt(x, y)$ gilt, so vereinfacht sich Gleichung (7.3) zu

   $$t \cdot x + \big(s - (x \div y) \cdot t\big) \cdot y = ggt(x, y).$$

   In der Funktion $\texttt{eggt}()$ ist q als x/y definiert, wobei dort der Operator "/" aber für die ganzzahlige Division mit Rest steht, so dass tatsächlich $q = x \div y$ gilt. Damit haben wir

   $$t \cdot x + (s - q \cdot t) \cdot y = ggt(x, y)$$

   und das ist wegen $\alpha = t$ und $\beta = s - q \cdot t$ die Behauptung.

Der Nachweis der Terminierung ist der Selbe wie bei der Funktion *ggtS2*() und wird daher nicht noch einmal angegeben. □

7.3 Der Fundamentalsatz der Arithmetik

Satz 72 (Lemma von Euler)
Es seien a und b natürliche Zahlen und p sei eine Primzahl. Dann gilt

$$p \mid a \cdot b \;\Rightarrow\; p \mid a \vee p \mid b.$$

In Worten: Wenn p das Produkt zweier Zahlen teilt, dann muss p eine der beiden Zahlen des Produkts teilen.

Beweis: Wenn p das Produkt $a \cdot b$ teilt, dann gibt es eine natürliche Zahl c, so dass

$$c \cdot p = a \cdot b \tag{7.4}$$

ist. Wir nehmen an, dass p kein Teiler von a ist. Dann müssen wir zeigen, dass p eine Teiler von b ist. Wenn p kein Teiler von a ist, dann folgt aus der Tatsache, dass p eine Primzahl ist, dass

$$ggt(p, a) = 1$$

gilt. Nach dem Lemma von Bezóut (Satz 64) gibt es also ganze Zahlen x und y, so dass

$$1 = x \cdot p + y \cdot a$$

gilt. Wir multiplizieren diese Gleichung mit b und erhalten

$$b = x \cdot p \cdot b + y \cdot a \cdot b.$$

An dieser Stelle nutzen wir aus, dass nach Gleichung (7.4) $a \cdot b = c \cdot p$ gilt und formen die obige Gleichung für b wie folgt um:

$$b = x \cdot p \cdot b + y \cdot c \cdot p.$$

Klammern wir hier p aus, so haben wir

$$b = (x \cdot b + y \cdot c) \cdot p.$$

und daraus sehen wir, dass p ein Teiler von b ist, was zu zeigen war. □

Eine *Primfaktor-Zerlegung* einer natürlichen Zahl n ist ein Produkt der Form

$$p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_k,$$

wobei alle Faktoren $p_1, \cdots, p_k$ Primzahlen sind. Beispielsweise ist

$$2 \cdot 3 \cdot 3 \cdot 5$$

eine Primfaktor-Zerlegung der Zahl 90. Üblicherweise fassen wir dabei noch gleiche Faktoren zusammen, in dem oberen Beispiel würden wir also

$$90 = 2 \cdot 3^2 \cdot 5$$

schreiben. Sind $p_1, \cdots, p_k$ verschiedene Primzahlen, die der Größe nach angeordnet sind, gilt also

$$p_1 < p_2 < \cdots < p_i < p_{i+1} < \cdots < p_k,$$

und sind $e_1, \cdots, e_k$ positive natürliche Zahl, so nennen wir einen Ausdruck der Form

$$\prod_{i=1}^{k} p_i^{e_i} = p_1^{e_1} \cdot \ \ldots \ \cdot p_k^{e_k}$$

eine *kanonische Primfaktor-Zerlegung*. Die Tasache, dass es für jede natürliche Zahl, die größer als 1 ist, eine kanonische Primfaktor-Zerlegung gibt, die darüber hinaus noch eindeutig ist, ist ein wesentliches Ergebnis der elementaren Zahlentheorie.

Theorem 73 (Fundamentalsatz der Arithmetik)
Es sei n eine natürliche Zahlen größer als 1. Dann läßt sich n auf genau eine Weise in der Form

$$n = p_1^{e_1} \cdot \ \ldots \ \cdot p_k^{e_k} \quad \text{mit Primzahlen } p_1 < p_2 < \cdots < p_k$$

und positiven ganzzahligen Exponenten $e_1, \cdots, e_n$ schreiben.

Beweis: Wir zeigen zunächst die Existenz einer Primfaktor-Zerlegung für jede natürliche Zahl n größer als 1. Wir führen diesen Nachweis durch Induktion nach n.

I.A. $n = 2$:

Da 2 eine Primzahl ist, können wir

$$n = 2^1$$

schreiben und haben damit eine kanonische Primfaktor-Zerlegung gefunden.

I.S. $2, \cdots, n-1 \mapsto n$:

Wir führen eine Fallunterscheidung durch.

(a) Fall: n ist eine Primzahl.
Dann ist $n = n^1$ bereits eine kanonische Primfaktor-Zerlegung von n.

(b) Fall: n ist keine Primzahl.
Dann gibt es natürliche Zahlen a und b mit

$$n = a \cdot b \quad \text{und } a > 1 \text{ und } b > 1,$$

denn wenn es keine solche Zerlegung gäbe, wäre n eine Primzahl. Damit ist klar, dass sowohl $a < n$ als auch $b < n$ gilt. Nach Induktions-Voraussetzung gibt es also Primfaktor-Zerlegungen für a und b:

$$a = p_1^{e_1} \cdot \ \ldots \ \cdot p_k^{e_k} \quad \text{und} \quad b = q_1^{f_1} \cdot \ \ldots \ \cdot q_l^{f_l}.$$

Multiplizieren wir diese Primfaktor-Zerlegungen, sortieren die Faktoren geeignet und fassen wir dann noch Faktoren mit der gleichen Basis zusammen, so erhalten wir offenbar eine Primfaktor-Zerlegung von $a \cdot b$ und damit von n.

Um den Beweis abzuschließen zeigen wir, dass die Primfaktor-Zerlegung eindeutig sein muss. Diesen Nachweis führen wir indirekt und nehmen an, dass n die kleinste natürliche Zahl ist, die zwei verschiedene Primfaktor-Zerlegung hat, beispielsweise die beiden Zerlegungen

$$n = p_1^{e_1} \cdot \ \ldots \ \cdot p_k^{e_k} \quad \text{und} \quad n = q_1^{f_1} \cdot \ \ldots \ \cdot q_l^{f_l}. \tag{7.5}$$

Zunächst stellen wir fest, dass dann die Mengen

$$\{p_1, \cdots, p_k\} \quad \text{und} \quad \{q_1, \cdots, q_l\}$$

disjunkt sein müssen, denn wenn beispielsweise $p_i = q_j$ wäre, könnten wir die Primfaktor-Zerlegung durch p_i teilen und hätten dann

$$p_1^{e_1} \cdot \ \ldots \ \cdot p_i^{e_i - 1} \cdot \ \ldots \ \cdot p_k^{e_k} = n/p_i = n/q_j = q_1^{f_1} \cdot \ \ldots \ \cdot q_j^{f_j - 1} \cdot \ \ldots \ \cdot q_l^{f_l}.$$

Damit hätte auch die Zahl n/p_i, die offenbar kleiner als n ist, zwei verschiedene Primfaktor-Zerlegungen, was im Widerspruch zu der Annahme steht, dass n die kleinste Zahl mit zwei verschiedenen Primfaktor-Zerlegungen ist. Wir sehen also, dass die Primfaktoren $p_1, \cdots, p_k$ und $q_1, \cdots, q_l$ voneinander verschieden sein müssen. Nun benutzen wir das Lemma von Euklid: Aus

$$p_1^{e_1} \cdot \ \ldots \ \cdot p_k^{e_k} = q_1^{f_1} \cdot \ \ldots \ \cdot q_l^{f_l}$$

folgt zunächst, dass p_1 ein Teiler von dem Produkt $q_1^{f_1} \cdot \ \ldots \ \cdot q_l^{f_l}$ ist. Nach dem Lemma von Euklid folgt nun, dass p_1 entweder $q_1^{f_1}$ oder $q_2^{f_2} \cdot \ \ldots \ \cdot q_l^{f_l}$ teilt. Da p_1 von q_1 verschieden ist, kann p_1 kein Teiler von $q_1^{f_1}$ sein. Durch Iteration dieses Arguments sehen wir, dass p_1 auch kein Teiler von $q_2^{f_2}, \cdots, q_{l-1}^{f_{l-1}}$ ist. Schließlich bleibt als einzige Möglichkeit, dass p_1 ein Teiler von $q_l^{f_l}$ ist, was aber wegen $p_1 \neq q_l$ ebenfalls unmöglich ist. Damit haben wir einen Widerspruch zu der Annahme, dass n zwei verschiedene Primfaktor-Zerlegungen besitzt und der Beweis ist abgeschlossen. □

7.4 Die Eulersche φ-Funktion

Es sei $n \in \mathbb{N}$ mit $n > 0$ gegeben. Die *multiplikative Gruppe* $\mathbb{Z}_n^*$ ist durch

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid \exists y \in \mathbb{Z}_n : x \cdot y \approx_n 1\}$$

definiert. Die Menge $\mathbb{Z}_n^*$ enthält also genau die Zahlen aus $\mathbb{Z}_n$, die bezüglich der Multiplikation ein Inverses modulo n haben. Beispielsweise gilt

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\},$$

denn alle Zahlen der Menge $\{1, 2, 3, 4\}$ haben ein Inverses bezüglich der Multiplikation modulo 5.

1. Wir haben $1 \cdot 1 \approx_5 1$, also ist 1 das multiplikative Inverse modulo 5 von 1.
2. Wir haben $2 \cdot 3 = 6 \approx_5 1$, also ist 3 das multiplikative Inverse modulo 5 von 2.
3. Wir haben $3 \cdot 2 = 6 \approx_5 1$, also ist 2 das multiplikative Inverse modulo 5 von 3.
4. Wir haben $4 \cdot 4 = 16 \approx_5 1$, also ist 4 das multiplikative Inverse modulo 5 von 4.

Auf der anderen Seite haben wir

$$\mathbb{Z}_4^* = \{1, 3\},$$

denn $3 \cdot 3 = 9 \approx_4 1$, so dass die Zahl 3 das multiplikative Inverse modulo 4 von 3 ist, aber die Zahl 2 hat kein multiplikative Inverses modulo 4, denn wir haben $2 \cdot 2 = 4 \approx_4 0$. Generell kann eine Zahl x, für die es ein $y \not\approx_n 0$ mit

$$x \cdot y \approx_n 0$$

gibt, kein multiplikatives Inverses haben, denn falls z ein solches Inverses wäre, so könnten wir die obige Gleichung einfach von links mit z multiplizieren und hätten dann

$$z \cdot x \cdot y \approx_n z \cdot 0,$$

woraus wegen $z \cdot x \approx_n 1$ sofort $y \approx_n 0$ folgen würde, was im Widerspruch zu der Voraussetzung $y \not\approx_n 0$ steht.

Bemerkung: Wir haben oben von der *multiplikativen Gruppe* $\mathbb{Z}_n^*$ gesprochen. Wenn wir von einer Gruppe sprechen, dann meinen wir damit genau genommen nicht nur die Menge $\mathbb{Z}_n^*$ sondern die Struktur

$$\langle \mathbb{Z}_n^*, 1, \cdot_n \rangle,$$

wobei die Funktion $\cdot_n : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ durch

$$x \cdot_n y := (x \cdot y) \,\%\, n$$

definiert ist. Dass die Menge $\mathbb{Z}_n^*$ mit der so definierten Multiplikation tatsächlich zu einer Gruppe wird, folgt letzlich aus der Verträglichkeit der Relation $\approx_n$ mit der gewöhnlichen Multiplikation. Die Details überlasse ich Ihnen in der folgenden Aufgabe.

Aufgabe 14: Zeigen Sie, dass die oben definierte Struktur $\langle \mathbb{Z}_n^*, 1, \cdot_n \rangle$ eine Gruppe ist.

Definition 74 (Eulersche φ-Funktion) Für alle natürlichen Zahlen $n > 1$ definieren wir

$$\varphi(n) := \mathit{card}\big(\mathbb{Z}_n^*\big).$$

Um spätere Definitionen zu vereinfachen, setzen wir außerdem $\varphi(1) := 1$. □

Satz 75 (Existenz von multiplikativen Inversen modulo n)
Es sei $n \in \mathbb{N}$ mit $n \geq 1$. Eine Zahl $a \in \mathbb{Z}_n$ hat genau dann ein multiplikatives Inverses modulo n, wenn $\mathit{ggt}(a, n) = 1$ gilt.

Beweis: Wir zerlegen den Beweis in zwei Teile.

1. "⇒": Wir nehmen an, dass a ein multiplikatives Inverses hat und zeigen, dass daraus $ggt(a, n) = 1$ folgt.

   Bezeichnen wir das multiplikative Inverse modulo n von a mit b, so gilt

   $$b \cdot a \approx_n 1$$

   Nach Definition der Relation $\approx_n$ gibt es dann eine natürliche Zahl k, so dass

   $$b \cdot a = 1 + k \cdot n$$

   gilt. Daraus folgt sofort

   $$b \cdot a - k \cdot n = 1. \tag{7.6}$$

   Sei nun d ein gemeinsamer Teiler von a und n. Dann ist d offenbar auch ein gemeinsamer Teiler von $b \cdot a$ und $k \cdot n$ und weil allgemein gilt, dass ein gemeinsamer Teiler zweier Zahlen x und y auch ein Teiler der Differenz $x - y$ ist, können wir folgern, dass d auch ein Teiler von $b \cdot a - k \cdot n$ ist:

   $$d \,|\, b \cdot a - k \cdot n.$$

   Aus Gleichung (7.6) folgt nun, dass d auch ein Teiler von 1 ist. Damit haben wir gezeigt, dass a und n nur den gemeinsamen Teiler 1 haben:

   $$ggt(a, n) = 1.$$

2. "⇐": Jetzt nehmen wir an, dass $ggt(a, n) = 1$ ist und zeigen, dass a dann ein multiplikatives Inverses modulo n besitzt.

   Sei also $ggt(a, n) = 1$. Nach dem Lemma von Bezóut (Satz 64) gibt es also ganze Zahlen x und y, so dass

   $$x \cdot a + y \cdot n = 1.$$

   gilt. Stellen wir diese Gleichung um, so erhalten wir

   $$x \cdot a = 1 - y \cdot n \approx_n 1, \quad \text{also } x \cdot a \approx_n 1.$$

   Damit ist x das multiplikative Inverse von a modulo n. □

Korollar 76 Für alle natürlichen Zahlen $n > 1$ gilt

$$\varphi(n) = \mathit{card}\big(\{x \in \mathbb{Z}_n \mid \mathit{ggt}(x, n) = 1\}\big).$$

Als Konsequenz des letzten Satzes können wir nun die Eulersche φ-Funktion für Potenzen von Primzahlen berechnen.

Satz 77 (Berechnung der φ-Funktion für Primzahl-Potenzen) Es sei p eine Primzahl und n eine positive natürliche Zahl. Dann gilt

$$\varphi\big(p^n\big) = p^{n-1} \cdot (p - 1).$$

Beweis: Nach Satz 75 müssen wir zählen, welche Zahlen in der Menge

$$\mathbb{Z}_{p^n} = \{0, 1, \cdots, p^n - 1\}$$

zu der Zahl p^n teilerfremd sind, denn es gilt

$$\varphi\big(p^n\big) = card\big(\{x \in \mathbb{Z}_{p^n} \mid ggt(x, p^n) = 1\}\big).$$

Wir definieren daher die Menge A als

$$A := \{x \in \mathbb{Z}_{p^n} \mid ggt(x, p^n) = 1\}.$$

Weiter ist es nützlich, das Komplement dieser Menge bezüglich $\mathbb{Z}_{p^n}$ zu betrachten. Daher definieren wir

$$\begin{aligned} B &:= \mathbb{Z}_{p^n} \backslash A \\ &= \mathbb{Z}_{p^n} \backslash \{x \in \mathbb{Z}_{p^n} \mid ggt(x, p^n) = 1\} \\ &= \{x \in \mathbb{Z}_{p^n} \mid ggt(x, p^n) > 1\}. \end{aligned}$$

Die Menge B enthält also die Zahlen aus $\mathbb{Z}_{p^n}$, die mit p^n einen gemeinsamen Teiler haben. Da p eine Primzahl ist, enthält die Menge B folglich genau die Vielfachen der Primzahl p, die kleiner als p^n sind. Daher können wir B wie folgt schreiben:

$$B := \big\{y \cdot p \mid y \in \{0, 1, \cdots, p^{n-1} - 1\}\big\}.$$

Offenbar gilt

$$card(B) = card\big(\{0, 1, \cdots, p^{n-1} - 1\}\big) = p^{n-1}.$$

Andererseits folgt aus der Gleichung $A = \mathbb{Z}_{p^n} \backslash B$ sofort

$$\varphi\big(p^n\big) = card(A) = card\big(\mathbb{Z}_{p^n}\big) - card(B) = p^n - p^{n-1} = p^{n-1} \cdot (p - 1).$$

Damit ist der Beweis abgeschlossen. □

Um das Produkt $\varphi(p \cdot q)$ für zwei verschiedene Primzahlen p und q berechnen zu können, benötigen wir den folgenden Satz.

Satz 78 (Chinesischer Restesatz, 1. Teil)
Es seien $m, n \in \mathbb{N}$ natürliche Zahlen größer als 1 und es gelte $ggt(m, n) = 1$. Weiter gelte $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$. Dann gibt es genau eine Zahl $x \in \mathbb{Z}_{m \cdot n}$, so dass

$$x \approx_m a \quad \text{und} \quad x \approx_n b$$

gilt.

Beweis: Wir zerlegen den Beweis in zwei Teile. Zunächst zeigen wir, dass tatsächlich ein $x \in \mathbb{Z}_{m \cdot n}$ existiert, das die beiden Gleichungen $x \approx_m a$ und $x \approx_n b$ erfüllt sind. Anschließend zeigen wir, dass dieses x eindeutig bestimmt ist.

1. Aus der Voraussetzung, dass $ggt(m, n) = 1$ folgt nach dem Satz über das multiplikative Inverse modulo n (Satz 75), dass die Zahl m ein multiplikatives Inverses modulo n und die Zahl n ein multiplikatives Inverses modulo m hat. Bezeichnen wir diese Inversen mit u bzw. v, so gilt also

   $$m \cdot u \approx_n 1 \quad \text{und} \quad n \cdot v \approx_m 1.$$

   Wir definieren nun

   $$x := (a \cdot n \cdot v + b \cdot m \cdot u) \,\%\, (m \cdot n).$$

   Nach dem Satz über die Division mit Rest hat x dann die Form

   $$x = a \cdot n \cdot v + b \cdot m \cdot u - k \cdot (m \cdot n)$$

   mit einem geeigneten k. Nach Definition von x ist klar, dass $x \in \mathbb{Z}_{m \cdot n}$ ist. Einerseits folgt aus der Verträglichkeit der Relation $\approx_m$ mit Addition und Multiplikation und der Tatsache, dass

   $$m \,\%\, m = 0, \quad \text{also } m \approx_m 0$$

   ist, dass auch

   $$b \cdot m \cdot u - k \cdot (m \cdot n) \approx_m 0$$

   gilt. Andererseits folgt aus $n \cdot v \approx_m 1$, dass

   $$a \cdot n \cdot v \approx_m a$$

gilt, so dass wir insgesamt

$$x = a \cdot n \cdot v + b \cdot m \cdot u - k \cdot (m \cdot n) \approx_m a$$

haben. Analog sehen wir, dass

$$a \cdot n \cdot v - k \cdot (m \cdot n) \approx_n 0$$

gilt. Weiter folgt aus $m \cdot u \approx_n 1$, dass

$$b \cdot m \cdot u \approx_m b$$

gilt, so dass wir außerdem

$$x = b \cdot m \cdot u + a \cdot n \cdot v - k \cdot (m \cdot n) \approx_n b$$

haben.

2. Es bleibt die Eindeutigkeit von x zu zeigen. Wir nehmen dazu an, dass für $x_1, x_2 \in \mathbb{Z}_{m \cdot n}$ sowohl

$$x_1 \approx_m a \text{ und } x_1 \approx_n b, \quad \text{als auch} \quad x_2 \approx_m a \text{ und } x_2 \approx_n b$$

gelte. O.B.d.A. gelte weiter $x_1 \leq x_2$. Wir wollen zeigen, dass dann $x_1 = x_2$ gelten muss. Aus $x_1 \approx_m a$ und $x_2 \approx_m a$ folgt $x_1 \approx_m x_2$. Also gibt es eine Zahl $k \in \mathbb{N}$, so dass

$$x_2 = x_1 + k \cdot m \tag{7.7}$$

gilt. Aus $x_1 \approx_n b$ und $x_2 \approx_n b$ folgt $x_1 \approx_n x_2$. Also gibt es eine Zahl $l \in \mathbb{N}$, so dass

$$x_2 = x_1 + l \cdot n \tag{7.8}$$

gilt. Aus den Gleichungen (7.7) und (7.8) folgt dann

$$k \cdot m = x_2 - x_1 = l \cdot n.$$

Da m und n teilerfremd sind, folgt daraus, dass m ein Teiler von l ist. Es gibt also eine natürliche Zahl i, so dass $l = i \cdot m$ ist. Damit haben wir dann insgesamt

$$x_2 - x_1 = i \cdot m \cdot n.$$

Da andererseits sowohl x_2 als auch x_1 Elemente von $\mathbb{Z}_{m \cdot n}$ sind, muss

$$x_2 - x_1 < m \cdot n$$

sein. Da i eine natürlich Zahl ist, geht das nur, wenn $i = 0$ ist. Wir haben also

$$x_2 - x_1 = 0 \cdot m \cdot n = 0$$

und folglich gilt $x_2 = x_1$. □

Korollar 79 (Chinesischer Restesatz, 2. Teil)
Sind $m, n \in \mathbb{N}$ mit $ggt(m, n) = 1$ und definieren wir die Funktion

$$\pi : \mathbb{Z}_{m \cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{durch} \quad \pi(x) := \langle x \,\%\, m, x \,\%\, n \rangle,$$

so ist Funktion π bijektiv.

