Eine Einführung in die Mathematik für Informatiker

— WS 2014/2015 —

DHBW Mannheim

Prof. Dr. Karl Stroetmann

19. November 2014

Dieses Skript ist einschließlich der LaTeX-Quellen sowie der in diesem Skript diskutierten Programme unter

`https://github.com/karlstroetmann/Lineare-Algebra`

im Netz verfügbar. Das Skript selbst finden Sie in dem Unterverzeichnis Script. Dort ist das Skript in der Datei `lineare-algebra.pdf` abgespeichert. Wenn Sie auf Ihrem Rechner `git` installieren und mein Repository mit Hilfe des Befehls

```
git clone https://github.com/karlstroetmann/Lineare-Algebra.git
```

klonen, dann können Sie durch den Befehl

```
git pull
```

die aktuelle Version meines Skripts aus dem Netz laden.

Inhaltsverzeichnis

Kapitel 1

Einführung

Das vorliegende Skript ist die Grundlage der Mathematik-Vorlesung des ersten Semesters. Einige Kapitel und Abschnitte in diesem Skript sind mit einem "*" versehen. Der dort vorgestellte Stoff ist für die Klausur nicht relevant. Das Skript enthält diese Abschnitte um eine der vielen Anwendungen der Mathematik, die Kryptologie, präsentieren zu können.

1.1 Motivation

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

(a) 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 durch die Gleichung

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

symbolisiert wird. Aufgrund der Tatsache, dass die Informatik aus der Mathematik gewachsen ist, bedient sich die Informatik an vielen Stellen mathematischer Sprech- und Denkweisen. Um diese verstehen zu können, ist eine Vertrautheit mit der formalen mathematischen Denkweise unabdingbar.

(b) 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.

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

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

$$a_{n+2} = a_{n+1} + a_n \quad \text{und die Anfangs-Bedingungen } a_0 = 0 \text{ und } a_1 = 1$$

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

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

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.

2. Elementare Zahlentheorie bildet die Grundlage moderner kryptografischer Verfahren. Konkret beinhaltet dieses Skript eine Beschreibung des RSA-Algorithmus zur asymetrischen Verschlüsselung. Allerdings werden wir das Kapitel zur Zahlen-Theorie, in dem der RSA-Algorithmus beschrieben wird, aus Zeitgründen nicht besprechen können, es handelt sich bei dem Kapitel also nur um Zusatzstoff, welchen Sie sich bei Bedarf selbst aneignen können. Ich habe das Kapitel hier deswegen eingefügt, damit Sie unmittelbar an Hand eines konkreten Beispiels sehen können, welche Bedeutung die Mathematik in der Informatik hat.

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, Ihnen ausreichend mathematische Fähigkeiten zu vermitteln, so dass Sie später in der Lage sind, sich die mathematischen Verfahren, die sie im Beruf tatsächlich benötigen, selbstständig anzueignen.

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

1. 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.

2. 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.

3. 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.

4. Im Internet finden Sie unter

http://www.computerworld.com/
article/2515483/enterprise-applications/epic-failures--11-infamous-software-bugs.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. Obwohl sowohl die Logik als auch die Mengenlehre zur Mathematik gehören, werden wir uns in dieser Mathematik-Vorlesung nur mit der Mengenlehre und der linearen Algebra beschäftigen. Die Behandlung der Logik erfolgt dann im Rahmen der Informatik-Vorlesung.

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.

(a) Mathematische Formeln dienen der Abkürzung. Sie werden aus den *Junktoren*

1. $\wedge$ ("*und*"),
2. $\vee$ ("*oder*"),
3. $\neg$ ("*nicht*"),
4. $\rightarrow$ ("*wenn* $\cdots$, *dann*") und
5. $\leftrightarrow$ ("*genau dann, wenn*")

sowie den *Quantoren*

1. $\forall$ ("*für alle*") und
2. $\exists$ ("*es gibt*")

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

(b) 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.

(c) Beweis-Prinzipien

In der Informatik benötigen wir im wesentlichen vier Arten von Beweisen:

1. 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.

2. Bei einem *Beweis durch Fallunterscheidung* teilen wir den Beweis dadurch auf, dass wir alle in einer bestimmten Situation möglichen Fälle untersuchen und zeigen, dass die zu beweisende Aussage in jedem der Fälle wahr ist. Beispielsweise können wir mit Hilfe einer Fallunterscheidung zeigen, dass die Zahl $n \cdot (n+1)$ für jede natürliche Zahl n gerade ist.
3. 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.
4. Ein induktiver Beweis hat das Ziel, eine Aussage für alle natürliche Zahlen zu beweisen. Beispielsweise werden wir zeigen, dass die Summenformel
   $$\sum_{i=1}^{n} i = \frac{1}{2} \cdot n \cdot (n+1)$$
   für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt.

(d) Grundlagen der Algebra

Wir besprechen *Gruppen*, *Ringe* und *Körper*. Diese abstrakten Konzepte verallgemeinern die Rechenregeln, die Sie von den reellen Zahlen kennen. Sie bilden darüber hinaus die Grundlage für die lineare Algebra.

(e) Zahlentheorie

Dieses Skript enthält ein optionales Kapitel, in dem wir uns mit der elementaren Zahlentheorie auseinandersetzen. Die Zahlentheorie ist die Grundlage von vielen modernen Verschlüsselungs-Algorithmen.

(f) 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 jede quadratische Gleichung eine Lösung in der Menge der komplexen Zahlen hat.

(g) 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.

(h) Lineare Gleichungs-Systeme

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

(i) 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.

(j) 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

`karl.stroetmann@dhbw-mannheim.de`

mitzuteilen. Alternativ können Sie mir auch über `https://github.com` einen `pull`-Request schicken.

1.3 Literaturhinweise

Zum Schluss dieser Einführung möchte ich noch einige Hinweise auf die Literatur geben. Dabei möchte ich zwei Bücher besonders hervorheben:

(a) Das Buch "*Set Theory and Related Topics*" von Seymour Lipschutz [Lip98] enthält den Stoff, der in diesem Skript in dem Kapitel über Mengenlehre abgehandelt wird.

(b) Das Buch "*Linear Algebra*" von Seymour Lipschutz und Marc Lipson [LL12] enthält den Stoff zur eigentlichen linearen Algebra.

Beide Bücher enthalten eine große Anzahl von Aufgaben mit Lösungen, was gerade für den Anfänger wichtig ist. Darüber hinaus sind die Bücher sehr preiswert.

Vor etwa 30 Jahren habe ich selbst die lineare Algebra aus den Büchern von Gerd Fischer [Fis08] und Hans-Joachim Kowalsky [Kow03] gelernt, an denen ich mich auch jetzt wieder orientiert habe. Zusätzlich habe ich in der Zwischenzeit das Buch "*Linear Algebra Done Right*" von Sheldon Axler [Axl97] gelesen, das sehr gut geschrieben ist und einen alternativen Zugang zur linearen Algebra bietet, bei dem die Theorie der Determinanten allerdings in den Hintergrund gerät. Der fachkundige Leser wird bei der Lektüre dieses Skripts unschwer Parallelen zu den oben zitierten Werken erkennen. Demjenigen Leser, der mehr wissen möchte als das, was im Rahmen dieser Vorlesung gezeigt werden kann, möchte ich auf die oben genannte Literatur verweisen, wobei mir persönlich die Darstellung des Buchs von Sheldon Axler am besten gefällt.

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:

(a) 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.

(b) 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.

(a) *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.

(b) *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.

(c) *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 $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$.

Benutzen wir Funktions-Zeichen nicht nur in der Präfix-Notation, sondern auch als Infix- oder Postfix-Operatoren, so müssen wir zusätzlich die *Bindungsstärke* und *Assoziativität* dieser Operatoren festlegen. Beispielsweise ist die Bindungsstärke des Operators "$\cdot$" in der üblichen Verwendung als Infix-Operator höher als die Bindungsstärke des Operators "+". Daher wird der Ausdruck

$$1 + 2 \cdot 3 \quad \text{implizit in der Form} \quad 1 + (2 \cdot 3)$$

geklammmert. Weiter ist der Operator "–" links-assoziativ. Daher wird der Ausdruck

$$1 - 2 - 3 \quad \text{in der Form} \quad (1 - 2) - 3$$

berechnet.

(d) *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.

(e) *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:

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

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 "·" 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 "¬" stärker bindet als "∧" und "∨" und dass diese beiden Operatoren stärker binden als "→". Schließlich bindet der Operator "↔" schwächer als alle anderen Operatoren. Mit diesen Vereinbarungen lautet die Formel

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

dann in einer vollständig geklammerten Schreibweise

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

(f) *Quantoren* geben an, in welcher Weise eine Variable in einer Formel verwendet wird. Wir kennen zwei Quantoren, den All-Quantor "∀" und den Existenz-Quantor "∃". 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:

$$\forall x \in M : F \overset{def}{\iff} \forall x \colon (x \in M \to F)$$

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

$$\exists x \in M : F \overset{def}{\iff} \exists x \colon (x \in M \wedge F)$$

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.

(a) Als *Konstanten* verwenden wir die Wörter

"`adam`", "`eva`", "`kain`" und "`abel`", "`lisa`".

(b) Als *Variablen* verwenden wir die Buchstaben

"x", "y" und "z".

(c) Als *Funktions-Zeichen* verwenden wir die Wörter

"`vater`" und "`mutter`".

Diese beiden Funktions-Zeichen sind einstellig.

(d) Als *Prädikats-Zeichen* verwenden wir die Wörter

"`bruder`", "`schwester`", "`männlich`" und "`weiblich`".

Hier sind die Prädikats-Zeichen "`männlich`" und "`weiblich`" einstellig, während "`bruder`" und "`schwester`" zweistellig sind. Als weiteres zweistelliges 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:

(a) "`kain`" ist ein Term, denn "`kain`" ist eine Konstante.

(b) "`vater`(`kain`)" ist ein Term, denn "`kain`" ist ein Term und "`vater`" ist ein einstelliges Funktions-Zeichen.

(c) "`mutter`$\big($`vater`(`kain`)$\big)$" ist ein Term, denn "`vater`(`kain`)" ist ein Term und "`mutter`" ist ein einstelliges Funktions-Zeichen,

(d) "`männlich`(`kain`)" ist eine Formel, denn "`kain`" ist ein Term und "`männlich`" ist ein einstelliges Prädikats-Zeichen.

(e) "`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.

(f) "$\texttt{vater}(x) = \texttt{vater}(y) \wedge \texttt{mutter}(x) = \texttt{mutter}(y) \rightarrow \texttt{bruder}(x, y) \vee \texttt{schwester}(x, y)$"

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.

(g) "$\forall x\colon \forall y\colon \texttt{bruder}(x, y) \vee \texttt{schwester}(x, y)$" 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.

Aufgabe 1: Nehmen Sie an, dass Sie nichts weiter über Frau Müller wissen. Ist eine der folgenden Aussagen wahrscheinlicher als alle anderen Aussagen oder ist das nicht der Fall? Begründen Sie Ihre Aussage!

(a) Frau Müller spielt Klavier und arbeitet in einer Bank.

(b) Frau Müller ist katholisch und arbeitet in einer Bank.

(c) Frau Müller ist evangelisch und arbeitet in einer Bank.

(d) Frau Müller hat zwei Kinder und arbeitet in einer Bank.

(e) Frau Müller arbeitet in einer Bank.

(f) Frau Müller arbeitet in der Commerzbank. ◇

Aufgabe 2: Nehmen Sie an, dass Sie nichts weiter über Frau Meyer wissen. Ist eine der folgenden Aussagen wahrscheinlicher als alle anderen Aussagen oder ist das nicht der Fall? Begründen Sie Ihre Aussage!

(a) Frau Meyer spielt Klavier und arbeitet in einer Bank.

(b) Frau Meyer ist katholisch oder Frau Meyer arbeitet in einer Bank.

(c) Frau Meyer ist katholisch.

(d) Frau Meyer hat zwei Kinder und arbeitet in einer Bank.

(e) Frau Meyer arbeitet in einer Bank.

(f) Frau Meyer arbeitet in der Commerzbank. ◇

Aufgabe 3:

(a) Das Prädikat $\mathit{isPrime}(n)$ soll für eine natürliche Zahl $n \in \mathbb{N}$ genau dann wahr sein, wenn n eine Primzahl ist. Definieren Sie dieses Prädikat mit Hilfe einer geeigneten prädikatenlogischen Formel.

(b) Formalisieren Sie die Aussage

"Es gibt keine größte Primzahl."

als prädikatenlogische Formel. Benutzen Sie dabei das in Teil (a) dieser Aufgabe definierte Prädikatszeichen *isPrime*. ◇

Aufgabe 4: Der Hilbert'sche Existenz-Quantor "$\exists!x$" wird als "es gibt genau ein x" gelesen. Falls $\phi(x)$ eine Formel ist, in der die Variable x vorkommt, dann wird also der Ausdruck

$$\exists!x : \phi(x) \quad \text{als} \quad \text{"Es gibt genau ein } x\text{, so dass } \phi(x) \text{ gilt."}$$

gelesen. Geben Sie eine Formel an, die zu der Formel $\exists!x : \phi(x)$ äquivalent ist, in der aber nur die gewöhnlichen Quantoren $\forall$ und $\exists$ verwendet werden. Zeigen Sie also, wie sich der Hilbert'sche Existenz-Quantor in der Prädikatenlogik definieren lässt. ◇

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 nicht 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:

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

(b) 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 wohldefiniert ist. 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 spielt in der Mengenlehre eine ähnliche Rolle wie die Zahl 0 in der Zahlentheorie.

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 werde ich dabei die Zahl 0 nicht 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:

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

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

(a) $\mathbb{N}_0$ ist die Menge der nicht-negativen ganzen Zahlen, es gilt also

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N}.$$

(b) $\mathbb{Z}$: Menge der ganzen Zahlen.

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

(c) $\mathbb{Q}$: Menge der rationalen Zahlen.

$$\left\{ \frac{p}{q} \mid p \in \mathbb{Z} \wedge q \in \mathbb{N} \right\}$$

(d) $\mathbb{R}$: Menge der reellen Zahlen.

Eine mathematisch saubere Definition der reellen Zahlen erfordert einiges an Aufwand. Wir werden die Konstruktion der rellen Zahlen im zweiten Semester kennenlernen.

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 als die Menge

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

geschrieben werden.

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 durch die Formel

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

definieren.

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 als

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

definiert werden.

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 diese Vereinigung als

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

definiert werden:

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 $M \cap N$ als

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

definieren.

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 als

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

definiert werden.

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 $f(M)$ als

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

definiert werden. 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 positiven Quadrat-Zahlen kann als

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

definiert werden. Alternativ können wir auch

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

schreiben. ◇

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 dieselben Elemente besitzen.

Mathematisch können wir diesen Sachverhalt durch die Formel

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

ausdrücken. 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 dieselben 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

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

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 dieselben Elemente enthalten. Wir haben die folgende Kette von Äquivalenzen:

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

Wir haben beim dritten Schritt dieser Äquivalenz-Kette ausgenutzt, dass eine Disjunktion der Form $F \vee G$ genau dann falsch ist, wenn sowohl F als auch G falsch ist, formal gilt

$$\neg(F \vee G) \leftrightarrow \neg F \wedge \neg G.$$

Wir werden diese Äquivalenz im Rahmen der Logik-Vorlesung noch formal beweisen.

Die übrigen der oben aufgeführten Gleichungen können nach dem selben Schema hergeleitet werden.

Aufgabe 5: Beweisen Sie die folgenden Gleichungen:

(a) $K \backslash (M \cap N) = (K \backslash M) \cup (K \backslash N)$,

(b) $M \cup (M \cap N) = M$,

(c) $K \backslash (M \backslash N) = (K \backslash M) \cup (K \cap N)$,

(d) $(K \backslash M) \backslash N = K \backslash (M \cup N)$. ◇

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:

$$x \notin M \iff^{def} \neg\, x \in M.$$

Eine analoge Notation verwenden wir auch für das Gleichheitszeichen: $x \neq y \iff^{def} \neg\, (x = y)$.

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. Dabei handelt es sich um grundlegende Konzepte, die jeder Informatiker kennen sollte.

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 $M := \{1, 2, 3\}$ und $N := \{1, 2, 3, 4, 5\}$. Wir definieren die Relation $R \subseteq M \times N$ als

$$R = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 3, 5\rangle\}.$$

Dann gilt

$$\mathrm{dom}(R) = \{1, 3\} \quad \text{und} \quad \mathrm{rng}(R) = \{1, 2, 5\}.$$

Dieses Beispiel zeigt, dass der Begriff der *Relation* eine Verallgemeinerung des Begriffs der Funktion ist. Das liegt daran, dass eine Funktion jedem Argument genau ein Wert zugeordnet wird. Bei einer Relation können hingegen einem Argument auch mehrere Werte zugeordnet werden. Ebenso ist es bei einer Relation möglich, dass einem Argument kein Wert zugeordnet wird. Beispielsweise ordnet die oben angegebene Relation R der Zahl 1 sowohl die Zahl 1 als auch die Zahl 2 zu, während der Zahl 2 kein Wert zugeordnet wird. ◇

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:

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

Dann könnte die binäre Relation

$$\mathit{Verkauf} \subseteq \mathit{Kunde} \times \mathit{Auto}$$

beispielsweise durch die folgende Menge gegeben sein:

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

Diese Relation würde ausdrücken, dass der Kunde Bauer einen Golf und einen Fox erworben hat, der Kunde Schmidt hat einen Polo gekauft und Herr 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 Funktionale Relationen

Wir hatten schon gesehen, dass Relationen als Verallgemeinerungen von Funktionen aufgefasst werden können. Wir wollen als nächstes untersuchen, unter welchen Umständen eine Relation als Funktion aufgefasst werden kann. Zu diesem Zweck folgt nun eine Definition.

Definition 3.1 (links-eindeutig, rechts-eindeutig) 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 $N = \{4, 5, 6\}$.

(a) 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.

(b) 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.

(c) 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 $2 \neq 3$.

Definition 3.2 (links-total, rechts-total) Eine binäre Relation $R \subseteq M \times N$ heißt *links-total auf* M, wenn

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

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 letzten 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

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

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 letzten 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 $y \neq 5$. ◇

Definition 3.3 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. ◇

Satz 3.4 Ist $R \subseteq M \times N$ eine funktionale Relation, so können wir eine Funktion $f_R : M \to N$ wie folgt definieren:

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

Beweis: 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. □

Bemerkung: 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 auf M, 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:

(a) 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.

(b) 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.

(c) 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. Das liegt daran, dass das Element 2 von der Relation R sowohl auf 3 als auch auf 4 abgebildet wird. ◇

Definition 3.5 (Bild) 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

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

3.13.2 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 auf N genau dann, wenn R rechts-total auf N ist. Ist eine Relation sowohl links-eindeutig als auch rechts-eindeutig und außerdem sowohl links-total auf M als auch rechts-total auf N, 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

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

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

3.13.3 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:

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

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, denn der *Join*-Operator, der in Datenbankabfrage-Sprachen wie SQL benutzt wird, ist eine Verallgemeinerung des relationalen Produkts.

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

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

Aufgabe 6: Es sei $R \subseteq L \times M$ eine funktionale Relation auf L und $Q \subseteq M \times N$ sei eine funktionale Relation auf M. Zeigen Sie, dass dann auch $R \circ Q$ eine funktionale Relation auf L ist und zeigen Sie weiter, dass die Funktion $f_{R \circ Q}$ wie folgt aus den Funktionen f_R und f_Q berechnet werden kann:

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

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 die Berechnung des *transitiven Abschlusses* einer Relation, die wir später noch geben werden, intuitiver wird. $\diamond$

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. $\diamond$

3.13.4 Eigenschaften des relationalen Produkts

Satz 3.6 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, dass

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

gilt. Dazu formen wir 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. □

Satz 3.7 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 Reihenfolge von Q und R hier vertauscht!

Beweis: Es 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:

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

Satz 3.8 (Distributiv-Gesetze für das relationale Produkt) 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 ohne Klammern schreiben zu können vereinbaren wir, dass der Kompositions-Operator $\circ$ stärker bindet als $\cup$ und $\cap$.

Beweis: Wir beweisen 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:

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

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

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

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. □

Aufgabe 7: Es seien M, N und L Mengen und es gelte $R \subseteq M \times N$ und $Q_1, Q_2 \subseteq N \times L$.

(a) Beweisen oder widerlegen Sie die Gleichung

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

(b) Beweisen oder widerlegen Sie die Behauptung

$$R \circ (Q_1 \cap Q_2) = R \circ Q_1 \cap R \circ Q_2.$$ ◇

Definition 3.9 (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

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

Bemerkung: Aus der Definition folgt sofort

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

Satz 3.10 Ist $R \subseteq M \times N$ eine binäre Relation, so gilt

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

Beweis: Wir weisen nur die zweite Gleichung nach, denn der Nachweis der ersten Gleichung verläuft analog zu dem Beweis der zweiten Gleichung. 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 das 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 8: Es sei $R \subseteq M \times N$. Welche Eigenschaften muss die Relation R besitzen, damit die Gleichung

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

richtig ist? Unter welchen Bedingungen gilt

$$R^{-1} \circ R = \mathrm{id}_N?$$ ◇

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:

$$\leq := \{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} \mid \exists z \in \mathbb{N}_0 \colon x + z = y\}.$$

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

Definition 3.11 (reflexiv) 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 3.12 Eine Relation $R \subseteq M \times M$ ist genau dann reflexiv auf M, wenn $\mathrm{id}_M \subseteq R$ gilt.

Beweis: Es gilt

$$\begin{aligned}
& \mathrm{id}_M \subseteq R \\
\leftrightarrow\ & \big\{\langle x, x\rangle \mid x \in M\big\} \subseteq R \\
\leftrightarrow\ & \forall x \in M : \langle x, x\rangle \in R \\
\leftrightarrow\ & R \text{ ist reflexiv auf } M.
\end{aligned}$$ □

Definition 3.13 (symmetrisch) 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 3.14 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

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

Vertauschen wir hier die Rollen der Variablen x und y, so ist dies gerade die Bedingung, dass die Relation R symmetrisch ist. □

Definition 3.15 (anti-symmetrisch) Eine Relation $R \subseteq M \times M$ ist *anti-symmetrisch* falls gilt:

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

Satz 3.16 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

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

gilt und zeigen, dass aus dieser Voraussetzung die Inklusions-Beziehung

$$R \cap R^{-1} \subseteq \mathrm{id}_M$$

folgt. Es gelte also

$$\langle x, y\rangle \in R \cap R^{-1}.$$

Daraus folgt

$$\langle x, y\rangle \in R \wedge \langle x, y\rangle \in R^{-1}.$$

Nach Definition von R^{-1} folgt daraus

$$\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R.$$

Nun folgt aber aus der Anti-Symmetrie von R

$$x = y$$

und das impliziert

$$\langle x, y\rangle \in \mathrm{id}_M.$$

Damit ist die Inklusion

$$R \cap R^{-1} \subseteq \mathrm{id}_M$$

gezeigt.

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

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

folgt. Seien also $x, y \in M$ und es gelte

$$\langle x, y\rangle \in R \text{ und } \langle y, x\rangle \in R.$$

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 $x = y$. □

Aufgabe 9:

(a) Geben Sie eine Menge M und eine Relation $R \subseteq M \times M$ an, so dass R sowohl anti-symmetrisch als auch symmetrisch ist.

(b) Geben Sie eine Menge M und eine Relation $R \subseteq M \times M$ an, so dass R weder anti-symmetrisch noch symmetrisch ist. ◇

Bemerkung: In der Literatur finden Sie noch den Begriff der *Asymmetrie*. Dort wird eine Relation $R \subseteq M^2$ als *asymmetrisch* definiert, wenn

$$\forall x, y \in M : \big(\langle x, y\rangle \in R \rightarrow \langle y, x\rangle \notin R\big)$$

gilt. Beachten Sie, dass der Begriff der *Asymmetrie* nicht die Negation des Begriffs der *Symmetrie* ist: Zwar kann eine symmetrische Relation nicht asymmetrisch sein, aber es gibt Relationen, die weder asymmetrisch noch symmetrisch sind. In dieser Vorlesung spielt der Begriff der *Asymmetrie* keine Rolle. Für Sie reicht es zu wissen, dass *Anti-Symmetrie* und *Asymmetrie* zwei verschiedene Begriffe sind. ◇

Definition 3.17 (transitiv) Eine Relation $R \subseteq M \times M$ ist *transitiv* falls gilt:

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

Satz 3.18 Eine Relation $R \subseteq M \times M$ ist genau dann transitiv, wenn $R \circ R \subseteq R$ ist.

Beweis:

"⇒": Wir nehmen zunächst an, dass R transitiv ist und damit

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

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

$$\langle x, y\rangle \in R \text{ und } \langle y, z\rangle \in R$$

gilt. Da R transitiv ist, folgt daraus

$$\langle x, z\rangle \in R$$

und das war zu zeigen.

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

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

folgt. Seien also $x, y, z \in M$ mit

$$\langle x, y\rangle \in R \text{ und } \langle y, z\rangle \in R$$

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 nun

$$\langle x, z\rangle \in R.$$ □

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

(a) $R_1 = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$.
R_1 ist reflexiv auf M, symmetrisch, anti-symmetrisch und transitiv.

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

R_2 ist nicht reflexiv auf M, 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 $M = \mathbb{N}$.

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

R_3 ist reflexiv auf $\mathbb{N}$, 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 sowohl $n \leq m$ als auch $m \leq n$ gilt, dann muss $m = n$ gelten. Schließlich ist R_3 auch transitiv, denn aus $k \leq m$ und $m \leq n$ folgt natürlich $k \leq n$.

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

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 auf $\mathbb{N}$ 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 anti-symmetrisch, 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.

3.15 Der transitive Abschluss einer Relation

Ist R eine Relation auf einer Menge M, die nicht transitiv ist, so können wir R zu einer transitiven Relation erweitern. Zu diesem Zweck definieren wir zunächst den Begriff der *Potenz* einer Relation auf M.

Definition 3.19 (Potenz einer Relation, R^n) Für eine Relation $R \subseteq M^2$ definieren wir für alle $n \in \mathbb{N}_0$ die *Potenz* R^n durch Induktion über n wie folgt:

(a) Induktions-Anfang: $n = 0$. Wir setzen

$$R^0 := \mathrm{id}_M.$$

(b) Induktions-Schritt: $n \to n+1$. Nach Induktions-Voraussetzung ist R^n bereits definiert. Daher können wir R^{n+1} als

$$R^{n+1} = R \circ R^n$$

definieren. ◇

Es zeigt sich, dass für die Potenzen einer Relation und das relationalen Produkt ein ähnlicher Zusammenhang besteht, wie für die Potenzen einer Zahl und das gewöhnliche Produkt, denn es gilt das folgende Gesetz.

Satz 3.20 (Potenz-Gesetz des relationalen Produkts)
Es sei $R \subseteq M \times M$. Für beliebige ganze Zahlen $k, l \in \mathbb{N}_0$ gilt:

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

Beweis: Wir führen den Beweis durch Induktion nach k.

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

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

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

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

□

Die nächste Definition zeigt, dass wir eine beliebige Relation $R \subseteq M^2$ zu einer transitiven Relation erweitern können.

Definition 3.21 (transitiver Abschluss einer Relation, R^+)
Es sei $R \subseteq M^2$. Wir definieren den *transitiven Abschluss* der Relation R als die Menge

$$R^+ := \bigcup_{n \in \mathbb{N}} R^n.$$

Dabei ist für eine Folge $(A_n)_n$ von Mengen der Ausdruck $\bigcup\limits_{n \in \mathbb{N}} A_n$ als

$$\bigcup_{n \in \mathbb{N}} A_n := \big\{ x \,\big|\, \exists n \in \mathbb{N} : x \in A_n \big\}.$$

definiert. Etwas weniger formal (aber dafür anschaulicher) können wie auch schreiben

$$\bigcup_{n \in \mathbb{N}} A_n := \bigcup_{i=1}^{\infty} A_n := A_1 \cup A_2 \cup A_3 \cup \cdots.$$

◇

Satz 3.22 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:

(a) R^+ ist transitiv.

(b) 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:

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

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

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

$$\langle x, y \rangle \in \bigcup_{n \in \mathbb{N}} R^n \quad \text{und} \quad \langle y, z \rangle \in \bigcup_{n \in \mathbb{N}} R^n.$$

Nach der Definition der Menge $\bigcup\limits_{n \in \mathbb{N}} R^n$ 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

$$\langle x, z\rangle \in \bigcup_{n\in\mathbb{N}} R^n.$$

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

(b) 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. Um diesen Nachweis zu führen, zeigen wir zunächst, dass für alle natürlichen Zahlen $n \in \mathbb{N}$ die folgende Inklusion gilt:

$$R^n \subseteq T.$$

Wir führen den Nachweis dieser Behauptung durch vollständige Induktion über $n \in \mathbb{N}$.

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 $R \subseteq T$. $\surd$

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

$$R^n \subseteq T$$

gilt. 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. $\surd$

Wir schließen den Beweis ab, indem wir

$$R^+ \subseteq T$$

zeigen. Sei $\langle x, y\rangle \in R^+$. Nach Definition von R^+ muss es dann eine 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

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

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

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

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

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

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 10: 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:

(a) R^2,

(b) R^3,

(c) R^n für beliebige $n \in \mathbb{N}$,

(d) R^+. ◇

Aufgabe 11: Wir definieren die Relation R auf der Menge $\mathbb{N}$ der natürlichen Zahlen als

$$R := \{\langle n, 2 \cdot n\rangle \mid n \in \mathbb{N}\}.$$

Berechnen Sie den transitiven Abschluss R^+. ◇

3.16 Äquivalenz-Relationen

Definition 3.23 (Äquivalenz-Relation) Eine Relation $R \subseteq M \times M$ ist eine *Äquivalenz-Relation* auf M genau dann, wenn folgende Bedingungen erfüllt sind:

(a) R ist reflexiv auf M,

(b) R ist symmetrisch und

(c) 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. Das folgende Beispiel zeigt eine nicht-triviale Äquivalenz-Relation, die später noch eine wichtige Rolle spielen wird.

Beispiel: Wir betrachten die Menge $\mathbb{Z}$ der ganzen Zahlen zusammen mit der Relation $\approx_n$, die wir für natürliche Zahlen $n \in \mathbb{N}$ als

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

definieren. Wir zeigen, dass die Relation $\approx_n$ für $n \in \mathbb{N}$ eine Äquivalenz-Relation auf $\mathbb{Z}$ definiert.

(a) Um zu zeigen, dass $\approx_n$ reflexiv ist, müssen wir nachweisen, dass für alle $x \in \mathbb{Z}$ die Beziehung

$$\langle x, x \rangle \in \approx_n.$$

gilt. Nach Definition von $\approx_n$ ist dies äquivalent zu

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

Für eine vorgegebene Zahl x ist dies 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. $\surd$

(b) 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. Multiplizieren wir diese Gleichung mit -1, so erhalten wir

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

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

(c) 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. Wir müssen zeigen, dass $\langle x, z \rangle \in \approx_n$ gilt. Dazu müssen wir zeigen, dass es ein $k_3 \in \mathbb{Z}$ gibt, so dass

$$k_3 \cdot n = x - z$$

gilt. Addieren wir die beiden Gleichungen für $x - y$ und $y - z$, so sehen wir, dass

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

gilt. Definieren wir $k_3 := k_1 + k_2$, so gilt also $k_3 \cdot n = x - z$ und damit haben wir

$$\langle x, z \rangle \in \approx_n$$

nachgewiesen und folglich die Transitivität von $\approx_n$ gezeigt. $\surd$ □

Aufgabe 12: Beweisen Sie, dass für alle ganzen Zahlen x und y die Beziehung

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

gilt. ◇

Aufgabe 13: Auf der Menge $\mathbb{N} \times \mathbb{N}$ definieren wir eine Relation R wie folgt:

$$R := \{ \big\langle \langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \big\rangle \in (\mathbb{N} \times \mathbb{N})^2 \mid x_1 + y_2 = x_2 + y_1 \}$$

Zeigen Sie, dass R dann eine Äquivalenz-Relation ist. ◇

Satz 3.24 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 der Reihe nach die Reflexivität, Symmetrie und Transitivität der Relation R_f nach:

(a) R_f ist reflexiv, denn es gilt

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

Daraus folgt sofort

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

(b) Um die Symmetrie von R_f nachzuweisen, müssen wir

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

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

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

(c) Um die Transitivität von R_f nachzuweisen, müssen wir

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

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

$$\langle x, z \rangle \in R_f. \; \surd$$

□

Bemerkung: Ist $f : M \to N$ 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 in einer Aufgabe gezeigt, dass für alle $x, y \in \mathbb{Z}$

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

gilt. ◇

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

$$sb : M \to S$$

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

Definition 3.25 (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 3.26 (Charakterisierung der Äquivalenz-Klassen)
Ist $R \subseteq M \times M$ eine Äquivalenz-Relation, so gilt:

(a) $\forall x \in M : x \in [x]_R$,

(b) $\forall x, y \in M : \big(x\,R\,y \rightarrow [x]_R = [y]_R\big)$,

(c) $\forall x, y \in M : \big(\neg x\,R\,y \rightarrow [x]_R \cap [y]_R = \emptyset\big)$.

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 derselben Reihenefolge wie oben angegeben.

(a) 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 $x\,R\,x$. Die Eigenschaft $x\,R\,x$ folgt aber unmittelbar aus der Reflexivität der Äquivalenz-Relation. $\surd$

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

1. 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.

2. 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.

Damit haben wir insgesamt die Gleichung $[x]_R = [y]_R$ gezeigt. $\surd$

(c) 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. $\surd$ □

Korollar 3.27 Aus dem letzten Satzes folgt sofort, dass

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

gilt. ◇

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

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

definieren. Das Korollar zum letzten 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 $R \subseteq M \times M$. ◇

Definition 3.28 (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 auf M 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 dieselbe Staatsbürgerschaft haben, so finden wir, dass die Äquivalenz-Klassen, die von dieser Äquivalenz-Relation erzeugt werden, gerade aus den Menschen besteht, die dieselbe Staatsbürgerschaft besitzen. ◇

Definition 3.29 (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 $\mathcal{P}$ die folgenden Eigenschaften hat:

(a) *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.

(b) *Separations-Eigenschaft*

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

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

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

Bemerkung: Der letzte Satz (Satz 3.26) 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 3.30 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.

(a) 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 $\mathcal{P}$. $\surd$

(b) 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

$$y \,R\, x. \;\surd$$

(c) Transitivität: Zu zeigen ist

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

Wir nehmen also an, dass

$$x \,R\, y \wedge y \,R\, z$$

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 $x \,R\, z$. $\surd$ □

3.17 Partielle und totale Ordnungen

In dem letzten Abschnitt dieses Kapitels definieren wir Ordnungs-Relationen. Darunter verstehen wir Relationen, die sich ähnlich verhalten wie die Relation $\leq$ auf den Zahlen.

Definition 3.31 (partielle Ordnung) Eine Relation $R \subseteq M \times M$ ist eine *partielle Ordnung (im Sinne von $\leq$) auf M* genau dann, wenn die Relation R

(a) reflexiv,

(b) anti-symmetrisch und

(c) transitiv ist.

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

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

gilt. ◇

Bemerkung: Eine totale Ordnung wird gelegentlich auch als *lineare Ordnung* bezeichnet. ◇

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.

(a) Reflexivität: Zu zeigen ist

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

Nach Definition der Relation `div` ist das äquivalent zu

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

Wir müssen also ein k finden, so dass die Gleichung $k \cdot x = x$ gilt. Setzen wir $k = 1$, so ist diese Gleichung sicher erfüllt und damit ist die Reflexivität gezeigt. $\surd$

(b) 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

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

Da x und y als natürliche Zahlen von 0 verschieden sind, muss dannn

$$k_1 \cdot k_2 = 1$$

gelten. Da aus $k_1 \cdot k_2 = 1$ sofort $k_1 = 1$ und $k_2 = 1$ folgt, denn auch k_1 und k_2 sind ja natürliche Zahlen, können wir wegen der ursprünglichen Gleichungen $k_1 \cdot x = y$ und $k_2 \cdot y = x$ sofort auf $x = y$ schließen. Damit ist die Anti-Symmetrie gezeigt. $\surd$

(c) 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

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

Damit haben wir die Transitivität nachgewiesen. $\surd$

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

Aufgabe 14: Auf der Menge der natürlichen Zahlen $\mathbb{N}$ definieren wir die Relation $\leq$ wie folgt:

$$\leq := \big\{ \langle x, y \rangle \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N}_0 : x + k = y \big\}.$$

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

Aufgabe 15: 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. ◇

Aufgabe 16: Auf der Menge $\mathbb{N} \times \mathbb{N}$ definieren wir die Relation $\sqsubseteq$ durch die Festlegung

$$\langle x_1, y_1 \rangle \sqsubseteq \langle x_2, y_2 \rangle \quad \text{g.d.w.} \quad x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \leq y_2).$$

Zeigen Sie, dass $\sqsubseteq$ eine totale Ordnung auf $\mathbb{N} \times \mathbb{N}$ ist. ◇

Wir schließen damit den theoretischen Teil unseres Ausflugs in die Mengenlehre und verweisen für weitere Details auf die Literatur, wobei ich Ihnen hier besonders das Buch von Seymour Lipschutz [Lip98] empfehlen möchte.

