Mathematik
für das
21te Jahrhundert

Ein Einblick in die moderne Mathematik für
Studienanfänger und Neugierige

Jon Nedelmann

Januar 2014

Einleitung

Wissen, so sagt man, ist im einundzwanzigsten Jahrhundert die wichtigste Ressource unserer Gesellschaft geworden. Was man aber wissen sollte, ist wiederum eine Frage, die nicht leicht zu beantworten ist. Bei der Suche nach einem gemeinsamen Nenner stellen viele *mathematisches Wissen* in den Vordergrund, denn angeblich ist Mathematik die Sprache, mit der die Wissenschaft die Natur beschreibt und in der Techniker miteinander kommunizieren. Andererseits kommen wir in unserem Alltagsleben selten mit mathematischen Problemen in Berührung, die nicht mit dem, was wir in der Schule bis zur siebten Klasse gelernt haben, zu lösen sind.

Dieses kleine Skriptum stellt einige mathematische Ergebnisse und Methoden vor. Gedacht ist es für Leser, die demnächst ein Mathematik- oder Informatikstudium aufnehmen wollen, aber auch für Naturwissenschaftler, Ingenieure und alle, die sich einfach so für Mathematik interessieren. Im Vordergrund stehen Fähigkeiten, die ein mathematisch denkender Mensch haben sollte; um welche es sich handelt, kann den Kapitelüberschriften entnommen werden. Damit soll eine kleine Einstimmung gegeben werden, wie Mathematik an der Universität vermittelt wird und wie sie sich von der Schulmathematik unterscheidet. Der Text ist so knapp gehalten, dass er problemlos während eines Sommerurlaubs durchgearbeitet werden kann (z. B. zwischen Abitur und Studienbeginn). Es ist nicht meine Absicht, die Themen, die normalerweise in den ersten Semestern unterrichtet werden, vorwegzunehmen.

So ist auch die Auswahl der Themen sehr subjektiv, geprägt von meiner Arbeit als wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt. Mein Ziel wäre erreicht, wenn ein Leser ein "Gefühl" für Mathematik entwickelt und sich nach der Lektüre auf die Mathematikvorlesungen an der Universität freut.

Mathematische Texte werden gerne in einer "Wir-Form" geschrieben, mit der der Autor dem Leser anbieten will, dass beide sich "gemeinsam" durch die Höhen und Tiefen des Texts durcharbeiten. Auch ich schließe mich diesem wir an. Worte oder Ausdrücke, die neu eingeführt werden, sind **fett** gedruckt. Diese Worte sind auch im Index zu finden. Jeder Abschnitt endet mit Übungsaufgaben, die in ihrem Schwierigkeitsgrad variieren. In einem letzten Abschnitt habe ich zu allen Aufgaben Lösungsvorschläge angegeben. Dort sind auch noch Empfehlungen zur weiteren Literatur zu finden.

Schließlich eine Warnung: Mathematische Texte lassen sich nicht wie die Zeitung am Frühstückstisch lesen. An einigen Stellen wird man hängenbleiben, ab und zu muss man zurückblättern, und einiges ist einfacher zu verstehen, wenn es auf einem Schmierblatt nachvollzogen wird. Du solltest also immer Papier und Bleistift bei der Lektüre griffbereit haben.

Inhaltsverzeichnis

1 Zählen **4**

2 Strukturieren **18**

3 Formalisieren **45**

4 Abstrahieren **62**

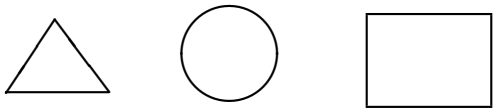
5 Rechnen **83**

6 Konstruieren **95**

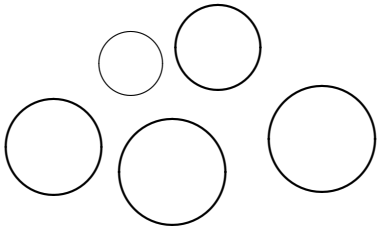
7 Lösungen und weitere Literatur **111**

1 Zählen

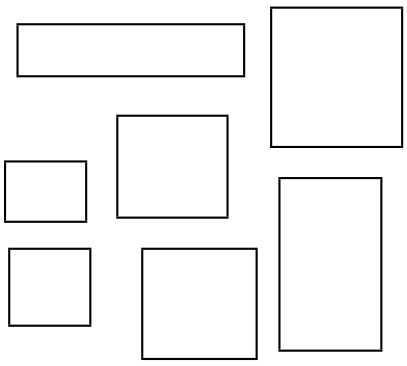
Wir wollen unsere ersten Ideen auf unserer Intuition aufbauen und vergessen, was wir schon alles wissen über Zahlen, Arithmetik und desgleichen. Versetzen wir uns in die Lage eines kleinen Kindes, das gerade gelernt hat, verschiedene Formen zu unterscheiden und zu benennen wie z. B. Dreiecke, Kreise und Rechtecke.



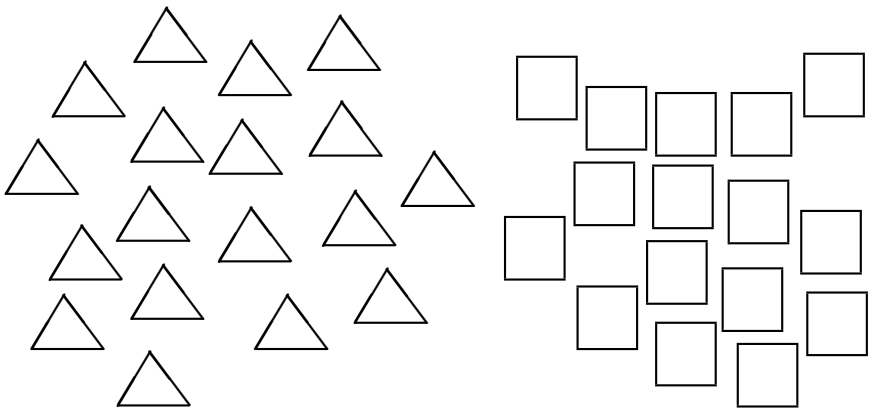
Betrachten wir nun ein Bild mit einigen Kreisen



und eines mit Rechtecken.



Bei beiden Bildern gelingt es, einen unmittelbaren Eindruck der **Anzahl** der Gegenstände zu erhalten; vor allem stellen wir fest, dass wir mehr Rechtecke als Kreise sehen. Schon bei dem nächsten Bild gelingt dies nicht mehr auf einem Blick:



Woran liegt das? Wir haben nur ein schwache Auffassungsgabe bei der Beurteilung von Anzahlen. Empirische Untersuchungen haben ergeben, dass die Grenze bei etwa sieben Objekten liegt. Bestimmte Tiere übertreffen uns Menschen deutlich. Raben können angeblich Anzahlen bis vierzehn erkennen[1]. Das heißt, sie haben ein Gespür, ob vor ihnen vierzehn, zwölf oder nur drei Gegenstände liegen. Jenseits der vierzehn fängt für Raben die Unendlichkeit an, sie haben nur noch ein Gespür, dass dort viele Gegenstände sind.

Fängt für den Menschen damit die Unendlichkeit bei acht an? Nein, wir helfen unserer Intuition auf die Sprünge, indem wir anfangen zu ordnen, Muster zu suchen, eine Reihenfolge festzulegen - in anderen Worten, indem wir anfangen zu zählen. Wir nehmen zum Beispiel unsere Finger zum

[1]siehe *O. Koehler*, The ability of birds to 'count', Bull. Animal Behaviour 9 (1950)

Abzählen, eine Tätigkeit, die dem Raben schwer fallen wird, oder zeichnen Dreiecke und Rechtecke nocheinmal, diesmal aber in zwei Zeilen untereinander angeordnet.

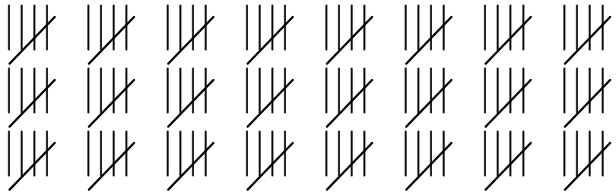
△ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Es springt uns sofort ins Auge, dass es mehr Drei- als Rechtecke gibt, wir können dieses mehr auch quantifizieren: △△. Einfacher ist es natürlich, statt △ oder □ einen Strich zu malen, damit erhalten wir die Strichlisten

|||||||||||||||||| ||||||||||||||

Jetzt können wir simultan auf beiden Seiten Striche wegstreichen bis auf einer Seite kein Strich mehr vorhanden ist. Übriggeblieben ist ||, im besten Einklang mit △△. Die Methode mit den Strichen wird schnell mühselig und ist fehleranfällig. Geschickter ist eine Darstellung der Form

Das bedeutet, nach |||| Strichen streichen wir mit dem nächsten diese durch, und wir erhalten einen **Block** ||||. Aber auch das wird schnell unübersichtlich, z. B. hat dieses Skriptum



Seiten. Wir suchen also eine kompaktere Schreibweise als unsere Strichlisten. Bevor wir uns diesem Problem widmen, klären wir einen Begriff. Wir werden oft Dingen Namen geben, damit wir sie unterscheiden und benennen können. Manchmal werden wir so viele Namen vergeben, dass einem schwindelig werden könnte. Der Stoff, aus dem diese Namen gebildet werden, sind **Symbole**. Was genau ein Symbol sein soll, ist eine knifflige Frage, die wir hier auch nicht beantworten wollen. Meistens werden wir Zeichen wie zum Beispiel

$$A, b, \mathbf{A}, \phi, \aleph, \mathbb{C}, *, \hat{}$$

benutzen und von dem Dreieck A, der Zahl b, der Klasse $\mathbb{C}$, dem Ausdruck $*$ sprechen. Wann zwei solche Zeichen als das gleiche Symbol angesehen werden, wird meistens stillschweigend vom Autor vorausgesetzt. Manche Betriebssysteme eines Computers unterscheiden nicht zwischen Groß- und Kleinbuchstaben. Für so ein System wäre A und a dasselbe Symbol. In den meisten mathematischen Texten wie auch in diesem wird sehr wohl zwischen Klein- und Großbuchstaben unterschieden; meistens hat der Autor gewisse Intentionen bei der Wahl, so wird man oft Ausdrücke der Form $x \in X$, aber selten welche der Gestalt $X \in x$ finden. Desweiteren wird gerne Fettdruck zur Unterscheidung von Symbolen benutzt, so sollen A und $\mathbf{A}$ zwei verschiedene Dinge darstellen. Verschiedene Schriftgrößen werden meistens nicht zur Unterscheidung benutzt, so stellen die Sterne

$$* \quad {}_{*} \quad *$$

ein und dasselbe Symbol dar. Bei verschiedenen Schriftarten ist Vorsicht angebracht; A und $\mathbb{A}$ sollen bestimmt verschiedene Symbole darstellen, aber ob das auch für A und A zutrifft, ist fragwürdig. Oft werden gerne an ein Zeichen andere Zeichen angehängt, so sollen A, A^{eq}, $\underline{A}$ verschiedene Symbole sein, die aber meist mathematische Objekte beschreiben, die in einem bestimmten Zusammenhang stehen; etwa in der Form, "A^{eq} entsteht aus A, indem..." Letztendlich müssen wir ein gewisses Gespür entwickeln, was welches Symbol ist.

Später werden wir viel mehr als Symbol zulassen: jedes mathematische Objekt, das ein reines Gedankenkonstrukt ist, kann selbst wieder als Symbol dienen. Damit werden wir Symbole haben, die wir nicht in Zeichen hinschreiben können – wir müssen gar nicht einmal erträumen können, wie diese Symbole aussehen.

Das Symbol, das wir bis jetzt benutzt haben, ist |, der Strich. Aus diesem haben wir Ausdrücke gebildet, die Strichlisten. Auf ähnliche Weise, nämlich einfach durch Hintereinanderschreiben, wollen wir Ausdrücke konstruieren, die aus mehreren Symbolen bestehen. Bei dem Umgang mit diesen neuen Ausdrücken benutzen wir Formulierungen wie, "das am weitesten rechts stehende Symbol", "eins nach links schieben", die selbsterklärend sind.

Wir führen nun neue Symbole ein, zum Beispiel ! für |, @ für || und # für |||. Dieses Spiel könnten wir noch eine Weile weiterspielen, aber je länger wir weiterspielen, desto mehr Symbole müssen wir uns merken; darum hören wir lieber

wieder schnell auf, sagen wir, % steht für |||| und $*$ für |||||. Wie stellen wir dann aber die Strichliste |||||| dar?

Wir nehmen wieder das Symbol für |, also !, und schieben es eine Stelle weiter nach links; um dies erkenntlich zu machen, brauchen wir noch ein Symbol, wir nehmen □, das an der rechten Stelle als Platzhalter steht; also entspricht |||||| gerade !□. Nun können wir problemlos fünfmal weiterzählen

!!	entspricht	|||||||
!@	entspricht	||||||||
!#	entspricht	|||||||||
!%	entspricht	||||||||||
!$*$	entspricht	|||||||||||

Jetzt verändern wir das linke Symbol:

@□ entspricht |||| |||| ||

Den nächsten Sprung machen wir bei $**$. Hier zählen wir als nächstes !□□. Für die oben angegebene Strichliste erhalten wir z.B. #@%.