Beweis: Wir zeigen Injektivität und Surjektivität der Funktion getrennt.

1. Injektivität: Es seien $x_1, x_2 \in \mathbb{Z}_{m \cdot n}$ und es gelte $\pi(x_1) = \pi(x_2)$. Nach Definition der Funktion π gilt dann

$$x_1 \,\%\, m = x_2 \,\%\, m \quad \text{und} \quad x_1 \,\%\, n = x_2 \,\%\, n.$$

Wir definieren $a := x_1 \,\%\, m$ und $b := x_1 \,\%\, n$ und haben dann sowohl

$$x_1 \approx_m a \quad \text{und} \quad x_1 \approx_n b$$

als auch

$$x_2 \approx_m a \quad \text{und} \quad x_2 \approx_n b.$$

Nach dem Chinesischen Restesatz gibt es aber nur genau ein $x \in \mathbb{Z}_{m \cdot n}$, welches die beiden Gleichungen

$$x \approx_m a \quad \text{und} \quad x \approx_n b.$$

gleichzeitig erfüllt. Folglich muss $x_1 = x_2$ sein.

2. Surjektivität: Nun sei $\langle a, b \rangle \in \mathbb{Z}_m \times \mathbb{Z}_n$ gegeben. Wir müssen zeigen, dass es ein $x \in \mathbb{Z}_{m \cdot n}$ gibt, so dass $\pi(x) = \langle a, b \rangle$ gilt. Nach dem Chinesischen Restesatz existiert ein $x \in \mathbb{Z}_{m \cdot n}$, so dass
$$x \approx_m a \quad \text{und} \quad x \approx_n b$$
gilt. Wegen $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ gilt $a \,\%\, m = a$ und $b \,\%\, n = b$ und daher können wir die beiden Gleichungen auch in der Form
$$x \,\%\, m = a \quad \text{und} \quad x \,\%\, n = b$$
schreiben. Damit gilt
$$\pi(x) = \langle x \,\%\, m, x \,\%\, n \rangle = \langle a, b \rangle$$
und der Beweis ist abgeschlossen. □

Aufgabe 15: Versuchen Sie den Chinesischen Restesatz so zu verallgemeinern, dass er für eine beliebige Liste $[m_1, m_2, \cdots, m_k]$ von paarweise teilerfremden Zahlen gilt und beweisen Sie den verallgemeinerten Satz.

Aufgabe 16: Implementieren Sie ein Programm, das mit Hilfe des Chinesischen Restesatzes Systeme von Kongruenzen der Form

$$x \,\%\, m_1 = a_1,\ x \,\%\, m_2 = a_2,\ \cdots,\ x \,\%\, m_k = a_k$$

lösen kann und lösen Sie mit diesem Programm das folgende Rätsel.

> A girl was carrying a basket of eggs, and a man riding a horse hit the basket and broke all the eggs. Wishing to pay for the damage, he asked the girl how many eggs there were. The girl said she did not know, but she remembered that when she counted them by twos, there was one left over; when she counted them by threes, there were two left over; when she counted them by fours, there were three left over; when she counted them by fives, there were four left; and when she counted them by sixes, there were five left over. Finally, when she counted them by sevens, there were none left over. 'Well,' said the man, 'I can tell you how many you had.' What was his answer?

Satz 80 Es seien m und n positive natürliche Zahlen. Dann gilt für alle positiven natürlichen Zahlen x die Äquivalenz

$$ggt(x, m \cdot n) = 1 \quad \Leftrightarrow \quad ggt(x, m) = 1 \ \wedge \ ggt(x, n) = 1.$$

Beweis: Dies folgt aus dem Fundamentalsatz der Arithmetik und dem Lemma von Euler: Ist p ein Primfaktor von x, so teilt p das Produkt $m \cdot n$ genau dann, wenn es einen der Faktoren teilt. □

Satz 81 (Produkt-Regel zur Berechnung der φ-Funktion)
Es seien m und n natürliche Zahlen größer als 1 und es gelte $ggt(m, n) = 1$. Dann gilt

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Beweis: Nach Definition der Eulerschen φ-Funktion müssen wir zeigen, dass unter den gegebenen Voraussetzungen

$$card(\mathbb{Z}^*_{m\cdot n}) = card(\mathbb{Z}^*_m) \cdot card(\mathbb{Z}^*_n)$$

gilt. Nach dem 2. Teil des Chinesischen Restesatzes (Korollar 79) ist die Funktion

$$\pi : \mathbb{Z}_{m\cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{mit } \pi(x) := \langle x \,\%\, m, x \,\%\, n\rangle$$

eine Bijektion vom $\mathbb{Z}_{m\cdot n}$ in das kartesische Produkt $\mathbb{Z}_m \times \mathbb{Z}_n$. Offenbar gilt

$$\mathbb{Z}^*_m \subseteq \mathbb{Z}_m, \quad \mathbb{Z}^*_n \subseteq \mathbb{Z}_n, \quad \text{und} \quad \mathbb{Z}^*_{m\cdot n} \subseteq \mathbb{Z}_{m\cdot n}.$$

Außerdem haben wir die folgende Kette von Schlussfolgerungen:

$$\begin{array}{lll}
 & x \in \mathbb{Z}^*_{m\cdot n} & \\
\Rightarrow & ggt(x, m\cdot n) = 1 & \text{nach Definition von } \mathbb{Z}^*_{m\cdot n} \\
\Rightarrow & ggt(x, m) = 1 \wedge ggt(x, n) = 1 & \text{Satz 80} \\
\Rightarrow & ggt(x \,\%\, m, m) = 1 \wedge ggt(x \,\%\, n, n) = 1 & \\
\Rightarrow & x \,\%\, m \in \mathbb{Z}^*_m \quad \text{und} \quad x \,\%\, n \in \mathbb{Z}^*_n & \\
\Rightarrow & \langle x \,\%\, m, x \,\%\, n\rangle \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n &
\end{array}$$

Dies zeigt, dass die Funktion π die Menge $\mathbb{Z}^*_{m\cdot n}$ in das kartesische Produkt $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$ abbildet. Haben wir umgekehrt ein Paar $\langle a, b\rangle \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$ gegeben, so zeigt zunächst der Chinesische Restesatz, dass es ein $x \in \mathbb{Z}_{m\cdot n}$ gibt, für das

$$x \,\%\, m = a \quad \text{und} \quad x \,\%\, n = b \text{ ist.}$$

Weiter haben wir dann die folgende Kette von Schlussfolgerungen:

$$\begin{array}{ll}
 & a \in \mathbb{Z}^*_m \wedge b \in \mathbb{Z}^*_n \\
\Rightarrow & ggt(a, m) = 1 \wedge ggt(b, n) = 1 \\
\Rightarrow & ggt(x \,\%\, m, m) = 1 \wedge ggt(x \,\%\, n, n) = 1 \\
\Rightarrow & ggt(x, m) = 1 \wedge ggt(x, n) = 1 \\
\Rightarrow & ggt(x, m\cdot n) = 1 \\
\Rightarrow & x \in \mathbb{Z}^*_{m\cdot n}
\end{array}$$

Dies zeigt, dass die Einschränkung der Funktion π auf die Menge $\mathbb{Z}^*_{m\cdot n}$ eine surjektive Abbildung auf das kartesische Produkt $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$ ist. Da wir weiterhin wissen, dass die Funktion π injektiv ist, müssen die Mengen $\mathbb{Z}^*_{m\cdot n}$ und $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$ die gleiche Anzahl von Elementen haben:

$$card(\mathbb{Z}^*_{m\cdot n}) = card(\mathbb{Z}^*_m \times \mathbb{Z}^*_n) = card(\mathbb{Z}^*_m) \cdot card(\mathbb{Z}^*_n)$$

Also gilt $\varphi(m\cdot n) = \varphi(m) \cdot \varphi(n)$. □

7.5 Die Sätze von Fermat und Euler

Der folgende Satz von Pierre de Fermat (160? - 1665) bildet die Grundlage verschiedener kryptografischer Verfahren.

Satz 82 (Kleiner Satz von Fermat)
Es sei p eine Primzahl. Dann gilt für jede Zahl $k \in \mathbb{Z}_p^*$

$$k^{p-1} \approx_p 1.$$

Beweis: Wir erinnern zunächst an die Definition der multiplikativen Gruppe $\mathbb{Z}_p^*$ als

$$\mathbb{Z}_p^* := \{x \in \mathbb{Z}_p \mid \exists y \in \mathbb{Z}_p : x \cdot y \approx_p 1\}.$$

Wir wissen nach Satz 77, dass

$$card(\mathbb{Z}_p^*) = \varphi(p) = p - 1$$

gilt. Da die 0 sicher kein Inverses bezüglich der Multiplikation modulo p haben, müssen alle Zahlen aus der Menge $\{1, \cdots, p-1\}$ ein multiplikatives Inverses haben und es gilt

$$\mathbb{Z}_p^* = \{1, \cdots, p-1\}.$$

Diese Behauptung hätten wir alternativ auch aus dem Satz 75 folgern können, denn für alle $x \in \{1, \cdots, p-1\}$ gilt $ggt(x, p) = 1$.

Als nächstes definieren wir eine Funktion

$$f : \mathbb{Z}_p^* \to \mathbb{Z}_p^* \quad \text{durch} \quad f(l) = (k \cdot l) \,\%\, p.$$

Zunächst müssen wir zeigen, dass für alle $l \in \mathbb{Z}_p^*$ tatsächlich

$$f(l) \in \mathbb{Z}_p^*$$

gilt. Dazu ist zu zeigen, dass $(k \cdot l) \,\%\, p \neq 0$ gilt, denn sonst hätte $k \cdot l$ kein multiplikatives Inverses. Falls $k \cdot l \approx_p 0$ wäre, dann wäre p ein Teiler von $k \cdot l$. Da p eine Primzahl ist, müsste p dann entweder k oder l teilen, was wegen $k, l < p$ nicht möglich ist.

Als nächstes zeigen wir, dass die Funktion f injektiv ist. Seien also $l_1, l_2 \in \mathbb{Z}_p^*$ gegeben, so dass

$$f(l_1) = f(l_2)$$

gilt. Nach Definition der Funktion f bedeutet dies

$$(k \cdot l_1) \,\%\, p = (k \cdot l_2) \,\%\, p,$$

was wir auch kürzer als

$$k \cdot l_1 \approx_p k \cdot l_2,$$

schreiben können. Da $k \in \mathbb{Z}_p^*$ ist, gibt es ein multiplikatives Inverses h zu k, für das $h \cdot k \approx_p 1$ gilt. Multiplizieren wir daher die obige Gleichung mit h, so erhalten wir

$$h \cdot k \cdot l_1 \approx_p h \cdot k \cdot l_2,$$

woraus sofort

$$l_1 \approx_p l_2$$

folgt. Da sowohl l_1 als auch l_2 Elemente der Menge $\mathbb{Z}_p^*$ sind, bedeutet dies $l_1 = l_2$ und damit ist die Injektivität der Funktion f gezeigt.

Nun folgt eine Zwischenüberlegung, die wir gleich benötigen. Ist allgemein $f : A \to B$ eine injektive Funktion, für die $n := card(A) = card(B)$ ist, so muss f auch surjektiv sein, was wir anschaulich wie folgt einsehen können: Wenn wir n verschiedene Murmeln (die Elemente von A) auf n Schubladen (die Elemente von B) verteilen müssen und wir (wegen der Injektivität von f)

niemals zwei Murmeln in die selbe Schublade legen dürfen, dann müssen wir tatsächlich in jede Schublade eine Murmel legen und letzteres heißt, dass f surjektiv sein muss.

Wir wenden nun die Zwischenüberlegung an: Da f eine Funktion von $\mathbb{Z}_p^*$ nach $\mathbb{Z}_p^*$ ist und trivialerweise $card(\mathbb{Z}_p^*) = card(\mathbb{Z}_p^*)$ gilt, können wir aus der Injektivität von f auf die Surjektivität von f schließen.

Der Schlüssel des Beweises liegt in der Betrachtung des folgenden Produkts:

$$P := \prod_{i=1}^{p-1} f(i) = f(1) \cdot f(2) \cdot \ \ldots \ \cdot f(p-1).$$

Aufgrund der Tatsache, dass die Funktion $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ surjektiv ist, wissen wir, dass

$$f(\mathbb{Z}_p^*) = \mathbb{Z}_p^*$$

gilt. Schreiben wir die Mengen auf beiden Seiten dieser Gleichung hin, so erhalten wir die Gleichung

$$\big\{f(1), f(2), \cdots, f(p-1)\big\} = \big\{1, 2, \cdots, p-1\big\}.$$

Damit können wir das oben definierte Produkt P auch anders schreiben, es gilt

$$f(1) \cdot f(2) \cdot \ \ldots \ \cdot f(p-1) = 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1),$$

denn auf beiden Seiten haben wir alle Elemente der Menge $\mathbb{Z}_p^*$ aufmultipliziert, lediglich die Reihenfolge ist eine andere. Setzen wir hier die Definition der Funktion f ein, so folgt zunächst

$$\big((k \cdot 1) \,\%\, p\big) \cdot \big((k \cdot 2) \,\%\, p\big) \cdot \ \ldots \ \cdot \big((k \cdot (p-1)) \,\%\, p\big) = 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1).$$

Da offenbar $(k \cdot i) \,\%\, p \approx_p k \cdot i$ gilt, folgt daraus

$$(k \cdot 1) \cdot (k \cdot 2) \cdot \ \ldots \ \cdot \big(k \cdot (p-1)\big) \approx_p 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1).$$

Ordnen wir die Terme auf der linken Seite dieser Gleichung um, so folgt

$$k^{p-1} \cdot 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1) \approx_p 1 \cdot 2 \cdot \ \ldots \ \cdot (p-1).$$

Da die Zahlen 1, 2, $\cdots$, p_1 modulo p ein multiplikatives Inverses haben, können diese Zahlen auf beiden Seiten der Gleichung herausgekürzt werden und wir erhalten

$$k^{p-1} \approx_p 1.$$

Das war gerade die Behauptung. □

Korollar 83 Es sei p eine Primzahl. Für alle $k \in \mathbb{Z}_p$ gilt dann $k^p \approx_p k$.

Beweis: Falls $k \in \mathbb{Z}_p^*$ ist, folgt die Behauptung, indem wir die Gleichung $k^{p-1} \approx_p 1$ mit k multiplizieren. Anderfalls gilt $k = 0$ und offenbar gilt $0^p = 0$. □

Der kleine Satz von Fermat $a^{p-1} \approx_p 1$ läßt sich auf den Fall, dass p keine Primzahl ist, verallgemeinern. Es ist dann lediglich zu fordern, dass die Zahlen a und n teilerfremd sind und an Stelle des Exponenten $p-1$ tritt nun die φ-Funktion. Diese Verallgemeinerung wurde von Leonhard Euler (1707 – 1783) gefunden.

Satz 84 (Satz von Euler)
Es sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}_n^*$. Dann gilt

$$a^{\varphi(n)} \approx_n 1.$$

Beweis: Wir gehen aus von der Definition von

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid \exists y \in \mathbb{Z}_n : x \cdot y \approx_p 1\}$$

als der Menge aller der Zahlen, die ein multiplikatives Inverses bezüglich der Multiplikation modulo n haben. Wir erinnern außerdem daran, dass

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid ggt(x, n) = 1\}$$

gilt. Nach Definition der φ-Funktion gilt

$$card(\mathbb{Z}_n^*) = \varphi(n).$$

gilt. Analog zum Beweis des Satzes von Fermat definieren wir eine Funktion

$$f : \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad \text{durch} \quad f(l) = (a \cdot l) \,\%\, n.$$

Zunächst müssen wir zeigen, dass für alle $l \in \mathbb{Z}_n^*$ tatsächlich

$$f(l) \in \mathbb{Z}_n^*$$

gilt. Dazu ist zu zeigen, dass $(a \cdot l) \,\%\, n \in \mathbb{Z}_n^*$ ist. Dies folgt aber sofort aus Satz 80, denn wegen $l \in \mathbb{Z}_n^*$ und $a \in \mathbb{Z}_n^*$ wissen wir, dass $ggt(l, n) = 1$ und $ggt(a, n) = 1$ ist und nach Satz 80 folgt dann auch $ggt(a \cdot l, n) = 1$, woraus $ggt\big((a \cdot l) \,\%\, n, n\big) = 1$ folgt und letzteres ist zu $(a \cdot l) \,\%\, n \in \mathbb{Z}_n^*$ äquivalent.

Als nächstes zeigen wir, dass die Funktion f injektiv ist. Seien also $l_1, l_2 \in \mathbb{Z}_n^*$ gegeben, so dass

$$f(l_1) = f(l_2)$$

gilt. Nach Definition der Funktion f bedeutet dies

$$(a \cdot l_1) \,\%\, n = (a \cdot l_2) \,\%\, n,$$

was wir auch kürzer als

$$a \cdot l_1 \approx_n a \cdot l_2,$$

schreiben können. Da $a \in \mathbb{Z}_n^*$ ist, gibt es ein multiplikatives Inverses b zu a, für das $b \cdot a \approx_n 1$ gilt. Multiplizieren wir daher die obige Gleichung mit b, so erhalten wir

$$b \cdot a \cdot l_1 \approx_n b \cdot a \cdot l_2,$$

woraus wegen $b \cdot a \approx_n 1$ sofort

$$l_1 \approx_n l_2$$

folgt. Da sowohl l_1 als auch l_2 Elemente der Menge $\mathbb{Z}_n^*$ sind, folgt $l_1 = l_2$ und damit ist die Injektivität der Funktion f gezeigt.

Genau wie im Beweis des kleinen Satzes von Fermat folgern wir nun aus der Injektivität der Funktion f, dass f auch surjektiv sein muss und betrachten das folgende Produkt:

$$P := \prod_{i \in \mathbb{Z}_n^*} f(i).$$

Aufgrund der Tatsache, dass die Funktion $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ surjektiv ist, wissen wir, dass

$$f(\mathbb{Z}_n^*) = \mathbb{Z}_n^*$$

gilt. Daher können wir P auch einfacher berechnen, es gilt

$$P = \prod_{i \in \mathbb{Z}_n^*} i,$$

die beiden Darstellungen von P unterscheiden sich nur in der Reihenfolge der Faktoren. Damit haben wir

$$\prod_{i \in \mathbb{Z}_n^*} f(i) = \prod_{i \in \mathbb{Z}_n^*} i.$$

Auf der linken Seite setzen wir nun die Definition von f ein und haben dann

$$\prod_{i \in \mathbb{Z}_n^*} (a \cdot i) \,\%\, n = \prod_{i \in \mathbb{Z}_n^*} i,$$

woraus

$$a^{card(\mathbb{Z}_n^*)} \cdot \prod_{i \in \mathbb{Z}_n^*} i \approx_n \prod_{i \in \mathbb{Z}_n^*} i$$

folgt. Kürzen wir nun das Produkt $\prod_{i \in \mathbb{Z}_n^*} i$ auf beiden Seiten dieser Gleichung weg und berücksichtigen, dass $card(\mathbb{Z}_n^*) = \varphi(n)$ ist, so haben wir die Gleichung

$$a^{\varphi(n)} \approx_n 1$$

bewiesen. □

7.6 Der RSA-Algorithmus

In diesem Abschnitt sehen wir, wozu die φ-Funktion nützlich ist: Wir präsentieren den Algorithmus von Rivest, Shamir und Adleman [RSA78] (kurz: RSA-Algorithmus), der zur Erstellung digitaler Signaturen verwendet werden kann.

Der RSA-Algorithmus beginnt damit, dass wir zwei *große* Primzahlen p und q mit $p \neq q$ erzeugen. *Groß* heißt in diesem Zusammenhang, dass zur Darstellung der beiden Zahlen p und q jeweils mehrere hundert Stellen benötigt werden. Anschließend bilden wir das Produkt

$$n := p \cdot q.$$

Das Produkt n machen wir öffentlich bekannt, aber die beiden Primzahlen p und q bleiben geheim. Weiter berechnen wir

$$\varphi(n) = \varphi(p \cdot q) = (p-1) \cdot (q-1)$$

und suchen eine natürliche Zahl $e < (p-1) \cdot (q-1)$, so dass

$$ggt\big(e, (p-1) \cdot (q-1)\big) = 1$$

gilt. Die Zahl e wird wieder öffentlich bekannt gemacht. Aufgrund der Tatsache, dass die beiden Zahlen e und $(p-1) \cdot (q-1)$ teilerfremd sind, gilt $e \in \mathbb{Z}^*_{(p-1)\cdot(q-1)}$ und damit hat die Zahl e ein multiplikatives Inverses d modulo $(p-1) \cdot (q-1)$, es gilt also

$$d \cdot e \approx_{(p-1)\cdot(q-1)} 1.$$

Wir erinnern an dieser Stelle daran, dass die Zahl d mit Hilfe des erweiterten Euklid'schen Algorithmus berechnet werden kann, denn da $ggt\big(e, (p-1) \cdot (q-1)\big) = 1$ ist, liefert der Euklid'sche Algorithmus Zahlen α und β, für die

$$\alpha \cdot e + \beta \cdot (p-1) \cdot (q-1) = 1$$

gilt. Definieren wir $d := \alpha \,\%\, \big((p-1) \cdot (q-1)\big)$, so sehen wir, dass in der Tat

$$d \cdot e \approx_{(p-1)\cdot(q-1)} 1.$$

gilt. Die Zahl d bleibt geheim. Wegen der letzten Gleichung gibt es ein $k \in \mathbb{N}$, so dass

$$d \cdot e = 1 + k \cdot (p-1) \cdot (q-1)$$

gilt. Wir definieren eine *Verschlüsselungs-Funktion*

$$f : \mathbb{Z}_n \to \mathbb{Z}_n \quad \text{durch} \quad f(x) := x^e \,\%\, n.$$

Weiter definieren wir eine Funktion

$$g : \mathbb{Z}_n \to \mathbb{Z}_n \quad \text{durch} \quad g(x) := x^d \,\%\, n.$$

Wir behaupten, dass für alle x, die kleiner als $m := \min(p, q)$ sind,

$$g\big(f(x)\big) = x$$

gilt. Dies rechnen wir wie folgt nach:

$$\begin{aligned}
g\big(f(x)\big) &= g\big(x^e \,\%\, n\big) \\
&= \big(x^e \,\%\, n\big)^d \,\%\, n \\
&= x^{e \cdot d} \,\%\, n \\
&= x^{1 + k \cdot (p-1) \cdot (q-1)} \,\%\, n \\
&= x \cdot x^{k \cdot (p-1) \cdot (q-1)} \,\%\, n
\end{aligned}$$

Um den Beweis abzuschließen, zeigen wir, dass

$$x^{k \cdot (p-1) \cdot (q-1)} \,\%\, n = 1$$

ist. Da $x < min(p, q)$ gilt und $n = p \cdot q$ ist, haben wir $ggt(x, n) = 1$. Daher gilt nach dem Satz von Euler

$$x^{\varphi(n)} \approx_n 1.$$

Da $n = p \cdot q$ ist und da p und q als verschiedene Primzahlen sicher teilerfremd sind, wissen wir, dass

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

gilt. Damit folgt aus dem Satz von Euler, dass

$$x^{(p-1)\cdot(q-1)} \approx_n 1 \tag{7.9}$$

gilt, woraus sofort

$$x^{k\cdot(p-1)\cdot(q-1)} \approx_n 1$$

folgt. Diese Gleichung können wir auch als

$$x^{k\cdot(p-1)\cdot(q-1)} \,\%\, n = 1$$

schreiben. Multiplizieren wir diese Gleichung mit x und berücksichtigen, dass $x \,\%\, n = x$, denn $x < n$, so erhalten wir

$$g\big(f(x)\big) = x \cdot x^{k\cdot(p-1)\cdot(q-1)} \,\%\, n = x$$

und damit kann $g(x)$ tatsächlich als *Entschlüsselungs-Funktion* benutzt werden um aus dem kodierten Wert $f(x)$ den ursprünglichen Wert x zurückzurechnen.