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 *mathematische Logik* zuständig, die ein Teil der Informatik-Vorlesung ist. Wir wenden uns hier den praktischen Beweis-Verfahren zu. Grob können wir zwischen vier Arten von Beweisen unterscheiden:

(a) direkten Beweisen,

(b) indirekten Beweisen,

(c) Beweise durch Fallunterscheidung,

(d) Beweise 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 4.1 (Pythagoreische Tripel)
Ein Tripel $\langle x, y, z\rangle \in \mathbb{N}\times\mathbb{N}\times\mathbb{N}$ heißt *Pythagoreisches 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 pythagoreisches Tripel, denn es gilt

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

Satz 4.2 Es seien u und v positive natürliche Zahlen mit $u > v$. Dann ist

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

ein pythagoreisches 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. □

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, wobei $k \in \mathbb{N}_0$ ist.

Lemma 4.3 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

$$p = 2 \cdot q + 1 \quad \text{mit} \quad q \in \mathbb{N}_0$$

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 4.4 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 4.3 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 4.5 (Abzählbar)
Eine unendliche Menge M heißt *abzählbar unendlich*, wenn eine surjektive Funktion

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

existiert. Zur Erinnerung: Eine Funktion $f : A \to B$ ist *surjektiv* genau dann, wenn es zu jedem $y \in B$ ein $x \in A$ gibt, so dass $f(x) = y$ ist.

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

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

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.

(a) $n \,\%\, 2 = 1$: Dann ist n ungerade, also ist $(n-1)$ gerade und die Division $(n-1)/2$ liefert eine ganze Zahl.

(b) $n \,\%\, 2 = 0$: In diesem Fall ist n gerade. Damit ist auch $(n-2)$ 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:

(a) Fall: $z > 0$.

Wir definieren $n := 2 \cdot (z-1) + 1$. Wegen $z > 0$ gilt $n > 0$ 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 $f(n) = z$.

(b) Fall: $z \leq 0$.

Wir definieren $n := -2 \cdot (z-1)$. Wegen $z \leq 0$ ist klar, dass n eine gerade natürliche Zahl ist. Damit haben wir

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

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

Satz 4.7 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 nach unserer Annahme 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 17: Zeigen Sie, dass das Intervall

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

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

$$x = 0,d_1d_2d_3\cdots \qquad \text{mit } d_i \in \{0,\cdots,9\} \text{ für alle } i \in \mathbb{N}$$

dargestellt sind, es gilt dann also

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

Um sicher zu stellen, dass diese Darstellung eindeutig ist, fordern wir, dass diese Darstellung nicht auf "Periode Neun" endet, es dürfen also ab einem bestimmten Index $n \in \mathbb{N}$ nicht alle Ziffern d_i den Wert 9 haben:

$$\neg\exists n \in \mathbb{N} : \forall i \in \mathbb{N} : i \geq n \rightarrow c_i = 9.$$

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

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

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

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

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

$$c = 0,c_1c_2c_3\cdots$$

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

Aufgabe 18: Zeigen Sie, dass die Menge

$$\mathbb{N}^{\mathbb{N}} := \{f \mid f : \mathbb{N} \rightarrow \mathbb{N}\},$$

also die Menge aller Funktionen von $\mathbb{N}$ nach $\mathbb{N}$ überabzählbar ist. ◇

Aufgabe 19: Zeigen Sie, dass die Menge $\mathbb{Q}_+$ der positiven rationalen Zahlen abzählbar ist. ◇

4.3 Beweise durch Fallunterscheidung

Wir haben in dem Kapitel über Mengenlehre bereits eine ganze Reihe direkter Beweise gesehen. Dort war es oft notwendig, den Beweis in zwei Teile aufzuspalten. Um beispielsweise die Gleichheit zweier Mengen A und B zu zeigen, sind wir häufig so vorgegangen, dass wir zunächst $A \subseteq B$ und anschließend $B \subseteq A$ gezeigt haben. So hatten wir beispielsweise 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. Beim Beweis durch *Fallunterscheidung* teilen wir den Beweis ebenfalls in mehrere Teile auf. Wir illustrieren das Konzept an einem Beispiel.

Satz 4.8 Es gibt irrationale Zahlen x und y, so dass x^y rational ist, es gilt also

$$\exists x,y \in \mathbb{R} : x \notin \mathbb{Q} \wedge y \notin \mathbb{Q} \wedge x^y \in \mathbb{Q}.$$

Beweis: Im letzten Abschnitt haben wir bereits gezeigt, dass die Zahl $\sqrt{2}$ irrational ist. Wir betrachten nun die Zahl

$$\sqrt{2}^{\sqrt{2}}.$$

Es gibt nur zwei Möglichkeiten: Entweder ist die Zahl $\sqrt{2}^{\sqrt{2}}$ rational oder nicht. Wir untersuchen diese beiden Fälle getrennt.

(a) Fall: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.

In diesem Fall definieren wir

$$x := \sqrt{2} \quad \text{und} \quad y := \sqrt{2}.$$

Da wir bereits wissen, dass $\sqrt{2} \notin \mathbb{Q}$ ist, und da nach der Voraussetzung der Fallunterscheidung $x^y \in \mathbb{Q}$ gilt, haben wir in diesem Fall bereits Zahlen x und y mit der behaupteten Eigenschaft gefunden.

(b) Fall: $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$.

In diesem Fall definieren wir

$$x := \sqrt{2}^{\sqrt{2}} \quad \text{und} \quad y := \sqrt{2}.$$

Jetzt ist x nach der Voraussetzung der Fallunterscheidung irrational und dass y irrational ist, haben wir bereits früher bewiesen. Außerdem gilt

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2 \in \mathbb{Q},$$

so dass die Behauptung auch im zweiten Fall bewiesen ist. □

Beachten Sie, dass es uns bei dem letzten Beweis nicht möglich war, die Zahlen x und y konkret anzugeben. Wir wissen nur, dass entweder die beiden Zahlen

$$x_1 := \sqrt{2} \text{ und } y_1 := \sqrt{2} \quad \text{oder} \quad \text{die Zahlen } x_2 := \sqrt{2}^{\sqrt{2}} \text{ und } y_2 := \sqrt{2}.$$

die behauptete Eigenschaft

$$x \notin \mathbb{Q} \wedge y \notin \mathbb{Q} \wedge x^y \in \mathbb{Q}$$

haben, aber der obige Beweis sagt nichts darüber, welches der beiden Paare $\langle x_1, y_1 \rangle$ und $\langle x_2, y_2 \rangle$ tatsächlich die obige Eigenschaft hat. Das war für den gerade angegebenen Beweis auch nicht erforderlich: Wir haben nur gezeigt, dass es ein Paar $\langle x, y \rangle$ mit der Eigenschaft

$$x \notin \mathbb{Q} \wedge y \notin \mathbb{Q} \wedge x^y \in \mathbb{Q}$$

geben muss, aber wir waren nicht in der Lage, x und y konkret auszurechnen. Daher ist der obige Beweis kein *konstruktiver* Beweis: Zwar zeigt der Beweis die Existenz eines Paares $\langle x, y \rangle$ mit den gewünschten Eigenschaften, aber das Paar $\langle x, y \rangle$ kann nicht konkret angegeben werden.

Bemerkung: Aus dem Gelfond-Schneider-Theorem kann gefolgert werden, dass $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ gilt. Der Nachweis dieses Theorem liegt aufgrund seiner Tiefe deutlich außerhalb des Rahmens einer einführenden Mathematik-Vorlesung.

Aufgabe 20: Zeigen Sie, dass für alle $n \in \mathbb{N}$ die Zahl

$$5 \cdot n^3 + 10 \cdot n$$

stets durch 3 teilbar ist. ◇

4.4 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.

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

Dieser Schritt wird als *Induktions-Anfang* bezeichnet.

(b) Dann zeigen wir, dass die Formel

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

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 $F(1)$ gilt, nach dem Induktions-Schritt gilt dann auch $F(2)$, daraus folgt dass auch $F(3)$ gilt, woraus wir auf die Gültigkeit von $F(4)$ 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 4.9 Es sei $F(x)$ eine Formel. Dann gilt

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

Beweis: Wir nehmen an, dass

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

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 $F(1)$ gilt, dass $n_0 \neq 1$ ist. Aus $n_0 - 1 < n_0$ folgt nun, dass

$$F(n_0 - 1)$$

gilt. Aus der Formel $\forall n \in \mathbb{N} : F(n) \rightarrow F(n+1)$ 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. Die in diesen Sätzen behaupteten Summenformeln sollten Sie sich gut merken, denn diese Formeln werden bei der Analyse der Komplexität von Algorithmen häufig verwendet.

Satz 4.10 Es gilt

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

Beweis: Wir führen den Beweis durch Induktion nach n.

(a) Induktions-Anfang: $n = 1$.

Wir haben einerseits

$$\sum_{i=1}^{1} i = 1$$

und andererseits gilt auch

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

Damit ist die Behauptung für $n = 1$ richtig.

(b) Induktions-Schritt: $n \mapsto n+1$.

Wir können nun voraussetzen, dass

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

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

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

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

$$\begin{aligned}
& \sum_{i=1}^{n+1} i \\
= \; & \sum_{i=1}^{n} i + (n+1) && \text{nach Definition der Summe} \\
= \; & \frac{1}{2} \cdot n \cdot (n+1) + (n+1) && \text{nach Induktions-Voraussetzung} \\
= \; & \frac{1}{2} \cdot \big(n^2 + n + 2 \cdot (n+1)\big) && \text{Hauptnenner} \\
= \; & \frac{1}{2} \cdot \big(n^2 + 3 \cdot n + 2\big)
\end{aligned}$$

Nun formen wir die rechte Seite um:

$$\begin{aligned} & \frac{1}{2} \cdot (n+1) \cdot \big((n+1)+1\big) \\ = \quad & \frac{1}{2} \cdot (n+1) \cdot (n+2) \\ = \quad & \frac{1}{2} \cdot (n^2 + 2 \cdot n + n + 2) \\ = \quad & \frac{1}{2} \cdot (n^2 + 3 \cdot n + 2) \end{aligned}$$

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

Aufgabe 21: Zeigen Sie, dass

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

gilt. ◇

Aufgabe 22: Zeigen Sie, dass im Falle $q \neq 1$

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1} \quad \text{für alle } n \in \mathbb{N}_0$$

gilt. Wie lautet die Formel im Falle $q = 1$? ◇

Satz 4.11 (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:

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

(a) 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

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

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

Aufgabe 23: Zeigen Sie, dass jede natürliche Zahl $n \geq 2$ entweder eine Primzahl ist oder aber sich als Produkt von zwei oder mehr Primzahlen darstellen lässt. ◇

Aufgabe 24: Es sei $x \in \mathbb{R}$. Zeigen Sie, dass für alle positiven natürlichen Zahlen die Ungleichung

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

gilt. ◇

Aufgabe 25: Zeigen Sie, dass die Zahl $2^{2 \cdot n} - 1$ für alle positiven natürlichen Zahlen n durch 3 teilbar ist, ◇

Aufgabe 26: Ein *Triomino* ist eine Figur, die aus einem Quadrat der Länge 2 dadurch entsteht, dass in einer der Ecken des ursprünglich gegebenen Quadrates der Länge 2 ein Quadrat der Länge 1 ausgeschnitten ist. Abbildung 4.1 zeigt ein Triomino, bei dem die rechte obere Ecke ausgeschnitten ist. Beweisen Sie, dass Sie ein Schachbrett, bei dem eines der Eckfelder ausgeschnitten ist, vollständig so durch Triominos so überdecken können, dass die einzelnen Triominos sich nicht überlappen. Dabei ist vorausgesetzt, dass die einzelnen Felder des Schachbretts Quadrate der Länge 1 sind.

Abbildung 4.1: Ein Triomino.

Hinweis 1: Beim Beweis einer mathematischen Behauptung ist es manchmal einfacher, zunächst ein Ergebnis zu beweisen, was allgemeiner ist als die eigentlich zu beweisende Behauptung. Das mag zwar kontraintuitiv erscheinen, weil Sie dann ja offensichtlich mehr beweisen müssen, aber dieses Beispiel soll Ihnen zeigen, dass es tatsächlich Fälle gibt, wo Sie das Problem am einfachsten durch Verallgemeinerung lösen können.

Hinweis 2: Um diese Aufgabe lösen zu können, müssen Sie kein Schachspieler sein. Für den Zweck der Aufgabe reicht es zu wissen, dass ein Schachbrett ein Quadrat der Länge 8 ist (was immer dabei die Längeneinheit ist), das in 8×8 Quadrate der Länge 1 unterteilt ist. ◇

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. Die Theorie der Gruppen ist ursprünglich aus dem Bestreben entstanden, Formeln für die Nullstellen von beliebigen Polynomen zu finden. Später hat die Gruppentheorie auch in anderen Gebieten der Mathematik, Physik und Informatik zahlreiche Anwendungen gefunden. Wir werden die Definition einer Gruppe später bei der Definition eines Vektorraums benötigen, denn ein Vektorraum ist eine kommutative Gruppe, für die zusätzlich eine Skalar-Multiplikation definiert ist.

5.1 Die Definition der Gruppe

Definition 5.1 (Gruppe) Ein Tripel $\langle G, e, \circ \rangle$ heißt *Gruppe* falls folgendes gilt:

(a) G ist eine Menge.

(b) e ist ein Element der Menge G.

(c) $\circ$ 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.

(d) 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.

(e) 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.

(f) 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.

(a) $\langle \mathbb{Z}, 0, + \rangle$ ist eine kommutative Gruppe, denn es gilt:

1. $0 + x = x$ für alle $x \in \mathbb{Z}$.
2. $-x + x = 0$ für alle $x \in \mathbb{Z}$,
   und damit ist die Zahl $-x$ das *Links-Inverse* der Zahl x bezüglich der Addition.
3. $(x + y) + z = x + (y + z)$ für alle $x, y, z \in \mathbb{Z}$.
4. $x + y = y + x$ 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.

(b) 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:

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

(c) 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:

1. $(e \circ e) \circ e = e \circ e = e$ und $e \circ (e \circ e) = e \circ e = e$. ✓
2. $(e \circ e) \circ a = e \circ a = a$ und $e \circ (e \circ a) = e \circ a = a$. ✓
3. $(e \circ a) \circ e = a \circ e = a$ und $e \circ (a \circ e) = e \circ a = a$. ✓
4. $(e \circ a) \circ a = a \circ a = e$ und $e \circ (a \circ a) = e \circ e = e$. ✓
5. $(a \circ e) \circ e = a \circ e = a$ und $a \circ (e \circ e) = a \circ e = a$. ✓
6. $(a \circ e) \circ a = a \circ a = e$ und $a \circ (e \circ a) = a \circ a = e$. ✓

7. $(a \circ a) \circ e = e \circ e = e$ und $a \circ (a \circ e) = a \circ a = e$. ✓
8. $(a \circ a) \circ a = e \circ a = a$ 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 Kapitel zur 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 5.2 (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 5.3 (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. "*rechts*" weg.

Satz 5.4 (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 5.5 (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

$$^{-1} : G \to G$$

definieren, die für alle $a \in G$ das zu a inverse Element berechnet: Es gilt also

$$a^{-1} \circ a = e \quad \text{und} \quad a \circ a^{-1} = e \quad \text{für alle } a \in G.$$

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 5.6 ($(a \circ b)^{-1} = b^{-1} \circ a^{-1}$)
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

$$\begin{array}{lcll}
(b^{-1} \circ a^{-1}) \circ (a \circ b) & = & b^{-1} \circ \big(a^{-1} \circ (a \circ b)\big) & \text{Assoziativ-Gesetz} \\
& = & b^{-1} \circ \big((a^{-1} \circ a) \circ b\big) & \text{Assoziativ-Gesetz} \\
& = & b^{-1} \circ (e \circ b) & \\
& = & b^{-1} \circ b & \\
& = & e &
\end{array}$$

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

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$ □

Satz 5.7 ($(a^{-1})^{-1} = a$) 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 $(a^{-1})^{-1} = a$. □

Definition 5.8 (Halb-Gruppe) Eine Paar $\langle G, \circ \rangle$ ist eine *Halb-Gruppe*, falls gilt:

(a) G ist eine Menge,

(b) $\circ$ 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.

(c) 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:

(a) Das Paar $\langle \mathbb{N}, + \rangle$ ist eine Halb-Gruppe.

(b) 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 5.9 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

$$\begin{array}{lcll} e \circ a & = & e \circ (b \circ c) & \text{wegen } b \circ c = a \\ & = & (e \circ b) \circ c & \text{Assoziativ-Gesetz} \\ & = & b \circ c & \text{wegen } e \circ b = b \\ & = & a & \text{wegen } b \circ c = a. \end{array}$$

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 5.10 (injektiv) Eine Funktion $f : M \to N$ 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 5.11 (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 5.12 (bijektiv)
Eine Funktion $f : M \rightarrow N$ ist *bijektiv* genau dann, wenn f sowohl injektiv als auch surjektiv ist.

Satz 5.13 Es sei M eine endliche Menge und die Funktion

$$f : M \rightarrow M$$

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 27: Es sei M eine endliche Menge und die Funktion

$$f : M \rightarrow M$$

sei surjektiv. Zeigen Sie, dass f dann auch injektiv ist.

Satz 5.14 Es sei $\langle G, \circ \rangle$ eine endliche Halb-Gruppe, in der die beiden Kürzungs-Regeln

$$a \circ c = b \circ c \rightarrow a = b \quad \text{und} \quad c \circ a = c \circ b \rightarrow a = b$$

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

$$a \circ x = b \quad \text{und} \quad y \circ a = b$$

Lösungen haben, denn dann folgt die Behauptung aus Satz 5.9. Zunächst definieren wir für jedes $a \in G$ eine Funktion

$$f_a : G \rightarrow G \quad \text{durch} \quad f_a(x) := a \circ x.$$

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 $\mathcal{S}_n$

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:

(a) Die Relation R ist links-total auf $\mathbb{Z}_n^+$:

$$\forall x \in \mathbb{Z}_n^+ : \exists y \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R.$$

(b) Die Relation R ist rechts-total auf $\mathbb{Z}_n^+$:

$$\forall y \in \mathbb{Z}_n^+ : \exists x \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R.$$

(c) 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 $\mathcal{S}_n$ als die Menge aller Permutationen auf der Menge $\mathbb{Z}_n^+$:

$$\mathcal{S}_n := \{R \subseteq \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid R \text{ ist Permutation auf } \mathbb{Z}_n^+\}.$$

Weiter definieren wir die identische Permutation E_n auf $\mathbb{Z}_n^+$ als

$$E_n := \{\langle x, x\rangle \mid x \in \mathbb{Z}_n^+\}.$$

Wir erinnern an die Definition des relationalen Produkts, es gilt:

$$R_1 \circ R_2 := \{\langle x, z\rangle \mid \exists y \in \mathbb{Z}_n^+ : \langle x, y\rangle \in R_1 \wedge \langle y, z\rangle \in R_2\}.$$

Die entscheidende Beobachtung ist nun, dass $R_1 \circ R_2$ eine Permutation ist, wenn R_1 und R_2 bereits Permutationen sind.

Aufgabe 28: Beweisen Sie

$$\forall R_1, R_2 \in \mathcal{S}_n : R_1 \circ R_2 \in \mathcal{S}_n. \qquad \square$$

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

$$E_n \circ R = R \quad \text{für alle } R \in \mathcal{S}_n$$

gilt. Weiter sehen wir: Ist $R \in \mathcal{S}_n$, 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 $\langle \mathcal{S}_n, E_n, \circ\rangle$ eine Gruppe ist. Diese Gruppe trägt den Namen *Permutations-Gruppe*.

Aufgabe 29: Zeigen Sie, dass $\mathcal{S}_3$ keine kommutative Gruppe ist. Schreiben Sie dazu eine *SetlX*-Programm, dass zunächst die Menge $\mathcal{S}_3$ berechnet und anschließend überprüft, ob in dieser Menge das Kommutativ-Gesetz gilt.

5.3 Untergruppen und Faktor-Gruppen

Definition 5.15 (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:

(a) $\forall x, y \in U : x \circ y \in U$,

die Menge U ist also unter der Operation $\circ$ abgeschlossen.

(b) $e \in U$,

das neutrale Element der Gruppe G ist also auch ein Element der Menge U.

(c) Bezeichnen wir das zu $x \in G$ bezüglich der Operation $\circ$ inverse Element mit x^{-1}, so gilt

$$\forall x \in U : x^{-1} \in U,$$

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:

(a) 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:

1. Die Addition zweier gerader Zahlen liefert wieder eine gerade Zahl:
$$2 \cdot x + 2 \cdot y = 2 \cdot (x + y) \in 2\mathbb{Z}.$$
2. $0 \in 2\mathbb{Z}$, denn $0 = 2 \cdot 0 \in \mathbb{Z}$.
3. Das bezüglich der Addition inverse Element einer geraden Zahl ist offenbar wieder gerade, denn es gilt
$$-(2 \cdot x) = 2 \cdot (-x) \in 2\mathbb{Z}.$$

(b) 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.

(c) 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.

Aufgabe 30: Berechnen Sie alle Untergruppen der Gruppe $\langle \mathcal{S}_3, E_3, \circ \rangle$. ◇

Untergruppen sind interessant, weil sich mit ihrer Hilfe unter bestimmten Umständen neue Gruppen bilden lassen, sogenannte *Faktor-Gruppen*.

Definition 5.16 (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 5.17 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:

"$\Rightarrow$" : 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

$$a - b \in U. \ \checkmark$$

"$\Leftarrow$" : 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.

1. 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 $x \in b + U$.
2. 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 31: 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:

$$x \approx_U y \stackrel{\text{def}}{\iff} x - y \in U.$$

Zeigen Sie, dass $\approx_U$ eine Äquivalenz-Relation auf G ist. ◇

Lemma 5.18 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 5.19 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.

(a) $0 + U$ ist das links-neutrale Element, denn wir haben

$$(0 + U) + (a + U) = (0 + a) + U = a + U \quad \text{für alle } a \in G.$$

(b) $-a + U$ ist das links-inverse Element zu $a + U$, denn wir haben

$$(-a + U) + (a + U) = (-a + a) + U = 0 + U \quad \text{für alle } a \in G.$$

(c) 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

$$\mathbb{Z}_k = \big\{l + k\mathbb{Z} \mid l \in \{0, \cdots, k-1\}\big\}.$$

Aufgabe 32: Es sei $\langle G, e, \circ \rangle$ eine endliche kommutative Gruppe und es gelte $U \leq G$. Zeigen Sie, dass dann $\texttt{card}(U)$ ein Teiler von $\texttt{card}(G)$ ist. ◇

Hinweis: Zeigen Sie, dass alle Nebenklassen von G bezüglich der Untergruppe U dieselbe Kardinalität haben.

Aufgabe 33: Es seien $\langle G_1, e_1, \circ \rangle$ und $\langle G_2, e_2, * \rangle$ kommutative Gruppen. Eine Abbildung

$$f : G_1 \to G_2$$

ist ein *Gruppen-Homomorphismus* genau dann, wenn

$$f(x \circ y) = f(x) * f(y) \quad \text{f.a. } x, y \in G_1$$

gilt. Lösen Sie die folgenden Teilaufgaben:

(a) Zeigen Sie, dass die Menge

$$f^{-1}(e_2) := \{x \in G_1 \mid f(x) = e_2\}$$

eine Untergruppe von G_1 ist.

(b) Es sei $U \leq G_1$. Zeigen Sie, dass dann auch

$$f(U) := \{f(x) \mid x \in U\}$$

eine Untergruppe von G_2 ist. ◇

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 6.1 (Ring) Ein 4-Tupel $\mathcal{R} = \langle R, 0, +, \cdot \rangle$ ist ein *Ring*, falls gilt:

(a) $\langle R, 0, + \rangle$ ist eine kommutative Gruppe,

(b) $\cdot : R \times R \to R$ ist eine Funktion für welche die folgenden Gesetze gelten:

1. Assoziativ-Gesetz: Für alle $x, y, z \in R$ gilt
$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$
2. 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 $\mathcal{R} = \langle R, 0, e, +, \cdot \rangle$, wir geben die Eins also explizit in der Struktur an.

Bemerkung: Bevor wir Beispiele betrachten, bemerken wir einige unmittelbare Konsequenzen der obigen Definition.

(a) 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 $0 \cdot x$ abziehen, dann erhalten wir die Gleichung

$$0 = 0 \cdot x.$$

Genauso gilt natürlich auch $x \cdot 0 = 0$.

(b) 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 $-(x \cdot y) = (-x) \cdot y$ ist, 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:

(a) Die Struktur $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ ist ein kommutativer Ring mit Eins.

(b) Die Struktur $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ ist ebenfalls ein kommutativer Ring mit Eins.

In dieser Vorlesung werden wir nur solche Ringe betrachten, die erstens kommutativ sind und zweitens eine Eins haben. Ein wichtiger Spezialfall ist der Fall eines kommutativen Rings $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ mit Eins, für den 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 6.2 (Körper) Ein 5-Tupel $\mathcal{K} = \langle K, 0, 1, +, \cdot \rangle$ ist ein *Körper*, falls gilt:

(a) $\langle K, 0, + \rangle$ ist eine kommutative Gruppe,

(b) $\langle K \backslash \{0\}, 1, \cdot \rangle$ ist ebenfalls eine kommutative Gruppe,

(c) Es gilt das Distributiv-Gesetz: Für alle $x, y, z \in K$ haben wir

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

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 $\mathcal{R}$ so zu einem Körper $\mathcal{K} = \langle K, 0, 1, +_4, \cdot_4 \rangle$ zu erweitern, dass $\{0, 1, 2, 3\} \subseteq K$ gelten würde, so müsste die 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 Widerspruch zeigt, dass sich der Ring $\mathcal{R}$ sicher nicht zu einem Körper erweitern lässt.

Definition 6.3 (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 nennen wir dann $\sim$ eine *Kongruenz-Relation* auf R. Die formale Definition folgt.

Definition 6.4 (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:

(a) $\forall a_1, a_2, b_1, b_2 \in R : \big(a_1 \sim a_2 \wedge b_1 \sim b_2 \rightarrow a_1 + b_1 \sim a_2 + b_2\big)$,
die Relation $\sim$ ist also *verträglich* mit der Addition auf R.

(b) $\forall a_1, a_2, b_1, b_2 \in R : \big(a_1 \sim a_2 \wedge b_1 \sim b_2 \rightarrow a_1 \cdot b_1 \sim a_2 \cdot b_2\big)$,
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 3.26 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 3.26

$$[a_1 + b_1]_\sim = [a_2 + b_2]_\sim.$$

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 6.5 (Faktor-Ring) Ist $\mathcal{R} = \langle R, 0, 1, +, \cdot \rangle$ ein kommutativer Ring mit Eins und ist $\sim$ eine Kongruenz-Relation auf diesem Ring, so ist die Struktur $\mathcal{R}/\!\sim = \langle R/\!\sim, [0]_\sim, [1]_\sim, +, \cdot \rangle$ mit den oben für Äquivalenz-Klassen definierten Operationen $+$ und $\cdot$ ein kommutativer Ring mit Eins.

Beweis: Wir weisen die Eigenschaften, die einen Ring auszeichnen, einzeln nach.

(a) Für die Operation "+" gilt das Assoziativ-Gesetz, denn für alle $[a]_\sim, [b]_\sim, [c]_\sim \in R/\!\sim$ gilt

$$\begin{aligned}
[a]_\sim + \big([b]_\sim + [c]_\sim\big) &= [a]_\sim + [b+c]_\sim \\
&= [a + (b+c)]_\sim \\
&= [(a+b) + c]_\sim \\
&= [a+b]_\sim + [c]_\sim \\
&= \big([a]_\sim + [b]_\sim\big) + [c]_\sim.
\end{aligned}$$

(b) Für die Operation "+" gilt das Kommutativ-Gesetz, denn für alle $[a]_\sim, [b]_\sim \in R/\sim$ gilt

$$[a]_\sim + [b]_\sim = [a+b]_\sim = [b+a]_\sim = [b]_\sim + [a]_\sim.$$

(c) $[0]_\sim$ ist das neutrale Element bezüglich der Addition, denn für alle $[a]_\sim \in R/\sim$ gilt

$$[a]_\sim + [0]_\sim = [a+0]_\sim = [a]_\sim.$$

(d) 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

$$[a]_\sim + [-a]_\sim = [a + -a]_\sim = [0]_\sim.$$

(e) 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.

(f) 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. □

Aufgabe 34: Es sei $\mathcal{K} = \langle K, 0_K, 1_K, +, \cdot\rangle$ ein Körper und die Menge K sei endlich. Dann können wir durch eine Funktion

$$\texttt{count} : \mathbb{N} \to K$$

definieren, welche die natürlichen Zahlen $\mathbb{N}$ in den Körper K abbildet. Die Definition von `count` erfolgt durch Induktion:

I.A.: $n = 0$:

$\texttt{count}(0) := 0_K$.

Beachten Sie hier, dass die 0, die auf der linken Seite dieser Gleichung auftritt, eine natürliche Zahl ist, während die 0_K auf der rechten Seite dieser Gleichung das neutrale Element der Addition in dem Körper $\mathcal{K}$ bezeichnet.

I.S.: $n \mapsto n+1$.

$\texttt{count}(n+1) := \texttt{count}(n) + 1_K$.

Auch hier bezeichnet die 1 auf der linken Seite der Definition eine natürliche Zahl, während die 1_K auf der rechten Seite dieser Gleichung das neutrale Element der Multiplikation in dem Körper $\mathcal{K}$ bezeichnet.

Falls die Menge K endlich ist, definieren wir die *Charakteristik* $\texttt{char}(\mathcal{K})$ des Körpers $\mathcal{K}$ als die kleinste natürliche Zahl k, für die $\texttt{count}(k) = 0_K$ gilt:

$$\texttt{char}(\mathcal{K}) = \min\bigl(\{k \in \mathbb{N} \mid k \geq 1 \wedge \texttt{count}(k) = 0_K\}\bigr).$$

Zeigen Sie, dass die Charakteristik eines endlichen Körpers immer eine Primzahl ist.

Aufgabe 35:

(a) Zeigen Sie, dass es einen Körper K mit drei Elementen gibt.

(b) Zeigen Sie, dass es einen Körper K mit vier Elementen gibt. ◇

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

$$Q := \bigl\{\langle x, y\rangle \in R \times R \mid y \neq 0\bigr\}$$

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:

$$\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle \stackrel{\text{def}}{\Longleftrightarrow} x_1 \cdot y_2 = x_2 \cdot y_1.$$

Satz 6.6 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 $\sim$:

   $$\begin{array}{ll} & \langle x, y\rangle \sim \langle x, y\rangle \\ \Leftrightarrow & x \cdot y = x \cdot y. \end{array}$$

   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 $+ : Q \times Q \rightarrow Q$ 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:

$$\begin{aligned}
& \langle x_1, y_1\rangle + \langle x_2, y_2\rangle \\
= \;& \langle x_1 \cdot y_2 + x_2 \cdot y_1, y_1 \cdot y_2\rangle \\
= \;& \langle x_2 \cdot y_1 + x_1 \cdot y_2, y_2 \cdot y_1\rangle \\
= \;& \langle x_2, y_2\rangle + \langle x_1, y_1\rangle.
\end{aligned}$$

   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.

   Aufgabe 36: Zeigen Sie, dass in $Q/\sim$ für die Multiplikation sowohl das Assoziativ-Gesetz als auch das Kommutativ-Gesetz gilt.

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 $\mathcal{R}$ 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 6.7 (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
   1. $0 \in 2\mathbb{Z}$, da $0 = 2 \cdot 0$ ist und somit ist 0 eine gerade Zahl.
   2. 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.
   3. 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.
   4. 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.
   1. $0 \in \mathit{gen}(k)$, da $0 = k \cdot 0$ gilt.
   2. 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 $a + b \in \mathit{gen}(k)$.
   3. Ist $a \in \mathit{gen}(k)$, so gibt es ein $x \in R$ mit $a = k \cdot x$. Dann gilt
   $$-a = -(k \cdot x) = k \cdot (-x) \in \mathit{gen}(a).$$
   4. 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 6.5 auf Seite 71) 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 6.8 (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 6.9 (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 (3.26 auf Seite 38) 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. □

Aufgabe 37: Es seien $a, b \in \mathbb{N}$ mit $0 < a < b$ und die Zahlen a, b seien teilerfremd, es gelte also $\texttt{ggt}(a, b) = 1$. Zeigen Sie durch Induktion über $b \in \mathbb{N}$, dass

$$\exists k, l \in \mathbb{Z} : k \cdot a + l \cdot b = 1$$

gilt.

Hinweis: Im Induktions-Schritt ist es nicht sinnvoll, von b auf $b + 1$ zu schließen. Statt dessen sollten Sie im Induktions-Schritt versuchen, die Behauptung für b aus der Tatsache zu folgern, dass die Behauptung für sowohl für $b - a$ als auch für a gilt. ◇

Bemerkung: Beim Beweis einer Behauptung, die für natürliche Zahlen gezeigt werden soll, hilft es manchmal, die Behauptung zunächst für kleine Zahlen zu überprüfen, denn das liefert oft eine Idee für den allgemeinen Fall.

Aufgabe 38: Wir betrachten den Ring der ganzen Zahlen $\mathbb{Z}$. Es sei $p \in \mathbb{Z}$ und wir definieren die Menge $p\mathbb{Z}$ als

$$p\mathbb{Z} := \{k \cdot p \mid k \in \mathbb{Z}\}.$$

Zeigen Sie, dass die Menge $p\mathbb{Z}$ genau dann ein maximales Ideal in dem Ring $\mathbb{Z}$ ist, wenn p eine Primzahl ist.

Hinweis: Um zu zeigen, dass für eine Primzahl p die Menge $p\mathbb{Z}$ ein maximales Ideal ist, ist es sinnvoll anzunehmen, dass es ein Ideal I gibt, so dass

$$p\mathbb{Z} \subseteq I \quad \text{und} \quad I \neq p\mathbb{Z}$$

gilt. Sie müssen zeigen, dass in diesem Fall $I = \mathbb{Z}$ ist und dazu reicht es zu zeigen, dass $1 \in I$ ist. Um diesen Nachweis zu führen, betrachten Sie die kleinste natürliche Zahl $r \in I \backslash p\mathbb{Z}$ und wenden anschließend auf r und p den in der vorhergehenden Aufgabe gezeigten Satz an. ◇

Aufgabe 39: Zeigen Sie, dass der Faktor-Ring $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ genau dann ein Körper ist, wenn p eine Primzahl 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 7.1 (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 $\texttt{gt(a,b)}$. 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 7.2 (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. □

Aufgabe 40: 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 3.16 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 7.3 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. "⇒": 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 7.2) gemachten Eindeutigkeits-Aussage, dass

   $$a \,\%\, n = b \,\%\, n$$

   gilt. ✓

2. "⇐": 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 7.4 Die Relation $\approx_n$ ist eine Kongruenz-Relation.

Beweis: Es gilt

$$\begin{aligned} & x \approx_n y \\ \Leftrightarrow \quad & \exists k \in \mathbb{Z} : x - y = k \cdot n \\ \Leftrightarrow \quad & x - y \in n\mathbb{Z} \\ \Leftrightarrow \quad & x \sim_{n\mathbb{Z}} y \end{aligned}$$

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 7.5 ($\mathbb{Z}$ 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 7.6 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 7.7 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 7.8 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 7.9 (Lemma von Bézout) Es seien $a, b \in \mathbb{N}$. Dann existieren $x, y \in \mathbb{Z}$, so dass

$$\mathit{ggt}(a, b) = x \cdot a + y \cdot b$$

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

$$d \,|\, a \quad \text{und} \quad d \,|\, b.$$

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:

$$e \,|\, a \quad \text{und} \quad e \,|\, b.$$

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

$$e \,|\, d$$

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 91 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 7.10 Sind $x, y \in \mathbb{Z}$, so gilt für alle $n \in \mathbb{N}_1$

$$x \,\%\, n = 0 \wedge y \,\%\, n = 0 \;\leftrightarrow\; (x + y) \,\%\, n = 0 \wedge y \,\%\, n = 0.$$

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 7.11 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 7.12 (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:

$$\forall x,y \in \mathbb{N} : \texttt{ggtS}(x,y) = ggt(x,y).$$

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

   $$ggt(x,y) = ggt(x,x) = x,$$

   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 $y < x$.

   1. $x < y$: In diesem Fall sagt die Induktions-Voraussetzung, dass das Ergebnis des rekursiven Aufrufs der Funktion $\texttt{ggtS}()$ korrekt ist, wir dürfen also voraussetzen, dass

      $$\texttt{ggtS}(x,y-x) = ggt(x,y-x)$$

      gilt. Zu zeigen ist

      $$\texttt{ggtS}(x,y) = ggt(x,y).$$

      Der Nachweis verläuft wie folgt:

      $$\begin{array}{rcll}
      \texttt{ggtS}(x,y) & = & \texttt{ggtS}(x,y-x) & \text{(nach Definition von } \texttt{ggtS}(x,y)) \\
      & \overset{IV}{=} & ggt(x,y-x) & \\
      & = & ggt(y-x,x) & \text{(denn } ggt(a,b) = ggt(b,a)) \\
      & = & ggt\big((y-x)+x,x\big) & \text{(nach Korollar 7.11)} \\
      & = & ggt(y,x) & \\
      & = & ggt(x,y) &
      \end{array}$$

      und das war zu zeigen.