Interessiert uns die Anzahl von Drei- und Rechtecken zusammen, dann hängen wir einfach die beiden Strichlisten

||||||||||||||||| |||||||||||||

hintereinander und erhalten

||||||||||||||||||||||||||||||

Wir sagen dann, wir **addieren** die beiden Strichlisten miteinander, nennen die neu entstandene Strichliste die **Summe** und schreiben auch

|||||||||||||||| + ||||||||||||||

für diese neue Strichliste.

Dasselbe funktioniert auch in der komfortableren Blockschreibweise, indem wir einfach die Blöcke hintereinanderschreiben und uns um die losen Striche danach kümmern. Also stimmen die folgenden beiden Strichlisten überein:

Komplizierter wird die Addition, wenn wir die Symbole $\square$, !,@, #, %, $*$ benutzen. Wir schauen uns zuerst ein paar kleine Fälle an, indem wir Strichlisten addieren und das Ergebnis in die neue Schreibweise übersetzen:

$\vert + \vert$ wird zu $\vert\vert$	!+! wird zu @
$\vert + \vert\vert$ wird zu $\vert\vert\vert$	! + @ wird zu #
$\vert + \vert\vert\vert$ wird zu $\vert\vert\vert\vert$	! + # wird zu %
$\vdots$	$\vdots$

Das können wir in einer Tabelle zusammenfassen:

+	!	@	#	%	*
!	@	#	%	*	!□
@	#	%	*	!□	!!
#	%	*	!□	!!	!@
%	*	!□	!!	!@	!#
*	!□	!!	!@	!#	!%

Geht es darum, zwei Ausdrücke zu addieren, die aus mehr als einem Zeichen bestehen, dann schreiben wir diese untereinander, so dass die Zeichen rechtsbündig untereinander stehen, und ziehen darunter einen Strich, z. B.

$$\begin{array}{rrr} ! & @ & * \\ & \% & ! \\ \hline \end{array}$$

Nun addieren wir die beiden Symbole, die am weitesten rechts stehen; besteht das Ergebnis aus zwei Zeichen, dann nennen wir das Zeichen links den **Übertrag**. Das rechte Zeichen dieser Summe notieren wir unter dem Strich unter den beiden gerade addierten Zeichen, den Übertrag notieren wir, etwas kleiner, eine Stelle weiter links über dem Strich. Nun wiederholen wir eine Stelle weiter links das Prozedere, addieren aber nicht nur die beiden Zeichen, sondern auch noch den gegebenenfalls entstandenen Übertrag dazu. Wir addieren also zweimal, zuerst die beiden Zeichen, dann die Summe mit dem Übertrag. Dabei können zwei neue Überträge entstehen, die wir wiederum addieren. Die Summe der beiden Überträge besteht aber nur aus einem Zeichen und wird

der neue Übertrag, der eine Stelle weiter links notiert wird. Dann geht es wieder eine Stelle weiter nach links. Kommen wir nun soweit, dass einer der beiden Ausdrücke auch mit Übertrag abgearbeitet ist, dann werden einfach die Symbole des verbliebenen Ausdrucks übernommen, das heißt, es wird unter dem Strich notiert, was über dem Strich steht. Für das Beispiel oben erhalten wir das folgende Resultat:

$$\begin{array}{ccc} ! & @ & * \\ {\scriptstyle !} & \%_{!} & ! \\ \hline @ & ! & \square \end{array}$$

Vorsicht, nun haben wir zum ersten Mal ein Rechenschema, oder etwas eleganter formuliert, einen **Algorithmus** kennengelernt, von dem wir wissen, wie wir ihn benutzen, aber nicht, warum das Ergebnis das ist, was es auch sein soll. Wie solche Erklärungen gegeben werden können, ist zentrales Thema dieses Texts. Wir kommen später, wenn wir auf mehr theoretisches Wissen zurückgreifen können, auf diesen Algorithmus zurück.

Wir können einen Ausdruck mit sich selbst addieren, das Ergebnis nocheinmal mit dem Ausdruck und so weiter. Machen wir uns das ganze an unseren Strichlisten einmal deutlich, z. B.

$$||||||||$$

addiert mit sich selbst ist

$$||||||||||||||$$

oder übersichtlicher

$$\begin{array}{l} ||||||||| \\ ||||||||| \end{array}$$

Wenn wir nocheinmal $||||||||$ zu dem Ergebnis addieren, erhalten wir

$$\begin{array}{l} ||||||||| \\ ||||||||| \\ ||||||||| \end{array}$$

Diese Ergebnisse können wir auch folgendermaßen notieren: wir notieren unsere ursprüngliche Strichliste, und für jede Zeile machen wir einen Strich in einer weiteren Liste. Diese beiden Listen dürfen wir nicht einfach hintereinanderschreiben, denn es handelt sich ja nicht um die Summe, stattdessen trennen wir sie durch das Symbol $\times$, schreiben also

$$||||||||\times|,\ |||||||||\times||,\ ||||||||\times|||,\ldots$$

und sprechen von dem **Produkt** von $||||||||$ mit $|$ bzw. $||$ bzw. $|||$, und sagen, dass wir die entsprechenden Strichlisten **multiplizieren**.

Damit taucht sofort wieder die Frage auf, wie wir die Multiplikation mittels der Symbole $\square, !, @, \#, \%, *$ beschreiben

können. Für kleine Werte, z. B. für einstellige Ausdrücke, machen wir das wieder, indem wir Ergebnisse, die wir mit Hilfe von Strichlisten erhalten haben, in die komplexere Schreibweise übersetzen, also

$$
\begin{array}{cc}
| \times | \text{ wird zu } | & !\times! \text{ wird zu } ! \\
| \times || \text{ wird zu } || & ! \times @ \text{ wird zu } @ \\
\vdots & \vdots \\
|| \times ||| \text{ wird zu } |||||| & @ \times \# \text{ wird zu } !\square \\
\vdots & \vdots
\end{array}
$$

Das Ganze können wir wieder in einer Tabelle festhalten:

$\times$	!	@	#	%	$*$
!	!	@	#	%	$*$
@	@	%	!$\square$	!@	!%
#	#	!$\square$	!#	@$\square$	@#
%	%	!@	@$\square$	@%	#@
$*$	$*$	!%	@#	#@	%!

Haben wir zwei Ausdrücke, bei denen mindestens einer aus mehreren Symbolen besteht, dann schreiben wir die beiden Ausdrücke nebeneinander, getrennt durch $\times$, z. B.

$$!@* \times \%!$$

Jetzt ziehen wir einen Strich und multiplizieren das am weitesten rechts stehende Zeichen des linken Ausdrucks mit dem

entsprechenden des rechten Ausdrucks, in unserem Beispiel also $*$ mit !. Das Ergebnis wird, wie wir der Tabelle entnehmen können, wieder aus höchstens zwei Zeichen bestehen; wir notieren das rechte Zeichen unter dem rechten Zeichen des linken Ausdrucks und merken uns den Übertrag. Dann wiederholen wir die Rechnung mit dem rechten Zeichen des rechten Ausdrucks und dem zweiten Zeichen von rechts des linken Ausdrucks, addieren zu dem Ergebnis den Übertrag. Das Ergebnis besteht wieder aus höchstens zwei Zeichen. Das rechte notieren wir links neben dem eben notierten Zeichen, also unter dem zweiten Zeichen von rechts des linken Ausdrucks, das andere Zeichen wird unser neuer Übertrag. Dann geht es weiter mit dem rechten Zeichen des rechten Ausdrucks und dem dritten Zeichen von rechts, falls es das überhaupt noch gibt. Irgendwann haben wir das Zeichen ganz rechts mit jedem Zeichen des linken Ausdrucks multipliziert. Dann wählen wir im rechten Ausdruck das zweite Zeichen von rechts und führen analoge Rechnungen durch, notieren das Ergebnis unter dem ersten Ergebnis, aber eins weiter nach links verschoben. Zum Schluss haben wir soviele neue Ausdrücke wie der rechte Ausdruck Zeichen hat. Diese addieren wir, und das Ergebnis ist unser Produkt. Für das Beispiel oben haben wir

		!	@	$*$	$\times$	%	!
		!	@	$*$			
	$*_!$	$*$	@				
!	□	□	%	$*$			

Die Symbole $\square, !, @, \#, \%, *$ können wir durch andere Symbole ersetzen, solange wir eine eineindeutige Zuordnung zwischen den alten und den neuen Symbolen herstellen können, d. h. jedem neuen Symbol wird genau ein altes Symbol zugeordnet und jedes alte Symbol muss dann auch eine Zuordnung haben. Eine solche Zuordnung ist z. B.

$$0 \mapsto \square,\ 1 \mapsto !,\ 2 \mapsto @, 3 \mapsto \#, 4 \mapsto \%, 5 \mapsto *$$

Alles Gesagte geht dann genauso durch, wenn wir in allen Rechnungen einfach die Symbole nach der gegebenen Zuordnung ersetzen. Die Multiplikation oben hat nun zum Beispiel folgendes Aussehen:

$$\begin{array}{cccccccc} & & 1 & 2 & 5 & \times & 4 & 1 \\ \hline & & 1 & 2 & 5 & & & \\ & 5_1 & 5 & 2 & & & & \\ \hline 1 & 0 & 0 & 4 & 5 & & & \end{array}$$

Das sieht nun schon viel vertrauter aus. Wir sehen also, es kommt nicht darauf an, mit welchen Symbolen wir rechnen, sondern mit wievielen. Diese Anzahl an Symbolen nennen wir die **Basis** unserer Zahldarstellung. Haben wir mehr oder weniger Symbole, also eine andere Basis, dann müssen wir erneut überlegen, wie zwei einzelne Zeichen addiert bzw. multipliziert werden. Das bedeutet, wir müssen das kleine **Einspluseins** und **Einmaleins** für diese Basis bestimmen. Das Schema, wie wir mit komplexeren Ausdrücken rechnen, verliert aber nicht an Gültigkeit.

Da wir so gerne mit unseren Fingern rechnen, ist es naheliegend, so viele Symbole zu nehmen, wie wir Finger haben, und wir kommen zu unserer wohlbekannten Zahldarstellung durch die Symbole $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ und sprechen von einer Darstellung im **Dezimalsystem**. Computer haben keine Finger, dafür können sie zwischen "Signal" und "kein Signal" gut unterscheiden. Sie verwenden intern daher das **Binärsystem**, also ein Zahldarstellung mit zwei Symbolen wie z.B. $0, 1$. Das kleine Einmaleins und Einspluseins des Computers ist somit

$+$	0	1
0	0	1
1	1	10

$\times$	0	1
0	0	0
1	0	1

Von nun an benutzen wir zumeist stillschweigend das uns geläufige Dezimalsystem. Es sind einige Fragen offen geblieben, trotzdem schließen wir nun dieses erste Kapitel über das Zählen und das symbolische Rechnen.

Aufgaben

1. Betrachte das Einmaleins und Einspluseins für die Symbole $\square, !, @, \#, \%, *$. Was fällt dir alles auf?

2. Berechne $*@! \; + \; @@$ und $!@! \times !@!$.

3. Seien die Symbole a, b, c, d mit Zuordnung $a \mapsto \square, b \mapsto |, c \mapsto ||, d \mapsto |||$ gegeben. Gib das kleine Einmaleins und Einspulseins an.

4. Multiplikation haben wir als "wiederholte Addition" eingeführt. Wie sieht eine wiederholte Multiplikation aus?

2 Strukturieren

Halten wir nocheinmal fest, was wir im ersten Kapitel getan haben: Wir haben einer Ansammlung von unterschiedlichen Objekten eine Zeichenreihe zugeordnet, eine Strichliste oder eine Zeichenfolge, mit der einzigen Prämisse, dass Ansammlungen, die unserer Wahrnehmung nach gleichviele Gegenstände enthalten, durch denselben Ausdruck innerhalb einer Notation ausgedrückt werden. Dann haben wir arithmetische Operationen auf diesen Zeichenreihen eingeführt: Addition, die das Zusammenfassen zweier Ansammlungen modelliert und Multiplikation, die das wiederholte Ausführen von Addition darstellt. Was ist aber nun eine Zahl? Das Zeichen 3, der Ausdruck $|||$? Diese Frage wollen wir in diesem Kapitel beantworten.

Dazu wollen wir uns ein wenig von unserer Intuition lösen, die uns so sehr im ersten Kapitel zur Seite stand, und ein "künstliches Universum schaffen". Dieses künstliche Universum werden wir nicht explizit darstellen können. Wir können aber Prinzipien angeben, auf denen dieses Universum beruht. Die zu beobachtenden Objekte nennen wir **Mengen**, die einzige im voraus gegebene Interaktion zwischen den Objekten die **Elementbeziehung**: x ist ein **Element von** X oder x ist **in/aus** X, in Zeichen $x \in X$. Damit wir nicht über nichts reden, formulieren wir das

Prinzip 1. Eine Menge existiert.