Der RSA-Algorithmus funktioniert nun wie folgt:

1. Zunächst wird die zu verschlüsselnde Nachricht in einzelne Blöcke aufgeteilt, die jeweils durch Zahlen x kodiert werden können, die kleiner als p und q sind.

2. Jede solche Zahl x wird nun zu dem Wert $x^e \,\%\, n$ verschlüsselt:

   $$x \mapsto x^e \,\%\, n.$$

3. Der Empfänger der Nachricht kann aus dem verschlüsselten Wert $y = x^e \,\%\, n$ die ursprüngliche Botschaft x wieder entschlüsseln, indem er die Transformation

   $$y \mapsto y^d \,\%\, n$$

   durchführt, denn wir hatten ja oben gezeigt, dass

   $$(x^e \,\%\, n)^d \,\%\, n = x$$

   ist. Dazu muss er allerdings den Wert von d kennen. Dieser Wert von d ist der geheime Schlüssel.

In der Praxis ist es so, dass die Werte von n und e veröffentlicht werden, der Wert von d bleibt geheim. Um den Wert von d zu berechnen, muss das Produkt $(p-1)\cdot(q-1)$ berechnet werden, was übrigens gerade $\varphi(n)$ ist. Nun ist bisher kein Algorithmus bekannt, mit dem ein Zahl n effizient in Primfaktoren zerlegt werden kann. Daher kann die Zahl d nur mit sehr hohen Aufwand bestimmt werden. Folglich kann, da n und e öffentlich bekannt sind, jeder eine Nachricht verschlüsseln, aber nur derjenige, der auch d kennt, kann die Nachricht wieder entschlüsseln.

Der RSA-Algorithmus kann auch zum digitalen Signieren eingesetzt werden. Dazu bleibt e geheim und d wird öffentlich gemacht. Eine Nachricht x wird dann als $f(x)$ verschlüsselt. Diese Nachricht kann jeder durch Anwendung der Funktion $x \mapsto g(x)$ wieder entschlüsseln, um aber eine gegebene Nachricht x als $f(x)$ zu verschlüsseln, bedarf es der Kenntnis von e.

Kapitel 8

Komplexe Zahlen

8.1 Einführung und Definition

Die Gleichung $x^2 = -1$ hat in den reelen Zahlen keine Lösung. Wir wollen uns überlegen, ob es eventuell möglich ist, die Menge der reellen Zahlen so zu erweitern, dass die Gleichung $x^2 = -1$ doch eine Lösung hat. Bezeichnen wir diese Lösung mit i, so muss für dieses i also

$$i \cdot i = -1$$

gelten. Wir definieren dann die Menge $\mathbb{C}$ der *komplexen Zahlen* als Menge von Paaren

$$\mathbb{C} := \{\langle x, y\rangle \mid x \in \mathbb{R} \wedge y \in \mathbb{R}\}.$$

Unser Ziel ist es, auf der Menge $\mathbb{C}$ Operationen $+$ und $\cdot$ so einzuführen, dass die Struktur

$$\langle \mathbb{C}, \langle 0, 0\rangle, \langle 1, 0\rangle, +, \cdot\rangle$$

damit ein Körper wird und das gleichzeitig für i die Gleichung $i \cdot i = -1$ erfüllt ist. Zur Vereinfachung der Schreibweise werden wir dass Paar

$$\langle x, y\rangle \quad \text{oft auch als} \quad x + i \cdot y$$

schreiben. Das diese Schreibweise tatsächlich sinnvoll ist, sehen wir später. Weiter definieren wir auf den komplexen Zahlen eine Addition, indem wir

$$\langle x_1, y_1\rangle + \langle x_2, y_2\rangle := \langle x_1 + x_2, y_1 + y_2\rangle$$

definieren. Es ist leicht nachzurechnen, dass für die so definierte Addition von Paaren das sowohl das Assoziativ-Gesetz als auch das Kommutativ-Gesetz gilt und das weiterhin das Paar $\langle 0, 0\rangle$ ein neutrales Element dieser Addition ist. Außerdem ist klar, dass mit dieser Definition das Paar $\langle -x, -y\rangle$ bezüglich der Addition ein inverses Element ist. Wir definieren daher

$$-\langle x, y\rangle := \langle -x, -y\rangle$$

und haben dann offenbar

$$\langle x, y\rangle + -\langle x, y\rangle = \langle 0, 0\rangle.$$

Damit ist die Struktur

$$\langle \mathbb{C}, \langle 0, 0\rangle, +\rangle$$

schon mal eine kommutative Gruppe.

Übertragen wir die Definition der Addition in die suggestive Schreibweise, so erhalten wir

$$(x_1 + i \cdot y_1) + (x_2 + i \cdot y_2) = (x_1 + x_2) + i \cdot (y_1 + y_2).$$

Beachten Sie, dass die Argumente des Operators $+$ auf der linken Seite dieser Gleichung komplexe Zahlen sind, auf der rechten Seite dieser Gleichung werden aber nur reelle Zahlen addiert.

Als nächstes wollen wir für komplexe Zahlen eine Multiplikation einführen. Das Ziel ist, diese Definition so zu wählen, dass wir mit den komplexen Zahlen suggestiv rechnen können und das dabei $i \cdot i = -1$ gilt. Wir rechnen ganz unbefangen das Produkt $(x_1 + i \cdot y_1) \cdot (x_2 + i \cdot y_2)$ aus und erhalten unter Verwendung des Distributiv-Gesetzes

$$\begin{aligned}
& (x_1 + i \cdot y_1) \cdot (x_2 + i \cdot y_2) \\
= \;& x_1 \cdot x_2 + x_1 \cdot i \cdot y_2 + i \cdot y_1 \cdot x_2 + i \cdot y_1 \cdot i \cdot y_2 \\
= \;& x_1 \cdot x_2 + i \cdot i \cdot y_1 \cdot y_2 + i \cdot (x_1 \cdot y_2 + y_1 \cdot x_2) \\
= \;& x_1 \cdot x_2 - y_1 \cdot y_2 + i \cdot (x_1 \cdot y_2 + y_1 \cdot x_2), \qquad \text{denn es soll } i \cdot i = -1 \text{ gelten.}
\end{aligned}$$

Wir definieren daher für Paare $\langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \in \mathbb{C}$ die Multiplikation durch die Festlegung

$$\langle x_1, y_1 \rangle \cdot \langle x_2, y_2 \rangle := \langle x_1 \cdot x_2 - y_1 \cdot y_2,\ x_1 \cdot y_2 + y_1 \cdot x_2 \rangle.$$

Es ist nun leicht zu sehen, dass für die so definierte Multiplikation das Kommutativ-Gesetz gilt. Auch die Gültigkeit des Assoziativ-Gesetzes läßt sich nachrechnen: Die Rechnung ist zwar etwas länger, sie verläuft aber völlig geradlinig. Außerdem können wir sehen, dass $\langle 1, 0 \rangle$ ein neutrales Element bezüglich der Multiplikation ist, denn wir haben

$$\begin{aligned}
\langle 1, 0 \rangle \cdot \langle x, y \rangle &= \langle 1 \cdot x - 0 \cdot y,\ 1 \cdot y + 0 \cdot x \rangle \\
&= \langle x, y \rangle.
\end{aligned}$$

Um das multiplikative Inverse zu der komplexen Zahl $\langle x, y \rangle$ im Falle $\langle x, y \rangle \neq \langle 0, 0 \rangle$ zu berechnen, versuchen wir eine komplexe Zahl $\langle a, b \rangle$ so zu bestimmen, dass

$$\langle a, b \rangle \cdot \langle x, y \rangle = \langle 1, 0 \rangle$$

gilt. Dazu führen wir das obige Produkt aus und erhalten

$$\langle a \cdot x - b \cdot y,\ a \cdot y + b \cdot x \rangle = \langle 1, 0 \rangle.$$

Das führt auf die beiden Gleichungen

$$a \cdot x - b \cdot y = 1 \quad \text{und} \quad a \cdot y + b \cdot x = 0. \tag{8.1}$$

Wir multiplizieren die erste dieser beiden Gleichungen mit y und die zweite Gleichung mit x. Das liefert

$$a \cdot x \cdot y - b \cdot y^2 = y \quad \text{und} \quad a \cdot x \cdot y + b \cdot x^2 = 0.$$

Nach der zweiten Gleichung gilt $a \cdot x \cdot y = -b \cdot x^2$ Ersetzen wir nun in der ersten Gleichung den Term $a \cdot x \cdot y$ durch $-b \cdot x^2$, so erhalten wir

$$-b \cdot x^2 - b \cdot y^2 = y, \quad \text{bzw.} \quad b \cdot (x^2 + y^2) = -y.$$

Also muss

$$b = \frac{-y}{x^2 + y^2}$$

gelten. Um auch a zu bestimmen, multiplizieren wir die erste der beiden Gleichungen in (8.1) mit x und die zweite mit y. Das liefert

$$a \cdot x^2 - b \cdot x \cdot y = x \quad \text{und} \quad a \cdot y^2 + b \cdot x \cdot y = 0.$$

Die zweite Gleichung zeigt, dass

$$-b \cdot x \cdot y = a \cdot y^2$$

gilt. Setzen wir dies in die erste Gleichung ein, so erhalten wir

$$a \cdot x^2 + a \cdot y^2 = x,$$

woraus sofort

$$a = \frac{x}{x^2 + y^2}$$

folgt. Damit sehen wir, dass

$$\left\langle \frac{x}{x^2 + y^2},\ \frac{-y}{x^2 + y^2} \right\rangle$$

das multiplikative Inverse von $\langle x, y\rangle$ ist. In suggestiver Schreibweise liest sich das als

$$(x + i \cdot y)^{-1} = \frac{1}{x^2 + y^2} \cdot (x - i \cdot y).$$

Sie können auch unmittelbar nachrechnen, dass für $\langle x, y\rangle \neq \langle 0, 0\rangle$ die Gleichung

$$\frac{1}{x^2 + y^2} \cdot (x - i \cdot y) \cdot (x + i \cdot y) = 1 + i \cdot 0 = 1$$

erfüllt ist. Damit haben wir nun insgesamt gezeigt, dass die Struktur

$$\big\langle \mathbb{C}, \langle 0, 0\rangle, \langle 1, 0\rangle, +, \cdot \big\rangle$$

ein Körper ist. Die Zahl i wird in diesem Körper durch das Paar $\langle 0, 1\rangle$ dargestellt und Sie können leicht sehen, dass

$$i \cdot i = \langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle -1, 0\rangle = -1$$

gilt. Damit hat in dem so definierten Körper $\mathbb{C}$ die Gleichung $z^2 = -1$ die Lösung $i = \langle 0, 1\rangle$. Wir schreiben daher auch $i = \sqrt{-1}$.

Ist $z = \langle x, y\rangle = x + i \cdot y$ eine komplexe Zahl, so ist bezeichnen wir x als den *Realteil* und y als den Imaginärteil von z.

Aufgabe 17: Zeigen Sie, dass für die oben definierte Multiplikation in $\mathbb{C}$ das Assoziativ-Gesetz gilt.

Aufgabe 18: Zeigen Sie, dass in der Menge $\mathbb{C}$ der komplexen Zahlen das Distributiv-Gesetz gilt.

8.2 Quadratwurzeln komplexer Zahlen

Wir überlegen uns nun, wie wir aus komplexen Zahlen die Wurzel ziehen können. Ist eine komplexe Zahl $x + i \cdot y$ gegeben, so suchen wir also nun eine komplexe Zahl $a + i \cdot b$, so dass

$$x + i \cdot y = (a + i \cdot b)^2$$

gilt. Führen wir das Quadrat auf der rechten Seite dieser Gleichung aus, so erhalten wir

$$x + i \cdot y = a^2 - b^2 + i \cdot 2 \cdot a \cdot b.$$

Durch Vergleich von Real- und Imaginärteil erhalten wir daraus die beiden Gleichungen

$$x = a^2 - b^2 \quad \text{und} \quad y = 2 \cdot a \cdot b. \tag{8.2}$$

Wir betrachten zunächst den Fall $a \neq 0$ und lösen die zweite Gleichung nach b auf. Wir erhalten

$$b = \frac{y}{2 \cdot a} \tag{8.3}$$

Setzen wir diesen Ausdruck in der ersten Gleichung von (8.2) ein, so erhalten wir die Gleichung

$$x = a^2 - \frac{y^2}{4 \cdot a^2}.$$

Wir multiplizieren diese Gleichung mit a^2. Das liefert

$$x \cdot a^2 = a^4 - \frac{y^2}{4},$$

was wir als quadratische Gleichung für die Unbekannte a^2 auffassen können. Diese Gleichung

stellen wir um und addieren außerdem die quadratische Ergänzung $\left(\frac{x}{2}\right)^2 = \frac{x^2}{4}$ auf beiden Seiten:

$$\frac{y^2}{4} + \frac{x^2}{4} = a^4 - x \cdot a^2 + \left(\frac{x}{2}\right)^2.$$

Diese Gleichung können wir auch anders als

$$\frac{y^2}{4} + \frac{x^2}{4} = \left(a^2 - \frac{x}{2}\right)^2$$

schreiben. Ziehen wir jetzt die Quadrat-Wurzel, so erhalten wir

$$\frac{1}{2} \cdot \sqrt{y^2 + x^2} = a^2 - \frac{x}{2}.$$

An dieser Stelle ist klar, dass bei der Wurzel nur das positive Vorzeichen in Frage kommt, denn a^2 muss positiv sein und der Ausdruck

$$\frac{x}{2} - \frac{1}{2} \cdot \sqrt{y^2 + x^2}$$

ist sicher negativ. Für a erhalten wir dann

$$a = \sqrt{\frac{1}{2} \cdot \left(x + \sqrt{x^2 + y^2}\right)}\,.$$

Setzen wir diesen Wert in Gleichung (8.3) ein, so ergibt sich für b der Wert

$$b = \frac{y}{\sqrt{2 \cdot \left(x + \sqrt{x^2 + y^2}\right)}}.$$

Insgesamt erhalten wir damit für die Quadrat-Wurzel der komplexen Zahl $x + i \cdot y$ das Ergebnis

$$\sqrt{x + i \cdot y} = \sqrt{\frac{1}{2} \cdot \left(x + \sqrt{x^2 + y^2}\right)} + i \cdot \frac{y}{\sqrt{2 \cdot \left(x + \sqrt{x^2 + y^2}\right)}},$$

was allerdings im Falle $y = 0$ nur richtig ist, solange $x > 0$ ist. Falls $y = 0$ und $x < 0$ gilt, dann gilt offenbar

$$\sqrt{x + i \cdot y} = i \cdot \sqrt{-x}.$$

Beispiele: Wir testen die obige Formel an zwei Beispielen:

1. $$\begin{aligned}
\sqrt{i} &= \sqrt{0 + i \cdot 1} \\
&= \sqrt{\frac{1}{2} \cdot \left(0 + \sqrt{0 + 1}\right)} + i \cdot \frac{1}{\sqrt{2 \cdot \left(0 + \sqrt{0 + 1}\right)}} \\
&= \sqrt{\frac{1}{2} \cdot 1} + i \cdot \frac{1}{\sqrt{2 \cdot 1}} \\
&= \frac{1}{\sqrt{2}} \cdot (1 + i).
\end{aligned}$$

$$
\begin{array}{lrcl}
2. & \sqrt{3 + i \cdot 4} & = & \sqrt{\frac{1}{2} \cdot \Big(3 + \sqrt{9+16}\Big)} + i \cdot \frac{4}{\sqrt{2 \cdot \Big(3 + \sqrt{9+16}\Big)}} \\
& & = & \sqrt{\frac{1}{2} \cdot (3+5)} + i \cdot \frac{4}{\sqrt{2 \cdot (3+5)}} \\
& & = & \sqrt{\frac{1}{2} \cdot (8)} + i \cdot \frac{4}{\sqrt{2 \cdot 8}} \\
& & = & \sqrt{4} + i \cdot \frac{4}{\sqrt{16}} \\
& & = & 2 + i \cdot \frac{4}{4} \\
& & = & 2 + i \cdot 1
\end{array}
$$

Bemerkung: Bei dem Rechnen mit Wurzeln aus komplexen Zahlen ist Vorsicht geboten, denn die Gleichung

$$\sqrt{z_1 \cdot z_2} = \sqrt{z_1} \cdot \sqrt{z_2} \quad \text{ist falsch!}$$

Um dies einzusehen, betrachten wir die folgende Gleichungskette

$$1 = \sqrt{1} = \sqrt{(-1) \cdot (-1)} \stackrel{?}{=} \sqrt{-1} \cdot \sqrt{-1} = i \cdot i = -1.$$

Hätten wir an der mit $\stackrel{?}{=}$ markierten Stelle dieser Gleichungskette tatsächlich eine Gleichheit, so hätten wir bewisen, dass $1 = -1$ ist, und das ist natürlich Unsinn.

8.3 Geometrische Interpretation

Ähnlich wie sich reele Zahlen auf der Zahlengeraden darstellen lassen, können wir auch komplexe Zahlen geometrisch interpretieren. Da komplexe Zahlen aus zwei Komponenten bestehen, benötigen wir nun zwei Dimensionen. Die komplexe Zahl $a + i \cdot b$ wird daher als der Punkt in der Ebene interpretiert, dessen x Koordinate den Wert a und dessen y Komponente den Wert b hat. Wir haben damit die Korrespondenz

$$a + i \cdot b \mathrel{\widehat{=}} \langle a, b \rangle.$$

Tragen wir komplexe Zahlen in dieser Weise geometrisch dar, so nennen wir die resultierende Zahlen-Ebene die *Gauß'sche Zahlen-Ebene*. Abbildung 8.1 zeigt diese Ebene. Dort ist die komplexe Zahl $a + i \cdot b$ eingezeichnet. Der Abstand, den der Punkt mit den Koordinaten $x = a$ und $y = b$ von dem Ursprungspunkt mit den Koordinaten $x = 0$ und $y = 0$ hat, beträgt nach dem Satz des Pythagoras $\sqrt{a^2 + b^2}$. Daher ist der Betrag einer komplexen Zahl wie folgt definiert:

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

Bezeichnen wir den Betrag der komplexen Zahl $a + i \cdot b$ mit r, setzen wir also $r := |a + i \cdot b|$, so besteht zwischen dem in der Abbildung eingezeichneten Winkel φ und den Komponenten a und b die Beziehung

$$a = r \cdot \cos(\varphi) \quad \text{und} \quad b = r \cdot \sin(\varphi).$$

Durch Division der zweiten Gleichung durch die erste Gleichung erhalten wir die Beziehung

$$\tan(\varphi) = \frac{b}{a}.$$

Solange wir uns im ersten Quadranten der Ebene befinden, können wir daraus den Winkel φ mit Hilfe der Gleichung

$$\varphi = \arctan\Big(\frac{b}{a}\Big)$$

ausrechnen. Das Paar $\langle r, \varphi \rangle$ bezeichnen wir als die *trigonometische Darstellung* der komplexen

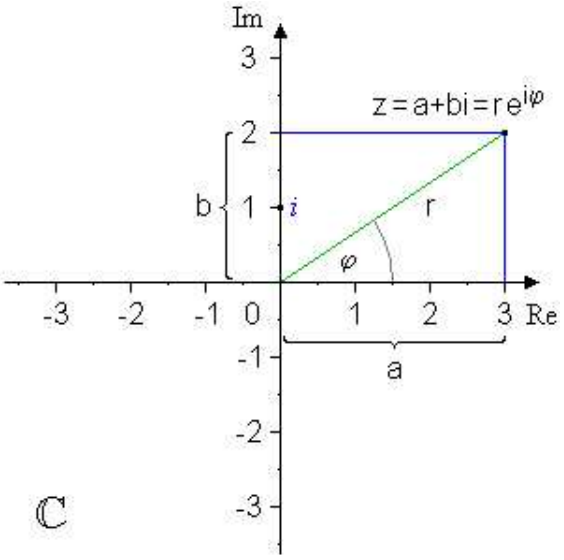

Abbildung 8.1: Die Gauß'sche Zahlen-Ebene.