   2. $y < x$: 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 7.13 Für $x, y \in \mathbb{Z}$, $n \in \mathbb{N}_1$ 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 7.14 Für $x, y \in \mathbb{Z}$ und $y \neq 0$ gilt
$$ggt(x, y) = ggt(y, x \,\%\, y).$$

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 dieselben 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 7.15 (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 7.14 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 7.16 (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 7.14 $ggt(y, x \,\%\, y) = ggt(x, y)$ 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 derselbe wie bei der Funktion *ggtS2*() und wird daher nicht noch einmal angegeben. □

7.3 Der Fundamentalsatz der Arithmetik

Satz 7.17 (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 7.9) 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 7.18 (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.

1. Fall: n ist eine Primzahl.
   Dann ist $n = n^1$ bereits eine kanonische Primfaktor-Zerlegung von n.
2. 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 41: Zeigen Sie, dass die oben definierte Struktur $\langle \mathbb{Z}_n^*, 1, \cdot_n \rangle$ eine Gruppe ist.

Definition 7.19 (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 7.20 (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. "$\Rightarrow$": 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. "$\Leftarrow$": 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 7.9) 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 7.21 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 7.22 (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 7.20 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 7.23 (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 7.20), 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 7.24 (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 42: 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 43: 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 7.25 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 7.26 (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 7.24) 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:

$$\begin{array}{lll}
 & x \in \mathbb{Z}^*_{m\cdot n} & \\
\Rightarrow & ggt(x, m\cdot n) = 1 & \text{nach Definition von } \mathbb{Z}^*_{m\cdot n} \\
\Rightarrow & ggt(x, m) = 1 \wedge ggt(x, n) = 1 & \text{Satz 7.25} \\
\Rightarrow & ggt(x \,\%\, m, m) = 1 \wedge ggt(x \,\%\, n, n) = 1 & \\
\Rightarrow & x \,\%\, m \in \mathbb{Z}^*_m \quad \text{und} \quad x \,\%\, n \in \mathbb{Z}^*_n & \\
\Rightarrow & \langle x \,\%\, m, x \,\%\, n\rangle \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n &
\end{array}$$

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 7.27 (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 7.22, 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 7.20 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 dieselbe 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 7.28 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 7.29 (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 7.25, 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 7.25 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 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

$$a \cdot x - b \cdot y = 1 \quad \text{und} \quad a \cdot y + b \cdot x = 0. \tag{8.1}$$

Dies sind zwei lineare Gleichungen für die beiden Unbekannten a und b. Zunächst bestimmen wir b und multiplizieren dazu die erste dieser beiden Gleichungen mit $-y$ und die zweite Gleichung mit x. Das liefert

$$-a \cdot x \cdot y + b \cdot y^2 = -y \quad \text{und} \quad a \cdot x \cdot y + b \cdot x^2 = 0.$$

Addieren wir diese Gleichungen, so erhalten wir

$$b \cdot x^2 + b \cdot y^2 = -y, \quad \text{also} \quad b \cdot (x^2 + y^2) = -y,$$

woraus

$$b = \frac{-y}{x^2 + y^2}$$

folgt. Um a zu bestimmen, multiplizieren wir die erste der beiden Gleichungen in (8.1) mit x und die zweite mit y. Das liefert

$$a \cdot x^2 - b \cdot x \cdot y = x \quad \text{und} \quad a \cdot y^2 + b \cdot x \cdot y = 0.$$

Durch Addition dieser Gleichungen erhalten wir

$$a \cdot x^2 + a \cdot y^2 = x, \quad \text{also} \quad a \cdot (x^2 + y^2) = x,$$

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 44:

(a) Zeigen Sie, dass für die Multiplikation in $\mathbb{C}$ das Assoziativ-Gesetz gilt.

(b) Zeigen Sie, dass in $\mathbb{C}$ 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 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. $$\begin{aligned}
\sqrt{i} &= \sqrt{0 + i \cdot 1} \\
&= \sqrt{\frac{1}{2} \cdot \left(0 + \sqrt{0 + 1}\right)} + i \cdot \frac{1}{\sqrt{2 \cdot \left(0 + \sqrt{0 + 1}\right)}} \\
&= \sqrt{\frac{1}{2} \cdot 1} + i \cdot \frac{1}{\sqrt{2 \cdot 1}} \\
&= \frac{1}{\sqrt{2}} \cdot (1 + i).
\end{aligned}$$

$$
\begin{array}{lrcl}
2. & \sqrt{3+i\cdot 4} & = & \sqrt{\frac{1}{2}\cdot\left(3+\sqrt{9+16}\right)}+i\cdot\frac{4}{\sqrt{2\cdot\left(3+\sqrt{9+16}\right)}} \\
& & = & \sqrt{\frac{1}{2}\cdot(3+5)}+i\cdot\frac{4}{\sqrt{2\cdot(3+5)}} \\
& & = & \sqrt{\frac{1}{2}\cdot(8)}+i\cdot\frac{4}{\sqrt{2\cdot 8}} \\
& & = & \sqrt{4}+i\cdot\frac{4}{\sqrt{16}} \\
& & = & 2+i\cdot\frac{4}{4} \\
& & = & 2+i\cdot 1
\end{array}
$$

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 bewiesen, 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

$$a+i\cdot b\mathrel{\widehat{=}}\langle a,b\rangle.$$

Stellen 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 *Polarform* der komplexen Zahl $a+i\cdot b$, während

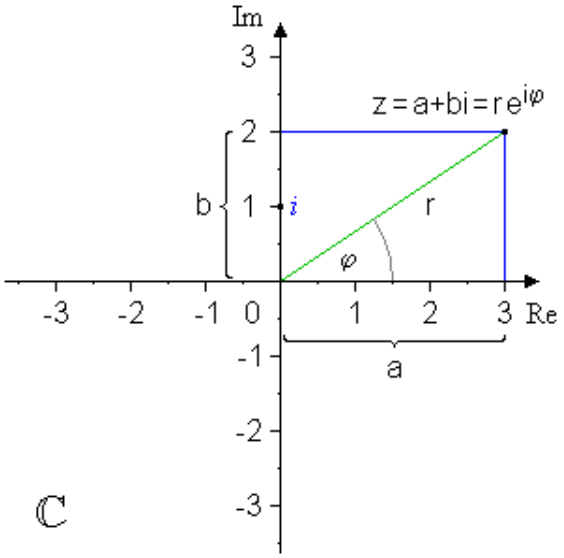

Abbildung 8.1: Die Gauß'sche Zahlen-Ebene.

wir das Paar $\langle a, b\rangle$ die *kartesische Darstellung* nennen. Es ist instruktiv zu sehen, was passiert, wenn wir zwei komplexe Zahlen in Polarform

$$r_1 \cdot \cos(\varphi_1) + i \cdot r_1 \cdot \sin(\varphi_1) \quad \text{und} \quad r_2 \cdot \cos(\varphi_2) + i \cdot r_2 \cdot \sin(\varphi_2)$$

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 einfach ist, komplexe Zahlen in der Polarform 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 Polarform 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

$$1 + i = \sqrt{2} \cdot \Big(\cos\left(\tfrac{\pi}{4}\right) + i \cdot \sin\left(\tfrac{\pi}{4}\right)\Big).$$

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 118 gezeigten Graphen.

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

$$\begin{aligned}
(u+v)^3 &= (u+v)^2 \cdot (u+v) \\
&= (u^2 + 2 \cdot u \cdot v + v^2) \cdot (u+v) \\
&= u^3 + u^2 \cdot v + 2 \cdot u^2 \cdot v + 2 \cdot u \cdot v^2 + u \cdot v^2 + v^3 \\
&= u^3 + 3 \cdot u^2 \cdot v + 3 \cdot u \cdot v^2 + v^3 \\
&= 3 \cdot u \cdot v \cdot (u+v) + u^3 + v^3
\end{aligned}$$

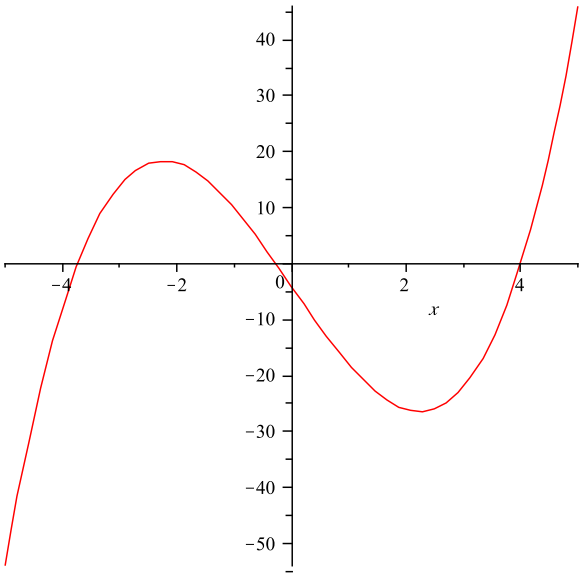

Abbildung 8.2: Die Funktion $x \mapsto x^3 - 15 \cdot x - 4$.

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 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

$$\alpha := u^3 \quad \text{und} \quad \beta := v^3.$$

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 erstmals 1545 von Geralomo Cardano veröffentlichte *Cardanische Formel*

$$\boxed{x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.}$$

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 konnten. 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

$$\begin{aligned} x_2 &= \zeta_3 \cdot u + \zeta_3^2 \cdot v \\ &= \zeta_3 \cdot (2+i) + \zeta_3^2 \cdot (2-i) \\ &= \Big(-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}\Big) \cdot (2+i) + \Big(-\frac{1}{2} - i \cdot \frac{\sqrt{3}}{2}\Big) \cdot (2-i) \\ &= \frac{1}{2} \cdot \big(-2 - \sqrt{3} + i \cdot (-1 + 2 \cdot \sqrt{3}) - 2 - \sqrt{3} + i \cdot (1 - 2 \cdot \sqrt{3})\big) \\ &= -2 - \sqrt{3}. \end{aligned}$$

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

$$x_k = 2 \cdot \sqrt{\tfrac{p}{3}} \cdot \cos\Big(\tfrac{1}{3} \cdot \arccos\big(\tfrac{3 \cdot q}{2 \cdot p} \cdot \sqrt{\tfrac{3}{p}}\big) - (k-1) \cdot \tfrac{2 \cdot \pi}{3}\Big) \quad \text{for } k = 1, 2, 3.$$

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.

Aufgabe 45: Bestimmen Sie mit Hilfe der Cardanischen Formel alle komplexen Lösungen der Gleichung

$$z^3 + z^2 + z + 1 = 0.$$

1. Hinweis: Machen Sie den Ansatz $z = x + c$ und wählen Sie c so, dass Sie für x eine Gleichung der Form

$$x^3 - p \cdot x - q = 0$$

erhalten. Diese Gleichung für x können Sie dann mit Hilfe der Cardanischen Formel lösen.
2. Hinweis: Die obige Gleichung ist so einfach, dass Sie eine der Lösungen auch raten könnten. Anschließend könnten Sie dann mit Hilfe der Polynom-Division die geratene Lösung aus dem Polynom $p(z) = z^3 + z^2 + z + 1$ heraus dividieren und die verbleibende quadratische Gleichung lösen. Das ist aber nicht der Sinn dieser Aufgabe! ◇

Aufgabe 46: Für welche $z \in \mathbb{C}$ gilt die Gleichung

$$\Big(\frac{1+z}{1-z}\Big)^2 = -1?$$ ◇

Aufgabe 47: Für welche Zahlen $x, y \in \mathbb{R}$ gilt

$$(5 + 6 \cdot i) \cdot (x - 3 \cdot i) = y - 3 \cdot i?$$ ◇

Aufgabe 48: Welche komplexen Zahlen $z \in \mathbb{C}$ lassen sich in der Form

$$\frac{1 + i \cdot x}{1 - i \cdot x} = z \quad \text{mit } x \in \mathbb{R}$$

schreiben?
Hinweis: Machen Sie für z den Ansatz $z = a + b \cdot i$ mit $a, b \in \mathbb{R}$ und setzen Sie diesen Ansatz in der obigen Gleichung für z ein. ◇

Aufgabe 49: Bestimmen Sie mit Hilfe der Cardanischen Formel alle Lösungen der Gleichung

$x^3 = 3 \cdot x - 2!$ ◇

8.5 Ausblick

In diesem letzten Abschnitt stellen wir wichtige Formeln und Eigenschaften der komplexen Zahlen zusammen, die wir allerdings jetzt noch nicht beweisen können.

8.5.1 Die Eulersche Formel

Zwischen der Exponential-Funktion $x \mapsto e^x$ und den trigonometrischen Funktionen $x \mapsto \sin(x)$ und $x \mapsto \cos(x)$ gibt es einen wichtigen Zusammenhang, der als *Eulersche Formel* bekannt ist. Es gilt

$$e^{i \cdot \varphi} = \cos(\varphi) + i \cdot \sin(\varphi).$$

Diese Formel können wir verstehen, wenn wir die Reihenentwicklung der beteiligten Funktionen kennen. In der Analysis werden wir später sehen, dass e^x, $\sin(x)$ und $\cos(x)$ wie folgt als Reihen dargestellt werden können:

1. $e^x = 1 + x + \frac{1}{2} \cdot x^2 + \frac{1}{6} \cdot x^3 + \cdots = \sum\limits_{n=0}^{\infty} \frac{1}{n!} \cdot x^n$,
2. $\sin(x) = x - \frac{1}{6} \cdot x^3 + \cdots = \sum\limits_{n=0}^{\infty} \frac{(-1)^n}{(2 \cdot n+1)!} \cdot x^{2 \cdot n+1}$,
3. $\cos(x) = 1 - \frac{1}{2} \cdot x^2 + \frac{1}{24} \cdot x^4 + \cdots = \sum\limits_{n=0}^{\infty} \frac{(-1)^n}{(2 \cdot n)!} \cdot x^{2 \cdot n}$.

Setzen wir diese Reihen in der Eulerschen Formel ein und vergleichen die Koeffizienten von x^n, so können wir die Gültigkeit der Eulerschen Formel nachvollziehen. Setzen wir in der eulerschen Formel für φ den Wert π ein, so erhalten wir die *eulersche Identität*

$$e^{i \cdot \pi} = -1.$$

Diese Formel liefert einen Zusammenhang zwischen π, e und der imaginären Einheit i.

8.5.2 Der Fundamentalsatz der Algebra

In diesem Abschnitt zitieren wir (ohne Beweis) den sogenannten *Fundamentalsatz der Algebra*. Dieser Satz besagt, dass jedes nicht-konstante Polynom

$$p(z) = \sum_{i=0}^{n} a_i \cdot z^i \quad \text{mit } n \geq 1 \text{ und } a_n \neq 0$$

im Körper der komplexen Zahlen eine Nullstelle hat, d.h. es gibt ein $z_1 \in \mathbb{C}$, so dass $p(z_1) = 0$ ist. Mit Hilfe der Polynom-Division können wir die Nullstelle z_1 aus dem Polynom $p(z)$ heraus dividieren und $p(z)$ in der Form

$$p(z) = (z - z_1) \cdot p_1(z)$$

schreiben, wobei $p_1(z)$ dann ein Polynom vom Grad $n-1$ ist. Falls $n - 1 \geq 1$ ist, hat auch $p_1(z)$ eine Nullstelle z_2, die wir aus $p_1(z)$ heraus dividieren können, so dass wir $p_1(z)$ in der Form

$$p_1(z) = (z - z_2) \cdot p_2(z)$$

schreiben können, wobei $p_2(z)$ ein Polynom vom Grad $n-2$ ist. Durch Iteration dieses Verfahrens finden wir also insgesamt n Zahlen $z_1, z_2, \cdots, z_n$, so dass wir $p(z)$ als das Produkt

$$p(z) = (z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_{n-1}) \cdot (z - z_n)$$

schreiben können. Dabei brauchen die komplexen Zahlen z_i keineswegs paarweise verschieden zu

sein, sondern sie können auch durchaus gleich sein. Wir bemerken noch, dass diese Darstellung bis auf die Reihenfolge der z_i eindeutig sein muss, denn die z_i sind genau die Nullstellen des Polynoms $p(z)$ und ein Polynom vom Grade n hat, wie die obigen Überlegungen zeigen, höchstens n verschiedene Nullstellen.

Bemerkung: Der Fundamentalsatz der Algebra zeigt, dass die Struktur der komplexen Zahlen aus algebraischer Sicht wesentlich reichhaltiger als die Struktur der reellen Zahlen ist, denn in den komplexen Zahlen hat jede Gleichung der Form

$$z^n + a_{n-1} \cdot z^{n-1} + \cdots + a_1 \cdot z + a_0 = 0 \quad \text{für } n \geq 1$$

eine Lösung. Es ist also nicht nur so, dass wir die Gleichung

$$z^2 + 1 = 0$$

in den komplexen Zahlen lösen können, sondern in den komplexen Zahlen können wir tatsächlich jede quadratische Gleichung lösen. Darüber hinaus können wir auch jede kubische Gleichung lösen und ganz allgemein hat jede Gleichung n-ten Grades eine Lösung, solange n nur positiv ist. Dies ist einer von vielen Gründen, warum die komplexen Zahlen so wichtig sind.

Der Beweis des Fundamentalsatzes der Algebra benötigt Hilfsmittel aus der Analysis, die wir nicht zur Verfügung haben. Der Beweis ist auch nicht ganz einfach: Das können Sie beispielsweise der Tatsache entnehmen, das der bedeutendste Mathematiker, der je gelebt hat, Carl Friedrich Gauß diesen Satz 1799 in seiner Dissertation bewiesen hat. Der Beweis, den Gauß damals gab, enthielt allerdings noch eine Lücke. Der erste vollständige Beweis des Fundamentalsatzes der Algebra wurde 1806 von Jean-Robert Argand angegeben.

Kapitel 9

Vektor-Räume

In diesem Kapitel werden wir zunächst den für den Rest dieser Vorlesung grundlegenden Begriff des *Vektor-Raums* einführen. Danach besprechen wir den Begriff des Untervektor-Raums. Die Theorie der Vektor-Räume bildet die Grundlage für unsere spätere Behandlung linearer Gleichungs-Systeme. Außerdem benötigen wir Vektor-Räume bei der Lösung von *Rekurrenz-Gleichungen*, die wir im letzten Kapitel dieses Skriptes diskutieren. Daneben gibt es zahlreiche weitere Anwendungen von Vektor-Räumen in der Informatik. Diese alle aufzulisten würde Ihnen jetzt wenig helfen, wir beginnen statt dessen mit der Definition eines Vektor-Raums.

9.1 Definition und Beispiele

Definition 9.1 (Vektor-Raum) Ein Paar $\mathcal{V} = \big\langle \langle V, \mathbf{0}, + \rangle, \cdot \big\rangle$ ist ein $\mathbb{K}$-*Vektor-Raum* falls gilt:

1. $\mathbb{K}$ ist ein Körper.

   In allen Beispielen, die uns in dieser Vorlesung begegnen werden, ist $\mathbb{K}$ entweder der Körper der reellen Zahlen $\mathbb{R}$ oder der Körper der komplexen Zahlen $\mathbb{C}$.

2. $\langle V, \mathbf{0}, + \rangle$ ist eine kommutative Gruppe.

3. $\cdot : \mathbb{K} \times V \to V$ ist eine Abbildung, die jeder Zahl $\lambda \in \mathbb{K}$ und jedem $\mathbf{x} \in V$ ein Element $\lambda \cdot \mathbf{x} \in V$ zuordnet. Diese Funktion wird als *Skalar-Multiplikation* bezeichnet und üblicherweise in Infix-Notation geschrieben.

   Die Skalar-Multiplikation muss außerdem den folgenden Gesetzen genügen:

   1. $(\alpha \cdot \beta) \cdot \mathbf{x} = \alpha \cdot (\beta \cdot \mathbf{x})$ f.a. $\alpha, \beta \in \mathbb{K}$, $\mathbf{x} \in V$.
      Beachten Sie, dass der Operator "$\cdot$", der hier in dem Ausdruck $(\alpha \cdot \beta)$ auftritt, die Multiplikation in dem Körper $\mathbb{K}$ bezeichnet, während alle anderen Auftreten des Operators "$\cdot$" die Skalar-Multiplikation bezeichnen.
      Dieses Gesetz wird als das *Assoziativ-Gesetz* bezeichnet. Es drückt aus, dass die Multiplikation in dem Körper $\mathbb{K}$ mit der Skalar-Multiplikation verträglich ist.
   2. $(\alpha + \beta) \cdot \mathbf{x} = \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}$ f.a. $\alpha, \beta \in \mathbb{K}$, $\mathbf{x} \in V$.
      Beachten Sie, dass der Operator "$+$", der hier in dem Ausdruck $(\alpha + \beta)$ auftritt, die Addition in dem Körper $\mathbb{K}$ bezeichnet, während der Operator "$+$" in dem Ausdruck auf der rechten Seite dieser Gleichung die Addition in der Gruppe $\langle V, \mathbf{0}, + \rangle$ bezeichnet. Daher sagt dieses Gesetz, dass die Addition in dem Körper $\mathbb{K}$ mit der Addition in dem Vektor-Raum $\mathcal{V}$ verträglich ist.
   3. $\alpha \cdot (\mathbf{x} + \mathbf{y}) = \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}$ f.a. $\alpha \in \mathbb{K}$, $\mathbf{x}, \mathbf{y} \in V$.
      Dieses Gesetz drückt aus, dass die Skalar-Multiplikation mit der Addition im Vektor-Raum $\mathcal{V}$ verträglich ist.
      Die letzten beiden Gesetze werden als *Distributiv-Gesetze* bezeichnet.

4. $1 \cdot \mathbf{x} = \mathbf{x}$ f.a. $\mathbf{x} \in V$.

Ist $\mathcal{V} = \big\langle\langle V, \mathbf{0}, +\rangle, \cdot\big\rangle$ ein $\mathbb{K}$-Vektor-Raum, so bezeichnen wir die Elemente der Menge V als *Vektoren*, während die Elemente aus dem Körper $\mathbb{K}$ *Skalare* genannt werden. Es ist üblich, Vektoren von Skalaren durch Fettdruck zu unterscheiden. Da an der Tafel ein Fettdruck schlecht möglich ist, werden die Vektoren dort mit Pfeilen verziert, wir schreiben an der Tafel also $\vec{x}$ an Stelle von $\mathbf{x}$. ◇

Falls bei einer Menge V aus dem Zusammenhang klar ist, was das neutrale Element "$\mathbf{0}$" ist und wie die Operatoren "$+$" und "$\cdot$" zu definieren sind, so dass $\big\langle\langle V, \mathbf{0}, +\rangle, \cdot\big\rangle$ ein $\mathbb{K}$-Vektor-Raum wird, dann sprechen wir in Zukunft von V als $\mathbb{K}$-Vektor-Raum und meinen damit, das das Tripel $\big\langle\langle V, \mathbf{0}, +\rangle, \mathbb{K}, \cdot\big\rangle$ ein $\mathbb{K}$-Vektor-Raum ist. Falls darüber hinaus klar ist, um welchen Körper es sich bei $\mathbb{K}$ handelt, so sprechen wir einfach von einem Vektor-Raum anstatt von einem $\mathbb{K}$-Vektor-Raum.

Beispiel: Wir haben die Menge $\mathbb{K}^n$ als die Menge aller Listen der Länge n definiert, deren Elemente aus der Menge $\mathbb{K}$ stammen. Setzen wir zunächst

$$\mathbf{0} := \underbrace{[0, \cdots, 0]}_{n}$$

und definieren dann eine Addition "$+$" auf $\mathbb{K}^n$ komponentenweise durch

$$[x_1, \cdots, x_n] + [y_1, \cdots, y_n] := [x_1 + y_1, \cdots, x_n + y_n],$$

so können Sie leicht nachrechnen, dass mit diesen Definitionen das Tripel

$$\langle \mathbb{K}^n, \mathbf{0}, + \rangle$$

eine kommutative Gruppe ist. Definieren wir weiter die Skalar-Multiplikation $\cdot$ durch

$$\alpha \cdot [x_1, \cdots, x_n] := [\alpha \cdot x_1, \cdots, \alpha \cdot x_n],$$

wobei in den Ausdrücken $\alpha \cdot x_i$ der Operator "$\cdot$" die Multiplikation in dem Körper $\mathbb{K}$ bezeichnet, dann lässt sich mit etwas Rechenaufwand einsehen, dass das Paar

$$\big\langle\langle \mathbb{K}^n, \mathbf{0}, +\rangle, \cdot\big\rangle$$

ein $\mathbb{K}$-Vektor-Raum ist. Der Kürze halber werden wir in Zukunft einfach von $\mathbb{K}^n$ als Vektor-Raum reden, wobei wir dann in Wahrheit das obige Paar meinen. ◇

Aufgabe 50: Beweisen Sie, dass $\mathbb{K}^n$ ein $\mathbb{K}$-Vektor-Raum ist. ◇

Der Begriff des Vektor-Raums versucht, die wesentliche algebraische Struktur der Menge $\mathbb{K}^n$ axiomatisch zu erfassen. Das ist deswegen nützlich, weil es neben dem Vektor-Raum $\mathbb{K}^n$ noch viele andere Beispiele für Räume gibt, welche dieselbe algebraische Struktur wie der Raum $\mathbb{K}^n$ aufweisen.

Beispiel: Es sei $\mathcal{C}(\mathbb{R})$ die Menge der Funktionen $f : \mathbb{R} \to \mathbb{R}$, die stetig sind, also

$$\mathcal{C}(\mathbb{R}) := \big\{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ ist stetig} \big\}.$$

Definieren wir die Addition zweier Funktionen punktweise, definieren wir für $f, g \in \mathcal{C}(\mathbb{R})$ also die Funktion $f + g$ indem wir

$$(f + g)(x) := f(x) + g(x) \quad \text{f.a. } x \in \mathbb{R}$$

setzen, so ist die so definierte Funktion $f + g$ wieder stetig. Für ein $\alpha \in \mathbb{R}$ und $f \in \mathcal{C}(R)$ definieren wir die Funktion $\alpha \cdot f$ als

$$(\alpha \cdot f)(x) := \alpha \cdot f(x) \quad \text{f.a. } x \in \mathbb{R}.$$

Dann ist auch die Funktion $\alpha \cdot f$ stetig. Schließlich definieren wir eine Funktion $\mathbf{0} : \mathbb{R} \to \mathbb{R}$, indem wir

$$\mathbf{0}(x) := 0 \quad \text{f.a. } x \in \mathbb{R}$$

setzen. Offensichtlich ist diese Funktion stetig und daher gilt $\mathbf{0} \in \mathcal{C}(\mathbb{R})$. Nun können Sie leicht

nachprüfen, dass die Struktur

$$\big\langle \langle \mathcal{C}, \mathbf{0}, + \rangle, \cdot \big\rangle$$

ein Vektor-Raum ist. Das folgt einfach daraus, dass das Assoziativ-Gesetz und das Distributiv-Gesetz für reelle Zahlen gilt. ◇

Beispiel: Es sei $\mathbb{K}$ ein Körper. Dann definieren wir $\mathbb{K}^{\mathbb{N}}$ als den Raum aller Folgen mit Elementen aus $\mathbb{K}$. Definieren wir für zwei Folgen $\big(x_n\big)_{n\in\mathbb{N}}$ und $\big(y_n\big)_{n\in\mathbb{N}}$ die Summe durch

$$\big(x_n\big)_{n\in\mathbb{N}} + \big(y_n\big)_{n\in\mathbb{N}} := \big(x_n + y_n\big)_{n\in\mathbb{N}}$$

und die Skalar-Multiplikation durch

$$\alpha \cdot \big(x_n\big)_{n\in\mathbb{N}} := \big(\alpha \cdot x_n\big)_{n\in\mathbb{N}},$$

so wird die Menge $\mathbb{K}^{\mathbb{N}}$ zu einem Vektor-Raum. ◇

Gegenstand der nächsten Aufgabe ist der Nachweis, dass die Skalar-Multiplikation mit 0, 1 und -1 sich so verhält, wie wir es intuitiv erwarten würden.

Aufgabe 51: Es sei V ein $\mathbb{K}$-Vektor-Raum. Beweisen Sie:

(a) $0 \cdot \mathbf{x} = \mathbf{0}$ f.a. $\mathbf{x} \in V$,

(b) $\forall \alpha \in \mathbb{K} : \forall \mathbf{x} \in V : \big(\alpha \cdot \mathbf{x} = \mathbf{0} \rightarrow \alpha = 0 \vee \mathbf{x} = 0\big)$,

(c) $(-1) \cdot \mathbf{x} = -\mathbf{x}$ f.a. $\mathbf{x} \in V$,
wobei hier mit $-\mathbf{x}$ das additive Inverse von x in der Gruppe $\langle V, \mathbf{0}, + \rangle$ bezeichnet wird. ◇

9.2 Basis und Dimension

In diesem Abschnitt führen wir den für die Theorie der Vektor-Räume zentralen Begriff der *Dimension* ein. Dazu definieren wir zunächst die Begriffe *Erzeugenden-System* und *lineare Unabhängigkeit*.

Definition 9.2 (Linear-Kombination) Es sei $\mathcal{V}$ ein $\mathbb{K}$-Vektor-Raum. Ein Vektor $\mathbf{x} \in \mathcal{V}$ ist eine *Linear-Kombination* der Vektor $\mathbf{y}_1, \cdots, \mathbf{y}_n \in \mathcal{V}$ genau dann, wenn es Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ gibt, so dass die Gleichung

$$\mathbf{x} = \alpha_1 \cdot \mathbf{y}_1 + \cdots + \alpha_n \cdot \mathbf{y}_n$$

gilt. Zusätzlich müssen die Vektoren $\mathbf{y}_i$ alle paarweise verschieden sein. Die obige Gleichung werden wir in Zukunft der Kürze halber gelegentlich auch in der Form

$$\mathbf{x} = \sum_{i=1}^{n} \alpha_i \cdot \mathbf{y}_i$$

schreiben. ◇

Beispiel: Definieren wir

$$\mathbf{y}_1 := [1, 0, 2], \quad \mathbf{y}_2 := [1, 2, 0], \quad \mathbf{y}_3 := [0, -1, 3] \quad \text{und} \quad \mathbf{x} := [3, 1, 11],$$

so ist $\mathbf{x}$ eine Linear-Kombination der Vektoren $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$, denn es gilt

$$\mathbf{x} = 1 \cdot \mathbf{y}_1 + 2 \cdot \mathbf{y}_2 + 3 \cdot \mathbf{y}_3.$$ ◇

Definition 9.3 (linear unabhängig) Es sei V ein Vektor-Raum. Eine Menge $B \subseteq V$ ist *linear unabhängig* genau dann, wenn

$$\forall n \in \mathbb{N} : \forall \alpha_1, \cdots, \alpha_n \in \mathbb{K} : \forall \mathbf{x_1}, \cdots, \mathbf{x_n} \in B :$$

$$\left(\mathbf{x}_i \text{ paarweise verschieden} \wedge \sum_{i=1}^{n} \alpha_i \cdot \mathbf{x}_i = \mathbf{0} \;\Rightarrow\; \forall i \in \{1, \cdots, n\} : \alpha_i = 0\right)$$

gilt. Mit anderen Worten: Der Nullvektor $\mathbf{0}$ lässt sich nur als die sogenannte *triviale Linear-Kombination* aus Vektoren der Menge B darstellen. Demgegenüber heißt eine Menge $B \subseteq V$ *linear abhängig* genau dann, wenn B nicht linear unabhängig ist. In diesem Fall gibt es dann Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_n \in B$, die paarweise verschieden sind, sowie Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$, so dass einerseits

$$\sum_{i=1}^{n} \alpha_i \cdot \mathbf{x}_i = \mathbf{0} \quad \text{aber andererseits} \quad \exists i \in \{1, \cdots, n\} : \alpha_i \neq 0$$

gilt. ◇

Beispiel: Definieren wir

$$\mathbf{y}_1 := [1, 0, 2], \quad \mathbf{y}_2 := [1, 2, 0] \quad \text{und} \quad \mathbf{y}_3 := [0, -1, 3],$$

so ist die Menge $B := \{\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3\}$ linear unabhängig. Zum Beweis dieser Behauptung nehmen wir zunächst an, dass es α_1, α_2 und α_3, gibt, so dass

$$\mathbf{0} = \alpha_1 \cdot [1, 0, 2] + \alpha_2 \cdot [1, 2, 0] + \alpha_3 \cdot [0, -1, 3]$$

gilt. Rechnen wir die rechte Seite dieser Gleichung aus, so erhalten wir

$$\mathbf{0} = [\alpha_1 + \alpha_2, 2 \cdot \alpha_2 - \alpha_3, 2 \cdot \alpha_1 + 3 \cdot \alpha_3].$$

Die drei Komponenten der Vektoren auf der linken und der rechten Seite dieser Gleichung müssen gleich sein. Damit müssen die drei Gleichungen

$$0 = \alpha_1 + \alpha_2, \quad 0 = 2 \cdot \alpha_2 - \alpha_3 \quad \text{und} \quad 0 = 2 \cdot \alpha_1 + 3 \cdot \alpha_3$$

gelten. Aus der zweiten Gleichung folgt nun $\alpha_3 = 2 \cdot \alpha_2$, während aus der ersten Gleichung $\alpha_1 = -\alpha_2$ folgt. Ersetzen wir nun in der letzten Gleichung sowohl α_1 als auch α_3 durch α_2, so erhalten wir die neue Gleichung

$$0 = 2 \cdot (-\alpha_2) + 3 \cdot 2 \cdot \alpha_2,$$

die wir auch als $0 = 4 \cdot \alpha_2$ schreiben können. Daraus folgt aber sofort $\alpha_2 = 0$ und das impliziert dann auch $\alpha_1 = 0$ und $\alpha_3 = 0$. Damit haben wir gezeigt, dass die drei Vektoren $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ sich nur trivial zu dem Null-Vektor $\mathbf{0}$ kombinieren lassen. Folglich ist die Menge B linear unabhängig. ◇

Definition 9.4 (Erzeugenden-System) Es sei V ein $\mathbb{K}$-Vektor-Raum und $B \subseteq V$. Die Teilmenge B ist ein *Erzeugenden-System* des Vektor-Raums V genau dann, wenn sich jeder Vektor $\mathbf{x} \in \mathbf{V}$ als Linear-Kombination von Vektoren aus B schreiben lässt. Als Formel schreibt sich dies wie folgt:

$$\forall \mathbf{x} \in V : \exists n \in \mathbb{N} : \exists \mathbf{y}_1, \cdots, \mathbf{y}_n \in B : \exists \alpha_1, \cdots, \alpha_n \in \mathbb{K} : \mathbf{x} = \sum_{i=1}^{n} \alpha_i \cdot \mathbf{y}_i. \qquad \diamond$$

Für jeden Vektor-Raum V gibt es ein triviales Erzeugenden-System, den natürlich ist die gesamte Menge V ein Erzeugenden-System von V. Um das einzusehen, setzen wir für einen gegebenen Vektor $\mathbf{x} \in V$ in der obigen Definition $n := 1$, $\mathbf{y}_1 := \mathbf{x}$ und $\alpha_1 := 1$ und haben dann trivialerweise

$$\mathbf{x} = 1 \cdot \mathbf{x} = 1 \cdot \mathbf{y}_1,$$

womit $\mathbf{x}$ als Linear-Kombination von Elementen der Menge V dargestellt ist. Aber natürlich ist ein solches Erzeugenden-System nicht sonderlich interessant. Interessanter sind Erzeugenden-Systeme, die *minimal* sind. Dies führt zu der folgenden zentralen Definition.

Definition 9.5 (Basis) Es sei V ein $\mathbb{K}$-Vektor-Raum und $B \subseteq V$. Die Teilmenge B ist eine *Basis* von V, wenn Folgendes gilt:

1. B ist ein Erzeugenden-System von V und
2. B ist linear unabhängig. ◇

Der nächste Satz zeigt, dass eine Basis eine maximale Menge linear unabhängiger Vektoren ist.

Satz 9.6 Es sei V ein $\mathbb{K}$-Vektor-Raum und B sei eine Basis von V. Ist $\mathbf{x} \in V \backslash B$, so ist die Menge $B \cup \{\mathbf{x}\}$ linear abhängig.

Beweis: Da B eine Basis ist, ist B insbesondere auch ein Erzeugenden-System von V. Damit gibt es ein $n \in \mathbb{N}$ und Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n \in B$ sowie Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$, so dass

$$\mathbf{x} = \alpha_1 \cdot \mathbf{y}_1 + \cdots + \alpha_n \cdot \mathbf{y}_n$$

gilt. Stellen wir diese Gleichung zu der Gleichung

$$\mathbf{0} = (-1) \cdot \mathbf{x} + \alpha_1 \cdot \mathbf{y}_1 + \cdots + \alpha_n \cdot \mathbf{y}_n$$

um, so haben wir eine nicht-triviale Linear-Kombination des Null-Vektors aus Vektoren der Menge $B \cup \{\mathbf{x}\}$ gefunden. Dies zeigt, dass die Menge $B \cup \{\mathbf{x}\}$ linear abhängig ist. □

Aufgabe 52: Überlegen Sie, an welcher Stelle die Voraussetzung $\mathbf{x} \notin B$ in dem obigen Beweis benutzt wird! ◇

Der letzte Satz lässt sich in dem folgenden Sinne umkehren.

Satz 9.7 Es sei V ein $\mathbb{K}$-Vektor-Raum und $B \subseteq V$. Falls B eine *maximale* linear unabhängige Teilmenge von V ist, falls also gilt:

1. B ist linear unabhängig und
2. für alle Vektoren $\mathbf{x} \in V \backslash B$ ist die Menge $B \cup \{\mathbf{x}\}$ linear abhängig,

dann ist B schon eine Basis von V.