Jetzt wissen wir, dass mindestens ein Objekt in unserem

Universum existiert. Wir werden gleich ein weiteres Prinzip angeben, das uns die Existenz von deutlich mehr Mengen sichern wird. Diese müssen wir vergleichen können. Also legen wir ein Prinzip fest, das sagt, wann zwei Mengen als gleich angesehen werden.

Prinzip 2. Zwei Mengen sind gleich, wenn sie dieselben Elemente haben.

Sind X und Y Mengen und jedes Element aus X auch ein Element von Y, dann sagen wir, dass X eine **Teilmenge** von Y ist, und wir schreiben $X \subseteq Y$. Existiert darüber hinaus ein Element y in Y, das nicht in X liegt, dann sagen wir, X ist eine **echte Teilmenge** und schreiben $X \subset Y$. Das folgende Prinzip gestattet uns, bestimmte Teilmengen zu bilden:

Prinzip 3. Ist P eine Eigenschaft, die ein Element der Menge Y haben oder nicht haben kann, dann können wir die Menge X aller Elemente aus Y angeben, die diese Eigenschaft erfüllen. Wir schreiben dann für X auch

$$\{x \in Y : x \text{ erfüllt } P\}.$$

Der Ausdruck "hat die Eigenschaft" ist ein bisschen schwammig, wir werden ihn im nächsten Kapitel präzisieren.

Die Eigenschaft P kann so gewählt werden, dass sie nie erfüllt werden kann. Ein Beispiel wäre, "P drückt aus, dass x in z liegt und dass gleichzeitig x nicht in z liegt." Die Menge $\{x \in Y : x \text{ erfüllt } P\}$ ist dann leer. Nach Prinzip

2 kann es nur eine solche Menge geben, wir nennen sie die **leere Menge** und schreiben $\emptyset$ für sie.

Sind zwei Mengen X und Y gegeben, dann können wir die Menge

$$\{x \in X : x \in Y\}$$

bilden. Diese Menge besteht aus allen Elementen, die in X *und* in Y liegen, und wir nennen sie den **Schnitt** von X und Y, in Zeichen $X \cap Y$. Genauso können wir auch drei oder vier Mengen schneiden, wir können aber noch etwas viel besseres machen: Ist U eine nichtleere Menge, dann bilden wir die Menge

$$\bigcap U = \{x \in X : X \in U \text{ und } x \in Y \text{ für alle } Y \in U\},$$

wir bilden also den Schnitt über alle Mengen, die in U enthalten sind. Eine weitere Menge, die wir aus zwei Mengen X und Y bilden können, ist das **Komplement** von X in Y bzw. Y **ohne** X

$$Y \setminus X = \{a \in Y : a \notin X\},$$

dabei ist $a \notin X$ als die Verneinung von $a \in X$ zu lesen. Mit dem Prinzip 3 konnten wir Schnitt und Komplement erklären. Dagegen müssen wir die Existenz einer Menge, die aus allen Elementen aus X und aus allen Elementen der Menge Y besteht, wieder postulieren.

Prinzip 4. Zu gegebenen Mengen X und Y existiert eine Menge Z, sodass a genau dann ein Element von Z ist, wenn a ein Element von X oder ein Element von Y ist.

Die Menge Z wird die **Vereinigungsmenge** von X und Y genannt, in Zeichen $X \cup Y$.

Das "oder" in der Mathematik ist übrigens immer einschließend zu verstehen. Es gilt "A oder B", wenn A gilt, wenn B gilt, wenn sowohl A als auch B gilt. Die Frage, "Möchtest Du Tee oder Kaffe?", kann somit in der Mathematik mit "Ja" beantwortet werden, und es gibt dann drei Möglichkeiten, diesen Wunsch zu erfüllen. Nachdem wir nun die Operationen $\cap, \cup, \setminus$ kennengelernt haben, ist es ein beliebtes Spiel, die Operationen auf verschiedene Weisen auf gegebene Mengen anzuwenden, und zu sehen, wann das Gleiche herauskommt. Ein Beispiel:

$$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$$

Das sehen wir folgendermaßen ein: Ist a ein Element der linken Menge, dann liegt a in X, aber nicht in $Y \cap Z$. Das bedeutet, a liegt nicht in Y oder a liegt nicht in Z. Also liegt a in $X \setminus Y$ oder in $X \setminus Z$ und damit in der Menge auf der rechten Seite. Liegt b in der Menge auf der rechten Seite, dann liegt b in $X \setminus Y$ oder in $X \setminus Z$. Auf jeden Fall liegt b in X, aber nicht in Y und Z. Deswegen muss b in der linken Menge liegen. Beachte, dass wir zuerst nachgewiesen haben, dass die Menge auf der linken Seite in der auf der rechten und dann, dass die rechte Menge in der linken enthalten ist. Das ist ein beliebtes Vorgehen beim Nachweis von Mengengleichheit.

Stellen wir uns nun die Situation vor, dass zwei Mengen X und Y gegeben sind, und wir Elemente aus X mit Elementen aus Y vergleichen wollen, z. B. das Element a aus X und b aus Y. Wie kann ausgedrückt werden, dass a und b im Vergleich stehen, wenn unser Universum als einzige Objekte Mengen zulässt? Indem wir eine Menge angeben, die genau das ausdrückt!

Diese Menge nennen wir das **Paar** mit **erster Komponente** a und **zweiter Komponenente** b und schreiben (a, b) dafür. Sie soll durch folgende Eigenschaft charakterisiert sein:

$$(a, b) = (x, y) \Leftrightarrow a = x \text{ und } b = y$$

Dabei bedeutet das Zeichen $\Leftrightarrow$, dass die Aussage links von dem Zeichen genau dann erfüllt ist, wenn die Aussage rechts davon erfüllt ist. Nun bilden wir für alle x aus X und alle y aus Y solche Paare und fassen alle zu der Menge $X \times Y$ zusammen. Dass wir das dürfen, erlaubt uns das

Prinzip 5. Zu zwei gegebenen Mengen X und Y können wir die Menge aller Paare $X \times Y$ bilden.

Diese Menge $X \times Y$ ist schon ein Vergleich, oder wie wir eleganter sagen, eine **Relation**, nämlich diejenige, die jedes Element aus X mit jedem Element aus Y in Relation setzt. Weil alle möglichen Elemente miteinander verglichen werden, sprechen wir auch von der **Allrelation**. Eine weitere Relation ist die sogenannte **Identität** auf X, die Menge der Paare (x, x) mit $x \in X$. Zwei Objekte stehen in Vergleich,

wenn sie gleich sind. Interessanter sind natürlich alle Relationen, die zwischen Identität und Allrelation liegen. Ist R eine Teilmenge von $X \times Y$, das heisst, jedes Element aus R ist auch Element von $X \times Y$, dann sagen wir, dass R eine **Relation** zwischen X und Y ist. Elemente aus R sind also Paare (x, y) mit x aus X und y aus Y. Wir schreiben aber lieber xRy anstelle von "(x, y) ist in R". Ist R eine Teilmenge von $X \times X$, dann sagen wir einfach, R ist eine **Relation auf** X. Die interessantesten sind die **Äquivalenzrelationen**, die die folgenden drei Eigenschaften haben:

Reflexivität	Für alle x aus X gilt xRx.
Symmetrie	Gilt xRy, dann auch yRx.
Transitivität	Gilt xRy und yRz, dann auch xRz.

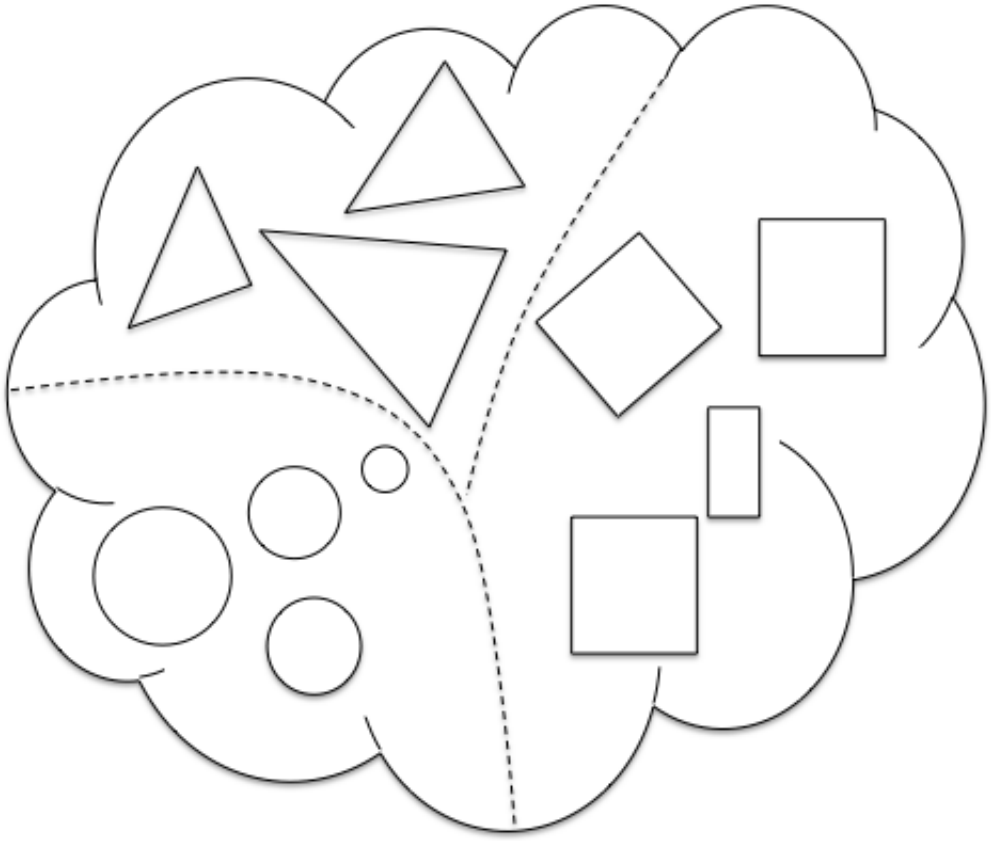
Zu jedem x aus X soll x/R aus allen Elementen y aus X mit xRy bestehen, also

$$x/R = \{y \in X : xRy\}$$

Wir nennen diese Menge die **Äquivalenzklasse** von x bzgl. R. Das Element x ist sicherlich selbst ein Element aus x/R wegen xRx. Gilt aber xRy, dann ist auch y ein Element von x/R.

Wenn wir im Alltagsleben mit Aussagen wie "x hat die gleiche Form wie y, x hat die gleiche Farbe wie y" beschreiben, dass Dinge ähnlich sind, dann erhalten wir Relationen, welche die eben beschriebenen Eigenschaften haben. Durch Äquivalenzrelationen führen wir also das Konzept

der Ähnlichkeit in unser Mengenuniversum ein und in Äquivalenzklassen werden ähnliche Elemente zusammengefasst. Wir werden in ein paar Seiten sehen, wie wir mit Hilfe von Äquivalenzrelationen neue Mengen erhalten, in denen die Mengen äquivalenter Elemente zu einem neuen Element zusammengefasst werden. Dafür benötigen wir aber erst einmal eine weitere Familie von Relationen.



Die Äquivalenzrelation "x und y haben dieselbe Form" führt zu den Äquivalenzklassen "Rechteck, Kreis, Dreieck".

Sei nun R eine Relation zwischen X und Y, also eine Teilmenge von $X \times Y$. Wir sagen, dass R **funktional** ist, falls aus xRy und xRz stets $y = z$ für alle y, z aus Y und alle $x \in X$ folgt. Eine **partielle Abbildung** f aus X in Y ist festgelegt durch die Angabe

- der Menge X,
- der Menge Y
- und einer funktionalen Relation $R \subseteq X \times Y$.

Wir schreiben dann $y = f(x)$, wenn xRy gilt. Gibt es zu $x \in X$ ein $y \in Y$ mit $x\,R\,y$, so sagt man, f ist für x **definiert** und die Menge aller dieser x ist der **Definitionsbereich** von f. Die Menge Y wird der **Wertebereich** bzw. die **Zielmenge** genannt. Die Menge

$$\{y \in Y : y = f(x) \text{ für ein } x \in X\}$$

nennen wir das **Bild** von X unter f.

Ist f auf ganz X definiert, so sagen wir, f sei eine **Abbildung** oder **Funktion** von X in Y. Wir schreiben dafür $f : X \to Y$ oder $X \xrightarrow{f} Y$ mit Abbildungsvorschrift $f(x) = y$ oder $x \mapsto y$.

Beispiel. Für jede Menge X existiert die **identische Abbildung** $id_X : X \to X$, gegeben durch $id_X(x) = x$. Die zu dieser Funktion gehörende funktionale Relation ist gerade die Identität auf X.