Zahl $a + i \cdot b$, während wir das Paar $\langle a, b \rangle$ die *kartesische Darstellung* nennen. Es ist instruktiv zu sehen, was in der trigonometrischen Darstellung passiert, wenn wir zwei komplexe Zahlen

$$r_1 \cdot \cos(\varphi_1) + i \cdot r_1 \cdot \sin(\varphi) \quad \text{und} \quad r_2 \cdot \cos(\varphi_2) + i \cdot r_2 \cdot \sin(\varphi)$$

multiplizieren. Wir haben nämlich

$$\begin{aligned}
& \big(r_1 \cdot \cos(\varphi_1) + i \cdot r_1 \cdot \sin(\varphi_1)\big) \cdot \big(r_2 \cdot \cos(\varphi_2) + i \cdot r_2 \cdot \sin(\varphi_2)\big) \\
= \;& r_1 \cdot r_2 \cdot \Big(\cos(\varphi_1) \cdot \cos(\varphi_2) - \sin(\varphi_1) \cdot \sin(\varphi_2) + i \cdot \big(\cos(\varphi_1) \cdot \sin(\varphi_2) + \sin(\varphi_1) \cdot \cos(\varphi_2)\big)\Big) \\
= \;& r_1 \cdot r_2 \cdot \big(\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)\big).
\end{aligned}$$

Im letzten Schritt dieser Umformung haben wir dabei die beiden Additions-Theoreme

$$\sin(\alpha + \beta) = \sin(\alpha) \cdot \cos(\beta) + \cos(\alpha) \cdot \sin(\beta) \quad \text{und}$$
$$\cos(\alpha + \beta) = \cos(\alpha) \cdot \cos(\beta) - \sin(\alpha) \cdot \sin(\beta)$$

benutzt. Wegen seiner Wichtigkeit halten wir das Ergebnis der obigen Rechnung in der folgenden Formel fest:

$$\big(\cos(\varphi_1) + i \cdot \sin(\varphi_1)\big) \cdot \big(\cos(\varphi_2) + i \cdot \sin(\varphi_2)\big) = \big(\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)\big). \tag{8.4}$$

Wir sehen, dass es in der trigonometrischen Darstellung einfach ist, komplexe Zahlen zu multiplizieren: Die Winkel der Zahlen werden addiert. Der Übersichtlichkeit halber habe ich die Beträge r_1 und r_2 in der oberen Formel weggelassen.

8.3.1 Potenzen und allgemeine Wurzeln

Ist eine komplexe Zahl in trigonometischer Darstellung gegeben, so ist es leicht, die Zahl zu potenzieren, denn nach Gleichung 8.4 gilt für alle natürlichen Zahlen $n \in \mathbb{N}$

$$\big(\cos(\varphi) + i \cdot \sin(\varphi)\big)^n = \cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi). \tag{8.5}$$

Diese Formel wird auch als *Satz von de Moivre* bezeichnet. Sie kann auch zum Ziehen beliebiger Wurzeln aus einer komplexen Zahl verwendet werden. Um mit Hilfe dieses Satzes Wurzeln ziehen zu können, bemerken wir zunächst, dass die Funktionen $\sin(x)$ und $\cos(x)$ periodisch mit der

Periode $2 \cdot \pi$ sind, es gilt also

$$\sin(x + 2 \cdot \pi) = \sin(x) \quad \text{und} \quad \cos(x + 2 \cdot \pi) = \cos(x).$$

Diese Gleichungen lassen sich für beliebige $k \in \mathbb{N}$ zu

$$\sin(\varphi + 2 \cdot k \cdot \pi) = \sin(\varphi) \quad \text{und} \quad \cos(\varphi + 2 \cdot k \cdot \pi) = \cos(\varphi)$$

verallgemeinern. Wir überlegen nun, für welche komplexe Zahlen der Form

$$z = \cos(\varphi) + i \cdot \sin(\varphi) \quad \text{die Gleichung} \quad z^n = 1$$

erfüllt ist. Solche Zahlen bezeichnen wir als n-te Einheitswurzeln. Da

$$1 = \cos(2 \cdot k \cdot \pi) + i \cdot \sin(2 \cdot k \cdot \pi)$$

gilt, muss nach Gleichung 8.5 für die Zahl $z = \cos(\varphi) + i \cdot \sin(\varphi)$ die Beziehung

$$\cos(2 \cdot k \cdot \pi) + i \cdot \sin(2 \cdot k \cdot \pi) = \cos(n \cdot \varphi) + i \cdot \sin(n \cdot \varphi) \tag{8.6}$$

erfüllt sein, wenn $z^n = 1$ sein soll. Die Gleichung 8.6 ist offensichtlich dann erfüllt, wenn

$$\varphi = \frac{2 \cdot k \cdot \pi}{n}$$

gilt, wobei wir k auf die Elemente der Menge $\{0, 1, \cdots, n-1\}$ beschränken können, denn größere Werte von k liefern Winkel, die größer als $2 \cdot \pi$ sind. Wir definieren daher

$$\zeta_n := \cos\left(\tfrac{2 \cdot \pi}{n}\right) + i \cdot \sin\left(\tfrac{2 \cdot \pi}{n}\right)$$

als die *primitive* n-te Einheitswurzel und sehen, dass die Zahlen

$$\zeta_n^k := \cos\left(\tfrac{2 \cdot k \cdot \pi}{n}\right) + i \cdot \sin\left(\tfrac{2 \cdot k \cdot \pi}{n}\right) \quad \text{für } k \in \{0, 1, \cdots, n-1\}$$

dann alle n-ten Einheitswurzeln sind.

Beispiel: Für die primitive dritte Einheitswurzel ζ_3 gilt

$$\zeta_3 = \cos\left(\tfrac{2 \cdot \pi}{3}\right) + i \cdot \sin\left(\tfrac{2 \cdot \pi}{3}\right) = -\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}.$$

Für ζ_3^2 finden wir nach kurzer Rechnung

$$\zeta_3^2 = \cos\left(\tfrac{4 \cdot \pi}{3}\right) + i \cdot \sin\left(\tfrac{4 \cdot \pi}{3}\right) = -\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}.$$

Sie können leicht nachrechnen, dass sowohl $\zeta_3^3 = 1$ als auch $(\zeta_3^2)^3 = 1$ gilt.

Mit Hilfe der n-ten Einheitswurzeln können wir jetzt allgemein für eine komplexe Zahl z und eine natürliche Zahl n die Lösungen der Gleichung $r^n = z$ angeben. Dazu ist zunächst z in trigonometrischen Koordinaten anzugeben. Falls

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

gilt, so ist offenbar für alle $k \in \{0, 1, \cdots, n-1\}$ die Zahl

$$r = \zeta_n^k \cdot \sqrt[n]{r} \cdot \left(cos\left(\frac{\varphi}{n}\right) + i \cdot \sin\left(\frac{\varphi}{n}\right)\right)$$

eine Lösung der Gleichung $r^n = z$.

Beispiel: Wir berechnen alle Lösungen der Gleichung $r^3 = 1 + i$. Dazu müssen wir zuächst die Zahl $1 + i$ in trigonometrischen Koordinaten darstellen. Setzen wir

$$\varphi = \arctan\left(\frac{1}{1}\right) = \arctan(1) = \frac{\pi}{4},$$

so gilt wegen $\sqrt{1^2 + 1^2} = \sqrt{2}$ offenbar

$$1 + i = \sqrt{2} \cdot \left(\cos\left(\tfrac{\pi}{4}\right) + i \cdot \sin\left(\tfrac{\pi}{4}\right)\right).$$

Damit erhalten wir dann als eine dritte Wurzel der Zahl $1+i$ den Ausdruck

$$r := \sqrt[6]{2} \cdot \Big(\cos\big(\tfrac{\pi}{12}\big) + i \cdot \sin\big(\tfrac{\pi}{12}\big)\Big).$$

Berücksichtigen wir noch, dass die Werte der trigonometrischen Funktionen für das Argument $\frac{\pi}{12}$ bekannt sind, es gilt nämlich

$$\cos\big(\tfrac{\pi}{12}\big) = \tfrac{1}{4} \cdot (\sqrt{6} + \sqrt{2}) \quad \text{und} \quad \sin\big(\tfrac{\pi}{12}\big) = \tfrac{1}{4} \cdot (\sqrt{6} - \sqrt{2}),$$

so erhalten wir für r den Ausdruck

$$r = \tfrac{1}{4} \cdot \sqrt[6]{2} \cdot \Big(\sqrt{6} + \sqrt{2} + i \cdot \big(\sqrt{6} - \sqrt{2}\big)\Big).$$

Ziehen wir hier $\sqrt{2}$ aus der Klammer und berücksichtigen, dass

$$\sqrt[6]{2} \cdot \sqrt{2} = 2^{\frac{1}{6}} \cdot 2^{\frac{1}{2}} = 2^{\frac{4}{6}} = 2^{\frac{2}{3}} = \sqrt[3]{4}$$

gilt, so können wir r als

$$r = \tfrac{1}{4} \cdot \sqrt[3]{4} \cdot \Big(\sqrt{3} + 1 + i \cdot \big(\sqrt{3} - 1\big)\Big)$$

schreiben. Die anderen beiden dritten Wurzeln erhalten wir daraus durch Multiplikation mit ζ_3 bzw. ζ_3^2.

Bemerkung: Bei der obigen Rechnung hatten wir Glück: Erstens konnten wir für den Winkel φ einen expliziten Ausdruck, nämlich $\frac{\pi}{4}$, angeben und zweitens konnten wir auch die Anwendung der trigonometrischen Funktionen auf $\frac{\varphi}{3} = \frac{\pi}{12}$ geschlossene Terme angeben. Normalerweise funktioniert das nicht und dann bleibt nur die numerische Rechnung.

8.4 Anwendung der komplexen Zahlen

Wir können jetzt zwar mit komplexen Zahlen rechnen, wir haben aber bisher noch nicht gesehen, warum der Gebrauch von komplexen Zahlen überhaupt notwendig ist. Es gibt in der Mathematik eine Vielzahl von Anwendung der komplexen Zahlen. Stellvertretend möchte ich an dieser Stelle die Fourier-Transformation einer Funktion nennen, die in der Signalverarbeitung eine große Rolle spielt. Darauf näher einzugehen ist aus Zeitgründen im Rahmen einer einführenden Mathematik-Vorlesung leider unmöglich. Auch für die Anwendung komplexer Zahlen bei der Lösung von Differenzial-Gleichungen ist es jetzt noch zu früh. Ich möchte statt dessen den historischen Weg gehen und zeigen, wie die komplexen Zahlen tatsächlich entdeckt worden sind. Ausgangspunkt unserer Überlegungen ist dabei die Gleichung

$$x^3 - 15 \cdot x - 4 = 0.$$

Wir wollen alle möglichen Lösungen dieser Gleichung bestimmen. Um uns einen Überblick zu verschaffen, skizzieren wir zunächst die Funktion $x \mapsto x^3 - 15 \cdot x - 4$. Wir erhalten den in Abbildung 8.2 auf Seite 110 gezeigten Graphen.

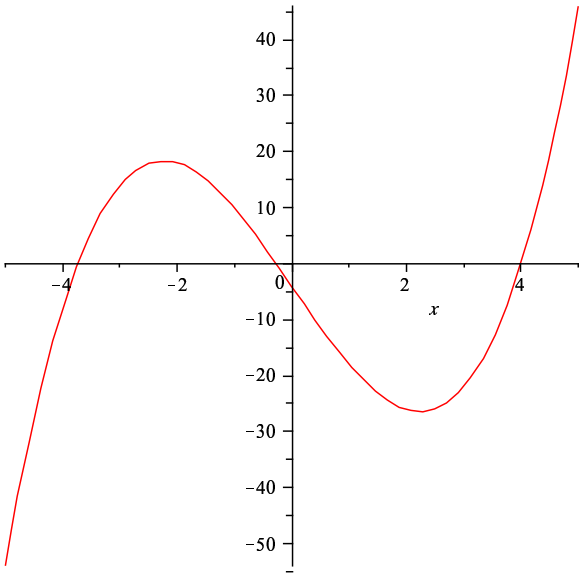

Abbildung 8.2: Die Funktion $x \mapsto x^3 - 15 \cdot x - 4$.

Es sieht so aus, als ob unsere Gleichung drei verschiedene Lösungen hat. Um diese Lösungen zu bestimmen, verallgemeinern wir unser Problem und versuchen, die kubische Gleichung

$$x^3 - p \cdot x - q = 0 \tag{8.7}$$

zu lösen. Wir machen dazu den Ansatz $x = u + v$. Nun gilt

$$\begin{aligned}
(u+v)^3 &= (u+v)^2 \cdot (u+v) \\
&= (u^2 + 2 \cdot u \cdot v + v^2) \cdot (u+v) \\
&= u^3 + u^2 \cdot v + 2 \cdot u^2 \cdot v + 2 \cdot u \cdot v^2 + u \cdot v^2 + v^3 \\
&= u^3 + 3 \cdot u^2 \cdot v + 3 \cdot u \cdot v^2 + v^3 \\
&= 3 \cdot u \cdot v \cdot (u+v) + u^3 + v^3
\end{aligned}$$

Daher können wir die kubische Gleichung mit dem Ansatz $x = u + v$ in die Gleichung

$$3 \cdot u \cdot v \cdot (u+v) + u^3 + v^3 - p \cdot (u+v) - q = 0$$

überführen, was wir noch zu

$$(3 \cdot u \cdot v - p) \cdot (u + v) + u^3 + v^3 - q = 0$$

umschreiben. Falls es uns nun gelingt, die Zahlen u und v so zu bestimmen, dass

$$p = 3 \cdot u \cdot v \quad \text{und} \quad q = u^3 + v^3$$

gilt, dann ist $x = u + v$ eine Lösung der kubischen Gleichung 8.7. Wir definieren nun

$$\alpha := u^3 \quad \text{und} \quad \beta := v^3.$$

Damit lassen sich die Gleichungen für u und v umschreiben in

$$p^3 = 27 \cdot \alpha \cdot \beta \quad \text{und} \quad q = \alpha + \beta$$

Ist $\alpha \neq 0$, so folgt aus der ersten Gleichung

$$\beta = \frac{p^3}{27 \cdot \alpha}.$$

Setzen wir diesen Wert in die zweite Gleichung ein, so erhalten wir

$$q = \alpha + \frac{p^3}{27 \cdot \alpha}.$$

Multiplikation dieser Gleichung mit α liefert uns eine quadratische Gleichung für α:

$$q \cdot \alpha = \alpha^2 + \frac{p^3}{27}.$$

Diese Gleichung stellen wir zu

$$-\frac{p^3}{27} = \alpha^2 - q \cdot \alpha$$

um. Addieren wir auf beiden Seiten die quadratische Ergänzung $\frac{q^2}{4}$, so erhalten wir die quadratische Gleichung

$$\frac{q^2}{4} - \frac{p^3}{27} = \left(\alpha - \frac{q}{2}\right)^2.$$

Diese Gleichung hat offenbar die Lösung

$$\alpha = \frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}.$$

Wegen $q = \alpha + \beta$ folgt daraus für β

$$\beta = \frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}.$$

Wir prüfen, ob für diese Werte von α und β auch die zweite Bedingung

$$\alpha \cdot \beta = \left(\frac{p}{3}\right)^3$$

erfüllt ist und finden tatsächlich

$$\begin{aligned} \alpha \cdot \beta &= \left(\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}\right) \cdot \left(\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}\right) \\ &= \frac{q^2}{4} - \left(\frac{q^2}{4} - \frac{p^3}{27}\right) \\ &= \frac{p^3}{27}. \end{aligned}$$

Berücksichtigen wir, dass $\alpha = u^3$, $\beta = v^3$ und $x = u + v$ ist, so erhalten wir zur Lösung der kubischen Gleichung 8.7 die *Cardanische Formel*

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}\ .$$

In unserem ursprünglichen Problem gilt $p = 15$ und $q = 4$. Dann haben wir

$$\alpha = \frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3} = 2 + \sqrt{4 - 125} = 2 + \sqrt{-121} = 2 + i \cdot 11.$$

Das ist aber eine komplexe Zahl, aus der wir jetzt noch die dritte Wurzel ziehen müssen. An dieser Stelle haben wir Glück, denn für die dritte Wurzel aus $2 + i \cdot 11$ und aus $2 - i \cdot 11$ läßt sich jeweils ein expliziter Wert angeben, es gilt

$$u = \sqrt[3]{2 + i \cdot 11} = 2 + i \quad \text{und} \quad v = \sqrt[3]{2 - i \cdot 11} = 2 - i.$$

Wir wollen dieses Ergebnis im ersten Fall nachrechnen. Es gilt

$$\begin{aligned}(2+i)^3 &= 2^3 + 3 \cdot 2^2 \cdot i + 3 \cdot 2 \cdot i^2 - i\ . \\ &= 8 - 6 + (12 - 1) \cdot i \\ &= 2 + 11 \cdot i\end{aligned}$$

Damit finden wir als eine Lösung der kubischen Gleichung $x^3 - 15 \cdot x - 4 = 0$ den Wert

$$x_1 = 2 + 11 \cdot i + 2 - 11 \cdot i = 4.$$

Sie sehen, dass wir ein Problem, dass mit komplexen Zahlen eigentlich nichts zu tun hat, durch die Verwendung komplexer Zahlen lösen können. Der Vollständigkeit halber wollen wir noch die anderen beiden Lösungen der kubischen Gleichung $x^3 - 15 \cdot x - 4 = 0$ bestimmen. Diese erhalten wir, wenn wir in der Cardanischen Formel auch die anderen Möglichkeiten für die dritte Wurzel einsetzen. Dabei müssen wir allerdings berücksichtigen, dass für die Zahlen u und v die Nebenbedingung $3 \cdot u \cdot v = p$ gilt. Multiplizieren wir beispielsweise u mit ζ_3 und v mit ζ_3^2, so haben wir

$$3 \cdot \zeta_3 \cdot u \cdot \zeta_3^2 \cdot v = 3 \cdot \zeta_3^3 \cdot u \cdot v = 3 \cdot u \cdot v = p,$$

denn offenbar gilt $\zeta_3^3 = 1$. Als eine weitere Lösung erhalten wir dann

$$\begin{aligned}x_2 &= \zeta_3 \cdot u + \zeta_3^2 \cdot v \\ &= \zeta_3 \cdot (2+i) + \zeta_3^2 \cdot (2-i) \\ &= \left(-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}\right) \cdot (2+i) + \left(-\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}\right) \cdot (2-i) \\ &= \frac{1}{2} \cdot \left(-2 - \sqrt{3} + i \cdot (-1 + 2 \cdot \sqrt{3}) - 2 - \sqrt{3} + i \cdot (1 - 2 \cdot \sqrt{3})\right) \\ &= -2 - \sqrt{3}.\end{aligned}$$

Auch hier ergibt sich also eine reelle Lösung. Für x_3 finden Sie nach einer ähnlichen Rechnung den Wert

$$x_3 = \zeta_3^2 \cdot u + \zeta_3 \cdot v = -2 + \sqrt{3}.$$

Insgesamt zeigt dieses Beispiel, dass auch für Probleme, deren Lösungen reelle Zahlen sind, der Umweg über die komplexen Zahlen sinnvoll sein kann. Zum Abschluß möchte ich noch bemerken, dass die Verwendung komplexer Zahlen zur Bestimmung der Nullstellen eines Polynoms dritten Grades nicht zwingend notwendig ist. Die Nullstellen lassen sich auch auf trigonometrischem Wege bestimmen. Dann ergibt sich die Formel

$$x_k = 2 \cdot \sqrt{\tfrac{p}{3}} \cdot \cos\left(\tfrac{1}{3} \cdot \arccos\left(\tfrac{3 \cdot q}{2 \cdot p} \cdot \sqrt{\tfrac{3}{p}}\right) - (k-1) \cdot \tfrac{2 \cdot \pi}{3}\right) \quad \text{for } k = 1, 2, 3.$$

Die trigonometrische Herleitung ist allerdings deutlich aufwendiger als die Herleitung die wir in diesem Kapitel auf algebraischem Wege mit Hilfe der komplexen Zahlen gefunden haben.

Kapitel 9

Lineare Gleichungs-Systeme

Wir wollen uns in diesem Kapitel mit der Lösung *linearer Gleichungs-Systeme* beschäftigen. Ein *Gleichungs-System* ist dabei einfach eine Menge von Gleichungen, in denen verschiedene Variablen auftreten. Bezeichnen wir die Variablen mit $x_1, \cdots, x_m$ und liegen die Gleichungen in der Form

$$\sum_{i=1}^{n} a_{i,j} \cdot x_j = b_i \quad \text{für alle } i = 1, \cdots, m$$

vor, wobei die Zahlen $a_{i,j}$ für $i = 1, \cdots, n$ und $j = 1, \cdots, m$ und b_i für $i = 1, \cdots, n$ entweder reell oder komplex sind, so nennen wir das Gleichungs-System *linear*. Anstatt in der obigen kompakten Notation verwenden wir zu Darstellung eines solchen Gleichungs-Systems auch die folgende *Matrix-Schreibweise*:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Hier haben wir die Koeffizienten $a_{i,j}$ der Variablen x_j zu der $n \times m$-*Matrix*

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}$$

zusammengefasst. Eine Matrix ist dabei nichts anderes als ein rechteckiges Schema, in dem die doppelt indizierte Koeffizienten $a_{i,j}$ übersichtlich dargestellt werden können. n bezeichnet die Anzahl der Zeilen der Matrix, während m die Anzahl der Spalten angibt. Gleichzeitig haben wir oben die Variablen $x_1, x_2, \cdots, x_m$ und die Konstanten $b_1, b_2, \cdots, b_n$ als *Vektoren* notiert. Definieren wir

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \quad \text{und} \quad \vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

so können wir das oben gegebene System von linearen Gleichungen auch kurz in der Form

$$A \cdot \vec{x} = \vec{y}$$

schreiben, wenn wir vereinbaren, dass die Multiplikation "$\cdot$" zwischen einer Matrix

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix} \quad \text{und einem Vektor} \quad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$$

als der Vektor

$$\vec{x} = \begin{pmatrix} \sum_{j=1}^{m} a_{1,j} \cdot x_j \\ \sum_{j=1}^{m} a_{2,j} \cdot x_j \\ \vdots \\ \sum_{j=1}^{m} a_{n,j} \cdot x_j \end{pmatrix}$$

definiert wird. Betrachten wir zur Verdeutlichung ein Beispiel: Die drei Gleichungen

$$\begin{aligned} 3 \cdot x + 5 \cdot y + 3 \cdot z &= 4, \qquad \text{(I)} \\ 4 \cdot x + 3 \cdot y + 2 \cdot z &= 3, \qquad \text{(II)} \\ 2 \cdot x + 2 \cdot y + 1 \cdot z &= 1, \qquad \text{(III)} \end{aligned} \tag{9.1}$$

die wir zur späteren Referenzierung mit römischen Zahlen nummeriert haben, können in Matrix-Schreibweise als

$$\begin{pmatrix} 3 & 5 & 3 \\ 4 & 3 & 2 \\ 2 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix}$$

geschrieben werden. Zur Lösung eines solchen Gleichungs-Systems werden wir zwei verschiedene Verfahren diskutieren: In diesem Kapitel betrachten wir das *Gauß'sche Eliminations-Verfahren*[1], später werden wir sehen, wie sich lineare Gleichungs-Systeme mit Hilfe von *Determinanten* lösen lassen.