Beweis: Wir müssen nur noch zeigen, dass B ein Erzeugenden-System von V ist. Dazu ist nachzuweisen, dass sich jeder Vektor $\mathbf{x} \in V$ als Linear-Kombination von Vektoren aus B schreiben lässt. Wir unterscheiden zwei Fälle:

1. $\mathbf{x} \in B$.

   In diesem Fall setzen wir $n := 1$, $\mathbf{y}_1 := \mathbf{x}$ und $\alpha_1 := 1$. Damit gilt offenbar

   $$\mathbf{x} = \alpha_1 \cdot \mathbf{y}_1$$

   und wir haben die gesuchte Linear-Kombination gefunden.

2. $\mathbf{x} \notin B$.

   Nach Voraussetzung ist die Menge $B \cup \{\mathbf{x}\}$ linear abhängig. Damit lässt sich der Null-Vektor als nicht-triviale Linear-Kombination von Vektoren aus $B \cup \{\mathbf{x}\}$ schreiben. Nun gibt es zwei Möglichkeiten:

   1. Der Vektor $\mathbf{x}$ wird bei dieser Linear-Kombination gar nicht benötigt. Dann hätten wir aber eine nicht-triviale Linear-Kombination des Null-Vektors aus Vektoren der Menge B. Da die Menge B nach Voraussetzung linear unabhängig ist, kann dieser Fall nicht eintreten.

2. Der Vektor $\mathbf{x}$ tritt in der nicht-trivialen Linear-Kombination des Null-Vektors auf. Es gibt dann ein $n \in \mathbb{N}$ sowie Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n$ und Skalare $\alpha_1, \cdots, \alpha_n, \alpha_{n+1}$ so dass

$$\mathbf{0} = \alpha_1 \cdot \mathbf{y}_1 + \cdots + \alpha_n \cdot \mathbf{y}_n + \alpha_{n+1} \cdot \mathbf{x}$$

gilt. Hierbei muss $\alpha_{n+1} \neq 0$ gelten, denn sonst würde $\mathbf{x}$ in der Linear-Kombination gar nicht benötigt, was wir ja bereits ausgeschlossen haben. Damit können wir die obige Gleichung zu

$$\mathbf{x} = -\frac{\alpha_1}{\alpha_{n+1}} \cdot \mathbf{y}_1 - \cdots - \frac{\alpha_n}{\alpha_{n+1}} \cdot \mathbf{y}_n$$

umstellen. Dies zeigt, dass $\mathbf{x}$ sich als Linear-Kombination von Vektoren aus B schreiben lässt.

Insgesamt haben wir jetzt gezeigt, dass sich jeder Vektor $\mathbf{x} \in V$ als Linear-Kombination von Vektoren aus B schreiben lässt und damit ist B ein Erzeugenden-System von V. □

Die letzten beiden Sätze lassen sich dahingehen zusammenfassen, dass eine Menge $B \subseteq V$ genau dann eine Basis von V ist, wenn B eine maximale linear unabhängige Teilmenge von V ist. Die nächsten beide Sätze zeigen, dass sich eine Basis auch als minimales Erzeugenden-System charakterisieren lässt.

Satz 9.8 Es sei V ein $\mathbb{K}$-Vektor-Raum und B sei eine Basis von V. Ist $\mathbf{x} \in B$, so ist die Menge $B \backslash \{\mathbf{x}\}$ kein Erzeugenden-System von V.

Beweis: Wir führen den Beweis indirekt und nehmen an, dass die Menge $B \backslash \{\mathbf{x}\}$ doch ein Erzeugenden-System von V wäre. Dann müsste sich insbesondere auch der Vektor $\mathbf{x}$ als Linear-Kombination von Vektoren aus $B \backslash \{\mathbf{x}\}$ schreiben lassen. Es gäbe dann also ein $n \in \mathbb{N}$ sowie Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n$ und Skalare $\alpha_1, \cdots, \alpha_n$, so dass

$$\mathbf{x} = \alpha_1 \cdot \mathbf{y_1} + \cdots + \alpha_n \cdot \mathbf{y}_n$$

gelten würde. Diese Gleichung können wir zu

$$\mathbf{0} = \alpha_1 \cdot \mathbf{y_1} + \cdots + \alpha_n \cdot \mathbf{y}_n + (-1) \cdot \mathbf{x}$$

umstellen. Da die Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n, \mathbf{x}$ verschiedene Vektoren aus B sind, hätten wir damit eine nicht-triviale Linear-Kombination des Null-Vektors gefunden, was der Tatsache widerspricht, dass die Menge B als Basis insbesondere linear unabhängig ist. □

Der letzte Satz zeigt, dass eine Basis ein *minimales Erzeugenden-System* des Vektor-Raums V ist. Wie wir jetzt sehen werden, lässt sich dieser Satz auch umkehren.

Satz 9.9 Es sei V ein $\mathbb{K}$-Vektor-Raum und $B \subseteq V$. Falls B eine *minimales Erzeugenden-System* von V ist, falls also gilt:

1. B ist ein Erzeugenden-System von V und
2. für alle Vektoren $\mathbf{x} \in B$ ist die Menge $B \backslash \{\mathbf{x}\}$ kein Erzeugenden-System von V,

dann ist B schon eine Basis von V.

Beweis: Da die Menge B nach Voraussetzung bereits ein Erzeugenden-System von V ist, müssen wir lediglich zeigen, dass B linear unabhängig ist. Wir führen auch diesen Beweis als Widerspruchsbeweis und nehmen an, dass B linear abhängig wäre. Mit dieser Annahme finden wir eine nicht-triviale Linear-Kombination des Null-Vektors mit Hilfe von Vektoren aus B, wir finden also ein $n \in \mathbb{N}$ sowie paarweise verschiedene Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n \in B$ und Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$, so dass

$$\mathbf{0} = \alpha_1 \cdot \mathbf{y}_1 + \cdots + \alpha_n \cdot \mathbf{y}_n$$

gilt, wobei wenigstens einer der Skalare α_i von 0 verschieden ist. Sei also $\alpha_i \neq 0$. Dann können wir die obige Gleichung zu

$$(-\alpha_i) \cdot \mathbf{y_i} = \sum_{\substack{j=1 \\ j \neq i}}^{n} \alpha_j \cdot \mathbf{y}_j$$

umstellen. Da $\alpha_i \neq 0$ ist, können wir durch α_i teilen und finden

$$\mathbf{y_i} = \sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{-\alpha_j}{\alpha_i} \cdot \mathbf{y}_j.$$

Die letzte Gleichung zeigt, dass sich $\mathbf{y}_i$ als Linear-Kombination der Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_{i-1}, \mathbf{y}_{i+1}, \cdots, \mathbf{y}_n$ schreiben lässt. Wir werden jetzt zeigen, dass damit dann auch die Menge $B \backslash \{\mathbf{y_i}\}$ ein Erzeugenden-System von V ist. Sei dazu $\mathbf{x}$ ein beliebiger Vektor aus V. Da B ein Erzeugenden-System von V ist, gibt es zunächst ein $m \in \mathbb{N}$ sowie Vektoren $\mathbf{z}_1, \cdots, \mathbf{z}_m \in B$ und Skalare $\beta_1, \cdots, \beta_m \in \mathbb{K}$, so dass

$$\mathbf{x} = \sum_{j=1}^{m} \beta_j \cdot \mathbf{z}_j$$

gilt. Falls alle Vektoren $\mathbf{z}_j$ von $\mathbf{y}_i$ verschieden sind, ist nichts mehr zu zeigen, denn dann haben wir $\mathbf{x}$ bereits als Linear-Kombination von Vektoren der Menge $B \backslash \{\mathbf{y_i}\}$ geschrieben. Sollte allerdings eines der $\mathbf{z}_j$, sagen wie $\mathbf{z}_k$, mit $\mathbf{y_i}$ identisch sein, dann können wir die obige Gleichung wie folgt umschreiben:

$$\mathbf{x} = \sum_{\substack{j=1 \\ j \neq k}}^{m} \beta_j \cdot \mathbf{z}_j + \beta_k \cdot \sum_{\substack{j=1 \\ j \neq i}} \frac{-\alpha_j}{\alpha_i} \cdot \mathbf{y}_j$$

Auch in diesem Fall haben wir also $\mathbf{x}$ als Linear-Kombination von Vektoren der Menge $B \backslash \{\mathbf{y}_i\}$ schreiben können. Dies zeigt, dass die Menge $B \backslash \{\mathbf{y}_i\}$ bereits ein Erzeugenden-System von V ist und steht im Widerspruch dazu, dass B ein minimales Erzeugenden-System ist. Dieser Widerspruch zeigt, dass die Annahme, dass B linear abhängig ist, falsch sein muss. □

Aufgabe 53: Es sei V ein $\mathbb{K}$-Vektor-Raum und es gelte $B := \{\mathbf{x}_1, \cdots, \mathbf{x}_n\} \subseteq V$. Zeigen Sie: B ist genau dann eine Basis von V, wenn sich jeder Vektor $\mathbf{y} \in V$ in eindeutiger Weise als Linear-Kombination der Vektoren aus B schreiben lässt.

Lemma 9.10 (Austausch-Lemma) Es sei V ein Vektor-Raum, B eine Basis von V, $U \subseteq B$, $\mathbf{x} \in V$ und die Menge $U \cup \{\mathbf{x}\}$ sei linear unabhängig. Dann gibt es einen Vektor $\mathbf{y} \in B \backslash U$, so dass die Menge $B \backslash \{\mathbf{y}\} \cup \{\mathbf{x}\}$ wieder eine Basis von V ist.

Beweis: Da B eine Basis ist, lässt sich $\mathbf{x}$ als Linear-Kombination von Vektoren aus B darstellen. Es gibt also ein $n \in \mathbb{N}$, Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ und Vektoren $\mathbf{y}_1, \cdots, \mathbf{y}_n \in B$, so dass

$$\mathbf{x} = \sum_{i=1}^{n} \alpha_i \cdot \mathbf{y}_i$$

gilt. Da die Menge $U \cup \{\mathbf{x}\}$ linear unabhängig ist, ist $\mathbf{x}$ sicher von $\mathbf{0}$ verschieden und damit können nicht alle α_i den Wert 0 haben. O.B.d.A. können wir sogar fordern, dass alle $\alpha_i \neq 0$ sind, denn falls $\alpha_i = 0$ wäre, würden wir den Term $\alpha_i \cdot \mathbf{y}_i$ in der obigen Summe einfach weglassen. Aus der Tatsache, dass die Menge $U \cup \{\mathbf{x}\}$ linear unabhängig ist, folgt außerdem, dass in der obigen Darstellung nicht alle Vektoren $\mathbf{y}_i$ Elemente der Menge U sind, denn wir können wir die obige Gleichung zu

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i \cdot \mathbf{y}_i + (-1) \cdot \mathbf{x}$$

umstellen und wenn nun alle $\mathbf{y}_i \in U$ wären, dann würde das der linearen Unabhängigkeit von $U \cup \{\mathbf{x}\}$ widersprechen. Es gibt also ein $k \in \{1, \cdots, n\}$ so dass $\mathbf{y}_k \in B \backslash U$ ist. Wir definieren

$$\mathbf{y} := \mathbf{y}_k, \quad \text{woraus bereits } \mathbf{y} \in B \backslash U \text{ folgt.}$$

Außerdem bemerken wir, dass $\mathbf{y}_i \in B\backslash\{\mathbf{y}\}$ ist für alle $i \in \{1, \cdots, n\}\backslash\{k\}$, denn die Vektoren $\mathbf{y}_i$ sind paarweise verschieden. Wir stellen die obige Gleichung für $\mathbf{x}$ wie folgt um:

$$\mathbf{x} = \sum_{\substack{i=1 \\ i \neq k}}^{n} \alpha_i \cdot \mathbf{y}_i + \alpha_k \cdot \mathbf{y}.$$

Diese Gleichung lösen wir nach $\mathbf{y}$ auf und erhalten

$$\mathbf{y} = \frac{1}{\alpha_k} \cdot \mathbf{x} - \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{\alpha_i}{\alpha_k} \cdot \mathbf{y}_i. \tag{$*$}$$

Wir müssen nun zeigen, dass die Menge

$$B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$$

eine Basis von V ist. Dazu sind zwei Dinge nachzuweisen.

1. Als erstes zeigen wir, dass $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$ ein Erzeugenden-System von V ist.

   Dazu betrachten wir einen beliebigen Vektor $\mathbf{z} \in V$. Da B ein Erzeugenden-System ist, lässt sich $\mathbf{z}$ als Linear-Kombination von Vektoren aus B darstellen. Es gibt also ein $m \in \mathbb{N}$, Skalare $\beta_1, \cdots, \beta_m \in \mathbb{K}$ und Vektoren $\mathbf{u}_1, \cdots, \mathbf{u}_m \in B$, so dass

   $$\mathbf{z} = \sum_{j=1}^{m} \beta_j \cdot \mathbf{u}_j$$

   gilt. Falls nun alle $\mathbf{u}_j$ von dem Vektor $\mathbf{y}$ verschieden sind, dann haben wir $\mathbf{z}$ bereits als Linear-Kombination von Vektoren der Menge $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$ dargestellt und der Beweis ist abgeschlossen. Andernfalls gilt $\mathbf{u}_l = \mathbf{y}$ für ein $l \in \{1, \cdots, m\}$. In diesem Fall haben wir

   $$\mathbf{z} = \sum_{\substack{j=1 \\ j \neq l}}^{m} \beta_j \cdot \mathbf{u}_j + \beta_l \cdot \mathbf{y}.$$

   Hier setzen wir für $\mathbf{y}$ den Wert ein, den wir in der Gleichung $(*)$ oben gefunden haben. Das liefert

   $$\mathbf{z} = \sum_{\substack{j=1 \\ j \neq l}}^{m} \beta_j \cdot \mathbf{u}_j + \frac{\beta_l}{\alpha_k} \cdot \mathbf{x} - \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{\beta_l \cdot \alpha_i}{\alpha_k} \cdot \mathbf{y}_i.$$

   In dieser Darstellung sind nun alle der beteiligten Vektoren Elemente der Menge $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$. Damit haben wir also gezeigt, dass der Vektor $\mathbf{z}$ als Linear-Kombination dieser Menge dargestellt werden kann. Da $\mathbf{z}$ ein beliebiger Vektor aus V war, ist damit gezeigt, dass die Menge $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$ ein Erzeugenden-System von V ist.

2. Als nächstes ist nachzuweisen, dass die Menge $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$ linear unabhängig ist. Dazu nehmen wir an, dass wir eine Linear-Kombination von Vektoren aus der Menge $B\backslash\{\mathbf{y}\} \cup \{\mathbf{x}\}$ haben, die den Null-Vektor ergibt. Wir haben dann also ein $m \in \mathbb{N}$, Skalare $\gamma_1, \cdots, \gamma_m, \delta \in \mathbb{K}$, sowie paarweise verschiedene Vektoren $\mathbf{v}_1, \cdots, \mathbf{v}_m \in B\backslash\{\mathbf{y}\}$, so dass

   $$\mathbf{0} = \sum_{j=1}^{m} \gamma_j \cdot \mathbf{v}_j + \delta \cdot \mathbf{x}$$

   gilt. Wir müssen nun zeigen, dass $\gamma_j = 0$ für alle $j \in \{1, \cdots, n\}$ gilt und dass außerdem $\delta = 0$ ist. Wir führen diesen Nachweis durch eine Fallunterscheidung.

   1. $\delta = 0$. Dann haben wir

      $$\mathbf{0} = \sum_{j=1}^{m} \gamma_j \cdot \mathbf{v}_j$$

      und da die Vektoren $\mathbf{v}_j$ Elemente der linear unabhängigen Menge B sind, folgt $\gamma_j = 0$ für alle $j \in \{1, \cdots, m\}$.
   2. $\delta \neq 0$. Jetzt setzen wir für $\mathbf{x}$ in der Darstellung des Null-Vektors den Wert

$$\mathbf{x} = \sum_{\substack{j=1 \\ j \neq k}}^{n} \alpha_j \cdot \mathbf{y}_j + \alpha_k \cdot \mathbf{y}$$

ein und erhalten

$$\mathbf{0} = \sum_{j=1}^{m} \gamma_j \cdot \mathbf{v}_j + \sum_{\substack{i=1 \\ i \neq k}}^{n} \delta \cdot \alpha_i \cdot \mathbf{y}_i + \delta \cdot \alpha_k \cdot \mathbf{y}.$$

Die Vektoren $\mathbf{v}_j$ sowie die Vektoren $\mathbf{y}_i$ mit $i \neq k$ sind Elemente der Menge $B \backslash \{\mathbf{y}\}$. Da $\mathbf{y} = \mathbf{y}_k \in B$ ist, haben wir dann insgesamt eine Linear-Kombination des Null-Vektors aus Elementen der Menge B. Da die Menge B linear unabhängig ist, folgt zunächst, dass der Koeffizient $\delta \cdot \alpha_k = 0$ ist. Wegen $\alpha_k \neq 0$ folgt daraus $\delta = 0$. Damit haben wir jetzt die Gleichung

$$\mathbf{0} = \sum_{j=1}^{m} \gamma_j \cdot \mathbf{v}_j.$$

Aus der linearen Unabhängigkeit von B folgt nun $\gamma_j = 0$ für alle $j \in \{1, \cdots, m\}$ und das war zu zeigen. □

Das gerade bewiesene Lemma zeigt uns, dass wir in einer Basis einen beliebigen von dem Nullvektor verschiedenen Vektor $\mathbf{x}$ gegen einen Vektor der Basis austauschen können. Der nächste Satz verallgemeinert diesen Tatbestand und zeigt, dass wir in einer Basis B eine linear unabhängige Menge U gegen Elemente aus B austauschen können.

Satz 9.11 (Basis-Austausch-Satz) Es sei V ein Vektor-Raum und B sei eine Basis von V. Weiter sei $U \subseteq V$ linear unabhängig. Dann gibt es eine Teilmenge $W \subseteq B$, so dass gilt

$$B \backslash W \cup U \text{ ist eine Basis von V} \quad \text{und} \quad \mathit{card}(W) = \mathit{card}(U).$$

Beweis: Wir definieren $n := \mathit{card}(U)$ und führen den Beweis durch Induktion nach n.

I.A.: $n = 0$.

Dann gilt offenbar $U = \{\}$ und wir können $W := \{\}$ definieren. Wegen

$$B \backslash W \cup U = B \backslash \{\} \cup \{\} = B \quad \text{und} \quad \mathit{card}(W) = \mathit{card}(\{\}) = \mathit{card}(U)$$

ist dann nichts mehr zu zeigen, denn B ist nach Voraussetzung eine Basis von V.

I.S.: $n \mapsto n + 1$.

Es gilt jetzt $\mathit{card}(U) = n + 1$. Da U damit nicht leer ist, gibt es einen Vektor $\mathbf{x} \in U$. Wir definieren $U' := U \backslash \{\mathbf{x}\}$. Damit folgt $\mathit{card}(U') = n$. Nach Induktions-Voraussetzung finden wir daher eine Menge $W' \subseteq B$, so dass einerseits

$$\mathit{card}(W') = \mathit{card}(U') = n$$

und andererseits die Menge $B \backslash W' \cup U'$ eine Basis von V ist. Wir wenden nun das Austausch-Lemma auf die Basis $B \backslash W' \cup U'$, den Vektor $\mathbf{x}$ und die Menge U' an. Damit finden wir ein $\mathbf{y} \in B \backslash W'$, so dass

$$\big(B \backslash W' \cup U'\big) \backslash \{\mathbf{y}\} \cup \{\mathbf{x}\}$$

eine Basis von V ist. Wir definieren nun

$$W := W' \cup \{\mathbf{y}\} \quad \text{und erinnern daran, dass} \quad U = U' \cup \{\mathbf{x}\}$$

gilt. Damit haben wir dann

$$\big(B \backslash W' \cup U'\big) \backslash \{\mathbf{y}\} \cup \{\mathbf{x}\} = B \backslash W \cup U.$$

Außerdem gilt

$$\begin{aligned} card(W) &= card(W' \cup \{\mathbf{y}\}) \ . \\ &= card(W') + 1 \\ &= card(U') + 1 \\ &= card(U' \cup \{\mathbf{x}\}) \\ &= card(U) \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Korollar 9.12 Ist V ein Vektor-Raum, B eine Basis von V und $U \subseteq V$ linear unabhängig, so gilt $card(U) \leq card(B)$.

Beweis: Der Basis-Austausch-Satz besagt, dass wir eine Teilmenge $W \subseteq B$ finden, so dass einerseits $card(W) = card(U)$ gilt und dass andererseits $B \backslash W \cup U$ eine Basis von B ist. Aus $W \subseteq B$ folgt $card(W) \leq card(B)$ und wegen $card(W) = card(U)$ folgt die Behauptung. □

Haben wir zwei verschiedene Basen B_1 und B_2 eines Vektor-Raums B, so können wir mit dem letzten Korollar sowohl $card(B_2) \leq card(B_1)$ als auch $card(B_1) \leq card(B_2)$ folgern. Das zeigt, dass zwei verschiedene Basen eines Vektor-Raums dieselbe Anzahl von Elementen haben. Ist diese Anzahl endlich und hat den Wert n, so bezeichnen wir sie als die *Dimension* des Vektor-Raums V und definieren

$$dim(V) := n.$$

Aufgabe 54:

(a) Zeigen Sie, dass der Vektor-Raum $\mathbb{K}^n$ die Dimension n hat.

(b) Zeigen Sie, dass der Vektor-Raum $\mathbb{K}^{\mathbb{N}}$ keine endliche Basis hat. ◇

9.3 Untervektor-Räume

Ist V ein Vektor-Raum und ist $U \subseteq V$, so dass U für sich betrachtet ebenfalls ein Vektor-Raum ist, so bezeichnen wir U als *Untervektor-Raum* von V. Eine zu dem eben Gesagten äquivalente Definition folgt.

Definition 9.13 (Untervektor-Raum) Es sei $\langle\langle V, \mathbf{0}, +\rangle, \cdot\rangle$ ein $\mathbb{K}$-Vektor-Raum und es gelte $U \subseteq V$. Dann ist U ein Untervektor-Raum von V genau dann, wenn Folgendes gilt:

1. $\mathbf{0} \in U$,
2. $\forall \mathbf{x}, \mathbf{y} \in U : \mathbf{x} + \mathbf{y} \in U$ und
3. $\forall \alpha \in \mathbb{K} : \forall \mathbf{x} \in U : \alpha \cdot \mathbf{x} \in U$. ◇

Eine Teilmenge U von V ist also ein Untervektor-Raum von V, falls U den Null-Vektor enthält und zusätzlich unter Addition und Skalar-Multiplikation abgeschlossen ist. Es lässt sich leicht zeigen, dass ein Untervektor-Raum U auch selbst ein Vektor-Raum ist: Die Gültigkeit des Assoziativ-Gesetzes und der Distributiv-Gesetze folgt einfach aus der Tatsache, dass diese Gesetze schon in V gelten und damit erst recht in U, denn U ist ja eine Teilmenge von V.

Beispiel: Es sei $V = \mathbb{R}^3$. Ist weiter $\mathbf{z} = [z_1, z_2, z_3] \in \mathbb{R}^3$ und definieren wir

$$U := \{\alpha \cdot \mathbf{z} \mid \alpha \in \mathbb{R}\},$$

so ist U ein Untervektor-Raum des $\mathbb{R}^3$.

Beweis: Es sind drei Eigenschaften zu prüfen:

1. Offenbar gilt $\mathbf{0} = 0 \cdot \mathbf{z} \in U$ und damit ist die erste Eigenschaft bereits gezeigt.

2. Seien $\mathbf{x}, \mathbf{y} \in U$. Dann gibt es $\alpha, \beta \in \mathbb{R}$, so dass

$$\mathbf{x} = \alpha \cdot \mathbf{z} \quad \text{und} \quad \mathbf{y} = \beta \cdot \mathbf{z}$$

gilt. Daraus folgt unter Benutzung des Distributiv-Gesetzes

$$\mathbf{x} + \mathbf{y} = \alpha \cdot \mathbf{z} + \beta \cdot \mathbf{z} = (\alpha + \beta) \cdot \mathbf{z} \in U.$$

3. Sei nun $\alpha \in \mathbb{R}$ und $z \in U$. Dann gibt es ein $\beta \in \mathbb{R}$, so dass $\mathbf{x} = \beta \cdot \mathbf{z}$ gilt. Mit Hilfe des Assoziativ-Gesetzes schließen wir nun wie folgt:

$$\alpha \cdot \mathbf{x} = \alpha \cdot (\beta \cdot \mathbf{z}) = (\alpha \cdot \beta) \cdot \mathbf{z} \in U.$$ □

Bemerkung: Geometrisch handelt es sich bei der Menge U um eine Gerade, die durch den Nullpunkt geht. Das nächste Beispiel verallgemeinert das letzte Beispiel in dem nun nicht mehr ein einzelner Vektor $\mathbf{z}$ den Raum U erzeugt, sondern der Untervektor-Raum durch eine beliebige Menge M von Vektoren erzeugt wird.

Beispiel: Es sei V ein $\mathbb{K}$-Vektor-Raum und $M \subseteq V$ sei eine nicht-leere Menge von Vektoren. Dann definieren wir die Menge $span_{\mathbb{K}}(M)$ als die Menge aller endlichen Linear-Kombinationen von Vektoren aus M, wir setzen also

$$span_{\mathbb{K}}(M) := \big\{\alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_n \cdot \mathbf{x}_n \mid n \in \mathbb{N} \wedge \forall i \in \{1, \cdots, n\} : \alpha_i \in \mathbb{K} \wedge \mathbf{x}_i \in M\big\}.$$

Dann ist die so definierte Menge $span_{\mathbb{K}}(M)$ ein Untervektor-Raum von V.

Beweis: Es sind drei Eigenschaften zu prüfen.

1. Da M nicht leer ist, finden wir ein $\mathbf{v} \in M$. Offenbar gilt

$$\mathbf{0} = 0 \cdot \mathbf{v} \in span_{\mathbb{K}}(M).$$

2. Es seien $\mathbf{x}, \mathbf{y} \in span_{\mathbb{K}}(M)$. Dann gibt es $m, n \in \mathbb{N}$, sowie $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n \in \mathbb{K}$ und $\mathbf{x}_1, \cdots, \mathbf{x}_m, \mathbf{y}_1, \cdots, \mathbf{y}_n \in M$, so dass

$$\mathbf{x} = \alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_m \cdot \mathbf{x}_m \quad \text{und} \quad \mathbf{y} = \beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n$$

gilt. Damit haben wir

$$\mathbf{x} + \mathbf{y} = \alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_m \cdot \mathbf{x}_m + \beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n \in span_{\mathbb{K}}(M)$$

denn die Summe $\alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_m \cdot \mathbf{x}_m + \beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n$ ist auch wieder eine Linear-Kombination von Vektoren aus M.

3. Nun sei $\mathbf{x} \in span_{\mathbb{K}}(M)$ und $\alpha \in \mathbb{K}$. Dann gibt es zunächst ein $n \in \mathbb{N}$ sowie Skalare $\beta_1, \cdots, \beta_n$ und Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_n \in M$, so dass

$$\mathbf{x} = \beta_1 \cdot \mathbf{x}_1 + \cdots + \beta_m \cdot \mathbf{x}_m$$

gilt. Damit haben wir

$$\alpha \cdot \mathbf{x} = \alpha \cdot (\beta_1 \cdot \mathbf{x}_1 + \cdots + \beta_m \cdot \mathbf{x}_m) = (\alpha \cdot \beta_1) \cdot \mathbf{x}_1 + \cdots + (\alpha \cdot \beta_m) \cdot \mathbf{x}_m \in span_{\mathbb{K}}(M).$$ □

Beispiel: Es sei $\mathcal{C}(\mathbb{R})$ die Menge der (bereits früher definierten) stetigen reellwertigen Funktionen. Weiter sei $c \in \mathbb{R}$ beliebig. Definieren wir die Menge N_c als

$$N_c := \{f \in \mathcal{C}(\mathbb{R}) \mid f(c) = 0\},$$

also als die Menge der stetigen Funktionen f, die bei c eine Nullstelle haben, dann ist N_c ein Untervektor-Raum von $\mathcal{C}(\mathbb{R})$.

Aufgabe 55: Beweisen Sie, dass N_c ein Untervektor-Raum von $\mathcal{C}(\mathbb{R})$ ist.

Satz 9.14 Ist V ein Vektor-Raum und sind U_1 und U_2 Untervektor-Räume von V, so ist auch die Menge $U_1 \cap U_2$ ein Untervektor-Raum von V.

Beweis: Wir haben drei Eigenschaften nachzuweisen.

1. Da U_1 und U_2 Untervektor-Räume sind, gilt
$$\mathbf{0} \in U_1 \quad \text{und} \quad \mathbf{0} \in U_2, \quad \text{woraus sofort} \quad \mathbf{0} \in U_1 \cap U_2 \quad \text{folgt.}$$
2. Seien $\mathbf{x}, \mathbf{y} \in U_1 \cap U_2$. Dann gilt natürlich
$$\mathbf{x} \in U_1, \quad \mathbf{x} \in U_2, \quad \mathbf{y} \in U_1, \quad \text{und} \quad \mathbf{y} \in U_2.$$
Da U_1 und U_2 Untervektor-Räume sind, folgt dann
$$\mathbf{x} + \mathbf{y} \in U_1 \quad \text{und} \quad \mathbf{x} + \mathbf{y} \in U_2,$$
also insgesamt
$$\mathbf{x} + \mathbf{y} \in U_1 \cap U_2.$$
3. Sei nun $\mathbf{x} \in U_1 \cap U_2$ und $\alpha \in \mathbb{K}$. Daraus folgt sofort
$$\mathbf{x} \in U_1 \quad \text{und} \quad \mathbf{x} \in U_2.$$
Da U_1 und U_2 Untervektor-Räume sind, können wir folgern, dass
$$\alpha \cdot \mathbf{x} \in U_1 \quad \text{und} \quad \alpha \cdot \mathbf{x} \in U_2$$
gilt, so dass wir insgesamt
$$\alpha \cdot \mathbf{x} \in U_1 \cap U_2$$
haben. □

Aufgabe 56: Es sei V ein Vektor-Raum und U_1 und U_2 seien Untervektor-Räume von V. Beweisen oder widerlegen Sie, dass dann auch die Menge $U_1 \cup U_2$ ein Untervektor-Raum von V ist.

Kapitel 10

Lineare Abbildungen

Der Begriff der *linearen Abbildungen* ist neben dem Begriff des Vektor-Raums einer der zentralen Begriffe in der Theorie der linearen Algebra. In diesem Kapitel führen wir lineare Abbildungen ein und zeigen, wie diese durch *Matrizen* dargestellt werden können. Wir definieren Addition und Multiplikation von Matrizen und zeigen, dass bestimmte Matrizen bezüglich der Multiplikation ein *Inverses* besitzen. Wir führen sogenannte *Elementar-Matrizen* ein und demonstrieren, wie sich mit Hilfe von Elementar-Matrizen das Inverse einer Matrix berechnen lässt.

Im Rest dieses Abschnittes bezeichnet $\mathbb{K}$ einen Körper. In den Anwendungen wird es sich dabei meistens um den Körper $\mathbb{R}$ der reellen Zahlen oder den Körper $\mathbb{C}$ der komplexen Zahlen handeln.

10.1 Definition der linearen Abbildungen

Definition 10.1 ($\mathcal{L}(V,W)$) Es seien V und W zwei $\mathbb{K}$-Vektor-Räume. Eine Funktion

$$f : V \to W$$

ist eine *lineare Abbildung* von V nach W genau dann, wenn Folgendes gilt:

1. $\forall \mathbf{x}, \mathbf{y} \in V : f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$,
   eine lineare Abbildung ist mit der Addition verträglich.
2. $\forall \alpha \in \mathbb{K} : \forall \mathbf{x} \in V : f(\alpha \cdot \mathbf{x}) = \alpha \cdot f(\mathbf{x})$,
   eine lineare Abbildung ist auch mit der Skalar-Multiplikation verträglich.

Die Menge aller linearen Abbildungen von V nach W wird mit $\mathcal{L}(V,W)$ bezeichnet, es gilt also

$$\mathcal{L}(V,W) := \{f \in W^V \mid f \text{ ist lineare Abbildung}\}.$$

Auf der Menge $\mathcal{L}(V,W)$ definieren wir eine Addition

$$+ : \mathcal{L}(V,W) \times \mathcal{L}(V,W) \to \mathcal{L}(V,W)$$

punktweise, das heißt für $f, g \in \mathcal{L}(V,W)$ definieren wir die lineare Abbildung $f + g$, indem wir fordern, dass für alle $\mathbf{x} \in V$

$$(f+g)(\mathbf{x}) := f(\mathbf{x}) + g(\mathbf{x})$$

gilt. Weiter definieren wir die Null-Abbildung $\mathbf{0} : V \to W$, indem wir für alle $\mathbf{x} \in V$

$$\mathbf{0}(\mathbf{x}) := \mathbf{0}$$

setzen. Schließlich definieren wir eine Skalar-Multiplikation von Elementen des Körpers $\mathbb{K}$ mit linearen Abbildung aus $\mathcal{L}(V,W)$. Diese Skalar-Multiplikation bezeichnen wir durch den Operator "$\cdot$". Es ist also

$$\cdot : \mathbb{K} \times \mathcal{L}(V,W) \to \mathcal{L}(V,W)$$

und wir definieren für alle $\alpha \in \mathbb{K}$, $f \in \mathcal{L}(V, W)$ und alle $\mathbf{x} \in V$

$$(\alpha \cdot f)(\mathbf{x}) := \alpha \cdot f(x).$$ ◇

Aufgabe 57: Es seien V und W zwei $\mathbb{K}$-Vektor-Räume und $\mathcal{L}(V, W)$ bezeichne die oben definierte Menge der linearen Abbildungen von V nach W. Beweisen Sie die folgenden Behauptungen:

1. Wenn $f, g \in \mathcal{L}(V, W)$ ist, dann gilt $f + g \in \mathcal{L}(V, W)$.
2. Wenn $\alpha \in \mathbb{K}$ und $f \in \mathcal{L}(V, W)$ ist, dann gilt $\alpha \cdot f \in \mathcal{L}(V, W)$.
3. $\big\langle \langle \mathcal{L}(V, W), \mathbf{0}, + \rangle, \cdot \big\rangle$ ist ein $\mathbb{K}$-Vektor-Raum. ◇

Bemerkung: Wir können die beiden Eigenschaften, die in der Definition einer linearen Abbildung gefordert werden, zu einer einzigen Eigenschaft zusammenfassen, denn die Abbildung $f : V \to W$ ist genau dann linear, wenn

$$\forall \alpha, \beta \in \mathbb{K} : \forall \mathbf{x}, \mathbf{y} \in V : f(\alpha \cdot \mathbf{x} + \beta \cdot \mathbf{y}) = \alpha \cdot f(\mathbf{x}) + \beta \cdot f(\mathbf{y})$$

gilt. Weiter bemerken wir, dass für eine lineare Abbildung $f : V \to W$ immer

$$f(\mathbf{0}) = \mathbf{0}$$

gilt, denn wir haben

$$f(\mathbf{0}) = f(0 \cdot \mathbf{0}) = 0 \cdot f(\mathbf{0}) = \mathbf{0}.$$ ◇

Bemerkung: In der Literatur wird eine lineare Abbildung $f : V \to W$ von einem Vektor-Raum V in einen Vektor-Raum W auch als ein *Vektor-Raum-Homomorphismus* oder kürzer als ein *Homomorphismus* bezeichnet. Ist die Abbildung f außerdem noch injektiv, so heißt f ein *Monomorphismus*. Ist f surjektiv, so sprechen wir von einem *Epimorphismus* und wenn f sowohl injektiv als auch surjektiv ist, dann ist f ein *Isomorphismus*. Gilt $V = W$, hat f also die Form $f : V \to V$, so nennen wir f einen *Endomorphismus* und wenn sowohl $V = W$ gilt, als auch die Funktion f bijektiv ist, dann ist f ein *Automorphismus*. Der Übersichtlichkeit halber fassen wir diese Begriffe wie folgt zusammen:

1. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ ist, dann ist f ein Homomorphismus.
2. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ injektiv ist, dann ist f ein Monomorphismus.
3. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ surjektiv ist, dann ist f ein Epimorphismus.
4. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ bijektiv ist, dann ist f ein Isomorphismus.
5. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{V})$ ist, dann ist f ein Endomorphismus.
6. Wenn $f \in \mathcal{L}(\mathcal{V}, \mathcal{V})$ bijektiv ist, dann ist f ein Automorphismus. ◇

In der englischen Literatur wird ein Endomorphismus $f \in \mathcal{L}(V, V)$ auch als ein *Operator auf* V bezeichnet. Wir definieren zur Abkürzung

$$\mathcal{L}(V) := \mathcal{L}(V, V).$$

Folglich bezeichnet $\mathcal{L}(V)$ die Menge der Operatoren auf dem Vektor-Raum V. ◇

Beispiel: Es sei $\mathbb{K}^{\mathbb{N}}$ der Vektor-Raum der $\mathbb{K}$-wertigen Folgen. Wir definieren eine Abbildung L, die eine gegebene Folge um das erste Element verkürzt, die also die Folge nach links schiebt. Formal setzen wir

$$L\big((x_n)_{n\in\mathbb{N}}\big) := (x_{n+1})_{n\in\mathbb{N}}.$$

Weniger formal aber dafür intuitiver könnten wir auch

$$L\big((x_0, x_1, x_2, x_3, \cdots)\big) := (x_1, x_2, x_3, \cdots)$$

schreiben. Dann ist die Abbildung L eine lineare Abbildung auf $\mathbb{K}^{\mathbb{N}}$. ◇

Beispiel: Es sei $\mathcal{C}(R)$ die Menge der stetigen Funktionen auf $\mathbb{R}$ und $\mathcal{D}(\mathbb{R})$ die Menge aller Funktionen $f : \mathbb{R} \to \mathbb{R}$, die überall differenzierbar sind und deren Ableitung stetig ist. Definieren wir eine Funktion

$$\tfrac{d}{dx} : \mathcal{D}(\mathbb{R}) \to \mathcal{C}(\mathbb{R}) \quad \text{durch } \tfrac{d}{dx}(f) := f'(x),$$

wobei $f'(x)$ die Ableitung der Funktion f an der Stelle x ist, so ist die Funktion $\frac{d}{dx}$ eine lineare Abbildung, denn für die Ableitung gilt

$$\tfrac{d}{dx}(\alpha \cdot f + \beta \cdot g) = \alpha \cdot \tfrac{d}{dx} f + \beta \cdot \tfrac{d}{dx} g.$$ ◇

10.1.1 Kern und Bild einer linearen Abbildung

Definition 10.2 (Kern) Es seien V und W zwei Vektor-Räume und $f : V \to W$ sei ein lineare Abbildung. Dann definieren wir

$$\mathit{Kern}(f) := \{\mathbf{x} \in V \mid f(\mathbf{x}) = \mathbf{0}\}.$$

Der Kern einer linearen Abbildung ist also die Menge aller Vektoren aus V, die auf den Null-Vektor abgebildet werden. ◇

Satz 10.3 Ist $f : V \to W$ eine lineare Abbildung, so ist $\mathit{Kern}(f)$ ein Untervektor-Raum von V.