Seien $f_1 : X_1 \to Y_1$ und $f_2 : X_2 \to Y_2$ Funktionen mit Definitionsbereichen X_1 bzw. X_2. Ist das Bild $f_1(X_1)$ des Definitionbereichs von f_1 Teil des Definitionsbereichs X_2 von f_2, so liefert die Relation $R \subseteq X_1 \times Y_2$ mit

> xRz gilt genau dann, wenn ein $y \in Y_1$ mit $f_1(x) = y$ und $f_2(y) = z$ existiert.

eine Funktion $f_2 \circ f_1 : X_1 \to Y_2$ mit Definitionsbereich X_1, die **Komposition**, lies: f_2 nach f_1. Wir können schreiben

$$z = (f_2 \circ f_1)(x) = f_2(f_1(x)).$$

Mit "Funktion" ist der zweite wesentliche Begriff nach "Menge" gefallen. Wir stellen uns hier auf den Standpunkt, dass Funktionen bestimmte Mengen sind, wollen aber nicht verschweigen, dass wir unser Universum auch auf dem Funktionsbegriff hätten aufbauen können. Nun werden wir einige Eigenschaften von Funktionen kennenlernen. Diese Eigenschaften wollen wir charakterisieren und vergleichen. Die Resultate werden wir in der üblichen Form der Mathematik präsentieren, als Lemma, Satz oder Korollar, gefolgt von einem Beweis. Diese neuen Begriffe benötigen noch einer Erklärung. In der Mathematik werden Aussagen aus anderen Aussagen - den Axiomen - abgeleitet. Man nennt diesen Vorgang **beweisen**. Wenn eine gewisse Aussage A bewiesen worden ist, und man aus A die Aussage B ableiten kann, so gilt auch B als bewiesen.

Aussagen werden in der Regel mit Namen belegt, die ihren Stellenwert innerhalb der Theorie andeuten. Dafür stehen unter anderem die Wörter **Satz, Theorem, Lemma, Korollar** zur Verfügung.

Eine Aussage, die wir für eine wichtige Erkenntniss halten, nennen wir **Satz**. Besonders wichtige Sätze werden oft auch **Theorem** genannt.

Lemma entspricht der deutschen Bezeichnung **Hilfssatz**. Dabei handelt es sich entweder um eine "rein technische" Aussage, die im Beweis eines der folgenden Sätze verwendet wird, oder es handelt sich um eine besonders wichtige Schlüsselaussage, die in vielen Situationen nützlich sein wird.

Ein **Korollar** ist eine Folgerung aus einem schon bewiesenen Satz. Also eine für sich interessante Aussage, die sich leicht aus dem vorhergehenden Resultat folgern läßt.

Wir nummerieren unsere Sätze, Lemmata, das ist der Plural von Lemma, oder Korollare mit Zahlen der Form $m.n$, wobei m das Kapitel und n die Nummerierung innerhalb eines Kapitels angibt. Hier ist nun unser erster Satz:

Satz 2.1 *Die Komposition von Funktionen ist assoziativ, d.h., haben wir Funktionen*

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W,$$

dann gilt die Gleichung $h \circ (g \circ f) = (h \circ g) \circ f$.

Beweis. Da es sich um den Beweis unseres allerersten Satzes handelt, wollen wir hier sehr ausführlich sein. Überlegen wir uns zunächst nocheinmal, was der Satz oben besagt: Es sind Abbildungen $f : X \to Y, g : Y \to Z$ und $h : Z \to W$ gegeben. Weil der Wertebereich von f gerade der Definitionsbereich von g und der Wertebereich von g gerade der Definitionsbereich von h ist, können wir die Kompositionen $g \circ f$ und $h \circ g$ bilden. Diese beiden Kompositionen sind wieder Funktionen, erstere eine mit Definitionsbereich X und Wertebereich Z, zweitere eine mit Definitionsbereich Y und Wertebereich W. Deswegen können wir weiter komponieren, und zwar $h \circ (g \circ f)$ und $(h \circ g) \circ f$. Im Satz wird nun behauptet, dass diese beiden Funktionen gleich sind.

Darum müssen wir uns zuerst daran erinnern, wann zwei Funktionen gleich sind. Dies ist der Fall, wenn sie denselben Definitions- bzw. Wertebereich und dieselbe Abbildungsvorschrift haben. Beide Funktionen haben aber nach Definition den Definitionsbereich X und den Wertebereich W, also müssen wir nur noch überprüfen, ob sie dieselbe Abbildungsvorschrift haben: Sei x ein festes aber beliebiges Element aus X. Sei $y = f(x)$, $z = g(y)$ und $w = h(z)$. Dann ist

$$h \circ (g \circ f)(x) = h(z) = w = (h \circ g)(y) = (h \circ g) \circ f(x),$$

was zu beweisen war. □

Das Zeichen □ in der Ecke rechts unten des Beweises zeigt übrigens an, dass der Beweis beendet wurde. Eine Konvention, die sich bei vielen Autoren durchgesetzt hat und das aus der Schule bekannte *quod erat demonstrandum* ersetzt.

Eine Abbildung $f : X \to Y$ heißt **injektiv**, wenn für alle $x, y \in X$ aus $f(x) = f(y)$ die Gleichung $x = y$ folgt.

Lemma 2.2 *Sei X nicht die leere Menge. Eine Abbildung $f : X \to Y$ ist injektiv genau dann, wenn es eine Abbildung $g : Y \to X$ gibt mit $g \circ f = id_X$, d. h., für alle $x \in X$ gilt $g(f(x)) = x$.*

Beweis. Angenommen, so ein g existiert und $f(x) = f(y)$, dann ist

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

Ist f injektiv, definiere g folgendermaßen: Definitionsbereich ist das Bild $f(X)$, Zielmenge X und

$$g(y) = x \Leftrightarrow f(x) = y.$$

Jetzt müssen wir testen, ob die Abbildungsvorschrift von g tatsächlich eine funktionale Relation R (mit yRx falls $g(y) = x$) liefert: Gilt yRx und yRz, dann gilt nach Definition von g, $f(x) = f(z) = y$, und aus der Injektivität von f folgt $x = z$. □

Lemma 2.3 *Die Komposition injektiver Abbildungen ist injektiv.*

Beweis. Aus $g(f(x)) = g(f(z))$ folgt $f(x) = f(z)$ mit der Injektivität von g und $x = z$ mit der Injektivität von f. □

Eine Abbildung $f : X \to Y$ heißt **surjektiv** oder Abbildung von X **auf** Y, wenn $f(X) = Y$, d.h. wenn für alle $y \in Y$ ein $x \in X$ mit $f(x) = y$ existiert.

Lemma 2.4 *Die Abbildung $f : X \to Y$ ist surjektiv, falls es eine Abbildung $g : Y \to X$ gibt mit $f \circ g = id_Y$, d.h. für alle y aus Y gilt $f(g(y)) = y$.*

Beweis. Angenommen, so ein g existiert. Ist $b \in Y$, dann $g(b) \in X$ und $f(g(b)) = b$, was die Surjektivität von f beweist. Nehmen wir nun an, dass f surjektiv ist. Zu $y \in Y$ wähle ein x mit $f(x) = y$ und setze $g(y) = x$. Dann ist g eine Funktion und $f \circ g = id_Y$. □

Lemma 2.5 *Die Komposition surjektiver Abbildungen ist surjektiv.*

Beweis. Gegeben seien surjektive Abbildungen $f : X \to Y$ und $g : Y \to Z$ und $c \in Z$. Wegen der Surjektivität von g

gibt es $b \in Y$ mit $g(b) = c$. Wegen der Surjektivität von f gibt es dann $a \in X$ mit $f(a) = b$. Also $g(f(a)) = c$. □

Eine Abbildung $f : X \to Y$ heißt **bijektiv**, wenn sie injektiv und surjektiv ist. Mit Lemma 2.3 und 2.5 erhalten wir sofort

Lemma 2.6 *Die Komposition bijektiver Abbildungen ist bijektiv.*

Eine Abbildung $g : Y \to X$ heißt **Umkehrabbildung** zu der Abbildung $f : X \to Y$, wenn $g \circ f = id_X$ und $f \circ g = id_Y$ gilt.

Lemma 2.7 *Eine Abbildung $f : X \to Y$ ist bijektiv genau dann, wenn sie eine Umkehrabbildung besitzt. Diese ist dann auch bijektiv.*

Beweis. Hat man eine Umkehrabbildung gegeben, so folgt die Bijektivität sofort mit Lemma 2.2 und 2.4. Sei nun $f : X \to Y$ bijektiv und $g : Y \to X$ nach Lemma 2.2 konstruiert. Dann gilt auch $f \circ g = id_Y$. □

Nachdem wir nun soviele Worte über Äquivalenzrelationen und Funktionen verwendet haben, wollen wir auch sehen, wie diese beiden Konzepte in Verbindung gebracht werden können. Das passiert anhand eines weiteren Prinzips:

Prinzip 6. Zu jeder Menge X und jeder Äquivalenzrelation R auf X existiert eine Menge Y und eine surjektive Abbildung $\pi_R : X \to Y$ mit

$$\pi_R(x) = \pi_R(y) \Leftrightarrow xRy.$$

Diese Abbildung π_R nennen wir die **Abstraktion** von X bzgl. R.

"Abstraktion" kann hier ganz anschaulich verstanden werden. Assoziieren wir z. B. mit der Menge X alle Tiere in einem Zoo und mit R die Relation "gehört zu derselben Gattung", dann soll Y gerade aus allen Gattungen von Tieren, die in diesem Zoo leben, bestehen. Die Abstraktion ordnet jedem Tier seine Gattung zu, abstrahiert also nach diesem Begriff. Ein beliebiges Element einer Äquivalenzklasse kann als **Repräsentant** dieser Klasse dienen. Oft werden Funktionen oder Konstruktionen anhand eines Repräsentanten erklärt. Dann ist es wichtig, dass gezeigt wird, dass das Vorgehen tatsächlich unabhängig von der Wahl eines solchen Repräsentanten ist. Wir sprechen dann von der **Wohldefiniertheit** der Funktion bzw. Konstruktion. Nicht wohldefiniert ist zum Beispiel die folgende Abbildung: Jeder Tiergattung wird ein Gewicht zugeordnet, indem ein Repräsentant der Klasse gewogen wird.

Zwei Mengen X und Y werden **gleichmächtig** genannt, wenn es eine bijektive Abbildung $f : X \to Y$ gibt. Wir schreiben in diesem Fall $|X| = |Y|$.

Lemma 2.8 *Für beliebige Mengen X, Y, Z gilt*

$$\begin{aligned} |X| &= |X| \\ |X| = |Y| &\Rightarrow |Y| = |X| \\ |X| = |Y| = |Z| &\Rightarrow |X| = |Z| \end{aligned}$$

Der Pfeil $\Rightarrow$ drückt aus, dass die Aussage auf der rechten Seite aus der Aussage auf der linken Seite folgt.

Beweis. Es ist jeweils eine bijektive Abbildung anzugeben. Im ersten Fall ist dies die identische Abbildung id_X, im zweiten Fall f^{-1}, wobei $f : X \to Y$ eine Bijektion ist, und im dritten Fall ist es $h \circ g$ mit bijektiven Abbildungen $X \xrightarrow{g} Y \xrightarrow{h} Z$, mehr ist nicht zu tun. □

Wir haben also unser Universum so weit entwickelt, dass wir über Gleichzahligkeit sprechen können. Eine natürliche Zahl soll nun eine Menge sein, die so etwas repräsentiert; eine besonders schöne konstruieren wir nun:

Prinzip 7. Es gibt eine Menge M so, dass

- $\emptyset \in M$
- Für jede Menge X gilt: $X \in M \Rightarrow X \cup \{X\} \in M$

Eine Menge, die diese beiden Eigenschaften erfüllt, nennen wir **induktiv**. Um die Existenz einer besonderen induktiven Menge nachweisen zu können, benötigen wir ein weiteres Prinzip:

Prinzip 8. Zu einer Menge M können wir eine Menge $\mathcal{P}(M)$ bilden, die als Elemente gerade alle Teilmengen von M enthält. Diese Menge wird die **Potenzmenge** von M genannt.

Lemma 2.9 *Es gibt genau eine induktive Menge ω, die in jeder induktiven Menge enthalten ist.*

Beweis. Sei M eine induktive Menge und U die Menge aller Teilmengen von M, die wiederum induktiv sind. Wir erhalten U, indem wir die Teilmenge von $\mathcal{P}(M)$ aller Elemente mit der Eigenschaft "induktiv sein" bilden. Sei $\omega = \bigcap U$. Dann ist $\emptyset \in \omega$ und ist $X \in \omega$, dann ist X ein Element von jedem Element von U. Damit ist aber auch $\{X\}$ Element von jedem Element aus U, und letztendlich haben wir $X \cup \{X\} \in \omega$. □

Diese Menge ω soll nun die Menge der natürlichen Zahlen sein. Wir schauen uns ein paar ihrer Elemente an: die leere Menge $\emptyset$ ist nach dem ersten Punkt in ihr enthalten; nach dem zweiten Punkt die Menge $\{\emptyset\}$, die nichts enthält außer der leeren Menge, desweiteren haben wir die Menge $\{\emptyset, \{\emptyset\}\}$ usw. Ordnen wir diesen Mengen unsere Dezimalziffern zu, dann wird daraus

$$\begin{aligned} 0 &\mapsto \emptyset \\ 1 &\mapsto \{\emptyset\} = \{0\} \\ 2 &\mapsto \{\emptyset, \{\emptyset\}\} = \{0, 1\} \end{aligned}$$

Die natürliche Zahl n ist somit die Menge, die aus allen kleineren natürlichen Zahlen besteht, z. B.

$$8 = \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

Das ist auf den ersten Blick etwas verwirrend, aber ansonsten eine ganz brauchbare Definition.