9.1 Das Gauß'sche Eliminations-Verfahren

Wir demonstrieren das Gauß'sche Eliminations-Verfahren zunächst an dem in (9.1) gezeigten Beispiel. Der Einfachheit halber benutzen wir hier noch keine Matrix-Schreibweise. Um die in (9.1) angegebenen Gleichungen zu lösen, versuchen wir im ersten Schritt, die Variable x aus der zweiten und der dritten Gleichung zu eliminieren. Um x aus der zweiten Gleichung loszuwerden, multiplizieren wir die erste Gleichung mit $-\frac{4}{3}$ und addieren die resultierende Gleichung zu der zweiten Gleichung. Wegen $-\frac{4}{3} \cdot 3 \cdot x + 4 \cdot x = 0$ fällt die Variable x dann aus der zweiten Gleichung heraus und wir erhalten statt der zweiten Gleichung die Gleichung

$$-\tfrac{4}{3} \cdot 5 \cdot y + 3 \cdot y - \tfrac{4}{3} \cdot 3 \cdot z + 2 \cdot z = -\tfrac{4}{3} \cdot 4 + 3,$$

die wir noch zu der Gleichung

$$-\tfrac{11}{3} \cdot y - 2 \cdot z = -\tfrac{7}{3}$$

vereinfachen. Um die Variable x aus der dritten Gleichung zu eliminieren, multiplizieren wir die

[1] Das *Gauß'sche Eliminations-Verfahren* wurde zwar nach Carl Friedrich Gauß benannt, es war aber bereits lange vor Gauß bekannt. Eine schriftliche Beschreibung des Verfahrens findet sich beispielsweise bereits bei Issac Newton, aber das Verfahren war schon deutlich vor Newton mathematisches Allgemeinwissen.

erste Gleichung mit $-\frac{2}{3}$ und addieren die so entstandene Gleichung zu der dritten Gleichung. Wieder fällt der Term mit der Variablen x weg und wir erhalten nun an Stelle der dritten Gleichung die Gleichung

$$(-\tfrac{2}{3} \cdot 5 + 2) \cdot y + (-\tfrac{2}{3} \cdot 3 + 1) \cdot z = -\tfrac{2}{3} \cdot 4 + 1,$$

die wir zu

$$-\tfrac{4}{3} \cdot y + (-1) \cdot z = -\tfrac{5}{3},$$

vereinfachen. Insgesamt haben wir damit das ursprüngliche Gleichungs-System zu dem äquivalenten Gleichungs-System

$$\begin{array}{rcrcrcr} 3 \cdot x & + & 5 \cdot y & + & 3 \cdot z & = & 4 \\ & & -\frac{11}{3} \cdot y & + & (-2) \cdot z & = & -\frac{7}{3} \\ & & -\frac{4}{3} \cdot y & + & (-1) \cdot z & = & -\frac{5}{3} \end{array} \tag{9.2}$$

umgeformt. Um aus der letzten Gleichung die Variable y zu entfernen, multiplizieren wir die zweite Gleichung mit

$$-\frac{-\frac{4}{3}}{-\frac{11}{3}} = -\frac{4}{11}$$

und addieren diese Gleichung zu der letzten Gleichung unseres Gleichungs-Systems. Damit erhalten wir dann an Stelle der letzten Gleichung die neue Gleichung

$$\big(-\tfrac{4}{11} \cdot (-2) + (-1)\big) \cdot z = \big(-\tfrac{4}{11}\big) \cdot \big(-\tfrac{7}{3}\big) - \tfrac{5}{3},$$

die wir zu

$$\big(-\tfrac{3}{11}\big) \cdot z = -\tfrac{9}{11}$$

vereinfachen. Insgesamt haben wir unser ursprüngliches Gleichungs-System jetzt zu dem Gleichungs-System

$$\begin{array}{rcrcrcr} 3 \cdot x & + & 5 \cdot y & + & 3 \cdot z & = & 4 \\ & & -\frac{11}{3} \cdot y & + & (-2) \cdot z & = & -\frac{7}{3} \\ & & & & -\frac{3}{11} \cdot z & = & -\frac{9}{11} \end{array} \tag{9.3}$$

umgeformt. Dieses Gleichungs-System hat, wie man sagt, *obere Dreiecks-Form*, denn unterhalb der Diagonalen haben alle Einträge der Matrix den Wert 0. Wir können es jetzt durch *Rückwärts-Substitution* lösen, indem wir zunächst die letzte Gleichung nach z auflösen, diesen Wert für z dann in die zweite Gleichung einsetzten, die zweite Gleichung nach y auflösen und weiter die Werte für y und z in der ersten Gleichung einsetzten, so dass wir schließlich den Wert von x bestimmen können. Die Auflösung der letzten Gleichung nach z liefert $z = 3$. Setzen wir diesen Wert in der zweiten Gleichung ein, so erhalten wir

$$-\tfrac{11}{3} \cdot y - 6 = -\tfrac{7}{3},$$

was sich zu

$$-\tfrac{11}{3} \cdot y = \tfrac{11}{3},$$

vereinfacht, woraus sofort $y = -1$ folgt. Setzen wir nun die Werte von x und y in der ersten Gleichung ein, so erhalten wir

$$3 \cdot x - 5 + 9 = 4,$$

woraus $x = 0$ folgt. Damit lautet die Lösung des ursprünglichen Gleichungs-Systems

$$x = 0, \quad y = -1, \quad z = 3.$$

Aufgabe 19: Bestimmen Sie die Lösung des folgenden Gleichungs-Systems mit Hilfe des Gauß'schen Eliminations-Verfahrens:

$$2 \cdot x + 1 \cdot y + 3 \cdot z = 2,$$
$$1 \cdot x + 3 \cdot y + 2 \cdot z = 0,$$
$$1 \cdot x + 2 \cdot y + 1 \cdot z = 0.$$

Hinweis: Die Lösungen sind keine ganzen Zahlen.

Wir beschreiben nun, wie ein lineares Gleichungs-System der Form

$$\sum_{j=1}^{m} a_{i,j} \cdot x_j = b_i$$

für eine gegebenen Matrix

$$A := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix} \quad \text{und einen gegebenen Vektor} \quad \vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

gelöst werden kann, wobei wir uns auf den Spezialfall $m = n$ beschränken wollen.

1. Im ersten Schritt eliminieren wir die Variable x_1 aus der 2-ten, 3-ten, $\cdots$, n-ten Gleichung. Um die Variable x_1 aus der i-ten Gleichung zu eliminieren, multiplizieren wir die erste Gleichung mit dem Faktor

   $$-\frac{a_{i,1}}{a_{1,1}}$$

   und addieren die so multiplizierte erste Gleichung zu der i-ten Gleichung. Wegen

   $$-\frac{a_{i,1}}{a_{1,1}} \cdot a_{1,1} \cdot x_1 + a_{i,1} \cdot x_1 = 0$$

   enthält die resultierende Gleichung die Variable x_1 nicht mehr. Die neue i-te Gleichung hat dann die Form

   $$\big(a_{i,2} - \frac{a_{i,1}}{a_{1,1}} \cdot a_{1,1}\big) \cdot x_2 + \cdots + \big(a_{i,n} - \frac{a_{i,1}}{a_{1,1}} \cdot a_{1,n}\big) \cdot x_n = b_i - \frac{a_{i,1}}{a_{1,1}} \cdot b_1,$$

   was sich unter Verwendung der Summen-Schreibweise auch kompakter in der Form

   $$\sum_{j=2}^{n} \big(a_{i,j} - \frac{a_{i,1}}{a_{1,1}} \cdot a_{1,j}\big) \cdot x_j = b_i - \frac{a_{i,1}}{a_{1,1}} \cdot b_1$$

   schreiben läßt.

   Bemerkung: An dieser Stelle fragen Sie sich vermutlich, was passiert, wenn $a_{1,1} = 0$ ist, denn dann ist der Ausdruck $\frac{a_{i,1}}{a_{1,1}}$ offenbar undefiniert. In so einem Fall vertauschen wir einfach die erste Gleichung mit einer anderen Gleichung, für die der Koeffizient der Variablen x_1 von 0 verschieden ist. In der Praxis hat es sich bewährt, immer die Gleichung als erste zu nehmen, für die der Koeffizient der Variablen x_1 den größten Betrag hat, denn dadurch fallen die bei einer numerischen Rechnung zwangsläufig auftretenden Rundungsfehler weniger schwer ins Gewicht als wenn wir die Reihenfolge der Gleichungen beliebig wählen. Diese Verfahren wird als *partielle Pivotisierung* bezeichnet.

2. Im k-ten Schritt nehmen wir an, dass wir die Variablen $x_1, \cdots, x_{k-1}$ bereits aus der k-ten, $(k{+}1)$-ten, $\cdots$, n-Gleichung entfernt haben und wollen nun die Variable x_k aus der $(k{+}1)$-ten bis n-ten Gleichung entfernen. Um die Variable x_k aus der i-ten Gleichung ($i \in \{k{+}1, \cdots, n\}$)

zu entfernen multiplizieren wir die k-te Gleichung mit dem Faktor

$$-\frac{a_{i,k}}{a_{k,k}}$$

und addieren die so multiplizierte k-te Gleichung zu der i-ten Gleichung. Wegen

$$-\frac{a_{i,k}}{a_{k,k}} \cdot a_{k,k} \cdot x_k + a_{i,k} \cdot x_k = 0$$

enthält die resultierende Gleichung die Variable x_k nicht mehr. Die Variablen $x_1, \cdots, x_{k-1}$ wurden aus der i-ten Gleichung bereits vorher eliminiert, so dass die neue i-te Gleichung dann die Form

$$\sum_{j=k+1}^{n} \Big(a_{i,j} - \frac{a_{i,k}}{a_{k,k}} \cdot a_{k,j}\Big) \cdot x_j = b_i - \frac{a_{i,k}}{a_{k,k}} \cdot b_k$$

hat. Aus Gründen der numerischen Stabilität kann wieder eine partielle Pivotisierung durchgeführt werden. Wir wollen im folgenden voraussetzen, dass dies immer möglich ist, dass heißt wir setzen voraus, dass es immer eine Gleichung unter den Gleichungen mit den Nummern $k, \cdots, n$ gibt, in denen die Variable x_k auch tatsächlich auftritt, so dass also immer für mindestens ein $i \in \{k, \cdots, n\}$ der Koeffizient $a_{i,k} \neq 0$ ist. Diese Voraussetzung ist äquivalent zu der Forderung, dass das ursprüngliche Gleichungs-System eindeutig lösbar ist.

3. Im letzten Schritt können wir voraussetzen, dass das Gleichungs-System eine obere Dreiecks-Form hat. Es bleiben nun noch n Teilschritte zur Berechnung der Variablen $x_1, \cdots, x_n$.

   (a) Im ersten Teilschritt lösen wir die n-te Gleichung nach x_n auf. Die n-te Gleichung hat die Form

   $$c_{n,n} \cdot x_n = d_n,$$

   wobei wir die Koeffizienten $c_{n,n}$ und d_n im zweiten Schritt berechnet haben. Die Lösung dieser Gleichung ist dann offenbar

   $$x_n = \frac{d_n}{c_{n,n}}.$$

   Sollte nun $c_{n,n} = 0$ gelten, so ist das Gleichungs-System nicht eindeutig lösbar.

   (b) Im i-ten Teilschritt können wir voraussetzen, dass wir die Variablen

   $$x_n,\ x_{n-1},\ \cdots,\ x_{n-(i-2)}$$

   bereits berechnet haben. Ziel ist nun die Bestimmung der Variablen $x_{n-(i-1)}$ mit Hilfe der $\big(n-(i-1)\big)$-ten Gleichung. Definieren wir zur Vereinfachung der Notation $k = n-(i-1)$, so hat die k-te Gleichung die Form

   $$\sum_{j=k}^{n} c_{k,j} \cdot x_j = d_k.$$

   Da nun die Variablen $x_{k+1}, \cdots, x_n$ bereits bekannt sind, können wir diese Gleichung nach x_k auflösen und erhalten

   $$x_k = \frac{1}{c_{k,k}} \Big(d_k - \sum_{j=k+1}^{n} c_{k,j} \cdot x_j\Big).$$

   Sollte hier $c_{k,k} = 0$ gelten, so ist das Gleichungs-System nicht eindeutig lösbar.

Abbildung 9.1 zeigt eine einfache Implementierung des Gauß'schen Algorithmus, welche die oben ausgeführten Überlegungen umsetzt. Wir diskutieren das Programm nun im Detail.

1. Die Funktion *solve*(a, b) erhält als erstes Argument a die Matrix und als zweites Argument b die rechte Seite des linearen Gleichungs-Systems

   $$a \cdot \vec{x} = b$$

```
1  solve := procedure(a, b) {
2      [ a, b ] := eliminate(a, b);
3      x := solveTriangular(a, b);
4      return x;
5  };
6  eliminate := procedure(a, b) {
7      n := #a;    // number of equations
8      pivot := procedure(a, n, i) {
9          r := i;  // index of row containing maximal element
10         for (j in [i+1 .. n]) {
11             if (abs(a(j)(i)) > abs(a(r)(i))) {
12                 r := j;
13             }
14         }
15         return r;
16     };
17     for (i in [1 .. n]) {
18         r := pivot(a, n, i);
19         [ u, v ] := [ a(r), a(i) ];
20         a(r) := v;
21         a(i) := u;
22         [ u, v ] := [ b(i), b(r) ];
23         b(i) := v;
24         b(r) := u;
25         for (j in [i+1 .. n]) {
26             f := 1.0 * a(j)(i) / a(i)(i);
27             a(j)(i) := 0;
28             for (k in [i+1 .. n]) {
29                 a(j)(k) -= f * a(i)(k);
30             }
31             b(j) -= f * b(i);
32         }
33     }
34     return [ a, b ];
35 };
36 solveTriangular := procedure(a, b) {
37     x := [];
38     n := #a;    // number of equations
39     i := n;     // index to equation
40     for (i in [n, n-1 .. 1]) {
41         r := b(i);
42         r -= +/ { a(i)(k) * x(k) : k in [i+1 .. n] };
43         x(i) := 1.0 * r / a(i)(i);
44     }
45     return x;
46 };
```

Abbildung 9.1: Implementierung des Gauß'schen Eliminations-Verfahrens in *SetlX*.

Zunächst bringen wir dieses Gleichungs-System in Zeile 2 mit Hilfe der Funktion *eliminate* auf eine obere Dreiecks-Form. Die Funktion *solveTriangular* löst dieses System dann durch Rückwärts-Substitution.

2. Die Funktion *eliminate*(a, b) hat die Aufgabe, das Gleichungs-System $a \cdot \vec{x} = b$ in eine obere Dreiecks-Form zu überführen. Wir gehen davon aus, dass die Matrix a quadratisch ist. Dann ist das in Zeile 7 bestimmte n sowohl die Anzahl der Zeilen der Matrix als auch die Anzahl der Variablen.

3. In den Zeilen 8 bis 16 definieren wir die lokale Funktion *pivot*(a, n, i). Diese Funktion hat die Aufgabe, diejenige Zeile r in der Matrix a zu finden, für die der Wert

   $$|a_{j,i}| \quad \text{für } j \in \{i, \cdots, n\}$$

   maximal wird.

4. Die Schleife in Zeile 17 setzt voraus, dass die ersten i Gleichungen bereits in oberer Dreiecksform vorliegen und das darüber hinaus die Variablen $x_1, \cdots, x_{i-1}$ bereits aus den Gleichungen $i, i+1, \cdots, n$ entfernt worden sind. Ziel ist es, die Variable x_i aus der $(i+1)$-sten bis zur n-ten Gleichung zu entfernen.

   (a) Dazu wird mit Hilfe des Funktions-Aufrufs *pivot*(a, n, i) bestimmt, in welcher Zeile der Betrag $a_{j,i}$ maximal ist.

   (b) In den Zeilen 20 - 24 wird diese Zeile mit der i-ten Zeile vertauscht.

   (c) Die `for`-Schleife in Zeile 25 zieht von der j-ten Zeile das

   $$\frac{a_{j,i}}{a_{i,i}}\text{-fache}$$

   der i-ten Zeile ab.

   Insgesamt hängt nun für jedes $i = 1, \cdots, n$ die i-te Gleichung nur noch von den Variablen $x_i, \cdots, x_n$ ab.

5. In der Prozedur *solveTriangular* wird das Gleichungs-System, das jetzt in oberer Dreiecks-Form vorliegt, durch Rückwärts-Substitution gelöst.

Kapitel 10

Rekurrenz-Gleichungen

In diesem Kapitel stellen wir Rekurrenz-Gleichungen[1] vor und zeigen, wie diese in einfachen Fällen gelöst werden können. Rekurrenz-Gleichungen treten in der Informatik bei der Analyse der Komplexität von Algorithmen auf.

10.1 Die Fibonacci-Zahlen

Wir wollen *Rekurrenz-Gleichungen* an Hand eines eher spielerischen Beispiels einführen. Dazu betrachten wir eine Kaninchen-Farm, für die wir einen Geschäftsplan erstellen wollen. Wir beschäftigen uns hier nur mit der Frage, wie sich eine Kaninchen-Population entwickelt. Wir gehen dabei von folgenden vereinfachenden Annahmen aus:

1. Jedes Kaninchen-Paar bringt jeden Monat ein neues Kaninchen-Paar zur Welt.
2. Kaninchen haben nach zwei Monaten zum ersten Mal Junge.
3. Kaninchen leben ewig.

Wir nehmen nun an, wir hätten ein neugeborenes Kaninchen-Paar und stellen uns die Frage, wie viele Kaninchen-Paare wir nach n Monaten haben. Bezeichnen wir die Zahl der Kaninchen-Paare nach n Monaten mit $k(n)$, so gilt:

1. $k(0) = 1$

   Wir starten mit einem neugeborenem Kaninchen-Paar.

2. $k(1) = 1$

   Kaninchen bekommen das erste Mal nach zwei Monaten Junge, also hat sich die Zahl der Kaninchen-Paare nach einem Monat noch nicht verändert.

3. $k(2) = 1 + 1$

   Nach zwei Monaten bekommt unser Kaninchen-Paar zum ersten Mal Junge.

4. Allgemein gilt nach $n + 2$ Monaten:

   $$k(n + 2) = k(n + 1) + k(n)$$

   Alle Kaninchen-Paare, die zum Zeitpunkt n schon da sind, bekommen zum Zeitpunkt $n + 2$ Junge. Dies erklärt den Term $k(n)$. Da wir zur Vereinfachung unserer Rechnung von genetisch manipulierten unsterblichen Kaninchen ausgehen, sind alle Kaninchen, die zum Zeitpunkt $n + 1$ vorhanden sind, auch noch zum Zeitpunkt $n + 2$ vorhanden. Dies erklärt den Term $k(n + 1)$.

[1] Rekurrenz-Gleichungen werden in der Literatur auch als *Rekursions-Gleichungen* bezeichnet.

Die Folge der Zahlen $\big(k(n)\big)_{n\in\mathbb{N}}$ ist im wesentlichen[2] die Folge der *Fibonacci-Zahlen*.

Das Programm in Abbildung 10.1 auf Seite 121 berechnet diese Zahlen.

```
1  fibonacci := procedure(n) {
2      if (n in {0, 1}) {
3          return 1;
4      }
5      return fibonacci(n-1) + fibonacci(n-2);
6  };
7
8  for (n in [0 .. 100]) {
9      print("fibonacci($n$) = $fibonacci(n)$");
10 }
```

Abbildung 10.1: Ein naives Programm zur Berechnung der Fibonacci-Zahlen.

Wenn wir dieses Programm laufen lassen, stellen wir fest, dass die Laufzeiten mit wachsendem Parameter n sehr schnell anwachsen. Um dieses Phänomen zu analysieren, untersuchen wir exemplarisch, wie viele Additionen bei der Berechnung von `fibonacci`(n) für ein gegebenes $n \in \mathbb{N}$ benötigt werden. Bezeichnen wir diese Zahl mit a_n, so finden wir:

1. $a_0 = 0$.
2. $a_1 = 0$.
3. $n \geq 2 \rightarrow a_n = a_{n-1} + a_{n-2} + 1$,

   denn in den rekursiven Aufrufen `fibonacci`$(n-1)$ und `fibonacci`$(n-2)$ haben wir a_{n-1} bzw. a_{n-2} Additionen und dazu kommt noch die Addition der Werte `fibonacci`$(n-1)$ und `fibonacci`$(n-2)$.