Beweis: Wir haben die drei Eigenschaften von Untervektor-Räumen nachzuweisen.

1. Wir haben oben bereits gesehen, dass für eine lineare Abbildung $f(\mathbf{0}) = \mathbf{0}$ gilt. Daraus folgt sofort $\mathbf{0} \in \mathit{Kern}(f)$.

2. Seien $\mathbf{x}, \mathbf{y} \in \mathit{Kern}(f)$. Dann haben wir nach Definition von $\mathit{Kern}(f)$

   $$f(\mathbf{x}) = \mathbf{0} \quad \text{und} \quad f(\mathbf{y}) = \mathbf{0}.$$

   Daraus folgt zunächst

   $$f(\mathbf{x}) + f(\mathbf{y}) = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

   und da f eine lineare Abbildung ist, können wir diese Gleichung zu

   $$f(\mathbf{x} + \mathbf{y}) = \mathbf{0}$$

   umformen, was uns zeigt, dass

   $$\mathbf{x} + \mathbf{y} \in \mathit{Kern}(f)$$

   ist, so dass die Menge $\mathit{Kern}(f)$ unter der Addition abgeschlossen ist.

3. Sei $\alpha \in \mathbb{K}$ und $\mathbf{x} \in \mathit{Kern}(f)$. Dann haben wir nach Definition von $\mathit{Kern}(f)$

   $$f(\mathbf{x}) = \mathbf{0}.$$

   Daraus folgt zunächst

   $$\alpha \cdot f(\mathbf{x}) = \alpha \cdot \mathbf{0} = \mathbf{0}$$

   und da f eine lineare Abbildung ist, können wir diese Gleichung zu

   $$f(\alpha \cdot \mathbf{x}) = \mathbf{0}$$

   umformen, was uns zeigt, dass

   $$\alpha \cdot \mathbf{x} \in \mathit{Kern}(f)$$

   ist, so dass die Menge $\mathit{Kern}(f)$ auch unter der Skalar-Multiplikation abgeschlossen ist. □

Satz 10.4 Es seien V und W Vektor-Räume und $f : V \to W$ sei eine lineare Abbildung. Dann ist f genau dann injektiv, wenn $\mathit{Kern}(f) = \{\mathbf{0}\}$ gilt.

Beweis: Wir zerlegen den Beweis in zwei Teile.

"⇒": Wir nehmen zunächst an, dass f injektiv ist. Es ist klar, dass

$$f(\mathbf{0}) = \mathbf{0}$$

gilt und damit gilt sicher $\mathbf{0} \in \mathit{Kern}(f)$. Sei nun zusätzlich $\mathbf{y} \in \mathit{Kern}(f)$, es gelte also

$$f(\mathbf{y}) = \mathbf{0}.$$

Da f injektiv ist, folgt aus $f(\mathbf{y}) = \mathbf{0}$ und $f(\mathbf{0}) = \mathbf{0}$

$$\mathbf{y} = \mathbf{0}$$

und damit ist $\mathit{Kern}(f) = \{\mathbf{0}\}$ gezeigt.

"⇐": Wir setzen jetzt $\mathit{Kern}(f) = \{\mathbf{0}\}$ voraus. Falls für $\mathbf{x}, \mathbf{y} \in V$ nun

$$f(\mathbf{x}) = f(\mathbf{y})$$

gilt, so können wir diese Gleichung auf Grund der Linearität von f zu

$$f(\mathbf{x} - \mathbf{y}) = \mathbf{0}$$

umschreiben. Daraus folgt aber

$$\mathbf{x} - \mathbf{y} \in \mathit{Kern}(f)$$

und da wir $\mathit{Kern}(f) = \{\mathbf{0}\}$ vorausgesetzt hatten, folgt

$$\mathbf{x} - \mathbf{y} = 0$$

woraus wir auf $\mathbf{x} = \mathbf{y}$ schließen können und das war zu zeigen. □

Definition 10.5 (Bild) Es seien V und W Vektor-Räume und $f : V \to W$ sei eine lineare Abbildung. Dann definieren wir

$$\mathit{Bild}(f) := \{f(\mathbf{x}) \mid \mathbf{x} \in V\}$$

als die Menge der Abbilder aller Vektoren aus V unter der Abbildung f. ◇

Aufgabe 58: Zeigen Sie: Ist $f : V \to W$ eine lineare Abbildung, so ist $\mathit{Bild}(f)$ ein Untervektor-Raum von W. ◇

Satz 10.6 (Dimensions-Satz) Es seien V_1 und V_2 endlich-dimensionale Vektor-Räume und die Funktion $f : V_1 \to V_2$ sei eine lineare Abbildung. Dann gilt

$$\mathit{dim}(V_1) = \mathit{dim}\big(\mathit{Kern}(f)\big) + \mathit{dim}\big(\mathit{Bild}(f)\big).$$

Beweis: Es sei $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ eine Basis von $\mathit{Kern}(f)$. Ist B eine Basis von V_1, so können wir mit Hilfe des Basis-Austausch-Satzes eine Menge W finden, so dass

$$B \backslash W \cup \{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$$

wieder eine Basis von V_1 ist. Es gelte

$$B \backslash W = \{\mathbf{y}_1, \cdots, \mathbf{y}_n\}.$$

Dann ist also insgesamt die Menge

$$\{\mathbf{x}_1, \cdots, \mathbf{x}_m, \mathbf{y}_1, \cdots, \mathbf{y}_n\}$$

eine Basis von V_1, so dass $\mathit{dim}(V_1) = m + n$. Wir müssen daher nur noch zeigen, dass

$$dim\big(Bild(f)\big) = n$$

gilt. Dazu zeigen wir, dass die Menge

$$\{f(\mathbf{y}_1), \cdots, f(\mathbf{y}_n)\}$$

eine Basis von $Bild(f)$ ist. Hier sind zwei Sachen nachzuweisen.

1. Wir zeigen: Die Menge $\{f(\mathbf{y}_1), \cdots, f(\mathbf{y}_n)\}$ ist ein Erzeugenden-System von $Bild(f)$.

   Sei $\mathbf{z} \in Bild(f)$. Dann gibt es ein $\mathbf{y} \in V_1$, so dass $\mathbf{z} = f(\mathbf{y})$ ist. Nun ist die Menge $\{\mathbf{x}_1, \cdots, \mathbf{x}_m, \mathbf{y}_1, \cdots, \mathbf{y}_n\}$ eine Basis von V_1. Folglich muss es Skalare $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n \in \mathbb{K}$ geben, so dass

   $$\alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_m \cdot \mathbf{x}_m + \beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n = \mathbf{y}$$

   ist. Wenden wir auf diese Gleichung die lineare Abbildung f an und berücksichtigen, dass $f(\mathbf{x}_i) = \mathbf{0}$ ist für alle $i \in \{1, \cdots, m\}$, denn $\mathbf{x}_i \in Kern(f)$, so erhalten wir

   $$\beta_1 \cdot f(\mathbf{y}_1) + \cdots + \beta_n \cdot f(\mathbf{y}_n) = \mathbf{z}.$$

   Damit haben wir $\mathbf{z}$ aber als Linear-Kombination der Menge $\{f(\mathbf{y}_1), \cdots, f(\mathbf{y}_n)\}$ dargestellt und das war zu zeigen.

2. Wir zeigen: Die Menge $\{f(\mathbf{y}_1), \cdots, f(\mathbf{y}_n)\}$ ist linear unabhängig.

   Seien $\beta_1, \cdots, \beta_n \in \mathbb{K}$ und gelte

   $$\beta_1 \cdot f(\mathbf{y}_1) + \cdots + \beta_n \cdot f(\mathbf{y}_n) = \mathbf{0}.$$

   Da f eine lineare Abbildung ist, können wir diese Gleichung zu

   $$f(\beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n) = \mathbf{0}$$

   umschreiben. Daraus folgt aber

   $$\beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n \in Kern(f).$$

   Da $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ eine Basis von $Kern(f)$ ist, muss es also Skalare $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ geben, so dass

   $$\alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_n \cdot \mathbf{x}_n = \beta_1 \cdot \mathbf{y}_1 + \cdots + \beta_n \cdot \mathbf{y}_n$$

   gilt. Diese Gleichung können wir zu

   $$\alpha_1 \cdot \mathbf{x}_1 + \cdots + \alpha_n \cdot \mathbf{x}_n + (-\beta_1) \cdot \mathbf{y}_1 + \cdots + (-\beta_n) \cdot \mathbf{y}_n = \mathbf{0}$$

   umstellen. Da die Menge $\{\mathbf{x}_1, \cdots, \mathbf{x}_m, \mathbf{y}_1, \cdots, \mathbf{y}_n\}$ eine Basis von V_1 ist, folgt daraus

   $$\alpha_1 = 0 \wedge \cdots \wedge \alpha_m = 0 \wedge -\beta_1 = 0 \wedge \cdots \wedge -\beta_n = 0.$$

   Damit haben also die β_i alle den Wert 0 und das war zu zeigen. □

Bemerkung: Der Dimensions-Satz wird in der Literatur auch als *Rang-Satz* bezeichnet. ◇

Aufgabe 59: Es sei V ein endlich-dimensionaler $\mathbb{K}$-Vektor-Raum und es sei $f \in \mathcal{L}(V)$. Zeigen Sie, dass f genau dann surjektiv ist, wenn f injektiv ist. ◇

10.2 Matrizen

Es seien V und W Vektor-Räume und f sei eine lineare Abbildung. Weiter sei $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ eine Basis von V und $\{\mathbf{y}_1, \cdots, \mathbf{y}_n\}$ sei eine Basis von W. Für alle $j \in \{1, \cdots, m\}$ ist zunächst $f(\mathbf{x}_j)$ ein Vektor aus W und da $\{\mathbf{y}_1, \cdots, \mathbf{y}_n\}$ ein Basis von W ist, gibt es dann eindeutig bestimmte Skalare $a_{i,j}$, so dass der Vektor $f(\mathbf{x}_j)$ sich als Linear-Kombination

$$f(\mathbf{x}_j) = \sum_{i=1}^{n} a_{i,j} \cdot \mathbf{y}_i$$

schreiben lässt. Ist nun allgemein $\mathbf{x}$ ein Vektor aus V, so lässt sich $\mathbf{x}$ in der Form

$$\mathbf{x} = \sum_{j=1}^{m} \beta_j \cdot \mathbf{x}_j$$

schreiben, denn $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ ist ja eine Basis von V. Wenden wir auf diese Gleichung die Funktion f an, so erhalten wir

$$\begin{aligned} f(\mathbf{x}) &= f\left(\sum_{j=1}^{m} \beta_j \cdot \mathbf{x}_j\right) \\ &= \sum_{j=1}^{m} \beta_j \cdot f(\mathbf{x}_j) \\ &= \sum_{j=1}^{m} \beta_i \cdot \sum_{i=1}^{n} a_{i,j} \cdot \mathbf{y}_i \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j} \cdot \beta_j\right) \cdot \mathbf{y}_i. \end{aligned}$$

Damit sehen wir, dass lineare Abbildung f in dem Moment, wo wir die Basen $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ von V und $\{\mathbf{y}_1, \cdots, \mathbf{y}_n\}$ von W festgelegt haben, vollständig durch die $n \cdot m$ Zahlen $\left(a_{i,j}\right)_{\substack{i=1,\cdots,n \\ j=1,\cdots,m}}$ festgelegt werden. Diese Zahlen werden daher zu einer $n \times m$ *Matrix*

$$A := \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

zusammengefasst. Die Menge aller $n \times m$ Matrizen mit Koeffizienten $a_{i,j} \in \mathbb{K}$ für alle $i \in \{1, \cdots, n\}$ und $j \in \{1, \cdots, m\}$ schreiben wir als $\mathbb{K}^{n \times m}$.

Definition 10.7 ($\mathcal{M}(f)$) Sind V und W zwei $\mathbb{K}$-Vektor-Räume und bilden die Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_m$ und $\mathbf{y}_1, \cdots, \mathbf{y}_n$ eine Basis von V beziehungsweise von W und ist weiter $f \in \mathcal{L}(V, W)$, so bezeichnen wir die oben definierte Matrix $A \in \mathbb{K}^{n \times m}$ mit $\mathcal{M}(f)$, wir setzen also

$$\mathcal{M}(f) := A. \qquad \diamond$$

Bemerkung: Eigentlich ist die Schreibweise $\mathcal{M}(f)$ nur dann eindeutig, wenn die Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_m$ und $\mathbf{y}_1, \cdots, \mathbf{y}_n$ festgelegt sind. Es gibt Autoren, die deswegen die Notation

$$\mathcal{M}(f; \mathbf{x}_1, \cdots, \mathbf{x}_m; \mathbf{y}_1, \cdots, \mathbf{y}_n) \quad \text{an Stelle von} \quad \mathcal{M}(f)$$

schreiben. Diese Schreibweise ist mir aber zu schwerfällig. Wir setzen im Folgenden voraus, dass immer, wenn die Funktion $\mathcal{M}$ verwendet wird, klar ist, auf Basis welcher Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_m$ und $\mathbf{y}_1, \cdots, \mathbf{y}_n$ der Ausdruck $\mathcal{M}(f)$ definiert ist.

Zusätzlich ist noch die folgende Spitzfindigkeit zu beachten: Wenn wir sagen, dass $B = \{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ eine Basis von V ist, dann ist die Reihenfolge der Vektoren nicht festgelegt, denn eine Basis ist eine Menge und dort gibt es keine Reihenfolge. Daher ist die oben definierte Abbildung $\mathcal{M} : \mathcal{L}(V, W) \to \mathbb{K}^{n \times m}$ streng genommen nur dann eindeutig definiert, wenn wir die Reihenfolge der Vektoren in den beteiligten Basen fixieren. Wir setzen im Folgenden voraus, dass es in den Anwendungen von $\mathcal{M}$ immer eine kanonische Reihenfolge der Elemente der beiden beteiligten Basen gibt, auf die wir uns bei der Definition von $\mathcal{M}(f)$ dann beziehen können. $\diamond$

Ist $A \in \mathbb{K}^{n \times m}$ eine Matrix und ist

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \mathbb{K}^m,$$

so definieren wir das *Produkt* $A \cdot \mathbf{x}$ als den Vektor

$$\mathbf{y} := A \cdot \mathbf{x} = \begin{pmatrix} \sum\limits_{j=1}^{m} a_{1,j} \cdot x_j \\ \vdots \\ \sum\limits_{j=1}^{m} a_{i,j} \cdot x_j \\ \vdots \\ \sum\limits_{j=1}^{m} a_{n,j} \cdot x_j \end{pmatrix}.$$

Zur Berechnung der i-ten Komponente des Vektors $A \cdot \mathbf{x}$ wird der Vektor $\mathbf{x}$ also komponentenweise mit der i-ten Zeile der Matrix A multipliziert und diese Produkte werden dann aufaddiert.

Bemerkung: Wir hatten die Vektoren aus $\mathbb{K}^n$ ursprünglich als Listen der Form $\mathbf{x} = [x_1, \cdots, x_n]$ mit $x_i \in \mathbb{K}$ für alle $i \in \{1, \cdots, n\}$ definiert. Diese Schreibweise ist wesentlich platzsparender als die Schreibweise

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix},$$

bei der wir $\mathbf{x}$ als *Spalten-Vektor* bezeichnen. Im Zusammenhang mit der Multiplikation von Matrizen mit Vektoren ist die Spaltenschreibweise allerdings suggestiver, so dass wir Vektoren in Zusammenhang mit der Matrizen-Multiplikation in der Spaltenschreibweise darstellen. ◇

Aufgabe 60: Es sei $A \in \mathbb{K}^{n \times m}$. Zeigen Sie, dass die Abbildung

$$f : \mathbb{K}^m \to \mathbb{K}^n,$$

die für alle $\mathbf{x} \in \mathbb{K}^m$ durch

$$f(\mathbf{x}) := A \cdot \mathbf{x}$$

definiert ist, eine lineare Abbildung ist. ◇

10.2.1 Addition und Skalar-Multiplikation von Matrizen

Es seien $A, B \in \mathbb{K}^{n \times m}$ und in Komponentenschreibweise gelte $A = (a_{i,j})$ und $B = (b_{i,j})$, wobei der Index i von 1 bis n und der Index j von 1 bis m läuft. Dann definieren wir die Summe $C := A + B$ so, dass $C = (a_{i,j} + b_{i,j})$ gilt, die Komponenten der Matrix C werden also durch Addition der Komponenten von A und B definiert. Mit dieser Definition ist leicht zu sehen, dass für beliebige Vektoren $\mathbf{x} \in \mathbb{K}^m$ die Gleichung

$$(A + B) \cdot \mathbf{x} = A \cdot \mathbf{x} + B \cdot \mathbf{x}$$

gilt. Dieses Distributiv-Gesetz ist der Grund dafür, dass die Addition von Matrizen wie oben angegeben definiert wird.

Für Matrizen lässt sich außerdem eine Skalar-Multiplikation definieren: Ist $\alpha \in \mathbb{K}$ und ist $A \in \mathbb{K}^{n \times m}$, wobei $A = (a_{i,j})$ gilt, so definieren wir die $n \times m$ Matrix $C := \alpha \cdot A$ so, dass in Komponentenschreibweise $C = (\alpha \cdot a_{i,j})$ gilt. Mit dieser Definition gilt für beliebige Vektoren $\mathbf{x} \in \mathbb{K}^m$ die Gleichung

$$\alpha \cdot (A \cdot \mathbf{x}) = (\alpha \cdot A) \cdot \mathbf{x} = A \cdot (\alpha \cdot \mathbf{x}).$$

Diese Gleichungen zeigen, dass die Skalar-Multiplikation für Matrizen mit der Multiplikation einer Matrix mit einem Vektor verträglich ist.

Bemerkung: Nachdem wir die Addition und Skalar-Multiplikation von Matrizen definiert haben, ist leicht nachzurechnen, dass die Menge $\mathbb{K}^{n\times m}$ der $n \times m$ Matrizen mit diesen Operationen zu einem Vektor-Raum wird. Das neutrale Element bezüglich der Addition ist die Null-Matrix, deren sämtliche Komponenten den Wert 0 haben.

Bemerkung: Sind V und W zwei endlich-dimensionale Vektor-Räume mit Basen $\{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ und $\{\mathbf{y}_1, \cdots, \mathbf{y}_n\}$ und sind $f, g \in \mathcal{L}(V, W)$ und ist $\alpha \in \mathbb{K}$, so gilt

$$\mathcal{M}(f + g) := \mathcal{M}(f) + \mathcal{M}(g) \quad \text{und} \quad \mathcal{M}(\alpha \cdot f) := \alpha \cdot \mathcal{M}(f).$$

Diese beiden Eigenschaften motivieren nachträglich sowohl die Definition der Addition von Matrizen als auch die Definition der Skalar-Multiplikation einer Matrizen. Sie zeigen, dass $\mathcal{M}$ eine lineare Abbildung des Vektor-Raums $\mathcal{L}(V, W)$ in den Vektor-Raum $\mathcal{K}^{m\times n}$ ist. Es handelt sich bei dieser Abbildung um einen Isomorphismus. ◇

10.2.2 Matrizen-Multiplikation

Sind $l, m, n \in \mathbb{N}$ und sind $A \in \mathbb{K}^{m\times l}$ und $B \in \mathbb{K}^{n\times m}$ Matrizen, so können wir zwei lineare Abbildungen

$$f : \mathbb{K}^l \to \mathbb{K}^m \quad \text{und} \quad g : \mathbb{K}^m \to \mathbb{K}^n$$

durch die Festlegung

$$f(\mathbf{x}) := A \cdot \mathbf{x} \quad \text{f.a. } \mathbf{x} \in \mathbb{K}^l, \quad \text{und} \quad g(\mathbf{y}) := B \cdot \mathbf{y} \quad \text{f.a. } \mathbf{y} \in \mathbb{K}^m,$$

definieren. Da der Werte-Bereich der Funktion f eine Teilmenge des Definitions-Bereichs der Funktion g ist, können wir die beiden Funktionen zu einer neuen Funktion h verknüpfen, indem wir

$$h(\mathbf{x}) := (g \circ f)(\mathbf{x}) = g(f(\mathbf{x}))$$

definieren. Sie können leicht nachweisen, dass die Funktion h wieder eine lineare Funktion ist und dass

$$h : \mathbb{K}^l \to \mathbb{K}^n$$

gilt. Folglich muss sich die Funktion h ebenfalls durch eine $l \times n$ Matrix C darstellen lassen, die wir nun berechnen wollen. Es gilt

$$
\begin{aligned}
h(\mathbf{x}) &= g(f(\mathbf{x})) \\
&= B \cdot (A \cdot \mathbf{x}) \\
&= B \cdot \begin{pmatrix} \vdots \\ \sum\limits_{j=1}^{l} a_{i,j} \cdot x_j \\ \vdots \end{pmatrix} \\
&= \begin{pmatrix} \vdots \\ \sum\limits_{k=1}^{m} b_{i,k} \cdot \left(\sum\limits_{j=1}^{l} a_{k,j} \cdot x_j \right) \\ \vdots \end{pmatrix} \\
&= \begin{pmatrix} \vdots \\ \sum\limits_{j=1}^{l} \left(\sum\limits_{k=1}^{m} b_{i,k} \cdot a_{k,j} \right) \cdot x_j \\ \vdots \end{pmatrix}.
\end{aligned}
$$

Definieren wir also die Komponenten der Matrix $C = (c_{i,j})$ als

$$c_{i,j} := \sum_{k=1}^{m} b_{i,k} \cdot a_{k,j} \quad \text{f.a. } i \in \{1, \cdots, n\}, j \in \{1, \cdots, m\},$$

so sehen wir, dass diese Matrix dasselbe bewirkt, wie die sukzessive Anwendung der Matrizen A und B. Daher definieren wir für eine $n \times m$ Matrix $B \in \mathbb{K}^{n \times m}$ der Form $B = (b_{i,k})$ und eine $m \times l$ Matrix $A \in \mathbb{K}^{m \times l}$ der Form $A = (a_{k,j})$ die Produkt-Matrix $C = B \cdot A$ als die Matrix $C = (c_{i,j})$, deren Komponenten durch die Gleichung

$$c_{i,j} := \sum_{k=1}^{m} b_{i,k} \cdot a_{k,j} \quad \text{f.a. } i \in \{1, \cdots, n\}, j \in \{1, \cdots, l\},$$

gegeben sind.

Bemerkung: Sind V_1, V_2 und V_3 Vektor-Räume mit

$$\texttt{dim}(V_1) = l, \quad \texttt{dim}(V_2) = m \quad \text{und} \quad \texttt{dim}(V_3) = n$$

und gilt

$$f \in \mathcal{L}(V_1, V_2) \text{ und } g \in \mathcal{L}(V_2, V_3),$$

dann haben wir die Matrizen-Multiplikation gerade so definiert, dass

$$\mathcal{M}(g \circ f) = \mathcal{M}(g) \cdot \mathcal{M}(f)$$

gilt. ◇

Aufgabe 61: Zeigen Sie, dass für die Matrizen-Multiplikation das Assoziativ-Gesetz gilt. ◇

Aufgabe 62: Beweisen oder widerlegen Sie, dass die Matrizen-Multiplikation kommutativ ist. ◇

Unser Ziel im Rest dieses Abschnittes ist es zu zeigen, dass bestimmte *quadratische Matrizen* ein Inverses besitzen. Dabei nennen wir eine Matrix $A \in \mathbb{K}^{m \times n}$ *quadratisch* falls $m = n$ ist. Um für die Matrizen-Multiplikation ein neutrales Element definieren zu können, definieren wir zunächst das nach Leopold Kronecker benannte *Kronecker-Delta*.

Definition 10.8 (Kronecker-Delta) Für $i, j \in \mathbb{N}$ definieren wir

$$\delta_{i,j} := \begin{cases} 1 & \text{falls } i = j; \\ 0 & \text{falls } i \neq j. \end{cases}$$ ◇

Damit sind wir in der Lage, für alle $n \in \mathbb{N}$ eine *Einheits-Matrix* E_n zu definieren. Wir definieren $\mathrm{E}_n \in \mathbb{K}^{n \times n}$ als die Matrix, die nur auf der fallenden Diagonale mit Einsen besetzt ist, alle anderen Einträge sind Null. Formal gilt

$$\mathrm{E}_n = \big(\delta_{i,j}\big)_{\substack{i=1,\cdots,n \\ j=1,\cdots,n}},$$

wobei $\delta_{i,j}$ das eben definierte Kronecker-Delta bezeichnet. Im Falle $n = 2$ haben wir beispielsweise

$$E_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und im Falle $n = 3$ gilt

$$E_3 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ist $A \in \mathbb{K}^{m \times n}$, so gilt

$$A \cdot \mathrm{E}_n = A,$$

denn wenn wir $C := A \cdot \mathrm{E}_n$ definieren und in Komponentenschreibweise $C = (c_{i,j})$ haben, so gilt nach der Definition der Matrizen-Multiplikation

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} \cdot \delta_{k,j} = a_{i,j},$$

wobei wir bei der letzten Gleichung ausgenutzt haben, dass auf Grund der Definition des Kronecker-Deltas von der Summe nur der Term mit $k = j$ übrig bleibt. Genauso lässt sich auch zeigen, dass $E_m \cdot A = A$ ist.

Definition 10.9 (Invertierbare Matrix) Eine quadratische Matrix $A \in \mathbb{K}^{n \times n}$ ist *invertierbar* genau dann, wenn es eine Matrix $B \in \mathbb{K}^{n \times n}$ gibt, so dass

$$A \cdot B = B \cdot A = \mathrm{E}_n$$

gilt. In diesem Fall definieren wir $A^{-1} := B$ und sagen, dass B das *Inverse* der Matrix A ist. □

Bemerkung: Wenn es eine Matrix B gibt, so dass $A \cdot B = E_n$ gilt, dann kann gezeigt werden, dass daraus bereits $B \cdot A = E_n$ folgt. ◇

Aufgabe 63: Es sei $A \in \mathbb{K}^{2 \times 2}$ gegeben als

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

und es gelte $a \cdot d \neq b \cdot c$. Zeigen Sie, dass die Matrix A ein Inverses hat und berechnen Sie dieses Inverse. Machen Sie dazu den Ansatz

$$A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

und bestimmen Sie die Zahlen e, f, g und h aus der Forderung, dass $A^{-1} \cdot A = E_2$ gelten muss. ◇

Bemerkung: Ein lineares Gleichungs-System mit n Gleichungen und n Variablen lässt sich in der Form $A \cdot \mathbf{x} = \mathbf{x}$ schreiben, wobei $A \in \mathbb{K}^{n \times n}$ ist. Beispielsweise können wir das lineare Gleichungs-System

$$\begin{aligned} 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 &= 4 \\ 5 \cdot x_1 + 6 \cdot x_2 + 7 \cdot x_3 &= 8 \\ 9 \cdot x_1 + 6 \cdot x_2 + 3 \cdot x_3 &= 1 \end{aligned}$$

kürzer als

$$A \cdot \mathbf{x} = \mathbf{b}$$

schreiben, wenn wir

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 6 & 3 \end{pmatrix} \quad \text{und} \quad \mathbf{b} := \begin{pmatrix} 4 \\ 8 \\ 1 \end{pmatrix}$$

definieren. Wenn wir nun Glück haben und die Matrix A invertierbar ist, so können wir die Gleichung $A \cdot \mathbf{x} = \mathbf{b}$ von links mit A^{-1} multiplizieren. Dann erhalten wir

$$A^{-1} \cdot A \cdot \mathbf{x} = A^{-1} \cdot \mathbf{b}$$

was wegen $A^{-1} \cdot A \cdot \mathbf{x} = \mathrm{E}_n \cdot \mathbf{x} = \mathbf{x}$ zu

$$\mathbf{x} = A^{-1} \cdot \mathbf{b}$$

äquivalent ist. Falls wir also in der Lage sind, die Matrix A zu invertieren, dann können wir anschließend das Lösen der Gleichung $A \cdot \mathbf{x} = \mathbf{b}$ auf eine Matrix-Multiplikation zurück führen. Da das Inverse A^{-1} nicht von dem Vektor $\mathbf{b}$ abhängt, ist dies dann ein sinnvolles Vorgehen, wenn die Gleichung $A \cdot \mathbf{x} = \mathbf{b}$ für mehrere verschiedene Werte von $\mathbf{b}$ gelöst werden soll. ◇

Definition 10.10 Es sei $n \in \mathbb{N}$, $k \in \{1, \cdots, m\}$ und $l \in \{1, \cdots, n\}$. Dann definieren wir die $n \times n$ *Atomar-Matrix* $\mathrm{A}(k,l)$ so, dass in Komponentenschreibweise

$$\mathrm{A}_n(k,l) = (\delta_{i,k} \cdot \delta_{l,j})_{\substack{i=1,\cdots,n \\ j=1,\cdots,n}}$$

gilt. Die Atomar-Matrix $\mathrm{A}(k,l)$ hat damit genau in der k-ten Zeile in der l-ten Spalte eine Eins und alle anderen Einträge der Matrix sind Null. ◇

Aufgabe 64: Es gelte $B \in \mathbb{K}^{n \times n}$ und $\mathrm{A}_n(k,l) \in \mathbb{K}^{n \times n}$ sei eine Atomar-Matrix. Wir definieren $C := \mathrm{A}_n(k,l) \cdot B$. Zeigen Sie, dass in C in genau eine Zeile von 0 verschiedene Werte auftreten. Dies ist die k-te Zeile und die Werte, die hier auftreten, sind die Werte, die in der l-ten Zeile von B stehen. Der Effekt der Multiplikation von $A(\mathrm{k},l)$ mit B besteht also darin, dass die l-te Zeile in die k-te Zeile verschoben wird und dass alle anderen Zeilen gelöscht werden. Schreiben wir die Matrix B in der Form

$$B = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix},$$

wobei $\mathbf{b}_i$ die i-te Zeile der Matrix B bezeichnet, die wir als Vektor auffassen und ist $l < k$, dann gilt also

$$\mathrm{A}_n(k,l) \cdot B = \mathrm{A}_n(k,l) \cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{0} \end{pmatrix},$$

falls $l < k$ ist. $\diamond$

Wir definieren nun drei verschiedene Arten von sogenannten *Elementar-Matrizen*. Die Zeilen-Additions-Matrizen $\mathrm{ZA}_n(k,l,\alpha)$ addieren das α-fache der l-ten Zeile zur k-ten Zeile, die Zeilen-Permutations-Matrizen $\mathrm{ZP}_n(k,l)$ vertauscht die k-te Zeile mit der l-ten Zeile und die Zeilen-Multiplikations-Matrix $\mathrm{ZM}_n(k,\alpha)$ multipliziert die k-te Zeile mit α.

Definition 10.11 (Elementar-Matrizen) Es sei $n \in \mathbb{N}$ mit $n \geq 1$. Weiter seien $k, l \in \{1, \cdots, n\}$ und es sei $\alpha \in \mathbb{K}$, wobei zusätzlich $\alpha \neq 0$ zu gelten hat. Dann definieren wir die Elementar-Matrizen wie folgt:

1. Für $k \neq l$ wird die $n \times n$ Zeilen-Additions-Matrix $\mathrm{ZA}_n(k,l,\alpha)$ durch
$$\mathrm{ZA}_n(k,l,\alpha) := \mathrm{E}_n + \alpha \cdot \mathrm{A}_n(k,l)$$
definiert. Multiplizieren wir $\mathrm{ZA}_n(k,l,\alpha)$ von rechts mit einer $n \times n$ Matrix B, so erhalten wir
$$\mathrm{ZA}_n(k,l,\alpha) \cdot B := \mathrm{E}_n \cdot B + \alpha \cdot \mathrm{A}_n(k,l) \cdot B = B + \alpha \cdot \mathrm{A}_n(k,l) \cdot B.$$
Die Matrix $\mathrm{A}_n(k,l) \cdot B$ besteht aus der l-ten Zeile von B, die allerdings in die k-te Zeile verschoben wird. Damit besteht der Effekt der Multiplikation $\mathrm{ZA}_n(k,l,\alpha) \cdot B$ darin, dass die l-te Zeile von B mit α multipliziert zur k-ten Zeile von B hinzu addiert wird. Im Falle $l < k$ gilt also
$$\mathrm{ZA}_n(k,l,\alpha) \cdot B = \mathrm{ZA}_n(k,l,\alpha) \cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_k + \alpha \cdot \mathbf{b}_l \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$

2. Die $n \times n$ Zeilen-Permutations-Matrix $\mathrm{ZP}_n(k,l)$ wird durch die Gleichung
$$\mathrm{ZP}_n(k,l) := \mathrm{E}_n + \mathrm{A}_n(k,l) + \mathrm{A}_n(l,k) - \mathrm{A}_n(k,k) - \mathrm{A}_n(l,l).$$
definiert. Multiplizieren wir eine $n \times n$ Matrix B von links mit $\mathrm{ZP}_n(k,l)$, so besteht der Effekt auf B darin, dass die k-te Zeile von B mit der l-ten Zeile von B vertauscht wird, es gilt also
$$\mathrm{ZP}_n(k,l) \cdot B = \mathrm{ZP}_n(k,l) \cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$
Dies können wir wie folgt einsehen:
$$\mathrm{ZA}_n(k,l) \cdot B = B + \mathrm{A}_n(k,l) \cdot B + \mathrm{A}_n(l,k) \cdot B - \mathrm{A}_n(k,k) \cdot B - \mathrm{A}_n(l,l) \cdot B$$
Der Term $\mathrm{A}_n(k,l) \cdot B$ transportiert die l-Zeile von B in die k-te Zeile, der Term $\mathrm{A}_n(l,k) \cdot B$ transportiert die k-te Zeile von B in die l-te Zeile und die beiden Terme $-\mathrm{A}_n(k,k) \cdot B$ und $-\mathrm{A}_n(l,l) \cdot B$ entfernen die k-te Zeile beziehungsweise die l-te Zeile von B.