Unendlichkeit haben wir bis jetzt nur mit Begriffen wie "und so weiter", "hört nicht auf" umschreiben oder mit drei Punkten wie in

$$|, ||, |||, ||||, |||||, \ldots$$

andeuten können. Die Menge ω der natürlichen Zahlen erlaubt es uns, den Begriff genauer zu fassen. Eine Menge X wird **endlich** genannt, wenn es eine bijektive Abbildung von X auf eine natürliche Zahl n gibt. Sind a, b, c zum Beispiel drei verschiedene Mengen, dann ist die Menge $\{a, b, c\}$ eine endliche Menge aufgrund der Zuordnung

$$a \mapsto 0, b \mapsto 1, c \mapsto 2.$$

Die Zahl n wird die **Anzahl** der Elemente von X bzw. deren **Mächtigkeit** genannt, in Zeichen $n = |X|$ (damit gilt auch

$n = |n|$). In dem Beispiel oben haben wir $|\{a, b, c\}| = 3$. Eine Menge ist **unendlich**, wenn sie nicht endlich ist.

Lemma 2.10 *Eine injektive oder surjektive Abbildung zwischen zwei endlichen gleichmächtigen Mengen ist bijektiv.*

Den Beweis verschieben wir in das vierte Kapitel.

Durch "x ist kleiner als y" wird eine binäre Relation beschrieben, die keine Äquivalenzrelation ist. Es scheitert an der Symmetrie: Wenn x kleiner als y ist, wird y nicht kleiner als x sein. Dafür ist die Transitivität weiterhin von Bestand:

> Ist x kleiner als y und y kleiner als z, dann ist x kleiner als z.

Desweiteren ist x nicht kleiner als x, diese Eigenschaft heißt **Irreflexivität**. Gilt außerdem

> Einer der drei Fälle tritt ein: x ist kleiner als y, y ist kleiner als x oder $x = y$,

dann sprechen wir von einer **linearen Ordnung**. Genauer, kommen die Elemente aus einer Menge X, dann ist eine **lineare Ordnung auf** X eine Relation auf X mit den oben genannten Eigenschaften. Meistens benutzen wir das Symbol $<$ für eine solche Relation. Gilt $a < b$ oder $a = b$, dann schreiben wir $a \leq b$ und sagen, dass a **kleiner gleich** b ist.

Natürliche Zahlen sind, wie wir oben gesehen haben, Mengen. Darum können wir eine Relation zwischen zwei natürlichen Zahlen einfach auf die folgende Weise definieren:

$$m <^{\mathbb{N}} n \Leftrightarrow m \subset n \Leftrightarrow m \in n$$

Damit erhalten wir eine lineare Ordnung auf den natürlichen Zahlen: Wegen $m \not\subset m$ und $m \subset n \subset p \Rightarrow m \subset p$ müssen wir nur noch testen, ob für je zwei solche Zahlen m, n einer der Fälle $m = n$, $m <^{\mathbb{N}} n$ oder $n <^{\mathbb{N}} m$ zutrifft. Dazu bilden wir die Menge $m \cap n$. Eine kurze Überlegung zeigt, dass $m \cap n$ auch wieder eine natürliche Zahl p ist, und dass $p \leq^{\mathbb{N}} m$ und $p \leq^{\mathbb{N}} n$ gilt. Dann ist aber entweder $p = m$ oder $p = n$. Denn wäre das nicht der Fall, dann gilt $p \subset m$, $p \subset n$, aber auch $p \in m$ und $p \in n$. Damit folgt $p + 1 = p \cup \{p\} \subseteq m$ und $p + 1 = p \cup \{p\} \subseteq n$, im Widerspruch zu $p = m \cap n$.

Eine Funktion $f : n \to X$ mit n einer natürlichen Zahl und X einer beliebigen Menge, nennen wir eine **Liste** vom Typ X. Für Listen führen wir eine spezielle Notation ein: Wir schreiben $[a_0, a_1, \ldots, a_{n-1}]$ für die Liste $f : n \to X$ mit $f(i) = a_i$ und sprechen von a_i als dem **i-ten Glied der Liste**. Im Fall $n = 0$ sprechen wir von der **leeren Liste**.

Die Menge aller Listen vom Typ X mit Definitionsbereich n bezeichnen wir mit X^n. Die Existenz dieser Menge muss wieder einmal postuliert werden:

Prinzip 9. Zu einer gegebenen Menge X und einer natürlichen Zahl n existiert die Menge X^n aller Listen vom Typ X mit Definitionsbereich n.

Eine Teilmenge von X^n wird eine **n-stellige Relation** genannt. In den Übungen werden wir sehen, dass wir X^2 mit $X \times X$ identifizieren können. Zweistellige Relationen auf X stimmen also mit dem, was wir vorher einfach Relation auf X genannt haben, überein. Eine Abbildung mit Definitionsbereich X^n und Zielmenge X wird eine **n-stellige** Operation auf X genannt.

Die Abbildungsvorschrift $x \mapsto x \cup \{x\}$ liefert eine Funktion von ω nach ω, die dem Addieren einer 1 entspricht, wir nennen sie die **Nachfolgerfunktion** und schreiben $\mathsf{succ}^{\mathbb{N}}$ (engl. successor=Nachfolger). Addition und Multiplikation sind nun Funktionen von $\omega \times \omega$ nach ω. Leider können wir nicht so elegant wie für den Nachfolger mittels der Mengenschreibweise die Abbildungsvorschrift angeben. Bei der Addition können wir uns noch retten, indem wir

$$n + m = \underbrace{\mathsf{succ}^{\mathbb{N}}(\mathsf{succ}^{N} \dots (\mathsf{succ}^{N}(m)) \dots)}_{n-mal}$$

schreiben. Bei der Multiplikation können wir uns bis jetzt höchstens auf das Rechenschema des ersten Kapitels berufen. Wie wir diese Funktionen doch noch elegant beschreiben können, sehen wir später. Jetzt steht uns nur noch eine Sache im Wege, um die natürlichen Zahlen als mathematische Struktur aufzufassen; es fehlt noch die Definition, was eine Struktur ist.

Eine **Struktur** A ist ein Objekt, das aus den folgenden vier Zutaten zusammengesetzt wird:

- Einer Menge, die die **Grundmenge** von A genannt wird, in Zeichen $\mathrm{dom}(A)$. Die Elemente von $\mathrm{dom}(A)$ werden die **Elemente** der Struktur genannt.
- Eine Liste von Elementen aus A, genannt die Konstanten von A.
- Für jede natürliche Zahl n eine Liste n-stelliger Relationen.
- Für jede natürliche Zahl n eine Liste n-stelliger Operationen.

All diese Mengen bzw. Listen können leer sein.

Die Struktur der **natürlichen Zahlen**

$$\mathbb{N} = (\omega, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, \mathsf{succ}^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}}, <^{\mathbb{N}})$$

besteht nun aus der kleinsten induktiven Menge

$$\mathrm{dom}(\mathbb{N}) = \omega = \{0, 1, 2, 3, \dots\}$$

zusammen mit der einstelligen Operation $\mathsf{succ}^{\mathbb{N}}$, den zweistelligen Operationen $+^{\mathbb{N}}$ und $\cdot^{\mathbb{N}}$, den Konstanten $0^{\mathbb{N}}$ und $1^{\mathbb{N}}$ und letztendlich der zweistelligen Relation $<^{\mathbb{N}}$. Wir haben an jedes Symbol eine kleines $\mathbb{N}$ angehängt; das hat System, wie wir im nächsten Kapitel sehen werden. Die Konstanten $0^{\mathbb{N}}$ und $1^{\mathbb{N}}$ sind natürlich nichts anderes als die Zahlen 0 und 1. Diese beiden Zahlen sind für uns aber so wichtig, dass sie mit in die Definition der Struktur genommen werden. Wir

haben die Menge der natürlichen Zahlen mit ω und diese Menge mit den eben beschriebenen Operationen und Relationen mit $\mathbb{N}$ bezeichnet. Viele meinen aber auch einfach die Menge der natürlichen Zahlen, wenn sie $\mathbb{N}$ schreiben; eine Konvention, der wir uns ab und zu anschließen werden.

Nachdem wir nun die natürlichen Zahlen als mathematische Struktur etabliert haben, können wir auch die Früchte der Arbeit ernten: Wir können neue Strukturen *konstruieren*, anstatt nur eine Beschreibung zu liefern. Das sechste Kapitel handelt von Konstruktionen, zwei elementare wollen wir nun vorstellen, die Konstruktion der ganzen und rationalen Zahlen. Ausdrücke der Form

$$x + 3 = 5 \quad x + 2 = 0 \quad 2x = 4 \quad 4x = 2 \quad x \cdot x = 2$$

nennen wir **Gleichungen**, Ausdrücke der Form

$$x + 3 < 5 \quad x + 5 < 3 \quad 2x < 4 \quad 4x < 2 \quad x \cdot x < 2$$

Ungleichungen. Das Symbol x spielt dabei die Rolle einer **Unbekannten**. Eine natürliche Zahl n erfüllt diese Gleichungen bzw. Ungleichungen, falls die Gleichung, in der x durch n ersetzt wird, eine wahre Aussage wird. Über Gleichungen, Ungleichungen und die Wahrheit von Aussagen reden wir im nächsten Kapitel ausführlicher, hier nur soviel: das Symbol n symbolisiert eine feste aber beliebige natürliche Zahl. Diese ist uns zwar auch unbekannt, sie hat aber

einen anderen Stellenwert als das bedeutungslose Zeichen x. Insbesondere stehen nach einer Ersetzung links und rechts vom Gleichheitszeichen Mengen und das Gleichheitszeichen kann als Mengengleichheit interpretiert werden. Zum Beispiel gilt

$$2 + 3 = 5,$$

also ist 2 eine Lösung der Gleichung $x + 3 = 5$. Eine interessante Frage ist, für welche Gleichungen bzw. Ungleichungen sich eine Lösung findet. Betrachten wir die Gleichung $x + 2 = 0$. Es gilt $0 \subset 2 \subseteq x + 2$. Damit ist diese Gleichung in den natürlichen Zahlen unlösbar. Andererseits können wir die noch nicht existente Lösung sehr präzise beschreiben: Addieren wir 2 dazu, dann erhalten wir 0. Damit kommen wir zu den negativen Zahlen: diese kennzeichnen wir mit einem Minuszeichen und schreiben -2 für die postulierte Lösung der Gleichung $x+2 = 0$ oder allgemeiner $-n$ für die Lösung der Gleichung $x + n = 0$. Somit erhalten wir die ganzen Zahlen

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Das ist sehr intuitiv, lässt sich aber nur über einen Umweg in unserem Mengenuniversum codieren. Hier ist dieser Umweg:

Sei X die Menge $\mathbb{N} \times \mathbb{N}$, $\sim$ die Äquivalenzrelation

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = n + m'$$

und $\mathbb{Z}$ sei $\mathbb{N}\times\mathbb{N}/\sim$. Gilt $m \leq n$, dann sagen wir, dass (m, n) eine **positive Zahl** repräsentiert. Wir können eine injektive Abbildung $f : \mathbb{N} \to \mathbb{Z}$ durch $f(n) = (0, n)$ angeben. Die Zahl 3 wird also von dem Paar $(0, 3)$ repräsentiert, und es gilt

$$(0, 3) \sim (1, 4) \sim (2, 5) \sim \ldots$$

Gilt $m > n$, dann sagen wir, dass (m, n) eine **negative Zahl** repräsentiert, und wir schreiben $-n$ für die durch $(n, 0)$ repräsentierte Äquivalenzklasse.