Wir setzen in der Gleichung $a_n = 1 + a_{n-1} + a_{n-2}$ für n den Wert $i+2$ ein und haben dann

$$a_{i+2} = a_{i+1} + a_i + 1 \tag{10.1}$$

Eine solche Gleichung nennen wir eine *lineare inhomogene Rekurrenz-Gleichung*. Die dieser Gleichung zugeordnete *homogene Rekurrenz-Gleichung* lautet

$$a_{i+2} = a_{i+1} + a_i \tag{10.2}$$

Wir lösen diese Gleichung mit folgendem Ansatz:

$$a_i = \lambda^i.$$

Einsetzen dieses Ansatzes in (10.2) führt auf die Gleichung

$$\lambda^{i+2} = \lambda^{i+1} + \lambda^i.$$

Wenn wir beide Seiten dieser Gleichung durch λ^i dividieren, erhalten wir die quadratische Gleichung

$$\lambda^2 = \lambda + 1,$$

die wir mit Hilfe einer quadratischen Ergänzung lösen:

[2] In der Literatur wird die Folge $(f_n)_{n\in\mathbb{N}}$ der Fibonacci-Zahlen meist durch die Gleichungen

$$f_0 = 0, \quad f_1 = 1 \quad \text{und} \quad f_{n+2} = f_{n+1} + f_n$$

definiert. Dann gilt $k(n) = f_{n+1}$, die Folge $\big(k(n)\big)_{n\in\mathbb{N}}$ geht also aus der Folge der Fibonacci-Zahlen $(f_n)_{n\in\mathbb{N}}$ dadurch hervor, dass der erste Wert der Folge abgeschnitten wird.

$$
\begin{array}{lcll}
\lambda^2 & = & \lambda + 1 & \mid -\lambda \\
\lambda^2 - 2 \cdot \frac{1}{2}\lambda & = & 1 & \mid + \frac{1}{4} \\
\lambda^2 - 2 \cdot \frac{1}{2}\lambda + \left(\frac{1}{2}\right)^2 & = & \frac{5}{4} & \\
\left(\lambda - \frac{1}{2}\right)^2 & = & \frac{5}{4} & \mid \sqrt{\ } \\
\lambda - \frac{1}{2} & = & \pm\frac{\sqrt{5}}{2} & \mid + \frac{1}{2} \\
\lambda_{1/2} & = & \frac{1}{2}(1 \pm \sqrt{5}) &
\end{array}
$$

Wir bemerken, dass jede Linear-Kombination der Form

$$a_n = \alpha \cdot \lambda_1^n + \beta \cdot \lambda_2^n$$

eine Lösung der homogenen Rekurrenz-Gleichung (10.2) ist. Wir bemerken weiter, dass für die Lösungen λ_1 und λ_2 folgende Identitäten gelten:

$$\lambda_1 - \lambda_2 = \sqrt{5} \quad \text{und} \quad \lambda_1 + \lambda_2 = 1 \tag{10.3}$$

Aus der letzen Gleichung folgt dann sofort

$$1 - \lambda_1 = \lambda_2 \quad \text{und} \quad 1 - \lambda_2 = \lambda_1 \tag{10.4}$$

Zur Lösung der ursprünglichen Rekurrenz-Gleichung (10.1) machen wir den Ansatz $a_i = c$, wobei c eine noch zu bestimmende Konstante ist. Setzen wir diesen Ansatz in der Gleichung (10.1) ein, so erhalten wir die Gleichung

$$c = c + c + 1,$$

welche die Lösung $c = -1$ hat. Diese Lösung bezeichnen wir als eine *spezielle Lösumg*. Die *allgemeine Lösung* der Rekurrenz-Gleichung (10.1) ergibt sich als Summe aus der Lösung der homogenen Rekurrenz-Gleichung und der speziellen Lösung und lautet daher

$$a_i = \alpha \cdot \lambda_1^i + \beta \cdot \lambda_2^i - 1$$

mit $\lambda_1 = \frac{1}{2}(1 + \sqrt{5})$ und $\lambda_2 = \frac{1}{2}(1 - \sqrt{5})$. Die Koeffizienten α und β sind jetzt so zu bestimmen, dass die Anfangs-Bedingungen $a_0 = 0$ und $a_1 = 0$ erfüllt sind. Das führt auf folgendes lineares Gleichungs-System:

$$
\begin{array}{lcl}
0 & = & \alpha \cdot \lambda_1^0 + \beta \cdot \lambda_2^0 - 1 \\
0 & = & \alpha \cdot \lambda_1^1 + \beta \cdot \lambda_2^1 - 1
\end{array}
$$

Addieren wir bei beiden Gleichungen 1 und vereinfachen für $i = 1, 2$ die Potenzen λ_i^0 zu 1 und λ_i^1 zu λ_i, so erhalten wir:

$$
\begin{array}{lcl}
1 & = & \alpha + \beta \\
1 & = & \alpha \cdot \lambda_1 + \beta \cdot \lambda_2
\end{array}
$$

Die erste dieser beiden Gleichungen liefert die Beziehung $\alpha = 1 - \beta$. Setzen wir dies für α in der zweiten Gleichung ein, so erhalten wir

$$
\begin{array}{lcll}
 & 1 & = & (1 - \beta) \cdot \lambda_1 + \beta \cdot \lambda_2 \\
\Leftrightarrow & 1 & = & \lambda_1 + \beta \cdot \big(\lambda_2 - \lambda_1\big) \\
\Leftrightarrow & 1 - \lambda_1 & = & \beta \cdot \big(\lambda_2 - \lambda_1\big) \\
\Leftrightarrow & \dfrac{1 - \lambda_1}{\lambda_2 - \lambda_1} & = & \beta
\end{array}
$$

Wegen $\alpha = 1 - \beta$ finden wir dann

$$\begin{aligned} \alpha &= 1 - \frac{1 - \lambda_1}{\lambda_2 - \lambda_1} \\ &= \frac{(\lambda_2 - \lambda_1) - (1 - \lambda_1)}{\lambda_2 - \lambda_1} \\ &= \frac{\lambda_2 - 1}{\lambda_2 - \lambda_1}. \end{aligned}$$

Verwenden wir hier die Gleichungen (10.3) und (10.4), so finden wir

$$\alpha = \frac{\lambda_1}{\sqrt{5}} \quad \text{und} \quad \beta = -\frac{\lambda_2}{\sqrt{5}}.$$

Damit können wir die Folge $(a_i)_i$ explizit angeben:

$$a_i = \frac{1}{\sqrt{5}} \cdot \left(\lambda_1^{i+1} - \lambda_2^{i+1}\right) - 1$$

Wegen $\lambda_1 \approx 1.61803$ und $\lambda_2 \approx -0.61803$ dominiert der erste Term der Summe und die Zahl der Additionen wächst exponentiell mit dem Faktor λ_1 an. Dies erklärt das starke Anwachsen der Rechenzeit.

Bemerkung: Die Zahl λ_1 wird auch als *goldener Schnitt* bezeichnet und spielt sowohl in der Geometrie als auch in der Kunst eine Rolle.

Die Ursache der Ineffezienz der Berechnung der Fibonacci-Zahlen ist leicht zu sehen: Berechnen wir den Wert `fibonacci(5)` mit dem Programm aus Abbildung 10.1, so müssen wir `fibonacci(4)` und `fibonacci(3)` berechnen. Die Berechnung von `fibonacci(4)` erfordert ihrerseits die Berechnung von `fibonacci(3)` und `fibonacci(2)`. Dann berechnen wir `fibonacci(3)` aber zweimal! Abbildung 10.2 zeigt den sogenannten *Rekursions-Baum* für den Aufruf von *fibonacci*(5), der den oben dargestellten Zusammenhang graphisch verdeutlicht.

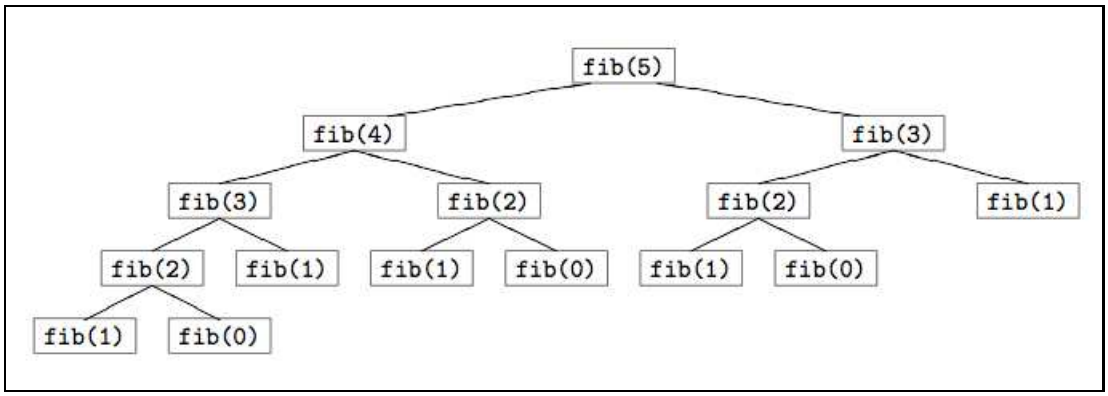

Abbildung 10.2: Rekursions-Baum für die Berechnung von *fibonacci*(5).

Wir können eine effizientere Berechnung der Fibonacci-Zahlen implementieren, indem wir uns die berechneten Werte merken. Dazu können wir eine Liste benutzen. Dies führt zu dem in Abbildung 10.3 auf Seite 124 angegebenen Programm. Da die Fibonacci-Zahlen f_n mit $n = 0$ beginnen, die Elemente einer Liste aber mit 1 beginnend indiziert werden, wird der Wert

fibonacci(i) in der Liste l an der Stelle $l(i + 1)$

gespeichert.

```
1  fibonacci := procedure(n) {
2      l := [1, 1] + [2 .. n];
3      for (k in [ 2 .. n ]) {
4          l(k+1) := l(k) + l(k-1);
5      }
6      return l(n+1);
7  };
8
9  for (n in [0 .. 10000]) {
10     print("fibonacci($n$) = $fibonacci(n)$");
11 }
```

Abbildung 10.3: Berechnung der Fibonacci-Zahlen mit Speicherung der Zwischenwerte.

10.2 Lineare Rekurrenz-Gleichung

Wir waren bei der Analyse der Komplexität des ersten Programms zur Berechnung der Fibonacci-Zahlen auf die Gleichung

$$a_{i+2} = a_{i+1} + a_i + 1 \quad \text{für alle } i \in \mathbb{N}$$

gestoßen. Gleichungen dieser Form treten bei der Analyse der Komplexität rekursiver Programme häufig auf. Wir wollen uns daher in diesem Abschnitt näher mit solchen Gleichungen beschäftigen.

Definition 85 (Lineare homogene Rekurrenz-Gleichung)
Die lineare homogene Rekurrenz-Gleichung der Ordnung k mit konstanten Koeffizienten *hat die Form*

$$a_{n+k} = c_{k-1} \cdot a_{n+k-1} + c_{k-2} \cdot a_{n+k-2} + \cdots + c_1 \cdot a_{n+1} + c_0 \cdot a_n \quad \textit{für alle } n \in \mathbb{N}. \tag{10.5}$$

In Summen-Schreibweise kann diese Gleichung kompakter als

$$a_{n+k} = \sum_{i=0}^{k-1} c_i \cdot a_{n+i} \quad \textit{für alle } n \in \mathbb{N}$$

geschreiben werden. Zusätzlich werden Anfangs-Bedingungen

$$a_0 = d_0, \cdots, a_{k-1} = d_{k-1}$$

für die Folge $(a_n)_{n\in\mathbb{N}}$ *vorgegeben.* □

Durch eine lineare homogene Rekurrenz-Gleichung wird die Folge $(a_n)_{n\in\mathbb{N}}$ eindeutig bestimmt: Die Werte a_n für $n < k$ sind durch die Anfangs-Bedingungen gegeben und alle weiteren Werte können dann durch die Rekurrenz-Gleichung (10.5) bestimmt werden. Noch etwas zur Nomenklatur:

1. Die Rekurrenz-Gleichung (10.5) heißt *linear*, weil die Glieder der Folge $(a_n)_n$ nur linear in der Gleichung (10.5) auftreten. Ein Beispiel für eine Rekurrenz-Gleichung, die nicht linear ist, wäre

   $$a_{n+1} = a_n^2 \quad \text{für alle } n \in \mathbb{N}.$$

   Nicht-lineare Rekurrenz-Gleichungen sind nur in Spezialfällen geschlossen lösbar.

2. Die Rekurrenz-Gleichung (10.5) heißt *homogen*, weil auf der rechten Seite dieser Gleichung kein konstantes Glied mehr auftritt. Ein Beispiel für eine Gleichung, die nicht homogen ist (wir sprechen auch von *inhomogenen* Rekurrenz-Gleichungen), wäre

   $$a_{n+2} = a_{n+1} + a_n + 1 \quad \text{für alle } n \in \mathbb{N}.$$

   Mit inhomogenen Rekurrenz-Gleichungen werden wir uns später noch beschäftigen.

3. Die Rekurrenz-Gleichung (10.5) hat *konstante Koeffizienten*, weil die Werte c_i Konstanten sind, die nicht von dem Index n abhängen. Ein Beispiel für eine Rekurrenz-Gleichung, die keine konstanten Koeffizienten hat, ist

   $$a_{n+1} = n \cdot a_n \quad \text{für alle } n \in \mathbb{N}.$$

   Solche Rekurrenz-Gleichungen können in vielen Fällen auf Rekurrenz-Gleichungen mit konstanten Koeffizienten zurück geführt werden. Wir werden das später noch im Detail besprechen.

Wie lösen wir eine lineare homogene Rekurrenz-Gleichung? Wir versuchen zunächst den Ansatz

$$a_n = \lambda^n \quad \text{für alle } n \in \mathbb{N}.$$

Einsetzen dieses Ansatzes in (10.5) führt auf die Gleichung

$$\lambda^{n+k} = \sum_{i=0}^{k-1} c_i \cdot \lambda^{n+i}$$

Dividieren wir diese Gleichung durch λ^n, so haben wir:

$$\lambda^k = \sum_{i=0}^{k-1} c_i \cdot \lambda^i$$

Das Polynom

$$\chi(x) = x^k - \sum_{i=0}^{k-1} c_i \cdot x^i$$

heißt *charakteristisches Polynom* der Rekurrenz-Gleichung (10.5). Wir betrachten zunächst den Fall, dass das charakteristische Polynom k verschiedene Nullstellen hat. In diesem Fall sagen, dass die Rekurrenz-Gleichung (10.5) *nicht entartet* ist. Bezeichnen wir diese Nullstellen mit

$$\lambda_1, \lambda_2, \cdots, \lambda_k,$$

so gilt für alle $j = 1, \cdots, k$

$$\lambda_j^{n+k} = \sum_{i=0}^{k-1} c_i \cdot \lambda_j^{n+i}.$$

Damit ist die Folge

$$\left(\lambda_j^n\right)_{n \in \mathbb{N}}$$

für alle $j = 1, \cdots, k$ eine Lösung der Rekurrenz-Gleichung (10.5). Außerdem ist auch jede Linear-Kombination dieser Lösungen eine Lösung von (10.5): Definieren wir die Folge a_n durch

$$a_n = \alpha_1 \cdot \lambda_1^n + \cdots + \alpha_k \cdot \lambda_k^n \quad \text{für alle } n \in \mathbb{N}$$

mit beliebigen Koeffizienten $\alpha_i \in \mathbb{R}$, so erfüllt auch die Folge $(a_n)_n$ die Gleichung (10.5). Die oben definierte Folge $(a_n)_n$ bezeichnen wir als die *allgemeine Lösung* der Rekurrenz-Gleichung (10.5). Die Koeffizienten α_i müssen wir für $i = 1, \cdots, k$ so wählen, dass die Anfangs-Bedingungen

$$a_0 = d_0, \cdots, a_{k-1} = d_{k-1}$$

erfüllt sind. Das liefert ein lineares Gleichungs-System für die Koeffizienten $\alpha_1, \cdots, \alpha_k$:

$$\begin{array}{lcl}
d_0 & = & \lambda_1^0 \cdot \alpha_1 + \cdots + \lambda_k^0 \cdot \alpha_k \\
d_1 & = & \lambda_1^1 \cdot \alpha_1 + \cdots + \lambda_k^1 \cdot \alpha_k \\
\vdots & & \vdots \\
d_{k-1} & = & \lambda_1^{k-1} \cdot \alpha_1 + \cdots + \lambda_k^{k-1} \cdot \alpha_k
\end{array}$$

Hier sind die Werte λ_i die Nullstellen des charakteristischen Polynoms. Die Matrix V, die diesem Gleichungs-System zugeordnet ist, lautet:

$$V = \begin{pmatrix} \lambda_1^0 & \cdots & \lambda_k^0 \\ \lambda_1^1 & \cdots & \lambda_k^1 \\ \vdots & & \vdots \\ \lambda_1^{k-1} & \cdots & \lambda_k^{k-1} \end{pmatrix}$$

Diese Matrix ist in der Mathematik als *Vandermonde*'sche Matrix bekannt. Es läßt sich zeigen, dass ein Gleichungs-System, das mit dieser Matrix gebildet wird, genau dann eindeutig lösbar ist, wenn die Nullstellen λ_i für $i = 1, \cdots, k$ paarweise verschieden sind.

Beispiel: Wie demonstrieren das Verfahren an einem Beispiel: Wie betrachten die Rekurrenz-Gleichung

$$F_{n+2} = F_{n+1} + F_n \quad \text{für alle } n \in \mathbb{N}$$

mit den Anfangs-Bedingungen $F_0 = 0$ und $F_1 = 1$. Die Lösung dieser Rekurrenz-Gleichung sind übrigens gerade die Fibonacci-Zahlen. Das *charakteristische Polynom* dieser Rekurrenz-Gleichung lautet:

$$\chi(x) = x^2 - x - 1.$$

Das führt auf die quadratische Gleichung

$$x^2 - x - 1 = 0$$

Wir haben eben schon gesehen, dass diese quadratische Gleichung die Lösung

$$x_{1/2} = \tfrac{1}{2} \cdot (1 \pm \sqrt{5})$$

hat. Wir definieren

$$\lambda_1 = \tfrac{1}{2} \cdot (1 + \sqrt{5}) \quad \text{und} \quad \lambda_2 = \tfrac{1}{2} \cdot (1 - \sqrt{5}).$$

Damit lautet die *allgemeine Lösung* der betrachteten Rekurrenz-Gleichung

$$F_n = \alpha_1 \cdot \lambda_1^n + \alpha_2 \cdot \lambda_2^n \quad \text{für alle } n \in \mathbb{N}.$$

Setzen wir hier die Anfangs-Bedingungen ein, so erhalten wir

$$\begin{array}{lcl} 0 & = & \lambda_1^0 \cdot \alpha_1 + \lambda_2^0 \cdot \alpha_2 \\ 1 & = & \lambda_1^1 \cdot \alpha_1 + \lambda_2^1 \cdot \alpha_2 \end{array}$$

Dies ist ein lineares Gleichungs-System in den Unbekannten α_1 und α_2. Vereinfachung führt auf

$$\begin{array}{lcl} 0 & = & \alpha_1 + \alpha_2 \\ 1 & = & \lambda_1 \cdot \alpha_1 + \lambda_2 \cdot \alpha_2 \end{array}$$

Die erste dieser beiden Gleichungen lösen wir nach α_2 auf und finden $\alpha_2 = -\alpha_1$. Diesen Wert setzen wir in der zweiten Gleichung ein. Das führt auf

$$\begin{array}{lcl} & 1 & = & \lambda_1 \cdot \alpha_1 - \lambda_2 \cdot \alpha_1 \\ \Leftrightarrow & 1 & = & (\lambda_1 - \lambda_2) \cdot \alpha_1 \\ \Leftrightarrow & \dfrac{1}{\lambda_1 - \lambda_2} & = & \alpha_1 \end{array}$$

Setzen wir diesen Wert in die Gleichung $\alpha_2 = -\alpha_1$ ein, so erhalten wir

$$\alpha_2 = \frac{-1}{\lambda_1 - \lambda_2}.$$

Setzen wir die Werte für λ_1 und λ_2 ein, so finden wir:

$$\alpha_1 = \frac{1}{\sqrt{5}} \quad \text{und} \quad \alpha_2 = -\frac{1}{\sqrt{5}}.$$

Die Lösung der Rekurrenz-Gleichung

$$F_{n+2} = F_{n+1} + F_n \quad \text{für alle } n \in \mathbb{N}$$

mit den Anfangs-Bedingungen $F_0 = 1$ und $F_1 = 1$ lautet also

$$F_n = \frac{1}{\sqrt{5}} \cdot (\lambda_1^n - \lambda_2^n) \quad \text{für alle } n \in \mathbb{N}.$$

Damit haben wir eine geschlossene Formel zur Berechnung der Fibonacci-Zahlen gefunden. Diese Formel zeigt uns, dass die Fibonacci-Zahlen selbst exponentiell anwachsen. Wir werden diese Formel später bei der Analyse des Laufzeitverhaltens des Euklidischen-Algorithmus benötigen.

Aufgabe: Lösen Sie die Rekurrenz-Gleichung $a_{n+2} = \frac{3}{2} \cdot a_{n+1} - \frac{1}{2} \cdot a_n$ mit den Anfangs-Bedingungen $a_0 = 3$ und $a_1 = \frac{5}{2}$.