3. Die $n \times n$ Zeilen-Multiplikations-Matrix $\mathrm{ZM}_n(k,\alpha)$ wird für $\alpha \neq 0$ durch die Gleichung
$$\mathrm{ZM}_n(k,\alpha) := E_n + (\alpha - 1) \cdot \mathrm{A}_n(k,k)$$
definiert. Multiplizieren wir eine $n \times n$ Matrix B von links mit $\mathrm{ZM}_n(k,\alpha)$, so besteht der Effekt

auf B darin, dass die k-te Zeile von B mit α multipliziert wird, es gilt also

$$\mathrm{ZM}_n(k,\alpha)\cdot B = \mathrm{ZM}_n(k,\alpha)\cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \alpha\cdot\mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$

Dies können wir wie folgt einsehen:

$$\mathrm{ZM}_n(k,\alpha)\cdot B = B + (\alpha-1)\cdot \mathrm{A}_n(k,k)\cdot B$$

Es wir also zu B das $(1-\alpha)$-fache der k-ten Zeile von Bzur k-ten Zeile hinzu addiert und damit steht die k-te Zeile im Ergebnis insgesamt $1+(\alpha-1)=\alpha$-mal. ◇

Die entscheidende Beobachtung ist nun die, dass die oben definierten Elementar-Matrizen alle invertierbar sind, im Einzelnen gilt:

1. $\big(\mathrm{ZA}_n(k,l,\alpha)\big)^{-1} = \mathrm{ZA}_n(k,l,-\alpha)$,
   denn für $k \neq l$ zieht die Anwendung der Matrix $\mathrm{ZA}_n(k,l,-\alpha)$ auf eine Matrix B das α-fache der l-ten Zeile von der k-ten Zeile ab. Wenn wir also das Produkt
   $$\mathrm{ZA}_n(k,l,-\alpha)\cdot\mathrm{ZA}_n(k,l,\alpha)\cdot\mathrm{E}_n$$
   betrachten, so addiert die Anwendung von $\mathrm{ZA}_n(k,l,\alpha)$ auf die Einheits-Matrix E_n zunächst das α-fache der l-ten Zeile von E_n zur k-ten Zeile, das dann durch die anschließende Anwendung von $\mathrm{ZA}_n(k,l,-\alpha)$ wieder abgezogen wird. Damit gilt insgesamt
   $$\mathrm{ZA}_n(k,l,-\alpha)\cdot\mathrm{ZA}_n(k,l,\alpha)\cdot\mathrm{E}_n = \mathrm{E}_n,$$
   was wir zu
   $$\mathrm{ZA}_n(k,l,-\alpha)\cdot\mathrm{ZA}_n(k,l,\alpha) = \mathrm{E}_n,$$
   vereinfachen können. Genauso lässt sich die Gleichung
   $$\mathrm{ZA}_n(k,l,\alpha)\cdot\mathrm{ZA}_n(k,l,-\alpha) = \mathrm{E}_n,$$
   zeigen.
2. $\big(\mathrm{ZP}_n(k,l)\big)^{-1} = \mathrm{ZP}_n(k,l)$,
   denn wenn wir die k-te Zeile mit der l-ten Zeile vertauschen und in der resultierenden Matrix wieder die k-te Zeile mit der l-ten Zeile vertauschen, sind wir wieder bei der Matrix, mit der wir gestartet sind.
3. $\big(\mathrm{ZM}_n(k,\alpha)\big)^{-1} = \mathrm{ZM}_n(k,\alpha^{-1})$,
   denn wenn wir die k-te Zeile erst mit α multiplizieren und in der resultierenden Matrix die k-te Zeile mit α^{-1} multiplizieren, haben wir die Matrix wegen der Gleichung $\alpha^{-1}\cdot\alpha = 1$ insgesamt nicht verändert. Dabei muss natürlich $\alpha \neq 0$ gelten, aber das ist bei den Elementar-Matrizen der Form $\mathrm{ZM}_n(k,\alpha)$ vorausgesetzt.

10.3 Berechnung des Inversen einer Matrix

Wir haben nun alles Material zusammen um für eine gegebene Matrix $A \in \mathbb{K}^{n\times n}$ überprüfen zu können, ob es zu A eine inverse Matrix A^{-1} gibt und diese gegebenenfalls auch zu berechnen. Die Idee, die dem Verfahren, dass wir gleich präsentieren werden, zu Grunde liegt, besteht darin, dass wir die Matrix A solange mit Elementar-Matrizen ZE_i multiplizieren, bis wir die Matrix A zur Einheits-Matrix E_n reduziert haben. Wir konstruieren also eine endliche Folge von Elementar-Matrizen

$$\mathrm{ZE}_1, \cdots, \mathrm{ZE}_k,$$

so, dass

$$\mathrm{ZE}_k \cdot \ldots \cdot \mathrm{ZE}_1 \cdot A = \mathrm{E}_n$$

gilt, denn dann haben wir offenbar

$$A^{-1} = \mathrm{ZE}_k \cdot \ldots \cdot \mathrm{ZE}_1.$$

Die Elementar-Matrizen werden dabei nicht explizit berechnet, denn es reicht, wenn wir die Umformungen, die den Elementar-Matrizen entsprechen, auf die Einheits-Matrix E_n anwenden. Wir berechnen A^{-1} dann nach der Formel

$$A^{-1} = \mathrm{ZE}_k \cdot \ldots \cdot \mathrm{ZE}_1 \cdot \mathrm{E}_n.$$

Bei dieser letzten Gleichung müssen wir keine Matrizen-Multiplikationen durchführen, denn wir wissen ja, welchen Effekt die Multiplikation einer Elementar-Matrix ZE_i mit einer Matrix B hat: Je nachdem, um was für eine Elementar-Matrix es sich handelt, addieren wir das α-fache einer Zeile zu einer anderen Zeile, wir vertauschen zwei Zeilen oder wir multiplizieren eine Zeile mit einem Skalar.

Die Transformation der Matrix $A \in \mathbb{K}^n$ verläuft in n Schritten, wobei wir im i-ten Schritt dafür sorgen, dass die i-te Spalte der Matrix gleich dem i-ten Einheits-Vektor $\mathbf{e}_i$ wird. Dabei hat der i-te Einheits-Vektor in der i-ten Komponente eine 1, alle anderen Komponenten sind 0. Im i-ten Schritt können wir davon ausgehen, dass in den ersten $i-1$ Spalten bereits die Einheits-Vektoren $\mathbf{e}_1$ bis $\mathbf{e}_{i-1}$ stehen. Um auch die i-te Spalte entsprechend zu transformieren, suchen wir zunächst diejenige Zeile $j \in \{i, \cdots, n\}$ für die $|a_{j,i}|$ maximal wird. Theoretisch würde es an dieser Stelle reichen, einfach irgend eine Zeile $j \in \{i, \cdots, n\}$ zu wählen, für die $a_{j,i} \neq 0$ ist. Das hier vorgestellte Verfahren, bei dem wir immer den Zeilen-Index j bestimmen, für den $a_{j,i}$ maximal ist, hat aber den Vorteil, dass es weniger anfällig für Rundungs-Fehler ist als das naive Vorgehen, bei dem j einfach so gewählt wird, dass $a_{j,i} \neq 0$ ist. Falls

$$\forall j \in \{i, \cdots, n\} : a_{j,i} = 0$$

gilt, dann lässt sich die Matrix nicht mehr zur Einheits-Matrix umformen und es kann gezeigt werden, dass die Matrix A dann nicht invertierbar ist. Falls wir einen Index j wie oben beschrieben finden können, dann vertauschen wir die i-te Zeile mit der j-ten Zeile und dividieren anschließend die i-te Zeile durch das Element $a_{i,i}$. Damit steht in der i-ten Zeile der i-ten Spalte schon mal eine 1. Damit die anderen Einträge der i-ten Spalte 0 werden, subtrahieren wir anschließend für alle $k \in \{1, \cdots, n\} \backslash \{i\}$ das $a_{k,i}$-fache der i-ten Zeile von der k-ten Zeile.

Abbildung 10.1 auf Seite 149 zeigt eine Implementierung des oben beschriebenen Algorithmus in der Sprache SetlX, die leichter zu verstehen ist, als die oben gegebene rein textuelle Beschreibung. Wir diskutieren diese Implementierung jetzt Zeile für Zeile:

1. Die Funktion `inverse` bekommt als Argument eine quadratische Matrix `a`, die als Liste von Listen dargestellt wird, es gilt also

   $$\mathtt{a} = [\mathtt{a}[1], \cdots, \mathtt{a}[n]].$$

   Dabei ist $\mathtt{a}[i]$ gerade die i-te Zeile der Matrix `a`. Auf die Komponente $\mathtt{a}_{i,j}$ kann dann mittels des Ausdrucks $\mathtt{a}[i][j]$ zugegriffen werden.

2. Zunächst wird in Zeile 2 mit Hilfe des Operators `#` die Dimension n der Matrix berechnet: Das ist gerade die Länge der Liste `a`.

3. Das Prinzip der Berechnung der inversen Matrix $\mathtt{a}^{-1}$ ist, dass `a` mittels elementarer Zeilen-Umformungen in die Einheits-Matrix E_n überführt wird. Gleichzeitig werden diese Zeilen-Umformungen auf die Einheits-Matrix E_n angewendet und am Ende enthält dann die umgeformte Einheits-Matrix das Inverse der Matrix `a`.

   Zu diesem Zweck berechnen wir in Zeile 3 die Einheits-Matrix E_n mit Hilfe der Funktion `identity`. Die Implementierung dieser Funktion wird in Abbildung 10.2 auf Seite 150 gezeigt.

```
1   inverse := procedure(a) {
2       n := #a;
3       e := identity(n);
4       for (i in [1 .. n]) {
5           r := pivot(a, n, i);
6           [ a[i], a[r] ] := [ a[r], a[i] ];
7           [ e[i], e[r] ] := [ e[r], e[i] ];
8           if (a[i][i] == 0) { return; }
9           f := 1 / a[i][i];
10          for (j in [1 .. n]) {
11              a[i][j] *= f; e[i][j] *= f;
12          }
13          for (k in [1 .. n] | k != i) {
14              f := a[k][i];
15              for (j in [1 .. n]) {
16                  a[k][j] -= f * a[i][j];
17                  e[k][j] -= f * e[i][j];
18              }
19          }
20      }
21      return e;
22  };
```

Abbildung 10.1: Berechnung der Inversen einer Matrix a.

4. Im i-ten Durchlauf der Schleife in Zeile 4 wird erreicht, dass die i-te Spalte von `a` mit dem i-ten Einheits-Vektor $\mathbf{e}_i$ übereinstimmt.

   1. Zunächst suchen wir mit der in Zeile 5 aufgerufenen Funktion `pivot` nach der Zeile r, für die der Betrag $|\mathtt{a}[i][r]|$ unter allen $r \in \{i, \cdots, n\}$ maximal wird. Diese Zeile wird dann in Zeile 6 des Programms mit der i-ten Zeile vertauscht. Anschließend wird in Zeile 7 dieselbe Operation auf der Matrix `e` ausgeführt.

      Die Implementierung der dabei verwendeten Funktion `pivot` wird in Abbildung 10.2 gezeigt.

   2. Falls nach der Vertauschung von Zeile i und Zeile r die Komponente $\mathtt{a}[i][i]$ den Wert 0 hat, dann haben alle Elemente in der i-ten Spalte ab dem Index i den Wert 0 und dann kann `a` nicht invertierbar sein. Dies wird in Zeile 8 des Programms überprüft: Falls $\mathtt{a}[i][i] = 0$ ist, wird die Funktion abgebrochen, ohne ein Ergebnis zurück zu liefern.

   3. Ansonsten teilen wir in Zeile 11 des Programms die i-Zeile von `a` und `e` durch $\mathtt{a}[i][i]$. Anschließend hat $a[i][i]$ natürlich den Wert 1.

   4. In der Schleife in Zeile 13 des Programms subtrahieren wir das $\mathtt{a}[k][i]$-fache der i-ten Zeile von der k-ten Zeile. Da die i-te Zeile an der Position i mittlerweile den Wert 1 hat, führt das dazu, dass danach der Wert von $\mathtt{a}[k][i]$ verschwindet, so dass in der i-ten Spalte alle Werte $\mathtt{a}[i][k]$ für $k \neq i$ gleich 0 sind.

   Nachdem i den Wert n erreicht hat, ist die ursprüngliche Matrix `a` zur Einheits-Matrix reduziert worden, sofern das Programm nicht vorher in Zeile 8 ergebnislos abgebrochen wurde. Gleichzeitig enthält dann die Variable `e` das Inverse der ursprünglich gegebenen Matrix.

```
delta := procedure(i, j) {
    if (i == j) { return 1; } else { return 0; }
};
identity := procedure(n) {
    return [ [ delta(i,j) : j in [1 .. n] ] : i in [1 .. n] ];
};
pivot := procedure(a, n, i) {
    r := i;  // index of row containing maximal element
    for (j in [i+1 .. n]) {
        if (abs(a[j][i]) > abs(a[r][i])) {
            r := j;
        }
    }
    return r;
};
```

Abbildung 10.2: Implementierung der in Abbildung 10.1 benötigten Hilfsfunktionen.

Beispiel: Wir testen das Programm, indem wir versuchen, das Inverse der Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

zu berechnen. Dazu wird in dem Programm die Variable `e` mit der Einheits-Matrix E_3 initialisiert. Danach haben wir

$$\mathtt{a} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

1. Im ersten Schritt suchen wir die Zeile der Matrix `a`, für die in der ersten Spalte das größte Element steht. Im vorliegenden Fall ist das die dritte Zeile, denn es gilt $\mathtt{a}_{3,1} = 3$ und alle anderen Einträge in der ersten Spalte sind kleiner als 3. Daher vertauschen wir die erste Zeile mit der dritten Zeile und finden für die Matrizen `a` und `e`

   $$\mathtt{a} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

2. Im nächsten Schritt normalisieren wir die erste Zeile, indem wir durch $\mathtt{a}_{1,1}$ teilen. Danach haben wir

   $$\mathtt{a} = \begin{pmatrix} 1 & \frac{1}{3} & \frac{2}{3} \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

   Unser nächstes Ziel ist es, alle Einträge $\mathtt{a}_{i,1}$ in der ersten Spalte, für die $i \neq 1$ ist, durch Addition der ersten Zeile zur i-ten Zeile zu entfernen. Dazu dienen die folgenden beiden Schritte:

3. Im nächsten Schritt subtrahieren wir das 2-fache der ersten Zeile von der zweiten Zeile und erhalten:

$$\mathtt{a} = \begin{pmatrix} 1 & \frac{1}{3} & \frac{2}{3} \\ 0 & \frac{7}{3} & -\frac{1}{3} \\ 1 & 2 & 3 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & 0 & \frac{1}{3} \\ 0 & 1 & -\frac{2}{3} \\ 1 & 0 & 0 \end{pmatrix}$$

4. Jetzt subtrahieren wir die erste Zeile von der dritten Zeile:
$$\mathtt{a} = \begin{pmatrix} 1 & \frac{1}{3} & \frac{2}{3} \\ 0 & \frac{7}{3} & -\frac{1}{3} \\ 0 & \frac{5}{3} & \frac{7}{3} \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & 0 & \frac{1}{3} \\ 0 & 1 & -\frac{2}{3} \\ 1 & 0 & -\frac{1}{3} \end{pmatrix}$$

5. In den folgenden Schritten geht es darum, die zweite Spalte der Matrix $\mathtt{a}$ in den Einheits-Vektor $\mathbf{e}_2$ zu überführen. Zunächst überprüfen wir, für welches $j \geq 2$ der Betrag $|\mathtt{a}_{2,j}|$ maximal wird. In diesem Fall ist der Betrag in der zweiten Zeile bereits maximal, so dass wir an dieser Stelle keine Zeilen-Vertauschung vornehmen müssen. Wir müssen die zweite Zeile aber noch normalisieren und multiplizieren daher die zweite Zeile mit $\frac{3}{7}$:
$$\mathtt{a} = \begin{pmatrix} 1 & \frac{1}{3} & \frac{2}{3} \\ 0 & 1 & -\frac{1}{7} \\ 0 & \frac{5}{3} & \frac{7}{3} \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & 0 & \frac{1}{3} \\ 0 & \frac{3}{7} & -\frac{2}{7} \\ 1 & 0 & -\frac{1}{3} \end{pmatrix}$$

6. Im nächsten Schritt geht es darum, die Matrix $\mathtt{a}$ durch Addition eines geeigneten Vielfachen der zweiten Zeile zur ersten Zeile so zu verändern, dass $\mathtt{a}_{2,1} = 0$ wird. Wir subtrahieren daher $\frac{1}{3}$ der zweiten Zeile von der ersten Zeile und erhalten
$$\mathtt{a} = \begin{pmatrix} 1 & 0 & \frac{5}{7} \\ 0 & 1 & -\frac{1}{7} \\ 0 & \frac{5}{3} & \frac{7}{3} \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & -\frac{1}{7} & \frac{3}{7} \\ 0 & \frac{3}{7} & -\frac{2}{7} \\ 1 & 0 & -\frac{1}{3} \end{pmatrix}$$

7. Anschließend subtrahieren wir $\frac{5}{3}$ der zweiten Zeile von der dritten Zeile und finden
$$\mathtt{a} = \begin{pmatrix} 1 & 0 & \frac{5}{7} \\ 0 & 1 & -\frac{1}{7} \\ 0 & 0 & \frac{18}{7} \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & -\frac{1}{7} & \frac{3}{7} \\ 0 & \frac{3}{7} & -\frac{2}{7} \\ 1 & -\frac{5}{7} & \frac{1}{7} \end{pmatrix}$$

8. In den verbleibenden Schritten geht es darum, die dritte Spalte der Matrix $\mathtt{a}$ in den Einheits-Vektor $\mathbf{e}_3$ zu überführen. Wir beginnen damit, dass wir die dritte Zeile durch $\frac{18}{7}$ teilen:
$$\mathtt{a} = \begin{pmatrix} 1 & 0 & \frac{5}{7} \\ 0 & 1 & -\frac{1}{7} \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} 0 & -\frac{1}{7} & \frac{3}{7} \\ 0 & \frac{3}{7} & -\frac{2}{7} \\ \frac{7}{18} & -\frac{5}{18} & \frac{1}{18} \end{pmatrix}$$

9. Jetzt ziehen wir $\frac{5}{7}$ der dritten Zeile von der ersten Zeile ab:
$$\mathtt{a} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{7} \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} -\frac{5}{18} & \frac{1}{18} & \frac{7}{18} \\ 0 & \frac{3}{7} & -\frac{2}{7} \\ \frac{7}{18} & -\frac{5}{18} & \frac{1}{18} \end{pmatrix}$$

10. Im letzten Schritt addieren wir $\frac{1}{7}$ der dritten Zeile zur zweiten Zeile:
$$\mathtt{a} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad \mathtt{e} = \begin{pmatrix} -\frac{5}{18} & \frac{1}{18} & \frac{7}{18} \\ \frac{1}{18} & \frac{7}{18} & -\frac{5}{18} \\ \frac{7}{18} & -\frac{5}{18} & \frac{1}{18} \end{pmatrix}$$

Damit haben wir das Inverse unserer ursprünglichen Matrix gefunden, es gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} -\frac{5}{18} & \frac{1}{18} & \frac{7}{18} \\ \frac{1}{18} & \frac{7}{18} & -\frac{5}{18} \\ \frac{7}{18} & -\frac{5}{18} & \frac{1}{18} \end{pmatrix}. \qquad \diamond$$

Kapitel 11

Determinanten

Der Begriff der *Determinante* ist einer der zentralen Begriff der linearen Algebra: Einerseits werden Determinanten bei der Berechnung von *Eigenwerten* zur Definition des *charakteristischen Polynoms* benötigt, andererseits spielen Determinanten auch außerhalb der linearen Algebra eine Rolle, beispielsweise bei der Berechnung mehrdimensionaler Integrale. Um Determinanten einführen zu können, müssen wir zunächst das *Signum* einer Permutation definieren. Bedauerlicherweise ist dies mit einigem technischen Aufwand verbunden.

11.1 Permutationen und Transpositionen

Wir erinnern an die Definition der Permutations-Gruppe $\mathcal{S}_n$. Ist $R \in \mathcal{S}_n$, so hat R die Form

$$R = \big\{\langle 1, x_1\rangle, \cdots, \langle n, x_n\rangle\big\} \quad \text{mit } \{x_1, \cdots, x_n\} = \{1, \cdots, n\}.$$

Da R durch die Angabe der Zahlen $x_1, \cdots, x_n$ vollständig bestimmt ist, vereinbaren wir, in Zukunft der Kürze halber die Permutation R auch als die Liste

$$R = [x_1, \cdots, x_n]$$

zu schreiben. Weiterhin werden wir R oft als Funktion auffassen und dann beispielsweise

$$R(k) = x_k \quad \text{schreiben, falls} \quad \langle k, x_k\rangle \in R \text{ gilt.}$$

Bemerkung: Es gilt $\texttt{card}(\mathcal{S}_n) = n!$, wobei der Ausdruck $n!$ (gelesen: n *Fakultät*) durch die Formel

$$n! := \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n$$

definiert ist. ◇

Beweis: Wir haben oben bereits gesehen, dass wir die Permutationen $R \in \mathcal{S}_n$ als Listen der Form

$$R = [x_1, \cdots, x_n] \quad \text{mit } x_i \in \{1, \cdots, n\}$$

schreiben können, wobei die x_i paarweise verschieden sind. Damit haben wir bei der Wahl von x_1 insgesamt n Möglichkeiten. Bei der Wahl von x_2 bleiben uns aufgrund der Einschränkung $x_2 \neq x_1$ noch $n-1$ Möglichkeiten. Falls die Elemente $x_1, \cdots, x_{i-1}$ bereits festgelegt sind, haben wir bei der Wahl von x_i noch $n-(i-1)$ Wahlmöglichkeiten. Insgesamt haben wir also

$$\prod_{i=1}^{n} \big(n - (i-1)\big) = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$$

Möglichkeiten bei der Wahl der Elemente x_i. □

Im Allgemeinen können Permutationen beliebig kompliziert sein. Es lohnt sich, zunächst ganz spezielle Permutationen zu betrachten, die nur zwei Elemente vertauschen. Das führt zu der folgenden Definition.

Definition 11.1 (Transposition) Eine Permutation $R \in \mathcal{S}_n$ ist eine *Transposition* genau dann, wenn die folgende Bedingung erfüllt ist:

$$\texttt{card}\big(\big\{\langle k,l\rangle \in R \mid k \neq l\big\}\big) = 2.$$

In Listen-Schreibweise können wir das folgendermaßen ausdrücken:

$$R = [x_1, \cdots, x_n] \text{ ist Transposition} \quad \text{g.d.w.} \quad \texttt{card}\big(\big\{i \in \{1, \cdots, n\} \mid x_i \neq i\big\}\big) = 2.$$

Da eine Transposition R durch die Angabe der beiden Elemente, die vertauscht werden, vollständig bestimmt wird, schreiben wir

$$R = \langle k, l\rangle$$

falls $k < l$ ist und R die Transposition ist, welche die Zahlen k und l vertauscht. In Listen-Schreibweise können wir diese Transposition auch als

$$\langle k,l\rangle \mathrel{\widehat{=}} [1, \cdots, k-1, l, k+1, \cdots, l-1, k, l+1, \cdots, n]$$

schreiben. Wollen wir die Transposition $\langle k,l\rangle$ als binäre Relation darstellen, so haben wir

$$\langle k,l\rangle \mathrel{\widehat{=}} \big\{\langle i,i\rangle \mid i \in \{1, \cdots, n\} \backslash \{k,l\}\big\} \cup \big\{\langle k,l\rangle, \langle l,k\rangle\big\}. \qquad \diamond$$

Beispiel: Die Permutation

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

ist eine Transposition und kann daher kürzer als

$$R = \langle 2,3\rangle$$

geschrieben werden. $\diamond$

Bemerkung: Schreiben wir eine Transposition τ in der Form $\tau = \langle k,l\rangle$, so ist a priori nicht klar, für welche natürliche Zahl n nun $\tau \in \mathcal{S}_n$ gilt. Das ist bei der Schreibweise $\tau = \langle k,l\rangle$ normalerweise kein Problem, denn einerseits geht meist aus dem Zusammenhang klar hervor, welches $n \in \mathbb{N}$ gemeint ist und andererseits ist es oft auch unwichtig, denn jede Permutation $\pi \in \mathcal{S}_n$ kann in trivialer Weise zu einer Permutation $\pi' \in \mathcal{S}_m$ erweitert werden, falls $m \geq n$ gilt. $\diamond$

Transpositionen sind einfacher als beliebige Permutationen und wir werden später insbesondere sehen, dass sich die noch zu definierende Funktion $\texttt{sgn}(R)$, die das *Vorzeichen* einer Permutation berechnet, für Transpositionen sofort berechnen lässt. Da der nächste Satz uns zeigt, dass sich alle nicht-trivialen Permutationen als Produkt von Transpositionen schreiben lassen, liefert uns dieser Satz dann ein einfaches Verfahren, das Vorzeichen beliebiger Permutationen zu berechnen.

Satz 11.2 Ist $n \geq 2$ und gilt $R \in \mathcal{S}_n$, so lässt sich R als Produkt von Transpositionen darstellen.

Beweis: Wir beweisen diesen Satz durch vollständige Induktion nach n.

I.A.: $n = 2$.

Verwenden wir die Listen-Schreibweise für Permutationen, so können wir $\mathcal{S}_2$ als

$$\{[1,2], [2,1]\}$$

schreiben. Die Permutation $[2,1]$ ist bereits eine Transposition und da

$$[1,2] = [2,1] \circ [2,1]$$

gilt, lässt sich offenbar auch die einzige andere Permutation aus $\mathcal{S}_2$ als Produkt zweier Transpositionen schreiben.

I.S.: $n \mapsto n+1$.

Wir definieren $k := R(n+1)$ und unterscheiden zwei Fälle.

1. Fall: $k = n + 1$.
   In diesem Fall enthält die Permutation R also das Paar $\langle n+1, n+1\rangle$. Dann definieren wir
   $$R' := R \backslash \{\langle n+1, n+1\rangle\}.$$
   Damit ist $R' \in \mathcal{S}_n$ und lässt sich folglich nach Induktions-Voraussetzung als Produkt von Transpositionen schreiben:
   $$R' = \tau_1 \circ \cdots \circ \tau_m \quad \text{mit } \tau_i \in \mathcal{S}_i.$$
   Fassen wir die Transpositionen τ_i nun als Elemente von S_{n+1} auf, so folgt sofort
   $$R = \tau_1 \circ \cdots \circ \tau_m.$$
2. Fall: $k \leq n$.
   In diesem Fall definieren wir eine Permutation R' als
   $$R' := R \circ \langle k, n+1\rangle.$$
   Wir berechnen den Wert von $R'(n+1)$: Es gilt
   $$R'(n+1) = \langle k, n+1\rangle\big(R(n+1)\big) = \langle k, n+1\rangle(k) = n+1.$$
   Damit bildet R' also die Zahl $n+1$ auf sich selbst ab und folglich erfüllt R' die Voraussetzung des ersten Falls. Da wir die Gültigkeit unserer Behauptung für den ersten Fall bereits bewiesen haben, finden wir also Transpositionen $\tau_1, \cdots, \tau_m$, so dass
   $$R' = \tau_1 \circ \cdots \circ \tau_m$$
   gilt. Setzen wir hier die Definition von R' ein, so erhalten wir
   $$R \circ \langle k, n+1\rangle = \tau_1 \circ \cdots \circ \tau_m$$
   Da jede Transposition bezüglich des relationalen Produktes ihr eigenes Inverses ist, können wir diese Gleichung von rechts mit $\langle k, n+1\rangle$ multiplizieren um
   $$R = \tau_1 \circ \cdots \circ \tau_m \circ \langle k, n+1\rangle$$
   zu erhalten. Damit haben wir R als Produkt von Transpositionen dargestellt. □

Definition 11.3 (Signum) Für Permutationen $R \in \mathcal{S}_n$ definieren wir für alle positiven natürlichen Zahlen n eine Funktion
$$\texttt{inv} : \mathcal{S}_n \mapsto 2^{\mathbb{Z}_n^+ \times \mathbb{Z}_n^+}$$
die jeder Permutation $R \in \mathcal{S}_n$ eine Menge von Paaren natürlicher Zahlen k und l zuordnet, für die
$$k < l \quad \text{und} \quad R(k) > R(l)$$
gilt. Formal definieren wir
$$\texttt{inv}(R) := \big\{\langle k, l\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid k < l \wedge R(k) > R(l)\big\}.$$
Die Menge $\texttt{inv}(R)$ bezeichnen wir als die Menge der *Inversionen* von R. Darauf aufbauend definieren wir das *Vorzeichen* (oder auch *Signum*) der Permutation R als
$$\texttt{sgn}(R) := (-1)^{\texttt{card}(\texttt{inv}(R))}.$$
Das Signum einer Permutation ist folglich 1, wenn die Anzahl der Inversionen von R eine gerade Zahl ist, ansonsten hat das Signum den Wert -1. □

Abbildung 11.1 auf Seite 156 zeigt eine Implementierung der Funktion `sgn` in der Sprache SetlX. Die Permutationen werden in diesem Programm als Listen dargestellt.

```
1  inv := procedure(r) {
2      n := #r;
3      return { [k,l] : [k, l] in {1..n}><{1..n} | k < l && r[k] > r[l] };
4  };
5  signum := procedure(r) {
6      return (-1) ** #inv(r);
7  };
```

Abbildung 11.1: Berechnung des Signums einer Permutation.

Aufgabe 65: Es sei $\mathtt{id}_n \in \mathcal{S}_n$ die identische Permutation aus R_n. Stellen wir diese Permutation durch eine Liste dar, so gilt also

$$\mathtt{id}_n = [1, 2, 3, \cdots, n].$$

Zeigen Sie, dass für alle positiven natürlichen Zahlen n die Gleichung

$$\mathtt{sgn}(\mathtt{id}_n) = 1$$

gilt. ◇

Aufgabe 66: Überlegen Sie, für welche Permutation $R \in \mathcal{S}_n$ die Kardinalität der Menge $\mathtt{inv}(R)$ maximal wird und berechnen Sie

$$\mathtt{card}(\mathtt{inv}(R))$$

für dieses R. ◇

Aufgabe 67: Die Transposition τ sei als

$$\tau = \langle k, l \rangle$$

definiert und es gelte $k < l$. Berechnen Sie $\mathtt{inv}(\tau)$ und $\mathtt{sgn}(\tau)$. ◇

Definition 11.4 (Elementare Transposition)
Eine Transposition τ ist eine *elementare Transposition* genau dann, wenn es ein $k \in \mathbb{N}$ gibt, so dass

$$\tau = \langle k, k+1 \rangle$$

gilt. Eine elementare Transposition vertauscht also benachbarte Indizes. ◇

Bemerkung: Ist $\tau = \langle k, k+1 \rangle$ eine elementare Transposition, so gilt

$$\mathtt{inv}(\tau) = \{\langle k, k+1 \rangle\}$$

und daraus folgt sofort $\mathtt{sgn}(\langle k, k+1 \rangle) = -1$. ◇

Lemma 11.5
Jede Transposition $\tau \in \mathcal{S}_n$ lässt sich als Produkt einer ungeraden Anzahl elementarer Transpositionen darstellen.

Beweis: Es gilt

$$\langle k, k+1 \rangle \circ \cdots \circ \langle l-1, l \rangle \circ \langle l-1, l-2 \rangle \circ \cdots \circ \langle k+2, k+1 \rangle \circ \langle k+1, k \rangle = \langle k, l \rangle.$$

Diese Gleichung können Sie nachrechnen, wenn Sie die Permutation auf der linken Seite auf alle $i \in \{1, \cdots, n\}$ anwenden. Dazu ist lediglich eine Fallunterscheidung erforderlich, bei der für i die Fälle

1. $i < k$,
2. $i = k$,
3. $i > k \wedge i < l$,
4. $i = l$ und
5. $i > l$

unterschieden werden. Diese Fallunterscheidung tatsächlich auszuführen ist eine gute Übungsaufgabe. Mit der obigen Gleichung haben wir $\langle k, l\rangle$ als Produkt elementarer Transpositionen dargestellt. Es bleibt zu zeigen, dass die Anzahl der Transpositionen insgesamt ungerade ist. Die Anzahl der elementaren Transpositionen in dem Produkt

$$\langle k, k+1\rangle \circ \cdots \circ \langle l-1, l\rangle$$

beträgt $(l-1) - k + 1 = l - k$, während das Produkt

$$\langle l-2, l-1\rangle \circ \cdots \circ \langle k+1, k+2\rangle$$

aus $(l-2)-(k+1)+1 = l-k-1$ Faktoren besteht. Insgesamt haben wir damit $(l-k)+(l-k)-1 = 2 \cdot (l-k) - 1$ elementare Transpositionen zur Darstellung von τ benötigt und diese Anzahl ist offenbar ungerade. □

Das nächste Lemma zeigt uns, wie elementare Transpositionen auf Permutationen wirken.

Lemma 11.6 Falls die Permutation $R \in \mathcal{S}_n$ in der Listen-Schreibweise die Form $R = [x_1, \cdots, x_n]$ hat und $\tau = \langle k, k+1\rangle$ eine elementare Transposition ist, dann gilt

$$\tau \circ R = \langle k, k+1\rangle \circ [x_1, \cdots, x_n] = [x_1, \cdots, x_{k-1}, x_{k+1}, x_k, x_{k+2}, \cdots, x_n].$$

Die Wirkung der Transposition τ auf die Permutation R besteht also darin, dass die Elemente x_k und x_{k+1} in der Liste, die R repräsentiert, ihre Positionen tauschen.

Beweis: Den Beweis der obigen Gleichung für $\tau \circ R$ können wir dadurch erbringen, dass wir die Permutation $\tau \circ R$ auf die verschiedenen Elemente der Menge $\{1, \cdots, n\}$ wirken lassen. Wir führen dazu eine Fallunterscheidung durch.

1. Fall: $i \notin \{k, k+1\}$. Dann haben wir
$$(\tau \circ R)(i) = R\big(\tau(i)\big) = R\big(\langle k, k+1\rangle(i)\big) = R(i) = x_i.$$
2. Fall: $i = k$. Es gilt
$$(\tau \circ R)(k) = R\big(\tau(k)\big) = R\big(\langle k, k+1\rangle(k)\big) = R(k+1) = x_{k+1}.$$
3. Fall: $i = k+1$. Jetzt gilt
$$(\tau \circ R)(k+1) = R\big(\tau(k+1)\big) = R\big(\langle k, k+1\rangle(k+1)\big) = R(k) = x_k.$$ □

Der Nachweis des folgenden Satzes stellt technisch gesehen die größte Hürde bei der Einführung der Determinanten dar. Ich habe mich für einen elementaren Beweis dieses Satzes entschieden: Dieser Beweis ist zwar einerseits länger als die Argumentation, die in der Literatur sonst oft benutzt wird, der Beweis ist aber andererseits elementarer und daher für den mathematisch weniger geübten Studenten leichter nachvollziehbar als die entsprechenden Beweise, die beispielsweise in [Fis08] oder [Kow03] zu finden sind.

Satz 11.7 Es sei $R \in \mathcal{S}_n$ und $\tau = \langle k, k+1\rangle$ sei eine elementare Transposition. Dann gilt

$$\mathtt{sgn}(\tau \circ R) = -\mathtt{sgn}(R).$$

Beweis: Das Signum einer Permutation R wird mit Hilfe der Menge der Inversionen $\texttt{inv}(R)$ berechnet, wobei die Menge $\texttt{inv}(R)$ als

$$\texttt{inv}(R) := \big\{\langle i, j\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid i < j \wedge R(i) > R(j)\big\}$$

definiert ist. Zur Vereinfachung der Notation definieren wir (nur für diesen Beweis) die Menge

$$P := \big\{\langle i, j\rangle \in \mathbb{Z}_n^+ \times \mathbb{Z}_n^+ \mid i < j\big\}.$$

Damit schreibt sich die Menge $\texttt{inv}(R)$ kürzer als

$$\texttt{inv}(R) = \big\{\langle i, j\rangle \in P \mid R(i) > R(j)\big\}.$$

Wir müssen untersuchen, wie sich die Mengen $\texttt{inv}(R)$ und $\texttt{inv}(\tau \circ R)$ unterscheiden. Dafür zerlegen wir die Menge P in sechs Teile:

$$P := P_1 \uplus P_2 \uplus P_3 \uplus P_4 \uplus P_5 \uplus P_6,$$

wobei das Zeichen $\uplus$ zum Ausdruck bringt, dass die vereinigten Mengen paarweise disjunkt sind. Die Mengen $P_1, \cdots, P_6$ werden dabei wie folgt definiert:

1. $P_1 := \big\{\langle i, j\rangle \in P \mid i, j \notin \{k, k+1\}\big\}$,
2. $P_2 := \big\{\langle k, j\rangle \in P \mid j > k+1\big\}$,
3. $P_3 := \big\{\langle k+1, j\rangle \in P \mid j > k+1\big\}$,
4. $P_4 := \big\{\langle i, k\rangle \in P \mid i < k\big\}$,
5. $P_5 := \big\{\langle i, k+1\rangle \in P \mid i < k\big\}$,
6. $P_6 := \big\{\langle k, k+1\rangle\big\}$.

Entsprechend der Zerlegung von P können wir nun auch die Menge $\texttt{inv}(R)$ in sechs paarweise disjunkte Teile zerlegen. Wir definieren

$$A_s := \big\{\langle i, j\rangle \in P_s \mid R(i) > R(j)\big\} \quad \text{für } s \in \{1, \cdots, 6\}.$$

Damit gilt

$$\texttt{inv}(R) = A_1 \uplus A_2 \uplus A_3 \uplus A_4 \uplus A_5 \uplus A_6.$$

Zur Berechnung von $\texttt{inv}(\tau \circ R)$ definieren wir entsprechend

$$B_s := \big\{\langle i, j\rangle \in P_s \mid R(\tau(i)) > R(\tau(j))\big\} \quad \text{für } s \in \{1, \cdots, 6\}.$$

Damit gilt offenbar

$$\texttt{inv}(\tau \circ R) = B_1 \uplus B_2 \uplus B_3 \uplus B_4 \uplus B_5 \uplus B_6.$$

Als nächstes vergleichen wir die Mengen A_s und B_s für alle $s \in \{1, \cdots, 6\}$. Unser Ziel ist es, folgende Gleichungen nachzuweisen:

1. $\texttt{card}(A_1) = \texttt{card}(B_1)$,
2. $\texttt{card}(A_2) = \texttt{card}(B_3)$,
3. $\texttt{card}(A_3) = \texttt{card}(B_2)$,
4. $\texttt{card}(A_4) = \texttt{card}(B_5)$,
5. $\texttt{card}(A_5) = \texttt{card}(B_4)$,
6. $|\texttt{card}(A_6) - \texttt{card}(B_6)| = 1$.