Nun können wir uns leicht überlegen, dass jede ganze Zahl eine Darstellung der Form n oder $-n$ mit einer natürlichen Zahl n hat. Intuition und Konstruktion laufen also auf dasselbe hinaus. Jetzt wollen wir Addition und Multiplikation so auf $\mathbb{Z}$ definieren, dass für positive Zahlen dasselbe wie für natürliche Zahlen gilt und weiterhin folgende Regeln gelten:

$$\begin{aligned} -1 \cdot n &= -n \\ n + (-n) &= 0 \\ (-n) + (-m) &= -(n + m) \end{aligned}$$

Fordern wir noch, dass $\sim$ eine **Kongruenzrelation** bzgl. der Addition ist, das heißt, dass aus $(m, n) \sim (m', n')$ und $(r, s) \sim (r', s')$ die Relation

$$(m + r, n + s) \sim (m' + r', n' + s')$$

folgt, dann ist die Addition dadurch schon eindeutig festgelegt, und wir schließen

$$(m, n) + (m', n') \sim (m + m', n + n')$$

Für die Multiplikation fordern wir:

$$\begin{array}{rcl} (0, m) \cdot (0, n) & \sim & (0, mn) \\ (m, 0) \cdot (n, 0) & \sim & (0, mn) \\ (m, 0) \cdot (0, n) & \sim & (mn, 0) \\ (0, m) \cdot (n, 0) & \sim & (mn, 0) \end{array}$$

Jede ganze Zahl hat einen Repräsentanten der Form $(m, 0)$ oder $(0, m)$, auf den diese Rechenregeln angewandt werden können. Damit ist auch die Multiplikation festgelegt. Nach dieser Konstruktion der ganzen Zahlen ist die Konstruktion der rationalen Zahlen unproblematisch. Ausgangspunkt ist die Unlösbarkeit einer Gleichung der Form $4x = 2$ in den ganzen Zahlen. Hier setzen wir $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}/\sim$ mit

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Wir schreiben intuitiver $\frac{a}{b}$ anstelle von $(a, b)/\sim$ und können nun Addition und Multiplikation folgendermaßen definieren:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Aufgaben

1. Welche der folgenden Mengen sind gleich?

   $$\{1,2\}, \{\{1\},\{2\}\}, \{\{1,2\}\}, \{1,2,2\}, \{\{2\},\{1\}\},$$
   $$\{1,2,2\} \setminus \{2\}, \{2,1\}$$

   Was ist der Unterschied zwischen $\{1,2,3\}$ und $[1,2,3]$? Sind $[1,2]$, $[1,2,2]$ und $[2,2,1]$ gleich? Sind $[\{1,2\},2]$ und $[\{2,1\},2]$ gleich? Wann sind zwei Listen $[a_1,\ldots,a_n]$ und $[b_1,\ldots,b_m]$ gleich?

2. Seien X, A, B Mengen. Zeige die folgenden Gleichungen zwischen Mengen.

   (a) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$

   (b) Es sei $A \subseteq X$. Dann gilt $X \setminus (X \setminus A) = A$.

3. Angenommen, wir können alle Menschen dieses Globus als Menge M in unser Universum einbauen. Welche Relationen sind dann Äquivalenzrelationen auf M?

   - x ist Bruder von y,
   - x und y haben dieselben Vorfahren,
   - x liebt y.

4. Zeige: Ist $f : Y \to Z$ injektiv und sind $g : X \to Y$ und $h : X \to Y$ Abbildungen so, dass $f \circ g = f \circ h$, so folgt $g = h$. Findest du eine analoge Aussage für surjektive Abbildungen?

5. Gib eine bijektive Abbildung von $X \times X$ nach X^2 an.

3 Formalisieren

Wir wollen uns davon lösen, dass die unseren Überlegungen zugrundeliegenden Prinzipien in natürlicher Sprache formuliert werden und führen sogenannte **formale Sprachen** ein, die a priori aus bedeutungslosen Zeichenreihen bestehen und erst durch Interpretation in einer mathematischen Struktur Bedeutung erlangen. Zunächst brauchen wir ein **Alphabet**, dies sei einfach eine Liste von Symbolen, die wir durch Aufzählen erhalten. Beispiele sind

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

$$[A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z]$$

$$[0, 1]$$

$$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]$$

$$[\square, !, @, \#, \&, *]$$

$$[|]$$

$$[\exists, \forall, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, x_{,0}, \mathsf{plus}, \mathsf{mal}, 0, 1, <, \mathsf{succ}]$$

Ein **Wort** eines bestimmten Alphabets sei einfach eine Liste von Zeichen dieses Alphabets. Damit werden z.B.

$$[h, a, l, l, o], [H, I, K, S], [1, 1, 0], [9, 9], [!, @, *], [|, |, |], [\mathsf{plus}, 0, 1]$$

Wörter des entsprechenden Alphabets. Die in dem Wort vorkommenden Zeichen nennen wir **Buchstaben**; das hat zur Folge, dass das Wort $[1, 1, 0]$ aus den Buchstaben 0 und 1 besteht, obwohl wir lieber von Ziffern sprechen würden.

Hier wollen wir aber gleich die Konvention einführen, Klammern und Kommas einer Liste wegzulassen, und schreiben stattdessen

$$hallo, HIKS, 110, 99, !@*, |||, \mathsf{plus}\ 0\ 1.$$

Eine **Sprache** in einem bestimmten Alphabet ist nun einfach eine Liste von Worten. Die leere Liste nennen wir in diesem Zusammenhang das **leere Wort** und schreiben dafür $\square$. Das leere Wort ist somit das einzige Wort, das mittels jeden Alphabets darstellbar ist. Eine **Grammatik** einer Sprache besteht aus folgenden Teilen:

- der Angabe eines Alphabets,
- der Angabe eines **Terminalalphabets**, dies ist eine Teilliste des Alphabets,
- der Angabe des **Startzeichens**, dies ist ein Zeichen des Alphabets, aber nicht eines des Terminalalphabets.
- der Angabe der **Regeln**, diese haben die Form

  $$v \to w,$$

  wobei v, w Wörter sind, v niemals das leere Wort und nicht aus Terminalzeichen bestehend.

Die aus der Grammatik **abgeleitete Sprache** besteht nun aus den Wörtern, deren Buchstaben Zeichen des Terminalalphabets sind, die aus dem Startzeichen abgeleitet werden können. Dabei nennen wir w eine **direkte Ableitung** von v, wenn eine Regel $v \to w$ existiert, und eine Ableitung, falls man durch endlich viele Regelanwendungen von v zu w kommt.

Wir schauen uns ein paar Beispiele an. Unsere Strichlisten des ersten Abschnitts haben folgende Grammatik: Alphabet $[S, |]$, dabei ist S das Startzeichen, und das Terminalalphabet besteht nur aus dem Strich $|$; es gibt zwei Regeln

$$\begin{aligned} S &\to \square \\ S &\to |S \end{aligned}$$

Wie erhalten wir z. B. die Strichliste $||||$? Durch folgende Regelanwendungen:

$$S \to |S \to ||S \to |||S \to ||||S \to ||||\square$$

Letzteres Wort ist $||||$.

Das war das letzte Mal, dass wir uns auf Strichlisten beziehen und machen jetzt etwas, was leider oft in der Mathematik passiert. Wir benutzen den Strich in einem anderen Zusammenhang. Haben wir zwei Regeln der Form $p \to q$ und $p \to r$, fassen wir das Ganze gerne zu $p \to q|r$ zusammen; das spart ein wenig Platz bei der Angabe einer größeren Grammatik.

Nun nehmen wir das Alphabet

$$[S, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z]$$

S ist wieder unser Startzeichen, der Rest das Terminalalphabet. Wir haben die folgenden Regeln:

$$S \to \square | aSa | bSb | \ldots | zSz$$

Die abgeleitete Sprache besteht genau aus den (kleingeschriebenen) **Palindromen**, also aus den Worten, die vorwärts wie rückwärts gelesen dasselbe ergeben, zum Beispiel ist $xyyx$ ein Wort dieser Sprache. Wir können auch bedingt natürliche Sprachen in dieses Schema pressen. Eine Grammatik der deutschen Sprache könnte folgende einfache Gestalt haben:

$$S \to \text{Aachen} | \ldots | \text{zytotoxisch},$$

also aus einer Auflistung aller Wörter eines Wörterbuchs bestehen. Diese Grammatik erlaubt es, "Fahrrad" und "laufen" als Worte der deutschen Sprache zu erkennen, "boat" und "xxxy" abzulehnen. Sie macht aber keine Angaben darüber, wie ein Satz gebildet wird. Wir können natürlich die Grammatik verfeinern: Zum Beispiel durch die Regeln

$$\begin{aligned} S &\to \text{NP VP} \\ \text{NP} &\to \mathit{Aachen} | \ldots | \mathit{Zytostoma} \end{aligned}$$

$$\text{VP} \rightarrow \mathit{abarbeiten}|\ldots|\mathit{zwitschern}$$

Damit erhalten wir Sätze der Fom "Peter lachen", "Haus umfallen". Diese Grammatik kann natürlich weiter und weiter verfeinert werden. Wir können zum Beispiel unterscheiden, ob ein Prädikat transitiv oder intransitiv ist, und je nachdem ein direktes Objekt anhängen. Wir können auch Adverbien, Adjektive, Artikel und Konjugationen der Verben einbauen, aber eine wirklich perfekte Grammatik wird es wohl nie werden. Dagegen lassen sich künstliche Logiksprachen präzise mittels solcher Grammatiken angeben. Hier kommt die Sprache, für die wir den ganzen Aufwand betrieben haben: Sie hat das Alphabet

$$[\exists, \forall, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, x, \ {}_0, \mathsf{plus}, \mathsf{mal}, -, 0, 1, <, \mathsf{succ}, T, A, F, S, V]$$

mit folgender Grammatik: Alle Zeichen bis auf T, A, F, S, V gehören zum Terminalalphabet, S ist das Startzeichen, und wir haben die folgenden Regeln:

$$\begin{aligned}
S &\rightarrow F \\
F &\rightarrow \neg F|\wedge\ F\ F|\vee\ F\ F|\rightarrow\ F\ F|\leftrightarrow\ F\ F \\
F &\rightarrow \exists x V F \\
F &\rightarrow \forall x V F \\
F &\rightarrow = TT|<TT \\
T &\rightarrow \mathsf{plus}\ T\ T|\mathsf{mal}\ T\ T \\
T &\rightarrow -T \\
T &\rightarrow \mathsf{succ}\ T \\
T &\rightarrow 0|1|xV \\
V &\rightarrow \square|_0|_0 V
\end{aligned}$$

Diese Grammatik ist deutlich komplexer als die Grammatiken, die wir bisher betrachtet haben, und wir brauchen ein wenig Zeit und Mühe, um die erzeugte Sprache zu verstehen. Wir arbeiten uns dabei von unten nach oben durch. Als erstes wollen wir verstehen, welche Worte von T abgeleitet werden können: T kann zu 0 oder zu 1 abgeleitet werden; T kann aber auch zuerst zu xV, dann zu x, x_0 oder x_0V abgeleitet werden; x_0V wiederum zu x_0, x_{00} oder $x_{00}V$ usw.

Wir haben nun also schon ein paar Worte kennengelernt und bevor wir fortfahren wollen, geben wir bestimmten Teilen der Sprache Namen und führen Abkürzungen ein, um nicht die Übersicht zu verlieren. Die Worte 0 und 1 nennen wir **Konstanten**, die Worte

$$x, x_0, x_{00}, x_{000}, \ldots$$

die **Variablen** der Sprache. Diese Namen sind natürlich schon im Vorgriff auf eine Interpretation in einer mathematischen Struktur gewählt: 0 und 1 werden feste Element einer Struktur werden, Variablen stehen auch für Elemente der Struktur, aber es ist noch nicht festgelegt für welche; wir schreiben von nun an anstatt

$$\underbrace{x_{0\ldots0}}_{n-mal}$$

einfach x_n. Außerdem benutzen wir auch gerne die Buchstaben y, z, u, v, w als Variablen. Damit schreiben wir zwar Wörter hin, die nicht zu der erzeugten Sprache gehören, aber

sie machen das Lesen von Ausdrücken deutlich einfacher, und es ist offensichtlich, wie die Ausdücke in formal korrekte Ausdrücke umgewandelt werden können. Nun weiter in dem Aufbau der Sprache:

T kann zu $\mathsf{plus}\ T\ T$, $\mathsf{mal}\ T\ T$, $-T$ oder $\mathsf{succ}\ T$ abgeleitet werden. Damit erhalten wir z. B.

$$\mathsf{plus}\ x_0x_1, \mathsf{mal}\ x_0\ \mathsf{succ}\ x_1, -\mathsf{plus}\ x_1\mathsf{mal}\ x_0x_2$$

Auch hier führen wir wieder Abkürzungen und bestimmte Konventionen ein. Schreiben wir $\mathsf{plus}\ x_0x_1$, dann benutzen wir diese Operation in sogenannter **Präfixnotation**, d. h., zuerst kommt der Name der Operation, gefolgt von einer Liste der Operanden. Lesbarer ist für eine zweistellige Operation die sogenannte **Infixnotation**, bei der der erste Operand vor dem Operationsnamen steht und der zweite dahinter, also $x_0\ \mathsf{plus}\ x_1$ anstelle von $\mathsf{plus}\ x_0x_1$. Für diese neue Notation benutzen wir auch ein neues aber altbekanntes Zeichen, wir schreiben $x_0 + x_1$ anstelle von $x_0\ \mathsf{plus}\ x_1$ und ebenso $x_0\ \cdot\ x_1$ anstelle von $\mathsf{mal}\ x_0\ x_1$. Diese einfache Schreibweise hat aber einen deutlichen Nachteil: Es ist nicht von vornherein klar, was der Ausdruck $x_0 + x_1 \cdot x_2$ bedeuten soll, $\mathsf{plus}\ x_0\ \mathsf{mal}\ x_1x_2$ oder $\mathsf{mal}\ \mathsf{plus}\ x_0x_1\ x_2$? Dieses Problem lösen wir, indem wir Klammern einführen: Bei der ersten Interpretation schreiben wir $x_0+(x_1\cdot x_2)$, bei der zweiten $(x_0 + x_1) \cdot x_2$. Mit diesen neuen Konventionen können wir die Termbildung auch folgendermaßen beschreiben:

- Die Konstanten $0, 1$ sind Terme.
- Jede Variable x_n, $n \in \mathbb{N}$, ist ein Term.
- Sind t_1, t_2 Terme, dann auch $-t_1, t_1 + t_2$, $t_1 \cdot t_2$, $\mathsf{succ}(t_1)$ und (t_1).
- Nichts anderes ist ein Term.