10.2.1 Entartete Rekurrenz-Gleichungen

Wir hatten oben zunächst den Fall betrachtet, dass das charakteristische Polynom der Rekurrenz-Gleichung (10.5) insgesamt k verschiedene Nullstellen hat. Dies muss keineswegs immer der Fall sein. Wir betrachten die Rekurrenz-Gleichung

$$a_{n+2} = 4 \cdot a_{n+1} - 4 \cdot a_n \quad \text{für alle } n \in \mathbb{N} \tag{10.6}$$

mit den Anfangs-Bedingungen $a_0 = 1$, $a_1 = 4$. Das charakteristische Polynom lautet

$$\chi(x) = x^2 - 4 \cdot x + 4 = (x-2)^2$$

und hat offensichtlich nur eine Nullstelle bei $x = 2$. Eine Lösung der Rekurrenz-Gleichung (10.6) lautet daher

$$a_n = 2^n \quad \text{für alle } n \in \mathbb{N}.$$

Eine weitere Lösung ist

$$a_n = n \cdot 2^n \quad \text{für alle } n \in \mathbb{N}.$$

Wir verifizieren dies durch Einsetzen:

$$\begin{array}{lrcll}
 & (n+2) \cdot 2^{n+2} & = & 4 \cdot (n+1) \cdot 2^{n+1} - 4 \cdot n \cdot 2^n & \mid \div 2^n \\
\Leftrightarrow & (n+2) \cdot 2^2 & = & 4 \cdot (n+1) \cdot 2^1 - 4 \cdot n & \mid \div 4 \\
\Leftrightarrow & n+2 & = & (n+1) \cdot 2 - n & \\
\Leftrightarrow & n+2 & = & 2 \cdot n + 2 - n & \\
\Leftrightarrow & n+2 & = & n+2 &
\end{array}$$

Die allgemeine Lösung der Rekurrenz-Gleichung finden wir durch Linear-Kombination der beiden Lösungen:

$$a_n = \alpha \cdot 2^n + \beta \cdot n \cdot 2^n \quad \text{für alle } n \in \mathbb{N}.$$

Setzen wir hier die Anfangs-Bedingungen $a_0 = 1$ und $a_2 = 4$ ein, so erhalten wir:

$$\left\{ \begin{array}{rcl} 1 & = & \alpha \cdot 2^0 + \beta \cdot 0 \cdot 2^0 \\ 4 & = & \alpha \cdot 2^1 + \beta \cdot 1 \cdot 2^1 \end{array} \right\} \quad \Leftrightarrow \quad \left\{ \begin{array}{rcl} 1 & = & \alpha \\ 4 & = & \alpha \cdot 2 + \beta \cdot 2 \end{array} \right\}$$

Die Lösung lautet offenbar $\alpha = 1$ und $\beta = 1$. Damit lautet die Lösung der Rekurrenz-Gleichung (10.6) mit den Anfangs-Bedingungen $a_0 = 1$ und $a_2 = 4$

$$a_n = 2^n + n \cdot 2^n = (n+1) \cdot 2^n \quad \text{für alle } n \in \mathbb{N}.$$

Im allgemeinen nennen wir die Rekurrenz-Gleichung

$$a_{n+k} = \sum_{i=0}^{k-1} c_i \cdot a_{n+i}$$

entartet, wenn das charakteristische Polynom

$$\chi(x) = x^k - \sum_{i=0}^{k-1} c_i \cdot x^i$$

weniger als k verschiedene Nullstellen hat. Dann läßt sich folgendes zeigen: Hat das charakteristische Polynom $\chi(x)$ eine r-fache Nullstelle λ, gilt also

$$\chi(x) = (x - \lambda)^r \cdot \phi(x)$$

mit einem geeigneten Polynom $\phi(x)$, so sind die Folgen

1. $(\lambda^n)_{n\in\mathbb{N}}$
2. $(n \cdot \lambda^n)_{n\in\mathbb{N}}$
3. $(n^2 \cdot \lambda^n)_{n\in\mathbb{N}}$
4. $\vdots$
5. $(n^{r-1} \cdot \lambda^n)_{n\in\mathbb{N}}$

Lösungen der Rekurrenz-Gleichung (10.6). Durch eine geeignete Linear-Kombination dieser Lösungen zusammen mit den Lösungen, die sich aus den anderen Nullstellen des Polynoms ϕ ergeben, läßt sich dann immer eine Lösung finden, die auch den Anfangs-Bedingungen genügt.

Aufgabe: Lösen Sie die Rekurrenz-Gleichung

$$a_{n+3} = a_{n+2} + a_{n+1} - a_n$$

für die Anfangs-Bedingungen $a_0 = 0$, $a_1 = 3$, $a_2 = 2$.

10.2.2 Inhomogene Rekurrenz-Gleichungen

Definition 86 (Lineare inhomogene Rekurrenz-Gleichung)
Die lineare inhomogene Rekurrenz-Gleichung der Ordnung k mit konstanten Koeffizienten und konstanter Inhomogenität *hat die Form*

$$a_{n+k} = \sum_{i=0}^{k-1} c_i \cdot a_{n+i} + c_{-1} \tag{10.7}$$

mit den Anfangs-Bedingungen $a_0 = d_0, \cdots, a_{k-1} = d_{k-1}$. *Dabei gilt für die Koeffizienten*

$$c_i \in \mathbb{R} \quad \textit{für alle } i = -1, 0, \cdots, k-1.$$

Für die Anfangs-Bedingungen $d_0, \cdots, d_{k-1}$ *gilt ebenfalls*

$$d_i \in \mathbb{R} \quad \textit{für alle } i = 0, \cdots, k-1.$$

Die Konstante c_{-1} *bezeichnen wir als die* Inhomogenität. □

Wie läßt sich die inhomogene Rekurrenz-Gleichung (10.7) lösen? Wir zeigen zunächst, wie sich eine *spezielle Lösung* der Rekurrenz-Gleichung (10.7) finden läßt. Dazu betrachten wir das charakteristische Polynom

$$\chi(x) = x^k - \sum_{i=0}^{k-1} c_i \cdot x^i$$

und definieren die *Spur* $\mathtt{sp}(\chi)$ wie folgt:

$$\mathtt{sp}(\chi) := \chi(1) = 1 - \sum_{i=0}^{k-1} c_i.$$

Es können zwei Fälle auftreten, $\mathtt{sp}(\chi) \neq 0$ und $\mathtt{sp}(\chi) = 0$. Wir betrachten die beiden Fälle getrennt.

1. $\mathtt{sp}(\chi) \neq 0$.

   Dann erhalten wir eine spezielle Lösung von (10.7) durch den Ansatz

   $$a_n = \delta \quad \text{für alle } n \in \mathbb{N}.$$

   Den Wert von δ bestimmen wir durch Einsetzen, es muß für alle $n \in \mathbb{N}$ gelten:

   $$\delta = \sum_{i=0}^{k-1} c_i \cdot \delta + c_{-1}.$$

   Daraus ergibt sich

   $$\delta \cdot \left(1 - \sum_{i=0}^{k-1} c_i\right) = c_{-1}.$$

   Das ist aber nichts anderes als

   $$\delta \cdot \mathtt{sp}(\chi) = c_{-1}$$

   und damit lautet eine spezielle Lösung von (10.7)

   $$a_n = \delta = \frac{c_{-1}}{\mathtt{sp}(\chi)}.$$

   Jetzt sehen wir auch, warum die Voraussetzung $\mathtt{sp}(\chi) \neq 0$ wichtig ist, denn anderfalls wäre der Quotient $\frac{c_{-1}}{\mathtt{sp}(\chi)}$ undefiniert.

2. $\mathtt{sp}(\chi) = 0$.

   In diesem Fall versuchen wir, eine spezielle Lösung von (10.7) durch den Ansatz

   $$a_n = \varepsilon \cdot n$$

zu finden. Den Wert ε erhalten wir durch Einsetzen, es muß für alle $n \in \mathbb{N}$ gelten:

$$\varepsilon \cdot (n+k) = \sum_{i=0}^{k-1} c_i \cdot \varepsilon \cdot (n+i) + c_{-1}$$

Dies formen wir wie folgt um:

$$\varepsilon \cdot n + \varepsilon \cdot k = \varepsilon \cdot n \cdot \sum_{i=0}^{k-1} c_i + \varepsilon \cdot \sum_{i=0}^{k-1} i \cdot c_i + c_{-1}$$

Aus $\mathtt{sp}(\chi) = 0$ folgt $1 = \sum_{i=0}^{k-1} c_i$ und damit gilt

$$\varepsilon \cdot n = \varepsilon \cdot n \cdot \sum_{i=0}^{k-1} c_i.$$

Daher vereinfacht sich die obige Gleichung zu

$$\begin{aligned} & \varepsilon \cdot k = \varepsilon \cdot \sum_{i=0}^{k-1} i \cdot c_i + c_{-1} \\ \Leftrightarrow \quad & \varepsilon \cdot \left(k - \sum_{i=0}^{k-1} i \cdot c_i \right) = c_{-1} \\ \Leftrightarrow \quad & \varepsilon = \frac{c_{-1}}{k - \sum_{i=0}^{k-1} i \cdot c_i} \end{aligned}$$

Wenn wir genau hin schauen, dann sehen wir, dass der Wert im Nenner nicht anderes ist als der Wert der Ableitung des charakteristischen Polynoms an der Stelle 1, denn es gilt:

$$\chi'(x) = \tfrac{d}{dx}\chi(x) = k \cdot x^{k-1} - \sum_{i=1}^{k-1} c_i \cdot i \cdot x^{i-1}$$

Setzen wir hier für x den Wert 1 ein, so finden wir

$$\chi'(1) = k - \sum_{i=1}^{k-1} c_i \cdot i = k - \sum_{i=0}^{k-1} c_i \cdot i.$$

Insgesamt haben wir damit also die folgende spezielle Lösung $(a_n)_{n\in\mathbb{N}}$ der Gleichung (10.7) gefunden:

$$a_n = \frac{c_{-1}}{\chi'(1)} \cdot n.$$

Wir haben oben zur Vereinfachung angenommen, dass dieser Wert von 0 verschieden ist, dass also das charakteristische Polynom $\chi(x)$ an der Stelle $x = 1$ keine mehrfache Nullstelle hat, denn nur dann ist ε durch die obige Gleichung wohldefiniert und wir haben eine spezielle Lösung der Rekurrenz-Gleichung (10.7) gefunden. Andernfalls können wir die Reihe nach die Ansätze $a_n = \varepsilon \cdot n^2$, $a_n = \varepsilon \cdot n^3$, $\cdots$ versuchen, denn es kann folgendes gezeigt werden: Hat das charakteristische Polynom $\chi(x)$ am Punkt $x = 1$ eine Nullstelle vom Rang r, so führt der Ansatz $a_n = \varepsilon \cdot n^r$ zu einer speziellen Lösung von (10.7).

Diese spezielle Lösung genügt i. a. noch nicht den Anfangs-Bedingungen. Eine Lösung, die auch den Anfangs-Bedingungen genügt, erhalten wir, wenn wir zu der speziellen Lösung die allgemeine Lösung der zugehörigen homogenen linearen Rekurrenz-Gleichung

$$a_{n+k} = c_{k-1} \cdot a_{n+k-1} + c_{k-2} \cdot a_{n+k-2} + \cdots + c_1 \cdot a_{n+1} + c_0 \cdot a_n$$

addieren und die Koeffizienten der allgemeinen Lösung so wählen, dass die Anfangs-Bedingungen erfüllt sind. Wir betrachten ein Beispiel: Die zu lösende Rekurrenz-Gleichung lautet

$$a_{n+2} = 3 \cdot a_{n+1} - 2 \cdot a_n - 1 \quad \text{für alle } n \in \mathbb{N}.$$

Die Anfangs-Bedingungen sind $a_0 = 1$ und $a_1 = 3$. Wir berechnen zunächst eine spezielle Lösung. Das charakteristische Polynom ist

$$\chi(x) = x^2 - 3 \cdot x + 2 = (x-1) \cdot (x-2).$$

Es gilt $\mathtt{sp}(\chi) = \chi(1) = 0$. Wir versuchen für die spezielle Lösung den Ansatz

$$a_n = \varepsilon \cdot n.$$

Einsetzen in die Rekurrenz-Gleichung liefert

$$\varepsilon \cdot (n+2) = 3 \cdot \varepsilon \cdot (n+1) - 2 \cdot \varepsilon \cdot n - 1 \quad \text{für alle } n \in \mathbb{N}.$$

Das ist äquivalent zu

$$\varepsilon \cdot (2-3) = -1$$

und daraus folgt sofort $\varepsilon = 1$. Damit lautet eine spezielle Lösung

$$a_n = n \quad \text{für alle } n \in \mathbb{N}.$$

Da die Nullstellen des charakteristischen Polynoms $\chi(x)$ bei 1 und 2 liegen, finden wir für die allgemeine Lösung

$$a_n = \alpha \cdot 1^n + \beta \cdot 2^n + n \quad \text{für alle } n \in \mathbb{N}.$$

Setzen wir hier für n die Werte 0 und 1 und für a_n die beiden Anfangs-Bedingungen ein, so erhalten wir das Gleichungs-System

$$\left\{ \begin{array}{rcl} 1 & = & \alpha \cdot 1^0 + \beta \cdot 2^0 + 0 \\ 3 & = & \alpha \cdot 1^1 + \beta \cdot 2^1 + 1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{rcl} 1 & = & \alpha + \beta \\ 3 & = & \alpha + 2 \cdot \beta + 1 \end{array} \right\}$$

Sie können leicht nachrechnen, dass dieses Gleichungs-System die Lösung $\alpha = 0$ und $\beta = 1$ hat. Damit lautet die Lösung der Rekurrenz-Gleichung

$$a_n = 2^n + n \quad \text{für alle } n \in \mathbb{N}.$$

Aufgabe: Lösen Sie die inhomogene Rekurrenz-Gleichung

$$a_{n+2} = 2 \cdot a_n - a_{n+1} + 3$$

für die Anfangs-Bedingungen $a_0 = 2$ und $a_1 = 1$.

10.2.3 Lineare inhomogene Rekurrenz-Gleichungen mit veränderlichen Inhomogenitäten

Gelegentlich tauchen in der Praxis Rekurrenz-Gleichungen auf, in denen die Inhomogenität keine Konstante ist, sondern von n abhängt. In solchen Fällen führt die Technik des *diskreten Differenzieren* oft zum Erfolg. Wir stellen die Technik an einem Beispiel vor und betrachten die Rekurrenz-Gleichung

$$a_{n+1} = 2 \cdot a_n + n \quad \text{für alle } n \in \mathbb{N} \tag{10.8}$$

und der Anfangs-Bedingungen $a_0 = 0$. Das Verfahren zur Lösung solcher Rekurrenz-Gleichung besteht aus vier Schritten:

1. Substitutions-Schritt: Im *Substitutions-Schritt* setzen wir in der ursprünglichen Rekurrenz-Gleichung (10.8) für n den Wert $n+1$ ein und erhalten

   $$a_{n+2} = 2 \cdot a_{n+1} + n + 1 \quad \text{für alle } n \in \mathbb{N} \tag{10.9}$$

2. Subtraktions-Schritt: Im *Subtraktions-Schritt* ziehen wir von der im Substitutions-Schritt erhaltenen Rekurrenz-Gleichung (10.9) die ursprüngliche gegebene Rekurrenz-Gleichung (10.8)

ab. In unserem Fall erhalten wir

$$a_{n+2} - a_{n+1} = 2 \cdot a_{n+1} + n + 1 - (2 \cdot a_n + n) \quad \text{für alle } n \in \mathbb{N}.$$

Vereinfachung dieser Gleichung liefert

$$a_{n+2} = 3 \cdot a_{n+1} - 2 \cdot a_n + 1 \quad \text{für alle } n \in \mathbb{N}. \tag{10.10}$$

Die beiden Schritte 1. und 2. bezeichnen wir zusammen als *diskretes Differenzieren* der Rekurrenz-Gleichung.

3. Berechnung zusätzlicher Anfangs-Bedingungen: Die Rekurrenz-Gleichung (10.10) ist eine inhomogene Rekurrenz-Gleichung der Ordnung 2 mit nun aber konstanter Inhomogenität. Wir haben bereits gesehen, wie eine solche Rekurrenz-Gleichung zu lösen ist, wir benötigen aber eine zusätzliche Anfangs-Bedingung für $n = 1$. Diese erhalten wir, indem wir in der ursprünglichen Rekurrenz-Gleichung (10.8) für n den Wert 0 einsetzen:

   $$a_1 = 2 \cdot a_0 + 0 = 0.$$

4. Lösen der inhomogenen Rekurrenz-Gleichung mit konstanter Inhomogenität: Das charakteristische Polynom der Rekurrenz-Gleichung (10.10) lautet:

   $$\chi(x) = x^2 - 3 \cdot x + 2 = (x - 2) \cdot (x - 1).$$

   Offenbar gilt $\mathtt{sp}(\chi) = 0$. Um eine spezielle Lösung der Rekurrenz-Gleichung (10.10) zu erhalten, machen wir daher den Ansatz

   $$a_n = \varepsilon \cdot n$$

   und erhalten

   $$\varepsilon \cdot (n + 2) = 3 \cdot \varepsilon \cdot (n + 1) - 2 \cdot \varepsilon \cdot n + 1$$

   Diese Gleichung liefert die Lösung

   $$\varepsilon = -1.$$

   Damit lautet die allgemeine Lösung der Rekurrenz-Gleichung (10.10):

   $$a_n = \alpha_1 \cdot 2^n + \alpha_2 \cdot 1^n - n$$

   Die Koeffizienten α_1 und α_2 finden wir nun durch Einsetzen der Anfangs-Bedingungen:

   $$\begin{array}{rcl} 0 & = & \alpha_1 + \alpha_2 \\ 0 & = & 2 \cdot \alpha_1 + \alpha_2 - 1 \end{array}$$

   Aus der ersten Gleichung folgt $\alpha_2 = -\alpha_1$. Damit vereinfacht sich die zweite Gleichung zu

   $$0 = 2 \cdot \alpha_1 - \alpha_1 - 1$$

   und damit lautet die Lösung $\alpha_1 = 1$ und $\alpha_2 = -1$. Die Lösung der ursprünglichen Rekurrenz-Gleichung (10.8) mit der Anfangs-Bedingung $a_0 = 0$ ist also

   $$a_n = 2^n - 1 - n.$$

Das oben gezeigte Verfahren funktioniert, wenn die Inhomogenität der Rekurrenz-Gleichung linear ist, also die Form $\delta \cdot n$. Ist die Inhomogenität quadratisch, so können wir die Gleichung durch diskretes Differenzieren auf eine Rekurrenz-Gleichung reduzieren, deren Inhomogenität linear ist. Diese kann dann aber mit dem eben gezeigten Verfahren gelöst werden. Allgemein gilt: Hat die Inhomogenität der Rekurrenz-Gleichung die Form

$$\delta \cdot n^r \quad r \in \mathbb{N} \text{ und } r > 0,$$

so kann die Rekurrenz-Gleichung durch r-maliges diskretes Differenzieren auf eine inhomogene Rekurrenz-Gleichung mit konstanter Inhomogenität reduziert werden.

Aufgabe: Lösen Sie die Rekurrenz-Gleichung

$$a_{n+1} = a_n + 2 \cdot n \quad \text{für alle } n \in \mathbb{N}$$

mit der Anfangs-Bedingung $a_0 = 0$.

Die oben vorgestellte Technik des diskreten Differenzierens führt in leicht variierter Form oft auch dann noch zu einer Lösung, wenn die Inhomogenität nicht die Form eines Polynoms hat. Wir betrachten als Beispiel die Rekurrenz-Gleichung

$$a_{n+1} = a_n + 2^n \quad \text{für alle } n \in \mathbb{N} \tag{10.11}$$

mit der Anfangs-Bedingungen $a_0 = 0$. Setzen wir in (10.11) für n den Wert $n+1$ ein, erhalten wir

$$a_{n+2} = a_{n+1} + 2^{n+1} \quad \text{für alle } n \in \mathbb{N} \tag{10.12}$$

Würden wir von Gleichung (10.12) die Gleichung (10.11) subtrahieren, so würde der Term 2^n erhalten bleiben. Um diesen Term zu eliminieren müssen wir statt dessen von Gleichung (10.12) 2 mal die Gleichung (10.11) subtrahieren:

$$a_{n+2} - 2 \cdot a_{n+1} = a_{n+1} + 2^{n+1} - 2 \cdot \big(a_n - 2^n\big)$$

Dies vereinfacht sich zu der homogenen Rekurrenz-Gleichung

$$a_{n+2} = 3 \cdot a_{n+1} - 2 \cdot a_n \quad \text{für alle } n \in \mathbb{N} \tag{10.13}$$

Das charakteristische Polynom lautet

$$\chi(x) = x^2 - 3 \cdot x + 2 = (x-1) \cdot (x-2).$$

Damit lautet die allgemeine Lösung der homogenen Rekurrenz-Gleichung

$$a_n = \alpha + \beta \cdot 2^n.$$

Da wir hier mit α und β zwei Unbekannte haben, brauchen wir eine zusätzliche Anfangs-Bedingung. Diese erhalten wir, indem wir in der Gleichung (10.11) für n den Wert 0 einsetzen:

$$a_1 = a_0 + 2^0 = 0 + 1 = 1.$$

Damit erhalten wir das Gleichungs-System

$$\begin{array}{rcl} 0 & = & \alpha + \beta \\ 1 & = & \alpha + 2 \cdot \beta \end{array}$$

Dieses Gleichungs-System hat die Lösung $\alpha = -1$ und $\beta = 1$. Damit lautet die Lösung der Rekurrenz-Gleichung (10.11) mit der Anfangs-Bedingung $a_0 = 0$

$$a_n = 2^n - 1.$$

10.2.4 Die Substitutions-Methode

Bei der Analyse von Algorithmen, die dem Paradigma *Teile-und-Herrsche* folgen, treten häufig Rekurrenz-Gleichungen auf, bei denen der Wert von a_n von dem Wert von $a_{n/2}$ oder gelegentlich auch $a_{n/3}$ oder sogar $a_{n/4}$ abhängt. Wir zeigen jetzt ein Verfahren, mit dessen Hilfe sich auch solche Rekurrenz-Gleichungen behandeln lassen. Wir demonstrieren das Verfahren an Hand der Rekurrenz-Gleichung

$$a_n = a_{n/2} + n \quad \text{für alle } n \in \{2^k \mid k \in \mathbb{N} \wedge k \geq 1\} \tag{10.14}$$

mit der Anfangs-Bedingung $a_1 = 0$. Um diese Rekurrenz-Gleichung zu lösen, machen wir den Ansatz

$$b_k = a_{2^k} \quad \text{für alle } k \in \mathbb{N}.$$

Setzen wir dies in die ursprüngliche Rekurrenz-Gleichung (10.14) ein, so erhalten wir

$$b_k = a_{2^k} = a_{2^k/2} + 2^k = a_{2^{k-1}} + 2^k = b_{k-1} + 2^k.$$

Setzen wir in dieser Gleichung für k den Wert $k+1$ ein, so sehen wir, dass die Folge $(b_k)_k$ der Rekurrenz-Gleichung

$$b_{k+1} = b_k + 2^{k+1} \quad \text{für alle } k \in \mathbb{N} \tag{10.15}$$

genügt. Dabei ist die Anfangs-Bedingung $b_0 = a_{2^0} = a_1 = 0$. Das ist eine lineare inhomogene Rekurrenz-Gleichung mit der Inhomogenität 2^{k+1}. Wir setzen in (10.15) für k den Wert $k+1$ ein und erhalten

$$b_{k+2} = b_{k+1} + 2^{k+2} \quad \text{für alle } k \in \mathbb{N}. \tag{10.16}$$

Wir multiplizieren nun die Rekurrenz-Gleichung (10.15) mit 2 und ziehen das Ergebnis von Gleichung (10.16) ab:

$$b_{k+2} - 2 \cdot b_{k+1} = b_{k+1} + 2^{k+2} - 2 \cdot b_k - 2 \cdot 2^{k+1} \quad \text{für alle } k \in \mathbb{N}.$$

Nach Vereinfachung erhalten wir

$$b_{k+2} = 3 \cdot b_{k+1} - 2 \cdot b_k \quad \text{für alle } k \in \mathbb{N}. \tag{10.17}$$

Die Anfangs-Bedingung für $k = 1$ berechnen wir aus (10.15)

$$b_1 = b_0 + 2^1 = 0 + 2 = 2.$$

Damit haben wir das ursprüngliche Problem auf eine homogene lineare Rekurrenz-Gleichung mit konstanten Koeffizienten zurück geführt. Das charakteristische Polynom dieser Rekurrenz-Gleichung ist

$$\chi(x) = x^2 - 3 \cdot x + 2 = (x-2) \cdot (x-1).$$

Damit lautet die allgemeine Lösung der Rekurrenz-Gleichung (10.17)

$$b_k = \alpha_1 \cdot 2^k + \alpha_2 \cdot 1^k \quad \text{für alle } k \in \mathbb{N}.$$

Wir setzen die Anfangs-Bedingungen ein und erhalten so für die Koeffizienten α_1 und α_2 das lineare Gleichungs-System

$$\begin{array}{rcl} 0 & = & \alpha_1 + \alpha_2 \\ 2 & = & 2 \cdot \alpha_1 + \alpha_2 \end{array}$$

Ziehen wir die erste Gleichung von der zweiten ab, so sehen wir $\alpha_1 = 2$. Dann folgt aus der ersten Gleichung $\alpha_2 = -2$. Damit haben wir

$$b_k = 2^{k+1} - 2 \quad \text{für alle } k \in \mathbb{N}.$$

Setzen wir hier $b_k = a_{2^k}$ ein, so finden wir

$$a_{2^k} = 2^{k+1} - 2 \quad \text{für alle } k \in \mathbb{N}.$$

Mit $n = 2^k$ erhalten wir die Lösung der Rekurrenz-Gleichung (10.14) mit der wir gestartet waren:

$$a_n = 2 \cdot n - 2 \quad \text{für alle } n \in \{2^k \mid k \in \mathbb{N}\}.$$

Aufgabe: Lösen Sie die Rekurrenz-Gleichung

$$a_n = a_{n/2} + 1 \quad \text{für alle } n \in \{2^k \mid k \in \mathbb{N} \wedge k \geq 1\}$$

mit der Anfangs-Bedingungen $a_1 = 1$.