Daraus folgt dann, dass auch

$$\big|\mathtt{card}\big(\mathtt{inv}(R)\big) - \mathtt{card}\big(\mathtt{inv}(\tau \circ R)\big)\big| = 1$$

und nach der Definition des Signums als

$$\mathtt{sgn}(R) = (-1)^{\mathtt{card}(\mathtt{inv}(R))}$$

folgt daraus, dass $\mathtt{sgn}(R)$ und $\mathtt{sgn}(\tau \circ R)$ verschiedenes Vorzeichen haben, also die Behauptung. Was bleibt ist der Nachweis der oben bezüglich der Kardinalitäten der Mengen A_i und B_i aufgestellten Gleichungen. Dieser Nachweis erfolgt durch eine Fallunterscheidung.

1. Falls $\langle i, j\rangle \in P_1$ ist, sind i und j sowohl von k als auch von $k+1$ verschieden. Damit haben wir einerseits

   $$R\big(\tau(i)\big) = R\big(\langle k, k+1\rangle(i)\big) = R(i)$$

   und andererseits

   $$R\big(\tau(j)\big) = R\big(\langle k, k+1\rangle(j)\big) = R(j).$$

   Also gilt

   $$(\tau \circ R)(i) > (\tau \circ R)(j) \;\Leftrightarrow\; R(i) > R(j).$$

   Folglich ist $A_1 = B_1$ und daraus folgt, dass die Mengen A_1 und B_1 dieselbe Kardinalität haben:

   $$\mathtt{card}(A_1) = \mathtt{card}(B_1).$$

2. Einerseits haben wir

   $$\begin{aligned} A_2 &= \big\{\langle i, j\rangle \in P_2 \mid R(i) > R(j)\big\} \\ &= \big\{\langle k, j\rangle \in P \mid j > k+1 \wedge R(k) > R(j)\big\}. \end{aligned}$$

   Andererseits gilt

   $$\begin{aligned} B_3 &= \big\{\langle i, j\rangle \in P_3 \mid R(\tau(i)) > R(\tau(j))\big\} \\ &= \big\{\langle k+1, j\rangle \in P \mid j > k+1 \wedge R(\tau(k+1)) > R(\tau(j))\big\} \\ &= \big\{\langle k+1, j\rangle \in P \mid j > k+1 \wedge R(k) > R(j)\big\} \end{aligned}$$

   Die Mengen A_2 und B_3 sind nicht gleich, denn in der ersten Komponente steht bei den Paaren aus A_2 die Zahl k, während dort bei den Paaren aus B_3 die Zahl $k+1$ steht. Nichtdestoweniger entspricht jedem Element aus A_2 genau ein Element aus B_3. Damit haben A_2 und B_3 die gleiche Anzahl von Elementen:

   $$\mathtt{card}(A_2) = \mathtt{card}(B_3).$$

3. Einerseits haben wir

   $$\begin{aligned} A_3 &= \big\{\langle i, j\rangle \in P_3 \mid R(i) > R(j)\big\} \\ &= \big\{\langle k+1, j\rangle \in P \mid j > k+1 \wedge R(k+1) > R(j)\big\}. \end{aligned}$$

   Andererseits gilt

   $$\begin{aligned} B_2 &= \big\{\langle i, j\rangle \in P_2 \mid R(\tau(i)) > R(\tau(j))\big\} \\ &= \big\{\langle k, j\rangle \in P \mid j > k+1 \wedge R(\tau(k)) > R(\tau(j))\big\} \\ &= \big\{\langle k, j\rangle \in P \mid j > k+1 \wedge R(k+1) > R(j)\big\} \end{aligned}$$

   Die Mengen A_3 und B_2 sind nicht gleich, denn in der ersten Komponente steht bei den Paaren aus A_3 die Zahl $k+1$, während dort bei den Paaren aus B_2 die Zahl k steht. Nichtdestoweniger entspricht jedem Element aus A_3 genau ein Element aus B_2. Damit gilt

$$\texttt{card}(A_3) = \texttt{card}(B_2).$$

4. Einerseits haben wir

$$\begin{aligned} A_4 &= \big\{\langle i,j\rangle \in P_4 \mid R(i) > R(j)\big\} \\ &= \big\{\langle i,k\rangle \in P \mid i < k \wedge R(i) > R(k)\big\}. \end{aligned}$$

Andererseits gilt

$$\begin{aligned} B_5 &= \big\{\langle i,j\rangle \in P_5 \mid R(\tau(i)) > R(\tau(j))\big\} \\ &= \big\{\langle i,k+1\rangle \in P \mid i < k \wedge R(\tau(i)) > R(\tau(k+1))\big\} \\ &= \big\{\langle i,k+1\rangle \in P \mid i < k \wedge R(i) > R(k)\big\} \end{aligned}$$

Analog wie im letzten Fall sehen wir

$$\texttt{card}(A_4) = \texttt{card}(B_5).$$

5. Einerseits haben wir

$$\begin{aligned} A_5 &= \big\{\langle i,j\rangle \in P_5 \mid R(i) > R(j)\big\} \\ &= \big\{\langle i,k+1\rangle \in P \mid i < k \wedge R(i) > R(k+1)\big\}. \end{aligned}$$

Andererseits gilt

$$\begin{aligned} B_4 &= \big\{\langle i,j\rangle \in P_4 \mid R(\tau(i)) > R(\tau(j))\big\} \\ &= \big\{\langle i,k\rangle \in P \mid i < k \wedge R(\tau(i)) > R(\tau(k))\big\} \\ &= \big\{\langle i,k\rangle \in P \mid i < k \wedge R(i) > R(k+1)\big\} \end{aligned}$$

Analog zum letzten Fall sehen wir

$$\texttt{card}(A_5) = \texttt{card}(B_4).$$

6. Einerseits gilt

$$\begin{aligned} A_6 &= \big\{\langle i,j\rangle \in P_6 \mid R(i) > R(j)\big\} \\ &= \big\{\langle k,k+1\rangle \in P \mid R(k) > R(k+1)\big\}. \end{aligned}$$

Andererseits haben wir

$$\begin{aligned} B_6 &= \big\{\langle i,j\rangle \in P_6 \mid R(\tau(i)) > R(\tau(j))\big\} \\ &= \big\{\langle k,k+1\rangle \in P \mid R(\tau(k)) > R(\tau(k+1))\big\} \\ &= \big\{\langle k,k+1\rangle \in P \mid R(k+1) > R(k)\big\}. \end{aligned}$$

Da R eine Permutation ist, sind die Werte von $R(k)$ und $R(k+1)$ verschieden. Folglich gilt entweder $R(k) > R(k+1)$ oder $R(k+1) > R(k)$. Damit ist dann genau ein der beiden Mengen A_6 und B_6 leer, während die andere dass Paar $\langle k, k+1\rangle$ enthält, formal gilt

$$|\texttt{card}(A_6) - \texttt{card}(B_6)| = 1.$$ □

Lemma 11.8 Es seien $\tau_1, \cdots, \tau_k \in \mathcal{S}_n$ elementare Transpositionen und es sei $R \in \mathcal{S}_n$. Dann gilt

$$\texttt{sgn}(\tau_1 \circ \ldots \circ \tau_k \circ R) = (-1)^k \cdot \texttt{sgn}(R).$$

Beweis: Der Beweis erfolgt durch Induktion über k.

I.A.: $k = 1$.

Hier folgt die Behauptung unmittelbar aus dem letzten Lemma.

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

Es gilt

$$\begin{aligned} \mathtt{sgn}(\tau_1 \circ \ldots \circ \tau_{k+1} \circ R) &= \mathtt{sgn}\big(\tau_1 \circ (\tau_2 \circ \ldots \circ \tau_{k+1} \circ R)\big) \\ &= -\mathtt{sgn}(\tau_2 \circ \ldots \circ \tau_{k+1} \circ R) \\ &\overset{IV}{=} -(-1)^k \cdot \mathtt{sgn}(R) \\ &= (-1)^{k+1} \cdot \mathtt{sgn}(R). \end{aligned}$$

□

Korollar 11.9 Ist $\tau \in \mathcal{S}_n$ eine Transposition und ist $R \in \mathcal{S}_n$, so gilt

$$\mathtt{sgn}(\tau \circ R) = -\mathtt{sgn}(R).$$

Beweis: Die Behauptung folgt aus dem letzten Lemma und der Tatsache, dass sich jede Transposition als Produkt einer ungeraden Anzahl von elementaren Transpositionen darstellen lässt. □

Korollar 11.10 Sind $\tau_1, \cdots, \tau_k \in \mathcal{S}_n$ Transpositionen, so gilt

$$\mathtt{sgn}(\tau_1 \circ \ldots \circ \tau_k) = (-1)^k.$$

Beweis: Die Behauptung kann mit Hilfe des letzten Korollars durch eine Induktion nach k gezeigt werden.

I.A.: $k = 1$. Es gilt

$$\mathtt{sgn}(\tau) = \mathtt{sgn}(\tau \circ \mathtt{id}_n) = -\mathtt{sgn}(\mathtt{id}_n) = -1 = (-1)^1.$$

I.A.: $k \mapsto k+1$. Wir haben

$$\begin{aligned} \mathtt{sgn}(\tau_1 \circ \tau_2 \circ \ldots \circ \tau_{k+1}) &= -\mathtt{sgn}(\tau_2 \circ \ldots \circ \tau_{k+1}) \\ &\overset{IV}{=} -(-1)^k \\ &= (-1)^{k+1}. \end{aligned}$$

□

Da sich jede Permutation $R \in \mathcal{S}_n$ als Produkt von Transpositionen darstellen lässt, sehen wir nun, dass das Vorzeichen $\mathtt{sgn}(R)$ genau dann den Wert $+1$ hat, wenn R sich als Produkt einer geraden Anzahl von Permutationen darstellen lässt. Andernfalls hat $\mathtt{sgn}(R)$ den Wert -1. Damit können wir nun den folgenden Satz beweisen.

Satz 11.11 Es seien $R_1, R_2 \in \mathcal{S}_n$. Dann gilt

$$\mathtt{sgn}(R_1 \circ R_2) = \mathtt{sgn}(R_1) \circ \mathtt{sgn}(R_2).$$

Beweis: Nach Satz 11.2 lassen sich sowohl R_1 als auch R_2 als Produkte von Transpositionen darstellen. Damit gibt es $k, l \in \mathbb{N}$ sowie Transpositionen $\sigma_1, \cdots, \sigma_k, \tau_1, \cdots, \tau_l \in \mathcal{S}_n$, so dass

$$R_1 = \sigma_1 \circ \ldots \circ \sigma_k \quad \text{und} \quad R_2 = \tau_1 \circ \ldots \circ \tau_l$$

gilt. Nach dem letzten Korollar haben wir dann:

1. $\mathtt{sgn}(R_1) = \mathtt{sgn}(\sigma_1 \circ \ldots \circ \sigma_k) = (-1)^k$,
2. $\mathtt{sgn}(R_2) = \mathtt{sgn}(\tau_1 \circ \ldots \circ \tau_l) = (-1)^l$,
3. $\mathtt{sgn}(R_1 \circ R_2) = \mathtt{sgn}(\sigma_1 \circ \ldots \circ \sigma_k \circ \tau_1 \circ \ldots \circ \tau_l) = (-1)^{k+l}$.

Also haben wir insgesamt

$$\mathtt{sgn}(R_1 \circ R_2) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \mathtt{sgn}(R_1) \cdot \mathtt{sgn}(R_2).$$

□

11.2 Die Definition der Determinante nach Leibniz

Wir haben nun alles Material zusammen um die Determinante einer $n \times n$ Matrix so zu definieren, wie dies 1690 von Gottfried Wilhelm Leibniz[1] vorgeschlagen wurde. Ist $A = (a_{i,j}) \in \mathbb{K}^{n\times n}$, wobei entweder $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ gilt, so definieren wir die *Determinate* von A (geschrieben $\mathtt{det}(A)$) über die Formel

$$\mathtt{det}(A) := \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} := \sum \big\{ \mathtt{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \;\big|\; \sigma \in \mathcal{S}_n \big\}.$$

Beispiel: Es sei A eine 2×2 Matrix, es gilt also

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

Zur Berechnung von $\mathtt{det}(A)$ müssen wir uns überlegen, wie $\mathcal{S}_2$ aussieht. Es gilt

$$\mathcal{S}_2 := \big\{[1,2],[2,1]\big\}.$$

Die Permutation $[1,2]$ ist die identische Permutation und damit gilt

$$\mathtt{sgn}([1,2]) = +1.$$

Die Permutation $[2,1]$ ist eine Transposition und hat daher ein negatives Vorzeichen:

$$\mathtt{sgn}([2,1]) = -1.$$

Damit finden wir

$$\mathtt{det}(A) = \mathtt{det}\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = (+1)\cdot a_{1,1}\cdot a_{2,2} + (-1)\cdot a_{1,2}\cdot a_{2,1} = a_{1,1}\cdot a_{2,2} - a_{1,2}\cdot a_{2,1} \quad \diamond$$

Aufgabe 68: Geben Sie die Formel zur Berechnung der Determinate einer 3×3 Matrix an! $\diamond$

Abbildung 11.2 auf Seite 163 zeigt ein Programm zur Berechnung der oben angegebenen Leibniz-Formel zur Berechnung der Determinante. Für $n = 4$ erhalten wir beispielsweise die in Abbildung 11.3 auf Seite 164 gezeigte Ausgabe. Es ist offensichtlich, dass die Leibniz-Formel für große Werte von n in der Praxis unbrauchbar ist, denn die Menge $\mathcal{S}_n$ aller Permutationen der Zahlen $\{1,\cdots,n\}$ enthält $n!$ verschiedene Elemente und die Fakultätsfunktion wächst schneller als jede Potenz. Wir werden daher ein anderes Verfahren zur Berechnung der Determinate entwickeln, bei dem nur etwa n^3 Rechenoperationen notwendig sind. Zu diesem Zweck beweisen wir zunächst einige Eigenschaften der Determinate.

Beim Beweis des nächsten Satzes wird sich das folgende Lemma als nützlich erweisen.

Lemma 11.12 Es sei τ eine Transposition. Dann gilt

$$\{\tau \circ \mu \mid \mu \in \mathcal{S}_n\} = \mathcal{S}_n.$$

Beweis: Wir zerlegen den Beweis in zwei Teile:

1. $\{\tau \circ \mu \mid \mu \in \mathcal{S}_n\} \subseteq \mathcal{S}_n$.

   Der Nachweis dieser Inklusion folgt aus der Tatsache, dass die Gruppe der Permutationen $\mathcal{S}_n$ unter Multiplikation abgeschlossen ist, was $\tau \circ \mu \in \mathcal{S}_n$ für alle $\mu \in \mathcal{S}_n$ impliziert.

2. $\mathcal{S}_n \subseteq \{\tau \circ \mu \mid \mu \in \mathcal{S}_n\}$.

   Sei $\sigma \in \mathcal{S}_n$. Wir definieren die Permutation μ als

   $$\mu := \tau \circ \sigma.$$

[1] In der Vorlesung hatte ich Gottfried Wilhelm Leibniz scherzhaft als den Erfinder des Butterkekses bezeichnet. Nach ihren eigenen Aussagen hat die Firma Bahlsen den Butterkeks tatsächlich nach dem Mathematiker Gottfried Wilhelm Leibniz benannt.

```
load("signum.stlx");
determinant := procedure(n) {
     det := "";
     for (l in allPermutations(n)) {
         if (signum(l) == 1) {
             det += " " * 6 + " +" + product(n, l);
         } else {
             det += " " * 6 + " -" + product(n, l);
         }
     }
     return det[10..];
 };
 product := procedure(n, l) {
     p := " ";
     for (i in [1 .. n]) {
         if (i > 1) {
             p += " * ";
         }
         p += "a[$i$, $l[i]$]";
     }
     return p + "\n";
 };
```

Abbildung 11.2: Berechnung der Leibniz-Formel in SetlX.

Offenbar ist $\mu \in \mathcal{S}_n$ und es gilt

$$\tau \circ \mu = \tau \circ \tau \circ \sigma = E_n \circ \sigma = \sigma,$$

denn da τ eine Transposition ist, gilt $\tau \circ \tau = E_n$, wobei E_n die identische Permutation bezeichnet. Aus $\sigma = \tau \circ \mu$ und $\mu \in \mathcal{S}_n$ folgt

$$\sigma \in \{\tau \circ \mu \mid \mu \in \mathcal{S}_n\}. \qquad \square$$

Wir werden bei den folgenden Sätzen eine Matrix $A \in \mathbb{K}^{n\times n}$ immer in der Form

$$A = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

angeben. Dabei bezeichnet $\mathbf{a}_i$ den i-ten Zeilenvektor der Matrix $A = (a_{i,j})$, es gilt also

$$a_i = [a_{i,1}, \cdots, a_{i,n}].$$

Satz 11.13 Die Funktion $\mathtt{det}(A)$ ist *alternierend*: Vertauschen wir zwei Zeilen der Matrix A, so dreht sich das Vorzeichen der Determinante um, genauer gilt für $k, l \in \{1, \cdots, n\}$ mit $k < l$:

$$\mathtt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_l \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = -\mathtt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a_k} \\ \vdots \\ \mathbf{a}_l \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$

```
det(A) = a[1, 1] * a[2, 2] * a[3, 3] * a[4, 4]
       - a[1, 1] * a[2, 2] * a[3, 4] * a[4, 3]
       - a[1, 1] * a[2, 3] * a[3, 2] * a[4, 4]
       + a[1, 1] * a[2, 3] * a[3, 4] * a[4, 2]
       + a[1, 1] * a[2, 4] * a[3, 2] * a[4, 3]
       - a[1, 1] * a[2, 4] * a[3, 3] * a[4, 2]
       - a[1, 2] * a[2, 1] * a[3, 3] * a[4, 4]
       + a[1, 2] * a[2, 1] * a[3, 4] * a[4, 3]
       + a[1, 2] * a[2, 3] * a[3, 1] * a[4, 4]
       - a[1, 2] * a[2, 3] * a[3, 4] * a[4, 1]
       - a[1, 2] * a[2, 4] * a[3, 1] * a[4, 3]
       + a[1, 2] * a[2, 4] * a[3, 3] * a[4, 1]
       + a[1, 3] * a[2, 1] * a[3, 2] * a[4, 4]
       - a[1, 3] * a[2, 1] * a[3, 4] * a[4, 2]
       - a[1, 3] * a[2, 2] * a[3, 1] * a[4, 4]
       + a[1, 3] * a[2, 2] * a[3, 4] * a[4, 1]
       + a[1, 3] * a[2, 4] * a[3, 1] * a[4, 2]
       - a[1, 3] * a[2, 4] * a[3, 2] * a[4, 1]
       - a[1, 4] * a[2, 1] * a[3, 2] * a[4, 3]
       + a[1, 4] * a[2, 1] * a[3, 3] * a[4, 2]
       + a[1, 4] * a[2, 2] * a[3, 1] * a[4, 3]
       - a[1, 4] * a[2, 2] * a[3, 3] * a[4, 1]
       - a[1, 4] * a[2, 3] * a[3, 1] * a[4, 2]
       + a[1, 4] * a[2, 3] * a[3, 2] * a[4, 1]
```

Abbildung 11.3: Ausgabe der Funktion `determinant` aus Abbildung 11.2 für $n = 4$.

Hier ist

$$A = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a_k} \\ \vdots \\ \mathbf{a}_l \\ \vdots \\ \mathbf{a}_n \end{pmatrix}, \quad \text{während die Matrix} \quad \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a_l} \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

aus A entsteht, wenn wir die k-te Zeile von A mit der l-ten Zeile A vertauschen.

Beweis: Es sei $\tau = \langle k, l \rangle$ die Transposition, die k mit l vertauscht. Wir definieren $\tau(A)$ als die Matrix, die aus der Matrix A durch Vertauschen der k-ten Zeile mit der l-ten Zeile hervorgeht, es gilt also

$$\tau(A) := \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a_l} \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$

In Komponentenschreibweise haben wir dann

$$\tau(A) = \left(a_{\tau(i),j}\right)_{\substack{i=1,\cdots,n\\ j=1,\cdots,n}}.$$

Nach Definition der Determinante gilt

$$\begin{aligned}
\mathtt{det}\big(\tau(A)\big) &= \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma)\cdot a_{\tau(1),\sigma(1)}\cdot\ldots\cdot a_{\tau(k),\sigma(k)}\cdot\ldots\cdot a_{\tau(l),\sigma(l)}\cdot\ldots\cdot a_{\tau(n),\sigma(n)} \\
&= \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma)\cdot a_{1,\sigma(1)}\cdot\ldots\cdot a_{l,\sigma(k)}\cdot\ldots\cdot a_{k,\sigma(l)}\cdot\ldots\cdot a_{n,\sigma(n)}, \\
&\quad \text{denn } \tau(i) = i \text{ für alle } i \notin \{k,l\} \text{ und } \tau(k) = l \text{ und } \tau(l) = k. \\
&= \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma)\cdot a_{1,\sigma(1)}\cdot\ldots\cdot a_{k,\sigma(l)}\cdot\ldots\cdot a_{l,\sigma(k)}\cdot\ldots\cdot a_{n,\sigma(n)} \\
&\quad \text{Hier wird nur das nach dem Kommutativ-Gesetz benutzt.} \\
&= \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma)\cdot a_{1,\sigma(\tau(1))}\cdot\ldots\cdot a_{k,\sigma(\tau(k))}\cdot\ldots\cdot a_{l,\sigma(\tau(k))}\cdot\ldots\cdot a_{n,\sigma(\tau(n))}, \\
&= \sum_{\sigma\in\mathcal{S}_n} \mathtt{sgn}(\sigma)\cdot a_{1,\tau\circ\sigma(1)}\cdot\ldots\cdot a_{n,\tau\circ\sigma(n)} \\
&= \sum_{\mu\in\mathcal{S}_n} \mathtt{sgn}(\tau\circ\mu)\cdot a_{1,\tau\circ(\tau\circ\mu)(1)}\cdot\ldots\cdot a_{n,\tau\circ(\tau\circ\mu)(n)} \\
&\quad \text{In diesem Schritt haben wir alle } \sigma \text{ durch } \tau\circ\mu \text{ ersetzt,} \\
&\quad \text{was nach dem Lemma 11.12 erlaubt ist.} \\
&= \sum_{\mu\in\mathcal{S}_n} \mathtt{sgn}(\tau)\cdot\mathtt{sgn}(\mu)\cdot a_{1,\tau\circ(\tau\circ\mu)(1)}\cdot\ldots\cdot a_{n,\tau\circ(\tau\circ\mu)(n)}, \\
&\quad \text{denn nach Satz 11.11 gilt } \mathtt{sgn}(\tau\circ\mu) = \mathtt{sgn}(\tau)\cdot\mathtt{sgn}(\mu) \\
&= -\sum_{\mu\in\mathcal{S}_n} \mathtt{sgn}(\mu)\cdot a_{1,(\tau\circ\tau)\circ\mu(1)}\cdot\ldots\cdot a_{n,(\tau\circ\tau)\circ\mu(n)}, \\
&\quad \text{denn da } \tau \text{ eine Transposition ist, gilt } \mathtt{sgn}(\tau) = -1. \\
&\quad \text{Außerdem haben wir benutzt, dass } \tau\circ(\tau\circ\mu) = (\tau\circ\tau)\circ\mu \text{ ist.} \\
&= -\sum_{\mu\in\mathcal{S}_n} \mathtt{sgn}(\mu)\cdot a_{1,\mu(1)}\cdot\ldots\cdot a_{n,\mu(n)} \\
&\quad \text{Da } \tau \text{ eine Transposition ist, gilt } \tau\circ\tau = E_n \text{ und } E_n\circ\mu = \mu. \\
&= -\mathtt{det}(A). \qquad \square
\end{aligned}$$

Bemerkung: Der gerade bewiesene Satz ist der am schwersten zu beweisende Satz in der Theorie der Determinanten. Das liegt daran, dass dies der einzige Satz in dieser Theorie ist, bei dessen Beweis wir die Eigenschaften der Funktion `sgn` tatsächlich benötigen. Der Rest der Theorie läuft jetzt wie von selber. ◇

Aufgabe 69: Wir definieren zu einer Matrix $A \in \mathbb{K}^{n\times n}$ die *transponierte Matrix* $A^t = (a^t_{i,j})$ indem wir

$$a^t_{i,j} := a_{j,i} \quad \text{für alle } i,j \in \{1,\cdots,n\}$$

setzen. Die Zeilen der transponierten Matrix A^t sind also die Spalten der ursprünglichen Matrix A. Beispielsweise haben wir für

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad \text{die transponierte Matrix} \quad A^t = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}.$$

Zeigen Sie, dass

$$\mathtt{det}(A^t) = \mathtt{det}(A)$$

gilt. Zum Nachweis dieses Satzes ist es nützlich, die beiden folgenden Lemmata nachzuweisen:

1. $\{\sigma^{-1} \mid \sigma \in \mathcal{S}_n\} = \mathcal{S}_n$.
2. $\big\{\langle i, \sigma(i)\rangle \mid i \in \{1, \cdots, n\}\big\} = \big\{\langle \sigma^{-1}(i), i\rangle \mid i \in \{1, \cdots, n\}\big\}$ für alle $\sigma \in \mathcal{S}_n$. ◇

Aufgabe 70: Zeigen Sie, dass für die $n \times n$ Einheits-Matrix $E_n = (\delta_{i,j})_{\substack{i=1,\cdots n\\ j=1,\cdots,n}}$

$$\texttt{det}(E_n) = 1$$

gilt. ◇

Aufgabe 71: Zeigen Sie, dass die Funktion `det` bezüglich jeder Zeile der Matrix *additiv* ist: Zeigen Sie also, dass in dem Fall, dass die Matrix A die Form

$$\texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

hat und sich die k-te Zeile als

$$\mathbf{a}_k = \mathbf{b} + \mathbf{c}$$

schreiben lässt, Folgendes gilt:

$$\texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{b}+\mathbf{c} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{b} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{c} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$ ◇

Aufgabe 72: Zeigen Sie, dass die Funktion `det` bezüglich jeder Zeile der Matrix *homogen* ist: Zeigen Sie also, dass in dem Fall, dass die Matrix A die Form

$$\texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

hat und sich die k-te Zeile als

$$\mathbf{a}_k = \lambda \cdot \mathbf{b}$$

schreiben lässt, Folgendes gilt:

$$\texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \lambda\cdot\mathbf{b} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \lambda \cdot \texttt{det}\begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{b} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$ ◇

Bemerkung: Die letzten Lemmata und die dazugehörigen Aufgaben können wir so zusammenfassen, dass wir sagen, dass die Determinante eine normierte, alternierende Multilinear-Form ist:

1. Normiertheit bedeutet
$$\mathtt{det}(\mathrm{E}_n) = 1.$$
2. Alternierend ist die Determinante, weil
$$\mathtt{det}(\cdots, \mathbf{a}_k, \cdots, \mathbf{a}_l, \cdots) = -\mathtt{det}(\cdots, \mathbf{a}_l, \cdots, \mathbf{a}_k, \cdots)$$
gilt. Das Vertauschen zweier Spalten ändert das Vorzeichen der Determinante.
3. Multilinear ist die Determinante, weil
$$\mathtt{det}(\cdots, \alpha \cdot \mathbf{a} + \beta \cdot \mathbf{b}, \cdots) = \alpha \cdot \mathtt{det}(\cdots, \mathbf{a}, \cdots) + \beta \cdot \mathtt{det}(\cdots, \mathbf{b}, \cdots)$$
gilt. Die Determinanten-Funktion ist also in jeder Spalte sowohl additiv als auch homogen.

Karl Theodor Wilhelm Weierstrass (1815-1897) hat gezeigt, dass die obigen Eigenschaften die Determinante bereits vollständig bestimmen: Jede Funktion
$$f : \mathbb{K}^{n\times n} \to \mathbb{K},$$
die normiert, alternierend und multilinear ist, stimmt mit der Determinanten-Funktion überein. Daher werden wir auch bei den folgenden Rechnungen nicht mehr auf die recht schwerfällige Definition der Determinante nach Leibniz zurück greifen, sondern wir werden nur noch die oben genannten Eigenschaften benutzen. ◇

Lemma 11.14 Es sei $A \in \mathbb{K}^{n\times n}$, $k, l \in \{1, \cdots, n\}$ mit $k \neq l$ und die k-te Zeile von A sei mit der l-ten Zeile von A identisch. Dann gilt
$$\mathtt{det}(A) = 0.$$

Beweis: Wir definieren die Transposition $\tau := \langle k, l\rangle$. Da die k-te Zeile mit der l-ten Zeile identisch ist, gilt $\tau(A) = A$. Andererseits wissen wir, dass sich bei dem Vertauschen zweier Zeilen das Vorzeichen der Determinante umdreht. Also haben wir
$$\mathtt{det}(A) = \mathtt{det}(\tau(A)) = -\mathtt{det}(A).$$
Daraus folgt
$$2 \cdot \mathtt{det}(A) = 0$$
und da wir annehmen[2], dass der Körper $\mathbb{K}$ entweder der Körper $\mathbb{R}$ der reellen Zahlen oder der Körper $\mathbb{C}$ der komplexen Zahlen ist, folgt $\mathtt{det}(A) = 0$. □

Lemma 11.15 Es sei $A \in \mathbb{K}^{n\times n}$, $k, l \in \{1, \cdots, n\}$ mit $k \neq l$, $\lambda \in \mathbb{K}$ und die Matrix B entstehe aus A, indem das λ-fache der k-ten Zeile zur l-ten Zeile addiert wird. Falls A die Form
$$A = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_l \\ \vdots \\ \mathbf{a}_n \end{pmatrix} \quad \text{hat, gilt also} \quad B = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a_k} \\ \vdots \\ \mathbf{a}_l + \lambda \cdot \mathbf{a}_k \\ \vdots \\ \mathbf{a}_n \end{pmatrix}.$$

[2] In einem endlichen Körper kann es passieren, dass $2 = 0$ ist. In einem solchen Fall dürften wir die obige Gleichung nicht durch 2 dividieren.

Dann gilt

$$\texttt{det}(B) = \texttt{det}(A).$$

Beweis: Zunächst betrachten wir die Matrix

$$C := \begin{pmatrix} \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_k \\ \vdots \end{pmatrix},$$

die aus A dadurch hervorgeht, dass wir die l-te Zeile durch die k-te Zeile ersetzen. Da in C dann die k-te Zeile mit der l-ten Zeile identisch ist, gilt nach dem gerade bewiesenen Lemma

$$\texttt{det}(C) = 0.$$

Definieren wir die Matrix D dadurch, dass wir in C die l-te Zeile mit λ multiplizieren, so haben wir wegen der Homogenität der Funktion `det`

$$\texttt{det}(D) = \texttt{det}\begin{pmatrix} \vdots \\ \mathbf{a}_k \\ \vdots \\ \lambda \cdot \mathbf{a}_k \\ \vdots \end{pmatrix} = \lambda \cdot \texttt{det}\begin{pmatrix} \vdots \\ \mathbf{a}_k \\ \vdots \\ \mathbf{a}_k \\ \vdots \end{pmatrix} = \lambda \cdot \texttt{det}(C) = \lambda \cdot 0 = 0.$$

Aufgrund der Additivität der Funktion `det` haben wir insgesamt

$$\begin{aligned}
\texttt{det}(B) &= \texttt{det}\begin{pmatrix} \vdots \\ \mathbf{a_k} \\ \vdots \\ \mathbf{a}_l + \lambda \cdot \mathbf{a}_k \\ \vdots \end{pmatrix} \\
&= \texttt{det}\begin{pmatrix} \vdots \\ \mathbf{a_k} \\ \vdots \\ \mathbf{a}_l \\ \vdots \end{pmatrix} + \texttt{det}\begin{pmatrix} \vdots \\ \mathbf{a_k} \\ \vdots \\ \lambda \cdot \mathbf{a}_k \\ \vdots \end{pmatrix} \\
&= \texttt{det}(A) + \texttt{det}(D) \\
&= \texttt{det}(A) + 0 \\
&= \texttt{det}(A).
\end{aligned}$$

□

Bemerkung: Ersetzen wir in dem letzten Lemma den Begriff "*Zeile*" durch "*Spalte*", so bleibt das Lemma gültig, denn die Determinante der transponierten Matrix A^t ist gleich der Determinante von A und beim Übergang von A zur transponierten Matrix A^t werden aus den Spalten der Matrix A die Zeilen der Matrix A^t. ◇

Lemma 11.16 Ist $A = (\mathbf{a}_1, \cdots, \mathbf{a}_n) \in \mathbb{K}^{n\times n}$ und ist die Menge der Spalten der Matrix A, also die Menge $\{\mathbf{a}_1, \cdots, \mathbf{a}_n\}$, linear abhängig, so gilt

$$\texttt{det}(A) = 0.$$

Beweis: Zunächst bemerken wir, dass die Determinante eine Matrix B sicher dann den Wert 0 hat, wenn eine der Spalten von B der Null-Vektor $\mathbf{0}$ ist. Dies können wir wie folgt aus der Homogenität der Determinanten-Funktion schließen: Nehmen wir an, dass die i-te Spalte von B der Null-Vektor ist, es gelte also

$$B = (\mathbf{b}_1, \cdots, \mathbf{b}_{i-1}, \mathbf{0}, \mathbf{b}_{i+1}, \cdots, \mathbf{b}_n).$$

Dann haben wir

$$\begin{aligned}
\texttt{det}(B) &= \texttt{det}(\mathbf{b}_1, \cdots, \mathbf{b}_{i-1}, \mathbf{0}, \mathbf{b}_{i+1}, \cdots, \mathbf{b}_n) \\
&= \texttt{det}(\mathbf{b}_1, \cdots, \mathbf{b}_{i-1}, 0 \cdot \mathbf{0}, \mathbf{b}_{i+1}, \cdots, \mathbf{b}_n) \\
&= 0 \cdot \texttt{det}(\mathbf{b}_1, \cdots, \mathbf{b}_{i-1}, \mathbf{0}, \mathbf{b}_{i+1}, \cdots, \mathbf{b}_n) \\
&= 0.
\end{aligned}$$

Aus der Voraussetzung, dass die Menge $\{\mathbf{a}_1, \cdots, \mathbf{a}_n\}$ linear abhängig ist, folgt, dass es Skalare $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$ gibt, so dass

$$\lambda_1 \cdot \mathbf{a}_1 + \cdots + \lambda_n \cdot \mathbf{a}_n = \mathbf{0},$$

wobei wenigstens für ein $k \in \{1, \cdots, n\}$ die Ungleichung $\lambda_k \neq 0$ gilt. Teilen wir die obige Gleichung dann durch dieses λ_k und bringen die Ausdrücke mit $i \neq k$ auf die andere Seite der Gleichung, so folgt

$$\mathbf{a}_k = -\sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{\lambda_i}{\lambda_k} \cdot \mathbf{a}_i.$$

Durch wiederholtes Anwenden des letzten Satzes können wir zur k-ten Spalte der Matrix A nacheinander das $-\dfrac{\lambda_i}{\lambda_k}$-fache der i-ten Spalte für alle $i \in \{1, \cdots, n\} \backslash \{k\}$ hinzuaddieren, ohne dass sich dabei der Wert der Determinante der Matrix ändert:

$$\begin{aligned}
\texttt{det}(A) &= \texttt{det}(\mathbf{a}_1, \cdots, \mathbf{a}_k, \cdots, \mathbf{a}_n) \\
&= \texttt{det}(\mathbf{a}_1, \cdots, \mathbf{a}_k - \frac{\lambda_1}{\lambda_k} \cdot \mathbf{a_1}, \cdots, \mathbf{a}_n) \\
&= \texttt{det}(\mathbf{a}_1, \cdots, \mathbf{a}_k - \frac{\lambda_1}{\lambda_k} \cdot \mathbf{a_1} - \frac{\lambda_2}{\lambda_k} \cdot \mathbf{a_2}, \cdots, \mathbf{a}_n) \\
&= \vdots \\
&= \texttt{det}(\mathbf{a}_1, \cdots, \mathbf{a}_k - \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{\lambda_i}{\lambda_k} \cdot \mathbf{a}_i, \cdots, \mathbf{a}_n) \\
&= \texttt{det}(\mathbf{a}_1, \cdots, \mathbf{0}, \cdots, \mathbf{a}_n) \\
&= 0.
\end{aligned}$$

Im letzten Schritt haben wir dann eine Matrix, deren k-te Spalte den Wert $\mathbf{0}$ hat und nach der am Beginn dieses Beweises gemachten Bemerkung ist die Determinante dieser Matrix 0. □

Genau wie wir für eine lineare Abbildung $f \in \mathcal{L}(V, W)$ im letzten Kapitel die Mengen $\texttt{Kern}(f)$ und $\texttt{Bild}(f)$ definiert haben, können wir auch für eine Matrix $A \in \mathbb{K}^{n \times m}$, die Mengen $\texttt{Kern}(A)$ und $\texttt{Bild}(A)$ definieren:

1. $\texttt{Kern}(A) := \big\{\mathbf{x} \in \mathbb{K}^m \;\big|\; A \cdot \mathbf{x} = \mathbf{0}\big\}$,
2. $\texttt{Bild}(A) := \big\{A \cdot \mathbf{x} \;\big|\; \mathbf{x} \in \mathbb{K}^m\big\}$.