Terme bezeichnen wir mit kleinen lateinischen Buchstaben. Die Variablen, die in einem Term vorkommen, nennen wir die **Variablen des Terms**. Ist t ein Term und $[x_1, \ldots, x_n]$ eine Liste von Variablen, in der alle Variablen von t vorkommen, schreiben wir auch gerne $t(x_1, \ldots, x_n)$ für diesen Term, oder noch knapper $t(\bar{x})$ im Vertrauen, dass n bekannt oder unwichtig ist.

Sind t_1, t_2 Terme, dann können wir nach einer weiteren Regelanwendung die Formeln $t_1 = t_2$ bzw. $t_1 < t_2$ (gleich in Infixnotation) bilden, diese Formeln wollen wir **atomar** nennen. Die **Variablen** der atomaren Formel $s = t$ seien die Variablen aus s zusammen mit denen aus t, wobei eine Variable, die sowohl in s als auch in t vorkommt, nicht doppelt gezählt wird. Bevor wir den Aufbau unserer formalen Sprache fortführen wollen, geben wir an, wie eine atomare Formel in den natürlichen Zahlen interpretiert werden kann:

Sei $t(\bar{x})$ ein Term und $\bar{a}$ eine Liste von natürlichen Zahlen. Wir nehmen an, dass $\bar{a}$ genauso lang wie $\bar{x}$ ist. Wir definieren das Element $t^{\mathbb{N}}[\bar{a}]$ aus $\mathbb{N}$, das die **Auswertung** von t durch $\bar{a}$ genannt wird, folgendermaßen:

- Ist t die Variable x_i, dann ist $t^{\mathbb{N}}[\bar{a}]$ gerade a_i.
- Ist t die Konstante 0, dann ist $t^{\mathbb{N}}[\bar{a}]$ das Element $0^{\mathbb{N}}$.
- Ist t die Konstante 1, dann ist $t^{\mathbb{N}}[\bar{a}]$ das Element $1^{\mathbb{N}}$.
- Ist t von der Form $s_1 + t_1$, wobei $s_1(\bar{x}), s_2(\bar{x})$ Terme sind, dann ist $(s_1 + t_1)^{\mathbb{N}}[\bar{a}] = s_1^{\mathbb{N}}[\bar{a}] +^{\mathbb{N}} t_1^{\mathbb{N}}[\bar{a}]$.
- Ist t von der Form $s_1 \cdot t_1$, wobei $s_1(\bar{x}), s_2(\bar{x})$ Terme sind, dann ist $(s_1 \cdot t_1)^{\mathbb{N}}[\bar{a}] = s_1^{\mathbb{N}}[\bar{a}] \cdot^{\mathbb{N}} t_1^{\mathbb{N}}[\bar{a}]$.
- Ist t von der Form $-s_1$, wobei $s_1(\bar{x})$ ein Term ist, dann ist $-s_1^{\mathbb{N}}[\bar{a}] = -(s_1^{\mathbb{N}}[\bar{a}])$.
- Ist t von der Form $\mathsf{succ}(s_1)$, wobei $s_1(\bar{x})$ ein Term ist, dann ist $(\mathsf{succ}(s_1[\bar{a}]))^{\mathbb{N}} = \mathsf{succ}^{\mathbb{N}}(s_1^{\mathbb{N}}[\bar{a}])$.

Wir sagen, die Aussage $(t_1 = t_2)[\bar{a}]$ ist **wahr** in den natürlichen Zahlen, falls $t_1^{\mathbb{N}}[\bar{a}] = t_2^{\mathbb{N}}[\bar{a}]$ gilt. Ebenso ist die Aussage $(t_1 < t_2)^{\mathbb{N}}[\bar{a}]$ wahr, falls $t_1^{\mathbb{N}}[\bar{a}] <^{\mathbb{N}} t_2^{\mathbb{N}}[\bar{a}]$. In dieser Situation scheiben wir auch

$$\mathbb{N} \models (t_1 = t_2)^{\mathbb{N}}[\bar{a}] \text{ bzw. } \mathbb{N} \models (t_1 < t_2)^{\mathbb{N}}[\bar{a}]$$

Ansonsten sind die Aussagen **falsch**,

$$\mathbb{N} \not\models (t_1 = t_2)^{\mathbb{N}}[\bar{a}] \text{ bzw. } \mathbb{N} \not\models (t_1 < t_2)^{\mathbb{N}}[\bar{a}].$$

Beispiele. Es gilt $\mathbb{N} \models 1 + 1 = \mathsf{succ}(1)$ (1+1=2), aber für alle $m, n \in \mathbb{N}$ mit $m, n \neq 0$, $\mathbb{N} \not\models m \cdot n < 1$.

Schließlich ist eine **Formel** entweder eine atomare Formel oder von der Gestalt

$$\phi \wedge \psi, \phi \vee \psi, \phi \to \psi, \phi \leftrightarrow \psi, \neg\phi, \exists x_n(\phi), \forall x_n(\phi), (\phi)$$

wobei ϕ und ψ schon vorher gebildete Formeln sind. Da wir wieder der Infixnotation den Vorzug gegeben haben, kommen wir nicht ohne Klammern aus. Wir geben aber einige Regeln an, die es uns erlauben, auf einige Klammern zu verzichten.

- $\phi_1 \wedge \phi_2 \wedge \phi_3$ ist eine Abkürzung für $\phi_1 \wedge (\phi_2 \wedge \phi_3)$
- Dieselbe Regel für $\vee, \to, \leftrightarrow$ statt $\wedge$.
- $\exists x_n.\phi$, $\forall x_n.\phi$ anstelle von $\exists x_n(\phi)$, $\forall x_n(\phi)$
- Wir bewerten $\wedge, \vee, \to, \leftrightarrow$ und $\neg$ mit einer sogenannten **Bindungsstärke**. Das bedeutet, dass Klammern dort gemacht werden, wo die Bindung stärker ist. Die Bewertung sieht folgendermaßen aus: $\wedge$ ist stärker als $\vee$, $\vee$ ist stärker als $\to$ und $\to$ stärker als $\leftrightarrow$. Das Symbol $\neg$ ist stärker als alle eben genannten Symbole. Somit ist

  $$\phi \to \psi \wedge \theta \vee \neg\phi$$

  eine Abkürzung für

  $$\phi \to ((\psi \wedge \theta) \vee (\neg\phi))$$

Schließlich ist noch wichtig, was die **freien Variablen** einer Formel sind: ist ϕ atomar, dann sind die freien Variablen von ϕ einfach die Variablen von ϕ, ist ϕ die Formel $\psi_1 \wedge \psi_2$, $\psi_1 \vee \psi_2$, $\psi_1 \rightarrow \psi_2$ oder $\psi_1 \leftrightarrow \psi_2$, dann sind die **freien Variablen** von ϕ gerade die frei in ψ_1 vorkommenden Variablen zusammen mit denen, die frei in ψ_2 vorkommen, wobei wieder Variablen, die sowohl in ψ_1 als auch in ψ_2 vorkommen, nicht doppelt gezählt werden. Die freien Variablen von $\exists x.\phi$ bzw. $\forall x.\phi$, sind die Variablen, die frei in ϕ vorkommen, aber x wird aus dieser Menge herausgenommen. Wir schreiben wieder $\phi(x_1, \ldots, x_n)$, um anzudeuten, dass die freien Variablen von ϕ in der Liste $[x_1, \ldots, x_n]$ auftauchen.

Die Interpretation einer Formel läuft nun nach folgendem Muster ab:

- Ist ϕ atomar, dann gilt '$\mathbb{N} \models \phi[\bar{a}]$' wie oben definiert,
- $\mathbb{N} \models \neg\phi[\bar{a}]$ genau dann, wenn $\mathbb{N} \models \phi[\bar{a}]$ nicht gilt,
- $\mathbb{N} \models \phi \wedge \psi[\bar{a}]$, wenn sowohl $\mathbb{N} \models \phi[\bar{a}]$ als auch $\mathbb{N} \models \psi[\bar{a}]$ gilt,
- $\mathbb{N} \models \phi \vee \psi[\bar{a}]$, wenn zumindest eine der beiden Aussagen $\mathbb{N} \models \phi[\bar{a}]$ bzw. $\mathbb{N} \models \psi[\bar{a}]$ eintrifft,
- Ist ϕ die Formel $\forall y \psi(y, \bar{x})$, dann gilt $\mathbb{N} \models \phi[\bar{a}]$ genau dann, wenn für alle Elemente b aus $\mathbb{N}$, $\mathbb{N} \models \psi[b, \bar{a}]$,
- Angenommen, ϕ ist $\exists y \psi(y, \bar{x})$. Dann gilt $\mathbb{N} \models \phi[\bar{a}]$ genau dann, wenn wir mindestens ein Element b aus $\mathbb{N}$ finden, so dass $\mathbb{N} \models \psi[b, \bar{a}]$.

Eine Formel, in der keine freie Variable vorkommt, wird **Satz** oder **Aussage** genannt. Aussagen sind damit unabhängig von einer Variablenbelegung und gelten damit in einer Struktur oder nicht. Ein wesentlicher Punkt ist immer, zu einer vorgegebenen Struktur charakteristische Aussagen zu finden, die in dieser Struktur gelten. Hier ist zum Beispiel eine Liste von Aussagen, **Robinson-Arithmetik** genannt, die in den natürlichen Zahlen gelten und dort eine wesentliche Rolle spielen:

R1 $\forall x.\mathsf{succ}(x) \neq 0$
R2 $\forall x \forall y.\mathsf{succ}(x) = \mathsf{succ}(y) \Rightarrow x = y$
R3 $\forall x.x + 0 = x$
R4 $\forall x \forall y.x + \mathsf{succ}(y) = \mathsf{succ}(x + y)$
R5 $\forall x.x \cdot 0 = 0$
R6 $\forall x \forall y.x \cdot \mathsf{succ}(y) = x \cdot y + x$
R7 $\forall x.\neg(x < 0)$
R8 $\forall x.\forall y.x < \mathsf{succ}(y) \leftrightarrow x < y \vee x = y$
R9 $\forall x.\forall y.x < y \vee x = y \vee y < x$

Beachte, dass zum Beispiel die Formel R9 formal eigentlich folgende Gestalt hätte:

$$\forall x \forall x_0 \vee < x x_0 \vee = x x_0 > x x_0$$

Unsere Konventionen sind wirklich eine große Hilfe beim Lesen einer Formel.

Wenn wir Strukturen mit anderen Operationen als die der Arithmetik beschreiben wollen, müssen wir nicht jedes Mal mit viel Aufwand eine neue formale Sprache konstruieren.

Alles Wichtige haben wir schon gesehen. Eine andere Struktur hat ggf. andere Operationen, andere Relationen und andere Konstanten. Wesentlich zum Aufbau ist die Angabe von Operationssymbolen, Relationssymbolen und Konstantensymbolen, außerdem zu jedem Operations- und Relationssymbol eine natürliche Zahl n, die die Stelligkeit angibt. Diese Informationen werden in der **Signatur** zusammengestellt. Die Signatur der natürlichen Zahlen, so wie wir sie in diesem Kapitel besprochen haben, besteht damit zum Beispiel aus den beiden zweistelligen Operationen $+$ und $\cdot$, der einstelligen Operation succ, der zweistelligen Relation $<$ sowie den beiden Konstanten 0 und 1.