10.2.5 Das Teleskop-Verfahren

Bestimmte Rekurrenz-Gleichungen lassen sich auf bereits bekannte Summen zurückführen. Wir demonstrieren das Verfahren an der Rekurrenz-Gleichung

$$a_n = a_{n-1} + n - 1 \quad \text{mit } a_0 = 0.$$

Diese Gleichung tritt bei der Analyse der Komplexität von Quick-Sort auf. Um diese Gleichung zu lösen, setzen wir zunächst für a_{n-1} den Wert $a_{n-2} + (n-1) - 1$ ein, dann ersetzen wir a_{n-2} durch $a_{n-3} + (n-2) - 2$ und fahren so fort, bis wir schließlich a_n auf a_0 zurück geführt haben. Damit erhalten wir insgesamt:

$$\begin{aligned}
a_n &= a_{n-1} + (n-1) \\
&= a_{n-2} + (n-2) + (n-1) \\
&= a_{n-3} + (n-3) + (n-2) + (n-1) \\
&= \vdots \\
&= a_0 + 0 + 1 + 2 + \cdots + (n-2) + (n-1) \\
&= 0 + 0 + 1 + 2 + \cdots + (n-2) + (n-1) \\
&= \sum_{i=0}^{n-1} i \\
&= \tfrac{1}{2} n \cdot (n-1) \\
&= \tfrac{1}{2} \cdot n^2 - \tfrac{1}{2} \cdot n.
\end{aligned}$$

Das eben demonstrierte Verfahren wird in der Literatur als *Teleskop-Verfahren* bezeichnet. In der allgemeinen Form des Teleskop-Verfahrens gehen wir von einer Rekurrenz-Gleichung der Form

$$a_n = a_{n-1} + g(n)$$

aus. Hierbei ist $g : \mathbb{N} \to \mathbb{R}$ eine reelwertige Funktion. Wenden wir das oben demonstrierte Schema an, so erhalten wir die folgende Rechnung:

$$\begin{aligned}
a_n &= a_{n-1} + g(n) \\
&= a_{n-2} + g(n-1) + g(n) \\
&= a_{n-3} + g(n-2) + g(n-1) + g(n) \\
&= \vdots \\
&= a_0 + g(1) + g(2) + \cdots + g(n-2) + g(n-1) + g(n) \\
&= a_0 + \sum_{i=1}^{n} g(i).
\end{aligned}$$

Falls wir in der Lage sind, für die Summe $\sum_{i=1}^{n} g(i)$ einen geschlossenen Ausdruck anzugeben, dann haben wir damit eine Lösung der Rekurrenz-Gleichung $a_n = a_{n-1} + g(n)$ gefunden. Die Berechnung von Summen ist Gegenstand des nächsten Abschnitts.

10.2.6 Berechnung von Summen

Der letzte Abschnitt hat gezeigt, dass Rekurrenz-Gleichung in bestimmten Fällen auf Summen zurück geführt werden können. In diesem Abschnitt zeigen wir, dass in vielen Fällen auch der umgekehrte Weg möglich ist und die Berechnung von Summen auf die Lösung von solchen Rekurrenz-Gleichungen zurückgeführt werden kann, die wir bereits lösen können. Wir demonstrieren das Verfahren am Beispiel der Berechnung der geometrischen Reihe. Hier wird die Summe s_n durch die Formel

$$s_n = \sum_{i=0}^{n} q^i \tag{10.18}$$

definiert, wobei wir zur Ersparung von Fallunterscheidungen voraussetzen wollen, dass $q \neq 1$ gilt. Diese Einschränkung ist nicht gravierend denn für $q = 1$ sehen wir sofort, dass $s_n = n+1$ gilt. Der erste Schritt besteht darin, dass wir aus der obigen Definition eine Rekurrenz-Gleichung herleiten. Dies erreichen wir dadurch, dass wir in Gleichung (10.18) für n den Wert $n + 1$ einsetzen. Wir erhalten dann die Gleichung

$$s_{n+1} = \sum_{i=0}^{n+1} q^i \tag{10.19}$$

Wir bilden nun die Differenz $s_{n+1} - q \cdot s_n$ und erhalten

$$\begin{aligned}
& s_{n+1} - s_n \cdot q \\
= & \sum_{i=0}^{n+1} q^i - q \cdot \sum_{i=0}^{n} q^i \\
= & \sum_{i=0}^{n+1} q^i - \sum_{i=0}^{n} q^{i+1} \\
= & \sum_{i=0}^{n+1} q^i - \sum_{i=1}^{n+1} q^i \\
= & 1,
\end{aligned}$$

was wir zu

$$s_{n+1} = q \cdot s_n + 1$$

umformen. Dies ist eine lineare inhomogene Rekurrenz-Gleichung mit konstanter Inhomogenität. Die Anfangs-Bedingung ist hier offenbar $s_0 = 1$. Das charakteristische Polynom lautet

$$\chi(x) = x - q.$$

Diese Polynom hat die Nullstelle $x = q$. Um die spezielle Lösung der Rekurrenz-Gleichung zu finden, berechnen wir die Spur des charakteristischen Polynoms. Es gilt

$$\mathtt{sp}(\chi) = \chi(1) = 1 - q \neq 0,$$

denn wir hatten ja $q \neq 1$ vorausgesetzt. Damit lautet die spezielle Lösung

$$s_n = \frac{c_{-1}}{\mathtt{sp}(\chi)} = \frac{1}{1-q}.$$

Folglich lautet die allgemeine Lösung

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

Um den Koeffizienten α zu bestimmen, setzen wir $n = 0$ und erhalten

$$1 = \alpha + \frac{1}{1-q}.$$

Lösen wir diese Gleichung nach α auf, so ergibt sich

$$\alpha = \frac{(1-q)-1}{1-q} = -\frac{q}{1-q}.$$

Damit lautet die Lösung

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

und wir haben für die geometrische Reihe die folgende Formel hergeleitet:

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

Aufgabe: Berechnen Sie eine geschlossene Formel für die Summe der Quadratzahlen

$$s_n := \sum_{i=0}^{n} i^2.$$

Stellen Sie dazu eine Rekurrenz-Gleichung für s_n auf und lösen Sie diese.

10.2.7 Weitere Rekurrenz-Gleichungen

Die Lösung allgemeiner Rekurrenz-Gleichungen kann beliebig schwierig sein und es gibt viele Fälle, in denen eine gegebene Rekurrenz-Gleichungen überhaupt keine Lösung hat, die sich durch elementare Funktionen als geschlossene Formel ausdrücken läßt. Wir wollen an Hand einer etwas komplizierteren Rekurrenz-Gleichung, die uns später bei der Behandlung der durchschnittlichen Komplexität des Quick-Sort-Algorithmus wiederbegegnen wird, zeigen, dass im Allgemeinen bei der Lösung einer Rekurrenz-Gleichung Kreativität gefragt ist. Wir gehen dazu von der folgenden Rekurrenz-Gleichung aus:

$$d_{n+1} = n + \frac{2}{n+1} \cdot \sum_{i=0}^{n} d_i \qquad \text{mit der Anfangs-Bedingung } d_0 = 0. \tag{10.20}$$

Zunächst versuchen wir, die Summe $\sum_{i=0}^{n} d_i$, die auf der rechten Seite dieser Rekurrenz-Gleichung auftritt, zu eliminieren. Wir versuchen, analog zu dem Verfahren des diskreten Differenzierens vorzugehen und substituieren zunächst $n \mapsto n+1$. Wir erhalten

$$d_{n+2} = n + 1 + \frac{2}{n+2} \cdot \sum_{i=0}^{n+1} d_i. \tag{10.21}$$

Wir multiplizieren nun Gleichung (10.21) mit $n+2$ und Gleichung (10.20) mit $n+1$ und haben dann

$$(n+2) \cdot d_{n+2} = (n+2) \cdot (n+1) + 2 \cdot \sum_{i=0}^{n+1} d_i \qquad \text{und} \tag{10.22}$$

$$(n+1) \cdot d_{n+1} = (n+1) \cdot n + 2 \cdot \sum_{i=0}^{n} d_i. \tag{10.23}$$

Wir bilden die Differenz der Gleichungen (10.22) und (10.23) und beachten, dass sich die Summationen bis auf den Term $2 \cdot d_{n+1}$ gerade gegenseitig aufheben. Das liefert

$$(n+2) \cdot d_{n+2} - (n+1) \cdot d_{n+1} = (n+2) \cdot (n+1) - (n+1) \cdot n + 2 \cdot d_{n+1}. \tag{10.24}$$

Diese Gleichung vereinfachen wir zu

$$(n+2) \cdot d_{n+2} = (n+3) \cdot d_{n+1} + 2 \cdot (n+1). \tag{10.25}$$

Um diese Gleichung zu *homogenisieren* teilen wir beide Seiten durch $(n+2) \cdot (n+3)$:

$$\frac{1}{n+3} \cdot d_{n+2} = \frac{1}{n+2} \cdot d_{n+1} + \frac{2 \cdot (n+1)}{(n+2) \cdot (n+3)}. \tag{10.26}$$

Wir definieren $a_n = \dfrac{d_n}{n+1}$ und erhalten dann aus der letzten Gleichung für die Folge $(a_n)_n$ die Beziehung

$$a_{n+2} = a_{n+1} + \frac{2 \cdot (n+1)}{(n+2) \cdot (n+3)}.$$

Die Substitution $n \mapsto n-2$ vereinfacht diese Gleichung zu

$$a_n = a_{n-1} + \frac{2 \cdot (n-1)}{n \cdot (n+1)}. \tag{10.27}$$

Diese Gleichung können wir mit dem Teleskop-Verfahren lösen. Um die dabei auftretenden Summen übersichlicher schreiben zu können, bilden wir die *Partialbruch-Zerlegung* von

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

Dazu machen wir den Ansatz

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

Wir multiplizieren diese Gleichung mit dem Hauptnenner und erhalten

$$2 \cdot n - 2 = \alpha \cdot (n+1) + \beta \cdot n,$$

was sich zu

$$2 \cdot n - 2 = (\alpha + \beta) \cdot n + \alpha$$

vereinfacht. Ein Koeffizientenvergleich liefert dann das lineare Gleichungs-System

$$\begin{aligned} 2 &= \alpha + \beta, \\ -2 &= \alpha. \end{aligned}$$

Setzen wir die zweite Gleichung in die erste Gleichung ein, so erhalten wir $\beta = 4$. Damit können wir die Gleichung (10.27) als

$$a_n = a_{n-1} - \frac{2}{n} + \frac{4}{n+1} \tag{10.28}$$

schreiben und mit dem Teleskop-Verfahren lösen. Wegen $a_0 = \frac{d_0}{1} = 0$ finden wir

$$a_n = 4 \cdot \sum_{i=1}^{n} \frac{1}{i+1} - 2 \cdot \sum_{i=1}^{n} \frac{1}{i}. \tag{10.29}$$

Wir vereinfachen diese Summe:

$$\begin{aligned} a_n &= 4 \cdot \sum_{i=1}^{n} \frac{1}{i+1} - 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \\ &= 4 \cdot \sum_{i=2}^{n+1} \frac{1}{i} - 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \\ &= 4 \cdot \frac{1}{n+1} - 4 \cdot \frac{1}{1} + 4 \cdot \sum_{i=1}^{n} \frac{1}{i} - 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \\ &= 4 \cdot \frac{1}{n+1} - 4 \cdot \frac{1}{1} + 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \\ &= -\frac{4 \cdot n}{n+1} + 2 \cdot \sum_{i=1}^{n} \frac{1}{i} \end{aligned}$$

Um unsere Rechnung abzuschließen, berechnen wir eine Näherung für die Summe

$$H_n = \sum_{i=1}^{n} \frac{1}{i}.$$

Der Wert H_n wird in der Mathematik als die n-te *harmonische Zahl* bezeichnet. Dieser Wert hängt mit dem Wert $\ln(n)$ zusammen: Leonhard Euler hat gezeigt, dass für große n die Approximation

$$\sum_{i=1}^{n} \frac{1}{i} \approx \ln(n) + \gamma + \frac{1}{2} \cdot \frac{1}{n}$$

benutzt werden kann. Hier ist γ die Euler-Mascheroni'sche Konstante, deren Wert durch

$$\gamma \approx 0,5772156649$$

gegeben ist. Damit haben wir für den Wert von a_n die Näherung

$$a_n = -\frac{4 \cdot n}{n+1} + 2 \cdot H_n \approx 2 \cdot \ln(n) + 2 \cdot \gamma - \frac{4 \cdot n}{n+1} + \frac{1}{n}$$

gefunden. Wegen $d_n = (n+1) \cdot a_n$ können wir für die Folge d_n also folgendes schreiben:

$$d_n \approx 2 \cdot (n+1) \cdot \ln(n) + 2 \cdot (n+1) \cdot \gamma - 4 \cdot n + \frac{n+1}{n}.$$

Wir verallgemeinern die Idee, die wir bei der Lösung des obigen Beispiels benutzt haben. Es seien $f : \mathbb{N} \to \mathbb{R}$, $g : \mathbb{N} \to \mathbb{R}$ und $h : \mathbb{N} \to \mathbb{R}$ reelwertige Folgen und es sei die Rekurrenz-Gleichung

$$f(n) \cdot a_n = g(n) \cdot a_{n-1} + h(n)$$

zu lösen. Die Idee ist, beide Seiten mit einem geeigneten Faktor, der im Allgemeinen von n abhängt, zu multiplizieren. Bezeichnen wir diesen Faktor mit $p(n)$, so erhalten wir die Rekurrenz-Gleichung

$$p(n) \cdot f(n) \cdot a_n = p(n) \cdot g(n) \cdot a_{n-1} + p(n) \cdot h(n).$$

Das Ziel ist dabei, den Faktor $p(n)$ so zu wählen, dass der Koeffizient von a_n die selbe Form hat wie der Koeffizient von a_{n-1}, es soll also

$$p(n) \cdot g(n) = p(n-1) \cdot f(n-1) \tag{10.30}$$

gelten, denn dann können wir die ursprüngliche Rekurrenz-Gleichung in der Form

$$p(n) \cdot f(n) \cdot a_n = p(n-1) \cdot f(n-1) \cdot a_{n-1} + p(n) \cdot h(n).$$

schreiben und anschließend durch die Substitution $b_n := p(n) \cdot f(n) \cdot a_n$ auf die Rekurrenz-Gleichung

$$b_n = b_{n-1} + p(n) \cdot h(n).$$

Diese Gleichung läßt sich mit dem Teleskop-Verfahren auf eine Summe zurückführen und die Lösung der ursprünglichen Gleichung kann schließlich über die Formel

$$a_n = \frac{1}{p(n) \cdot f(n)} \cdot b_n$$

aus b_n berechnet werden. Es bleibt also zu klären, wie wir den Faktor $p(n)$ so wählen können, dass Gleichung (10.30) erfüllt ist. Dazu schreiben wir diese Gleichung als Rekurrenz-Gleichung für $p(n)$ um und erhalten

$$p(n) = \frac{f(n-1)}{g(n)} \cdot p(n-1)$$

Diese Gleichung können wir mit einer Variante des Teleskop-Verfahrens lösen:

$$\begin{aligned}
p(n) &= \tfrac{f(n-1)}{g(n)} \cdot p(n-1) \\
&= \tfrac{f(n-1)}{g(n)} \cdot \tfrac{f(n-2)}{g(n-1)} \cdot p(n-2) \\
&= \tfrac{f(n-1)}{g(n)} \cdot \tfrac{f(n-2)}{g(n-1)} \cdot \tfrac{f(n-3)}{g(n-2)} \cdot p(n-3) \\
&= \tfrac{f(n-1)}{g(n)} \cdot \tfrac{f(n-2)}{g(n-1)} \cdot \tfrac{f(n-3)}{g(n-2)} \cdot p(n-3) \\
&\vdots \\
&= \tfrac{f(n-1)}{g(n)} \cdot \tfrac{f(n-2)}{g(n-1)} \cdot \tfrac{f(n-3)}{g(n-2)} \cdot \ldots\ldots \tfrac{f(2)}{g(3)} \cdot \tfrac{f(1)}{g(2)} \cdot p(1)
\end{aligned}$$

Wir setzen willkürlich $p(1) = 1$ und haben dann für $p(n)$ die Lösung

$$p(n) = \prod_{i=1}^{n-1} \frac{f(i)}{g(i+1)}$$

gefunden. Bei der Rekurrenz-Gleichung

$$n \cdot d_n = (n+1) \cdot d_{n-1} + 2 \cdot (n-1),$$

die aus der Rekurrenz-Gleichung (10.25) durch die Substitution $n \mapsto n-2$ hervorgeht, gilt $f(n) = n$ und $g(n) = n+1$. Damit haben wir dann

$$\begin{aligned}
p(n) &= \prod_{i=1}^{n-1} \tfrac{f(i)}{g(i+1)} \\
&= \prod_{i=1}^{n-1} \tfrac{i}{i+2} \\
&= \tfrac{1}{3} \cdot \tfrac{2}{4} \cdot \tfrac{3}{5} \cdot \ldots\ldots \tfrac{n-3}{n-1} \cdot \tfrac{n-2}{n} \cdot \tfrac{n-1}{n+1} \\
&= 2 \cdot \tfrac{1}{n} \cdot \tfrac{1}{n+1}.
\end{aligned}$$

Die Konstante 2 ist hier unwichtig und wir sehen, dass der Faktor $\frac{1}{n \cdot (n+1)}$ benutzt werden kann, um die ursprüngliche Rekurrenz-Gleichung zu homogenisieren.

Aufgabe 20: Lösen Sie die Rekurrenz-Gleichung

$$a_n = 2 \cdot a_{n-1} + 1 \quad \text{mit } a_0 = 0$$

mit Hilfe einer geeigneten Homogenisierung. Gehen Sie dabei analog zu dem im letzten Abschnitt beschriebenen Verfahren vor.

Literaturverzeichnis

[Can95] Cantor, Georg: Beiträge zur Begründung der transfiniten Mengenlehre. In: *Mathematische Annalen* 46 (1895), S. 481–512

[Har06] Hartmann, Peter: *Mathematik für Informatiker: Ein praxisbezogenes Lehrbuch.* Vierte Auflage. Vieweg Verlag, 2006

[Lip98] Lipschutz, Seymour: *Set Theory and Related Topics.* McGraw-Hill, New York, 1998

[MM06] Meinel, Christoph ; Mundhenk, Martin: *Mathematische Grundlagen der Informatik: Mathematisches Denken und Beweisen; eine Einführung.* Vierte Auflage. Vieweg+Teubner, 2006 (Lehrbuch Informatik)

[RSA78] Rivest, R. L. ; Shamir, A. ; Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Crypto-Systems. In: *Communications of the ACM* 21 (1978), Nr. 2, S. 120–126

[Sch07] Schubert, Matthias: *Mathematik für Informatiker.* Vieweg+Teubner, 2007

[TT08] Teschl, Gerald ; Teschl, Susanne ; Berlin, Springer (Hrsg.): *Mathematik für Informatiker: Band 1: Diskrete Mathematik und Lineare Algebra.* Dritte Auflage. Springer Verlag, 2008