Da die Abbildung $\mathbf{x} \mapsto A \cdot \mathbf{x}$ eine lineare Abbildung ist, ist $\texttt{Kern}(A)$ ein Unter-Vektorraum von $\mathbb{K}^m$ und $\texttt{Bild}(A)$ ist ein Unter-Vektorraum von $\mathbb{K}^n$. Nach dem Dimensions-Satz folgt dann

$$n = \texttt{dim}(\texttt{Kern}(A)) + \texttt{dim}(\texttt{Bild}(A)).$$

Im Falle eine quadratischen Matrix gilt $m = n$ und folglich gilt in diesem Fall

$$\texttt{dim}(\texttt{Kern}(A)) = 0 \;\Leftrightarrow\; n = \texttt{dim}(\texttt{Bild}(A)).$$

Wir nehmen im Folgenden an, dass $\texttt{dim}(\texttt{Kern}(A)) = 0$ ist und damit auch $n = \texttt{dim}(\texttt{Bild}(A))$ gilt. Die Bedingung $\texttt{dim}(\texttt{Kern}(A)) = 0$ impliziert, dass die Abbildung $\mathbf{x} \mapsto A \cdot \mathbf{x}$ injektiv ist, während die Bedingung $\texttt{dim}(\texttt{Bild}(A)) = n$ impliziert, dass die Abbildung $\mathbf{x} \mapsto A \cdot \mathbf{x}$ surjektiv ist. Folglich ist diese Abbildung insgesamt bijektiv und besitzt damit eine Umkehr-Abbildung. Bezeichnen wir die Abbildung $\mathbf{x} \mapsto A \cdot x$ mit f, setzen wir also

$$f(\mathbf{x}) := A \cdot \mathbf{x}$$

und bezeichnen wir die Umkehr-Abbildung mit f^{-1}, so können wir sehen, dass f^{-1} ebenfalls eine lineare Abbildung ist, denn es gilt

$$\begin{array}{ll} & f^{-1}(\mathbf{x} + \mathbf{y}) = f^{-1}(\mathbf{x}) + f^{-1}(\mathbf{y}) \\ \Leftrightarrow & f\big(f^{-1}(\mathbf{x} + \mathbf{y})\big) = f\big(f^{-1}(\mathbf{x}) + f^{-1}(\mathbf{y})\big) \\ & \text{denn } f \text{ ist injektiv} \\ \Leftrightarrow & \mathbf{x} + \mathbf{y} = f\big(f^{-1}(\mathbf{x})\big) + f\big(f^{-1}(\mathbf{y})\big) \\ & \text{denn } f \text{ ist linear} \\ \Leftrightarrow & \mathbf{x} + \mathbf{y} = \mathbf{x} + \mathbf{y}. \end{array}$$

Folglich lässt sich die Umkehr-Abbildung f^{-1} wieder durch eine Matrix B darstellen, so dass sich die beiden Gleichungen

$$f^{-1}\big(f(\mathbf{x})\big) = \mathbf{x} \quad \text{und} \quad f\big(f^{-1}(\mathbf{x})\big) = \mathbf{x}$$

dann in der Form

$$B \cdot A \cdot \mathbf{x} = \mathbf{x} \quad \text{und} \quad A \cdot B \cdot \mathbf{x} = \mathbf{x}$$

schreiben lassen. Weil diese Gleichungen für alle $\mathbf{x} \in \mathbb{K}^n$ gelten, folgt

$$B \cdot A = \mathrm{E}_n \quad \text{und} \quad A \cdot B = \mathrm{E}_n,$$

wobei E_n die $n \times n$ Einheits-Matrix bezeichnet. Damit ist B die zu A inverse Matrix, es gilt also $B = A^{-1}$.

Lemma 11.17 Die Matrix $A \in \mathbf{K}^{n \times n}$ sei invertierbar. Dann gilt $\texttt{det}(A) \neq 0$.

Beweis: Im letzten Kapitel hatten wir gezeigt, wie sich zu einer invertierbaren Matrix A die Inverse Matrix A^{-1} berechnen lässt. Wir hatten damals die Matrix A solange mit Elementar-Matrizen multipliziert, bis wir A zur Einheits-Matrix reduziert hatten. Konkret hatten wie eine endliche Folge $\mathrm{ZE}_1, \cdots, \mathrm{ZE}_k$ von Elementar-Matrizen berechnet, so dass die Gleichung

$$\mathrm{ZE}_k \cdot \ldots \cdot \mathrm{ZE}_1 \cdot A = \mathrm{E}_n$$

erfüllt war. Wir wissen, dass die Elementar-Matrizen alle invertierbar sind. Daher lässt sich die obige Gleichung zu

$$A = \mathrm{ZE}_1^{-1} \cdot \ldots \cdot \mathrm{ZE}_k^{-1} \cdot \mathrm{E}_n$$

umschreiben. Wir wissen, dass die Determinante der Einheits-Matrix E_n den Wert 1 hat. Wir untersuchen nun, wie sich dieser Wert durch die Multiplikation mit den Elementar-Matrizen ändert und zeigen allgemein, dass für jede Elementar-Matrix ZE_i und eine beliebige Matrix B folgendes gilt:

$$\texttt{det}(B) \neq 0 \rightarrow \texttt{det}(\mathrm{ZE}_i \cdot B) \neq 0$$

Den Nachweis dieser Behauptung führen wir durch eine Fallunterscheidung nach der Art von ZE_i.

1. Fall: $\mathrm{ZE}_i = \mathrm{ZA}_n(k,l,\alpha)$.

   Wir haben im letzten Kapitel gezeigt, dass

   $$\big(\mathrm{ZA}_n(k,l,\alpha)\big)^{-1} = \mathrm{ZA}_n(k,l,-\alpha)$$

   gilt. Die Wirkung der Multiplikation der Zeilen-Additions-Matrix $\mathrm{ZA}_n(k,l,-\alpha)$ mit einer Matrix B besteht darin, dass die die l-te Zeile von B mit $-\alpha$ multipliziert zur k-ten Zeile von B hinzu addiert wird. Nach Lemma 11.15 ändert sich der Wert der Determinante dabei nicht und folglich gilt

   $$\mathtt{det}\big(\mathrm{ZA}_n(k,l,\alpha)\cdot B\big) = \mathtt{det}(B) \neq 0.$$

2. Fall: $\mathrm{ZE}_i = \mathrm{ZP}_n(k,l)$.

   Wir haben im letzten Kapitel gezeigt, dass

   $$\mathrm{ZP}_n(k,l)^{-1} = \mathrm{ZP}_n(k,l)$$

   gilt. Die $n \times n$ Zeilen-Permutations-Matrix $\mathrm{ZP}_n(k,l)$ war als

   $$\mathrm{ZP}_n(k,l) := \mathrm{E}_n + \mathrm{A}_n(k,l) + \mathrm{A}_n(l,k) - \mathrm{A}_n(k,k) - \mathrm{A}_n(l,l).$$

   definiert. Multiplizieren wir eine $n \times n$ Matrix B von links mit $\mathrm{ZP}_n(k,l)$, so besteht der Effekt auf B darin, dass die k-te Zeile von B mit der l-ten Zeile von B vertauscht wird, es gilt also

   $$\mathrm{ZP}_n(k,l)\cdot B = \mathrm{ZP}_n(k,l)\cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_l \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$

   Da das Vertauschen zweier Zeilen das Vorzeichen der Determinante verdreht, haben wir

   $$\mathtt{det}\big(\mathrm{ZP}_n(k,l)\cdot B\big) = -\mathtt{det}(B) \neq 0.$$

3. Fall: $\mathrm{ZE}_i = \mathrm{ZM}_n(k,\alpha) \quad$ mit $\alpha \neq 0$.

   Wir haben im letzten Kapitel gezeigt, dass

   $$\mathrm{ZM}_n(k,\alpha)^{-1} = \mathrm{ZM}_n(k,\alpha^{-1})$$

   gilt. Multiplizieren wir eine $n \times n$ Matrix B von links mit $\mathrm{ZM}_n(k,\alpha^{-1})$, so besteht der Effekt auf B darin, dass die k-te Zeile von B mit α^{-1} multipliziert wird, es gilt also

   $$\mathrm{ZM}_n(k,\alpha^{-1})\cdot B = \mathrm{ZM}_n(k,\alpha^{-1})\cdot \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \alpha^{-1}\cdot\mathbf{b}_k \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$

   Da der Effekt der Multiplikation von $\mathrm{ZM}_n(k,\alpha^{-1})$ mit B darin besteht, die k-te Zeile von B mit α^{-1} zu multiplizieren, haben wir auf Grund der Homogenität der Determinanten-Funktion

   $$\mathtt{det}\big(\mathrm{ZM}_n(k,\alpha^{-1})\cdot B\big) = \alpha^{-1}\cdot\mathtt{det}(B) \neq 0.$$

Da die Determinante der Einheits-Matrix E_n den Wert 1 hat und damit von 0 verschieden ist, folgt durch Iteration der gerade gezeigten Behauptung, dass die Determinante der Matrix

$$A = \mathrm{ZE}_1^{-1} \cdot \ldots \cdot \mathrm{ZE}_k^{-1} \cdot \mathrm{E}_n$$

ebenfalls von 0 verschieden ist. □

Aufgabe 73: Zeigen Sie, dass für eine invertierbare Matrix $A \in \mathbb{K}^{n\times n}$ und eine beliebige Matrix $B \in \mathbb{K}^{n\times n}$ die Gleichung

$$\mathtt{det}(A) \cdot \mathtt{det}(B) = \mathtt{det}(A \cdot B)$$

richtig ist.

Hinweis: Zeigen Sie die Behauptung zunächst für den Fall, dass A eine Elementar-Matrix ist. ◇

Satz 11.18 Für eine $n \times n$ Matrix $A \in \mathbb{K}^{n\times n}$ gilt

$$\mathtt{det}(A) = 0 \quad \text{g.d.w.} \quad A \text{ ist nicht invertierbar.}$$

Beweis: Wir zerlegen den Beweis dieses Satzes in zwei Teile.

"⇒" Es sei als $\mathtt{det}(A) = 0$. Wäre A invertierbar, so würde nach dem eben bewiesenen Lemma folgen, dass $\mathtt{det}(A) \neq 0$ wäre. Folglich kann A nicht invertierbar sein.

"⇐" Nun sei A nicht invertierbar. Dann gilt $\mathtt{Kern}(A) \neq \{\mathbf{0}\}$. Also gibt es einen Vektor $\mathbf{x}$, so dass $A \cdot \mathbf{x} = \mathbf{0}$ ist. Schreiben wir A als

$$A = (\mathbf{a}_1, \cdots, \mathbf{a}_n),$$

wobei $\mathbf{a}_1, \cdots, \mathbf{a}_n$ die der Spalten-Vektoren von A sind, so folgt aus der Gleichung $A \cdot \mathbf{x} = \mathbf{0}$ die Gleichung

$$\sum_{i=1}^{n} x_i \cdot \mathbf{a}_i = \mathbf{0},$$

wobei hier die x_i die Komponenten des Vektors $\mathbf{x}$ bezeichnen. Damit sind aber die Spalten-Vektoren der Matrix A linear abhängig und nach einem früher bewiesenen Lemma folgt $\mathtt{det}(A) = 0$. □

Aufgabe 74: Zeigen Sie, dass die Gleichung

$$\mathtt{det}(A) \cdot \mathtt{det}(B) = \mathtt{det}(A \cdot B)$$

für beliebige Matrizen $A, B \in \mathbb{K}^{n\times n}$ gilt. ◇

Aufgabe 75: Eine Matrix $A = (a_{i,j}) \in \mathbb{K}^{n\times n}$ ist eine *obere Dreiecks-Matrix* genau dann, wenn alle Einträge der Matrix unterhalb der Diagonalen den Wert 0 haben, formal gilt

$$\forall i, j \in \{1, \cdots, n\} : i > j \rightarrow a_{i,j} = 0.$$

Zeigen Sie, dass für eine obere Dreiecks-Matrix $A = (a_{i,j}) \in \mathbb{K}^{n\times n}$ die Determinante nach der Formel

$$\mathtt{det}(A) = \prod_{i=1}^{n} a_{i,i}$$

berechnet werden kann.

Hinweis: Der Beweis der Behauptung kann am einfachsten unter Verwendung der Definition der Determinante nach Leibniz erbracht werden. ◇

Bemerkung: Die in der letzten Aufgabe angegebene Formel zur Berechnung der Determinante einer oberen Dreiecks-Matrix liefert ein effizientes Verfahren um die Determinante einer beliebigen Matrix A zu berechnen: Zunächst wird die Matrix A durch die Multiplikation mit geeigneten Elementar-Matrizen zu einer oberen Dreiecks-Matrix D umgeformt. Wenn dabei nur Elementar-Matrizen der Form $\mathrm{ZA}_n(k, l, \alpha)$ und $\mathrm{ZP}_n(k, l)$ verwendet werden, dann hat die Matrix D bis auf

das Vorzeichen dieselbe Determinante wie die Matrix A und die Determinante von D lässt sich als Produkt der Diagonal-Elemente der Matrix D berechnen.

```
1  determinant := procedure(a) {
2      n := #a;
3      sign := 1;
4      for (i in [1 .. n]) {
5          r := pivot(a, n, i);
6          if (r != i) {
7              [ a[i], a[r] ] := [ a[r], a[i] ];
8              sign := -sign;
9          }
10         if (a[i][i] == 0) {
11             return 0;
12         }
13         for (k in [i+1 .. n] | k != i) {
14             f := a[k][i]/a[i][i];
15             for (j in [i .. n]) {
16                 a[k][j] -= f * a[i][j];
17             }
18         }
19     }
20     return sign */ { a[i][i] : i in {1 .. n} };
21 };
```

Abbildung 11.4: Berechnung der Determinante.

Abbildung zeigt ein SetlX-Programm, das den oben beschriebenen Algorithmus zur Berechnung umsetzt. Wir diskutieren es Zeile für Zeile.

1. Die Matrix `a`, deren Determinante berechnet werden soll, wird als Liste ihrer Zeilen dargestellt. Das ist dieselbe Darstellung, die wir auch bei dem in Abbildung 10.1 auf Seite 149 gezeigten Programm zur Berechnung der Inversen einer Matrix verwendet haben.

2. `n` ist die Anzahl der Zeilen der Matrix.

3. In der Variablen `sign` merken wir uns, wie oft wir bei der Berechnung der Determinanten Zeilen vertauscht haben. Solange diese Anzahl gerade ist, hat `sign` den Wert $+1$, aber wenn die Anzahl ungerade ist, hat `sign` den Wert -1.

4. Die Schleife in Zeile 4 des Programms hat die Aufgabe, die Elemente von `a`, die in der Spalte unter dem Element `a[i][i]` stehen, durch Addition geeignete Vielfacher der `i`-ten Zeile zu 0 zu reduzieren.

5. Aus Gründen der numerischen Stabilität des Verfahrens ist es sinnvoll, zunächst die Zeile `r` zu bestimmen, für die der Absolutbetrag `a[r][i]` maximal wird. Die Berechnung dieser Zeile geschieht mit Hilfe der Funktion `pivot`, deren Implementierung in Abbildung 10.2 gezeigt ist. Wir hatten diese Funktion bereits bei der Berechnung des Inversen der Matrix A benutzt.

6. Falls wir tatsächlich eine Vertauschung von Zeilen vornehmen, falls also `r` $\neq$ `i` ist, drehen wir das Vorzeichen `sign` um.

7. Sollte `a[i][i]` den Wert 0 haben, so brauchen wir nicht weitermachen, denn wenn ein Element auf der Diagonalen einer Dreiecks-Matrix 0 ist, ist natürlich auch das Produkt aller Diagonal-Elemente 0. Wir geben daher in diesem Fall in Zeile 11 den Wert 0 zurück.

8. Ansonsten ziehen wir nun das

   $\frac{a_{k,i}}{a_{i,i}}$-fache der i-ten Zeile von der k-ten Zeile ab,

   so dass danach `a[k][i]` den Wert 0 hat.

9. Am Ende berechnen wir das Produkt aller Diagonal-Elemente und multiplizieren es noch mit dem Vorzeichen `sign`, denn dies ist die gesuchte Determinante der Matrix `a`. ◇

Aufgabe 76: Berechnen Sie die Determinante der Matrix

$$A := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

mit dem Algorithmus, der in dem in Abbildung 11.4 gezeigten Programm implementiert ist. ◇

Kapitel 12

Eigenwerte und Eigenvektoren

Eigenwerte und Eigenvektoren gehören zu den wichtigsten Anwendungen der linearen Algebra:

1. Die Schrödinger-Gleichung

   $$H\Psi = E \cdot \Psi$$

   ist eine Eigenwert-Gleichung. Hier ist H der sogenannte Hamilton-Operator, der auf die Wellenfunktion Ψ angewendet wird. Dabei kommt wieder die Wellenfunktion Ψ als Ergebnis heraus, allerdings multipliziert mit dem Eigenwert E, der als die Energie der Wellenfunktion Ψ interpretiert werden kann.

   Die Schrödinger-Gleichung ist die Grundlage der Quanten-Mechanik. Natürlich erwarte ich von Ihnen nicht, dass Sie diese Gleichung verstehen. Ich habe diese Gleichung als erstes aufgelistet, weil dies einerseits früher einer der wichtigsten Anwendung von Eigenvektoren war und weil ich andererseits selber im Rahmen meiner Diplomarbeit im wesentlichen nichts anderes gemacht habe, als auf numerischem Wege Schrödinger-Gleichungen zu lösen. Um die Schrödinger-Gleichungen numerisch zu lösen, wird der Hamilton-Operator zunächst durch eine Matrix approximiert und anschließend werden die Eigenwerte dieser Matrix berechnet.

2. In der Informatik werden Eigenvektoren unter anderem bei der *Unabhängigkeits-Analyse* benötigt. Die Unabhängigkeits-Analyse kann beispielsweise dazu benutzt werden, das Cocktail-Party-Problem zu lösen. Bei diesem Problem geht es darum, verschiedene Geräuschquellen zu isolieren: Stellen Sie sich vor, Sie sind auf einer Cocktail-Party. Im Hintergrund spielt ein Klavier und Sie unterhalten sich mit einem Gesprächspartner. Ihre Ohren hören sowohl das Klavier als auch den Gesprächspartner, aber solange Sie noch nicht zu viele Cocktails getrunken haben, ist Ihr Gehirn in der Lage, das, was Ihr Gesprächspartner Ihnen erzählt, aus dem Gesamtgeräusch heraus zu filtern.

   Neben dem Cocktail-Party-Problem gibt es zahlreiche anderen Anwendungen der Unabhängigkeits-Analyse sowohl in der Informatik im Bereich des *Data-Minings* als auch in vielen anderen Bereichen der Wissenschaft.

3. Eine andere Anwendung von Eigenvektoren ist die Lösung von solchen Rekurrenz-Gleichungen, die bei Komplexitätsanalyse von Algorithmen auftreten.

4. Die Liste der Anwendungen von Eigenvektoren ließe sich problemlos fortsetzen. Allerdings würden Ihnen die meisten Anwendungen zum jetzigen Zeitpunkt Ihres Studiums noch wenig sagen. Daher spare ich mir hier weitere Beispiele.

In diesem Kapitel führen wir zunächst Eigenwerte und Eigenvektoren ein und zeigen dann, wie sich lineare Rekurrenz-Gleichungen mit Hilfe von Eigenvektoren lösen lassen.

12.1 Definition und Berechnung von Eigenwerten

Definition 12.1 (Eigenwert) Es sei $A \in \mathbb{K}^{n\times n}$ eine quadratische Matrix. Ein Vektor $\mathbf{x} \in \mathbb{K}^n$ mit $\mathbf{x} \neq \mathbf{0}$ ist ein *Eigenvektor* der Matrix A zum *Eigenwert* $\lambda \in \mathbb{K}$ genau dann, wenn

$$A \cdot \mathbf{x} = \lambda \cdot \mathbf{x}$$

gilt. ◇

Beispiel: Die Matrix $A \in \mathbb{R}^{2\times 2}$ sei als

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

gegeben. Die Vektoren $\mathbf{x}$ und $\mathbf{y}$ seien definiert als

$$\mathbf{x} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{und} \quad \mathbf{y} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Dann gilt

$$A \cdot \mathbf{x} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3 \cdot \mathbf{x} \quad \text{und} \quad A \cdot \mathbf{y} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot \mathbf{y}.$$

Folglich ist $\mathbf{x}$ eine Eigenvektor von A zum Eigenwert 3, während $\mathbf{y}$ ein Eigenvektor von A zum Eigenwert 1 ist. ◇

Bemerkung: Der Begriff des Eigenwerts und des Eigenvektors lässt sich auf beliebige lineare Operatoren ausdehnen. Ist $\mathrm{H} \in \mathcal{L}(V)$ ein Operator auf dem Vektor-Raum V, so ist $\mathbf{x} \in V$ genau dann ein Eigenvektor zum Eigenwert λ, wenn

$$\mathrm{H}(\mathbf{x}) = \lambda \cdot \mathbf{x}$$

gilt. Beispielsweise hat der Differential-Operator

$$\mathrm{D} : \mathcal{C}^\infty(\mathbb{R}) \to \mathcal{C}^\infty(\mathbb{R}),$$

der auf dem Raum

$$\mathcal{C}^\infty := \left\{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ ist beliebig oft differenzierbar} \right\}$$

durch die Gleichung

$$\mathrm{D}(f) := \frac{\mathrm{d}f}{\mathrm{d}x}$$

definiert ist, die Funktion $x \mapsto e^x$ als Eigenvektor zum Eigenwert 1. Der Vektor-Raum $\mathcal{C}^\infty$ der unendlich oft differenzierbaren Funktionen ist unendlich-dimensional und hat daher eine wesentlich komplexere Struktur als die endlich-dimensionalen Vektor-Räume, mit denen wir uns im Rest dieser Vorlesung beschäftigen werden. Da bei endlich-dimensionalen Vektor-Räumen jede lineare Abbildung durch eine Matrix dargestellt werden kann, verlieren wir nichts, wenn wir uns auf die Bestimmung von Eigenvektoren und Eigenwerten von Matrizen beschränken. ◇

Der folgende Satz stellt einen Zusammenhang zwischen Eigenwerten und Determinanten her. Dieser Satz ist der Grund, warum wir den Begriff der Determinanten im letzten Kapitel eingeführt haben.

Satz 12.2 Es sei $A \in \mathbb{K}^{n\times n}$. Dann ist $\lambda \in \mathbb{K}$ genau dann ein Eigenwert von A, wenn

$$\mathtt{det}(\lambda \cdot \mathrm{E}_n - A) = 0$$

gilt.

Beweis: Falls $\mathbf{x} \neq \mathbf{0}$ ein Eigenvektor von A zum Eigenwert λ ist, so haben wir die folgende Kette von Äquivalenzen:

$$\begin{array}{ll} & \exists \mathbf{x} \in \mathbb{K}^n : \mathbf{x} \neq \mathbf{0} \wedge A \cdot \mathbf{x} = \lambda \cdot \mathbf{x} \\ \Leftrightarrow & \exists \mathbf{x} \in \mathbb{K}^n : \mathbf{x} \neq \mathbf{0} \wedge A \cdot \mathbf{x} - \lambda \cdot \mathrm{E}_n \cdot \mathbf{x} = \mathbf{0} \\ \Leftrightarrow & \exists \mathbf{x} \in \mathbb{K}^n : \mathbf{x} \neq \mathbf{0} \wedge (A - \lambda \cdot \mathrm{E}_n) \cdot \mathbf{x} = \mathbf{0} \\ \Leftrightarrow & \mathtt{Kern}(A - \lambda \cdot \mathrm{E}_n) \neq \{\mathbf{0}\} \\ \Leftrightarrow & A - \lambda \cdot \mathrm{E}_n \text{ ist nicht invertierbar} \\ \Leftrightarrow & \mathtt{det}(A - \lambda \cdot \mathrm{E}_n) = 0 \\ \Leftrightarrow & \mathtt{det}(\lambda \cdot \mathrm{E}_n - A) = 0 \end{array}$$

□

Nach dem letzten Satz sind die Eigenwerte genau die Werte λ, für die der Ausdruck

$$\mathtt{det}(\lambda \cdot \mathrm{E}_n - A)$$

den Wert 0 annimmt. Berechnen wir diesen Ausdruck mit Hilfe der von Leibniz angegebenen Formel, so erhalten wir ein Polynom in der Unbestimmten λ. Dieses Polynom heißt das *charakteristische Polynom* der Matrix A und ist formal als

$$\chi_A(\lambda) = \mathtt{det}(\lambda \cdot \mathrm{E}_n - A)$$

definiert. Die Nullstellen von χ_A sind also gerade die Eigenwerte von A, formal gilt

$$\lambda \text{ ist Eigenwert von } A \quad \text{g.d.w.} \quad \chi_A(\lambda) = 0.$$

Beispiel: Die Matrix $A \in \mathbb{R}^{2\times 2}$ sei wie oben als

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

gegeben. Dann kann das charakteristische Polynom $\chi_A(\lambda)$ wie folgt berechnet werden:

$$\begin{array}{rcl} \chi_A(\lambda) & = & \mathtt{det}(\lambda \cdot \mathrm{E}_n - A) \\ & = & \mathtt{det} \begin{pmatrix} \lambda - 2 & -1 \\ -1 & \lambda - 2 \end{pmatrix} \\ & = & (\lambda - 2) \cdot (\lambda - 2) - (-1) \cdot (-1) \\ & = & \lambda^2 - 4 \cdot \lambda + 4 - 1 \\ & = & \lambda^2 - 4 \cdot \lambda + 3 \\ & = & (\lambda - 3) \cdot (\lambda - 1). \end{array}$$

Offenbar hat dieses Polynom die Nullstellen $\lambda = 3$ und $\lambda = 1$. Um beispielsweise den Eigenvektor zum Eigenwert $\lambda = 3$ zu berechnen, müssen wir die Gleichung

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 3 \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

lösen. Das liefert die beiden Gleichungen

$$2 \cdot x_1 + x_2 = 3 \cdot x_1 \quad \text{und} \quad x_1 + 2 \cdot x_2 = 3 \cdot x_2$$

die wir zu

$$-x_1 + x_2 = 0 \quad \text{und} \quad x_1 - x_2 = 0.$$

vereinfachen. Offenbar ist die zweite Gleichung zur ersten Gleichung äquivalent und kann daher weggelassen werden. Da wir dann nur noch eine Gleichung aber zwei Unbekannte haben, können wir eine der Unbekannten frei wählen. Wie müssen lediglich darauf achten, dass der Vektor $\binom{x_1}{x_2}$ vom Nullvektor verschieden ist. Wir setzen daher $x_1 := 1$ und finden dann $x_2 = 1$. Damit haben wir den Vektor $\mathbf{x} = \binom{1}{1}$ als Eigenvektor der Matrix A zum Eigenwert 3 gefunden.

Aufgabe 77: Überlegen Sie sich, für welche Werte von a, b und c die Matrix

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

zwei verschiedene reelle Eigenwerte besitzt. ◇

Aufgabe 78: Für welche Werte von φ hat die Matrix

$$A = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

keinen reellen Eigenwert? ◇

Definition 12.3 (Diagonalisierbarkeit) Eine Matrix $A \in \mathbb{K}^{n\times n}$ ist *diagonalisierbar* genau dann, wenn die Matrix n linear unabhängige Eigenvektoren besitzt. ◇

Bemerkung: Ist $A \in \mathbb{K}^{n\times n}$ diagonalisierbar, so gibt es also n verschiedene Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_n$, so dass

$$A \cdot \mathbf{x}_i = \lambda_i \cdot \mathbf{x}_i \quad \text{für alle } i = \{1, \cdots, n\}$$

gilt. Fassen wir die n Eigenvektoren $\mathbf{x}_i$ zu einer $n \times n$ Matrix X zusammen, die wir als

$$X = (\mathbf{x}_1, \cdots, \mathbf{x}_n)$$

schreiben, wobei die $\mathbf{x}_i$ die Spalten der Matrix X sind, so gilt

$$A \cdot X = (\lambda_1 \cdot \mathbf{x}_1, \cdots, \lambda_n \cdot \mathbf{x}_n) = X \cdot D,$$

wobei wir die Matrix D als Diagonal-Matrix definieren, deren Diagonal-Elemente die Eigenwerte λ_i sind, während alle anderen Einträge den Wert 0 haben. Damit gilt

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

In Komponentenschreibweise können wir die Matrix D als

$$D = (d_{i,j}) \quad \text{mit } d_{i,j} := \lambda_i \cdot \delta_{i,j} \quad \text{für alle } i, j \in \{1, \cdots, n\}$$

schreiben, wobei $\delta_{i,j}$ das bereits früher definierte Kronecker-Delta bezeichnet. Da die n Vektoren $\mathbf{x}_1, \cdots, \mathbf{x}_n$ linear unabhängig sind, ist die Matrix $X = (\mathbf{x}_1, \cdots, \mathbf{x}_n)$ invertierbar. Damit können wir die Gleichung

$$A \cdot X = X \cdot D$$

von rechts mit der Matrix X^{-1} multiplizieren und erhalten

$$A = X \cdot D \cdot X^{-1}.$$

Dies ist nützlich, wenn wir Potenzen der Matrix A bilden wollen. Beispielsweise gilt

$$A^2 = X \cdot D \cdot X^{-1} \cdot X \cdot D \cdot X^{-1} = X \cdot D^2 \cdot X^{-1}$$

und durch eine einfache Induktion nach k können wir nach dem selben Prinzip zeigen, dass

$$A^k = X \cdot D^k \cdot X^{-1} \quad \text{für alle } k \in \mathbb{N}$$

gilt. Diese Beobachtung ist deswegen nützlich, weil die Potenzen der Diagonal-Matrix D wesentlich leichter zu berechnen sind als die Potenzen von A, denn es gilt

$$D^k = \begin{pmatrix} \lambda_1^k & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2^k & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3^k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-1}^k & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_n^k \end{pmatrix}.$$

Diese Beobachtung wird uns im nächsten Abschnitt die Berechnung der *Fibonacci-Zahlen* ermöglichen.

12.2 Die Berechnung der Fibonacci-Zahlen

Die Folge $(f_n)_{n\in\mathbb{N}}$ der Fibonacci-Zahlen ist rekursiv durch die Gleichung

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

zusammen mit den Anfangs-Bedingungen $f_0 = 0$ und $f_1 = 1$ definiert. Eine Gleichung der obigen Form wird als *lineare Rekurrenz-Gleichung* bezeichnet. Solche Gleichungen werden uns später bei der Abschätzung der Komplexität von Algorithmen häufig begegnen und wir zeigen nun am Beispiel der Fibonacci-Zahlen, wie sich eine solche Rekurrenz-Gleichung lösen lässt. Dazu definieren wir zunächst die Matrix A als

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Weiter definieren wir den Vektor $\mathbf{x}_n$ für alle $n \in \mathbb{N}$ als $\mathbf{x}_n := \begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix}$. Dann haben wir

$$\mathbf{x}_{n+1} = A \cdot \mathbf{x}_n \quad \text{für alle } n \in \mathbb{N},$$

denn wenn wir die Gleichung $\mathbf{x}_{n+1} = A \cdot \mathbf{x}_n$ komponentenweise schreiben, dann bekommen wir die beiden Gleichungen

$$\begin{aligned} f_{n+1} &= 0 \cdot f_n + 1 \cdot f_{n+1}, \\ f_{n+2} &= 1 \cdot f_n + 1 \cdot f_{n+1}. \end{aligned}$$

Die erste dieser beiden Gleichungen ist trivial, die zweite Gleichung ist nichts anderes als die Rekurrenz-Gleichung für die Fibonacci-Zahlen. Aus der Gleichung $\mathbf{x}_{n+1} = A \cdot \mathbf{x}_n$ folgt durch eine triviale Induktion nach n, dass

$$\mathbf{x}_n = A^n \cdot \mathbf{x}_0$$

gilt, wobei $A^0 = \mathrm{E}_2$ ist und $\mathbf{x}_0 = \binom{0}{1}$ gilt. Wollen wir Potenzen A^n berechnen, so ist es zweckmäßig, die Matrix A vorher zu diagonalisieren. Wir berechnen zunächst das charakteristische Polynom von A:

$$\chi_A(\lambda) = \texttt{det}(\lambda \cdot \mathrm{E}_2 - A) = \texttt{det} \begin{pmatrix} \lambda & -1 \\ -1 & \lambda - 1 \end{pmatrix} = \lambda \cdot (\lambda - 1) - 1 = \lambda^2 - \lambda - 1.$$

Nun bestimmen wir die Nullstellen von $\chi_A(\lambda)$, denn das sind die Eigenwerte von A:

$$
\begin{aligned}
& \chi_A(\lambda) = 0 \\
\Leftrightarrow\quad & \lambda^2 - \lambda - 1 = 0 \\
\Leftrightarrow\quad & \lambda^2 - \lambda = 1 \\
\Leftrightarrow\quad & \lambda^2 - \lambda + \left(\tfrac{1}{2}\right)^2 = 1 + \tfrac{1}{4} \\
\Leftrightarrow\quad & \left(\lambda - \frac{1}{2}\right)^2 = \frac{5}{4} \\
\Leftrightarrow\quad & \lambda = \frac{1}{2} + \frac{\sqrt{5}}{2} \;\vee\; \lambda = \frac{1}{2} - \frac{\sqrt{5}}{2}
\end{aligned}
$$

Wir definieren daher

$$\lambda_1 = \tfrac{1}{2} \cdot (1 + \sqrt{5}) \quad \text{und} \quad \lambda_2 = \tfrac{1}{2} \cdot (1 - \sqrt{5}).$$

Als nächstes müssen wir die Eigenvektoren bestimmen, die diesen beiden Eigenwerten zugeordnet sind. Bezeichnen wir den Eigenvektor, der λ_1 zugeordnet ist, als $\mathbf{y} := \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, so haben wir also

$$A \cdot \mathbf{y} = \lambda_1 \cdot \mathbf{y}$$

und aus dieser Gleichung folgt, dass für die Komponenten y_1 und y_2

$$y_2 = \lambda_1 \cdot y_1 \quad \text{und} \quad y_1 + y_2 = \lambda_1 \cdot y_2$$

gelten muss. Es lässt sich zeigen, dass die zweite Gleichung aus der ersten folgt. Setzen wir $y_1 := 1$, so erhalten wir aus der ersten Gleichung $y_2 = \lambda_1$. Damit hat der Eigenvektor $\mathbf{y}$ die Form

$$\mathbf{y} = \begin{pmatrix} 1 \\ \lambda_1 \end{pmatrix}.$$

Auf analoge Weise finden wie für den zweiten Eigenvektor $\mathbf{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ das Ergebnis

$$\mathbf{z} = \begin{pmatrix} 1 \\ \lambda_2 \end{pmatrix}.$$

Damit hat die Matrix der Eigenvektoren die Form

$$X := \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix}.$$

Diese Matrix hat die Determinante $\texttt{det}(X) = \lambda_2 - \lambda_1 = -\sqrt{5}$. Wir hatten in einer Übungsaufgabe eine Formel zur Berechnung des Inversen einer beliebigen 2×2 Matrix hergeleitet. Nach dieser Formel ist das Inverse der Matrix X durch

$$X^{-1} = -\frac{1}{\sqrt{5}} \cdot \begin{pmatrix} \lambda_2 & -1 \\ -\lambda_1 & 1 \end{pmatrix} = \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} -\lambda_2 & 1 \\ \lambda_1 & -1 \end{pmatrix}$$

gegeben. Damit gilt also

$$
\begin{aligned}
\mathbf{x}_n &= A^n \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} -\lambda_2 & 1 \\ \lambda_1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
&= \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
&= \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1^n \\ -\lambda_2^n \end{pmatrix} \\
&= \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} \lambda_1^n - \lambda_2^n \\ \lambda_1^{n+1} - \lambda_2^{n+1} \end{pmatrix}
\end{aligned}
$$

Die erste Komponente von $\mathbf{x}_n$ ist gleich f_n. Daher haben wir für die n-te Fibonacci-Zahl f_n die Gleichung

$$\boxed{f_n = \frac{1}{\sqrt{5}} \cdot (\lambda_1^n - \lambda_2^n)}$$

gefunden.

Aufgabe 79: Lösen Sie die Rekurrenz-Gleichung

$$a_{n+2} = 3 \cdot a_{n+1} - 2 \cdot a_n \quad \text{für die Anfangs-Bedingungen } a_0 = 0,\ a_1 = 1$$

mit Hilfe der in diesem Abschnitt vorgestellten Methode.

Literaturverzeichnis

[Axl97] Sheldon Axler. *Linear Algebra Done Right*. Springer, 2nd edition, 1997.

[Can95] Georg Cantor. Beiträge zur Begründung der transfiniten Mengenlehre. *Mathematische Annalen*, 46:481–512, 1895.

[Fis08] Gerd Fischer. *Lineare Algebra*. Vieweg+Teubner Verlag, 16th edition, 2008.

[Kow03] Hans-Joachim Kowalsky. *Lineare Algebra*. deGruyter, 12th edition, 2003.

[Lip98] Seymour Lipschutz. *Set Theory and Related Topics*. McGraw-Hill, New York, 1998.

[LL12] Seymour Lipschutz and Marc Lipson. *Linear Algebra*. McGraw-Hill, 5th edition, 2012.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Crypto-Systems. *Communications of the ACM*, 21(2):120–126, 1978.