Wir spielen das Spiel nun einmal andersherum und sammeln Sätze, ohne eine Struktur im Hintergrund zu haben, in der diese Sätze gelten sollen. Im diesen Zusammenhang nennen wir solche Sätze auch **Axiome**. Die Angabe der Axiome entspricht dann einer Wunschliste. Ob wir dann ein Modell finden, dass uns unsere ganzen Wünsche erfüllt, ist natürlich nicht gewährleistet. Die Axiome, die wir jetzt aufstellen, sollen die Prinzipien des Mengenuniversums wiedergeben. Die formale Sprache selbst wird durch ihre Signatur festgelegt. Da wir als einzige Interaktion die Elementbeziehung hatten, besteht die Signatur auch nur aus dem binären Relationssymbol $\in$. Prinzip 1 ist leicht zu formalisieren:

$$\exists x.x = x$$

Auch Prinzip 2 bringt uns keine Probleme:

$$\forall x \forall y \forall z.(z \in x \leftrightarrow z \in y) \rightarrow x = y$$

Prinzip 3 wird erst jetzt richtig verständlich. Die Eigenschaft P ist etwas, das durch eine Formel beschrieben wird. Ist $\phi(x)$ eine Formel der Signatur $\in$, dann sei

$$\forall x \exists y \forall z.z \in y \leftrightarrow (z \in x \wedge \phi(z))$$

ein Axiom. Wir haben damit ein sogenanntes **Axiomenschema**: jeder Formel in einer freien Variablen wird ein Axiom zugeordnet. Es folgt Prinzip 4:

$$\forall x \forall y \exists z. \forall u.u \in z \leftrightarrow u \in x \vee u \in y$$

Wir machen nun einen Sprung zu den Prinzipien 7 und 8. Hier wird jeweils die Existenz einer bestimmten Menge gefordert, einer induktiven Menge oder einer Potenzmenge. Der erste naive Ansatz, Prinzip 7 anzugeben, ist

$$\exists x.\emptyset \in x \wedge \forall y.y \in x \rightarrow y \cup \{y\} \in x.$$

Leider sind $\emptyset$ und $y \cup \{y\}$ keine Aussagen unserer Sprache. Darum müssen wir ein wenig komplizierter formulieren:

$$\exists x.(\forall y \forall z.\neg z \in y \rightarrow y \in x) \wedge \forall y.$$
$$y \in x \rightarrow \exists z.z \in x \wedge y \in z \wedge \forall v.v \in y \rightarrow v \in z$$

Prinzip 7 ist übrigens stärker als Prinzip 1. Da wir die Existenz einer induktiven Menge fordern, müssen wir nicht noch die Existenz einer beliebigen Menge fordern. Wir können damit Prinzip 1 wieder von unserer Wunschliste streichen.

Prinzip 8 ist wieder einfacher:

$$\forall x \exists y. \forall z (\forall v. v \in z \to v \in x) \to z \in y$$

Für die Prinzipien 5 und 6 müssen wir ein wenig in die Trickkiste greifen. Geben wir uns zuerst ein Axiom vor, das besagt, dass wir Paare basteln dürfen:

$$\forall x \forall y \exists z. \forall u. u \in z \leftrightarrow u = x \vee u = y$$

So ein Paar, das aus den Mengen x und y besteht, schreiben wir einfach in der Form $\{x, y\}$. Jetzt können wir wiederum das Paar $\{x, \{x, y\}\}$ bilden. Diese Menge hat folgenden schöne Eigenschaft: Gilt

$$\{x, \{x, y\}\} = \{a, \{a, b\}\},$$

dann muss $x = a$ und $y = b$ gelten. Das ist genau die Eigenschaft, die wir von einem geordneten Paar fordern. Wir definieren also

$$(x, y) := \{x, \{x, y\}\}$$

Jetzt ist $X \times Y$ gerade

$$\{z \in \mathcal{P}(\mathcal{P}(X \cup Y) \cup X) : z = \{x, \{x, y\}\} \wedge x \in X \wedge y \in Y\},$$

damit ist auch Prinzip 5 abgehakt. Mit dem bis jetzt Erarbeiteten können wir auch Prinzip 6 angeben. Denn sei $x/R = \{y \in X : yRx\}$, damit ist

$$Y = \{Z \in \mathcal{P}(X) : Z = x/R \wedge x \in X\}$$

und

$$\pi_R = \{(a, b) \in X \times Y : a/R = b\}.$$

Um Prinzip 9 anzugeben, brauchen wir kein neues Axiom. Die Herleitung dieses Prinzips überlassen wir dem Leser. Listen wir nun nocheinmal auf, welche Aussagen wir benutzt haben, um unsere Prinzipien angeben zu können.

Extensionalitätsaxiom	$\forall x \forall y \forall z.(z \in x \leftrightarrow z \in y) \rightarrow x = y$
Aussonderungsschema	$\forall x \exists y \forall z.z \in y \leftrightarrow (z \in x \wedge \phi(z))$
Induktionsaxiom	$\exists x.(\forall y \forall z.\neg z \in y \rightarrow y \in x) \wedge \forall y.y \in x \rightarrow$ $\exists z.z \in x \wedge y \in z \wedge \forall v.v \in y \rightarrow v \in z$
Potenzmengenaxion	$\forall x \exists y.\forall z(\forall v.v \in z \rightarrow v \in x) \rightarrow z \in y$
Paarmengenaxion	$\forall x \forall y \exists z.\forall u.u \in z \leftrightarrow u = x \vee u = y$
Vereinigungsmengenaxiom	$\forall x \forall y \exists z.\forall u.u \in z \leftrightarrow u \in x \vee u \in y$

Diese Axiome sind in der Tat Teil einer Axiomatisierung des mengentheoretischen Universums, die zu Beginn des zwanzigsten Jahrhunderts von Ernst Zermelo und Abraham Fraenkel angegeben wurde und heutzutage von vielen Mathematikern (aber nicht allen) als *die* Grundlage der Mathematik angesehen wird.

Aufgaben

1. Gegeben sei die folgende Grammatik:

$$\begin{aligned}
\sigma &\rightarrow \alpha\beta\gamma|\alpha\xi\beta\gamma \\
\xi\beta &\rightarrow \beta\xi \\
\xi\gamma &\rightarrow \eta\beta\gamma\gamma \\
\beta\eta &\rightarrow \eta\beta \\
\alpha\eta &\rightarrow \alpha\alpha\xi|\alpha\alpha \\
\alpha &\rightarrow a \\
\beta &\rightarrow b \\
\gamma &\rightarrow c
\end{aligned}$$

   Dabei besteht das Terminalalphabet aus den Zeichen a, b, c und σ ist das Startzeichen. Wie sieht die von dieser Grammatik erzeugte Sprache aus?

2. Seien

$$\begin{aligned}
r(x) &= \mathsf{mal}(x, \mathsf{succ}(\mathsf{succ}(0))) \\
t(x, y) &= \mathsf{plus}(x, \mathsf{mal}(y, y))
\end{aligned}$$

   gegeben. Berechne $(r + t)^{\mathbb{N}}[1, 0]$, $(r \cdot t)^{\mathbb{N}}[0, 1]$ und $((r + r) \cdot t)^{\mathbb{N}}[1, 1]$.

3. Sei X eine vorgegebene Menge. Wie sieht dann die Menge $\{x \in X : x \notin x\}$ aus?

4 Abstrahieren

Die Arithmetik natürlicher Zahlen haben wir jetzt schon öfters betrachtet. Hier wollen wir einmal einen anderen Blickwinkel auf sie einnehmen: Wir schränken uns auf die Konstante 0 und die Operation succ ein und beobachten in welchem Verhältnis diese Struktur zu ähnlichen Strukturen steht. Die Begriffe "ähnlich" und "im Vergleich stehen" müssen wir uns noch erarbeiten.

Seien A, B Strukturen derselben Signatur L. Ein **Homomorphismus** f von A nach B, in Zeichen $f : A \to B$, ist eine Funktion f von $\mathrm{dom}(A)$ nach $\mathrm{dom}(B)$ mit den folgenden drei Eigenschaften:

- Für jede Konstante c aus L gilt $f(c^A) = c^B$.
- Für jede natürliche Zahl $n > 0$, jedes n-stellige Relationssymbol R aus L und jedes n-Tupel $(a_1, \ldots, a_n)$ aus A gilt: Wenn $(a_1, \ldots, a_n) \in R^A$, dann gilt auch $(f(a_1), \ldots, f(a_n)) \in R^B$.
- Für jede natürliche Zahl $n > 0$, jedes n-stellige Funktionssymbol F aus L und jedes n-Tupel $(a_1, \ldots, a_n)$ aus A gilt $f(F^A(a_1, \ldots, a_n)) = F^B(f(a_1), \ldots, f(a_n))$.

Eine **Einbettung** von A nach B ist nichts anderes als ein Homomorphismus $f : A \to B$, der injektiv ist und folgende stärkere Version für Relationen erfüllt:

- Für jede natürliche Zahl $n > 0$ und jedes n-stellige Relationssymbol R aus L und n-Tupel $(a_1, \ldots, a_n)$ aus A gilt: Genau dann, wenn $(a_1, \ldots, a_n) \in R^A$, gilt auch $(f(a_1), \ldots, f(a_n)) \in R^B$.

Beispiele. Wir betrachten die ganzen Zahlen $\mathbb{Z}$ und die rationalen Zahlen $\mathbb{Q}$, beide als Strukturen mit Signatur $(+, -, 0)$. Die Abbildung $\phi : \mathbb{Z} \to \mathbb{Q}$ mit $\phi(z) = \frac{z}{2}$ ist eine Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$, denn

$$\begin{aligned} \phi(z + z') &= \frac{1}{2}(z + z') = \frac{1}{2}z + \frac{1}{2}z' = \phi(z) + \phi(z') \\ \phi(-z) &= \frac{1}{2}(-z) = -\frac{1}{2}z = -\phi(z) \\ \phi(0) &= \frac{1}{2}0 = 0 \end{aligned}$$

zeigt, dass wir einen Homomorphismus haben und die Implikation

$$\frac{1}{2}z = \frac{1}{2}z' \Rightarrow z = z'$$

beweist, dass es sogar eine Einbettung ist. Die Abbildung ψ mit demselben Definitions- und Wertebereich und $\psi(z) = \frac{1}{z}$ ist hingegen kein Homomorphisums, denn z. B. gilt

$$\psi(2 + 3) = \frac{1}{5} \neq \frac{5}{6} = \frac{1}{2} + \frac{1}{3} = \psi(2) + \psi(3).$$

Ein **Isomorphismus** ist eine surjektive Einbettung. Wir sagen, dass A **isomorph** zu B ist, in Zeichen $A \cong B$, falls ein Isomorphismus von A nach B existiert. Ein Isomorphismus ist somit eine bijektive Abbildung, die sich mit Relationen und Operationen der Struktur verträgt. Damit ist folgendes gemeint: Auf Elemente $a_1, \ldots, a_n$ aus A kann eine Operation F^A angewendet und dann das Ergebnis mit Hilfe des Isomorphismus f nach B abgebildet werden. Andererseits könnten wir auch zuerst die einzelnen Elemente nach B abbilden und auf diese Bilder die gleichnamige Operation F^B anwenden; das Ergebnis ist dasselbe. Damit unterscheiden sich isomorphe Strukturen nur noch dadurch, durch welche speziellen Elemente innerhalb eines mengentheoretischen Universums sie realisiert werden, die "Struktur" als solche ist davon nicht betroffen. Darum interessieren sich Mathematiker oft nur für Eindeutigkeit bis auf Isomorphie.

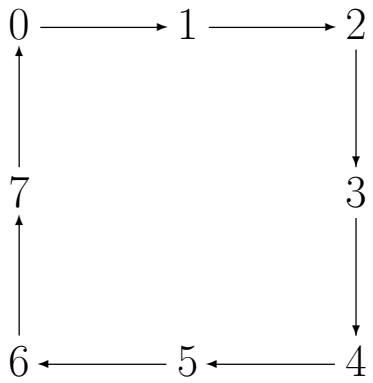
Eine Struktur, deren einzige Operation eine einstellige Operation succ ist, und die ansonsten nur noch eine Konstante 0 hat, nennen wir einen **Orbit**. Einen Orbit kennen wir schon, die natürlichen Zahlen mit der Konstanten $0^{\mathbb{N}}$ und der Nachfolgerfunktion $\mathsf{succ}^{\mathbb{N}}$. Gleich werden wir sehen, dass dieser Orbit in einem gewissen Sinne universell ist, und damit der "beste aller Orbits" ist. Trotzdem können wir leicht andere angeben:

$$\mathrm{dom}(A) = \{0, \ldots, 7\}, 0^A = 0, \mathsf{succ}^A(x) = \begin{cases} x+1 & x \neq 7 \\ 0 & x = 7 \end{cases}$$

Orbits können wir auch schön graphisch darstellen, die natürlichen Zahlen z. B. durch

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow 6 \longrightarrow 7 \longrightarrow \ldots$$

den Orbit A folgendermaßen



Wir zeichnen also einen Pfeil $a \to b$, wenn $\mathsf{succ}^A(a) = b$ gilt.

Das **Induktionsprinzip** für einen Orbit N ist die folgende Regel:

(N0) Für alle $X \subseteq N$ gilt: Falls $0^N \in X$ und $\mathsf{succ}^N(x) \in X$ für alle $x \in X$, dann ist $X = N$.

Die Nummer (N0) signalisiert, dass wir noch an anderen Gesetzen interessiert sind:

(N1) $\mathsf{succ}^N(n) \neq 0^N$ für alle $n \in N$.

(N2) $\mathsf{succ}^N(n) = \mathsf{succ}^N(m) \Rightarrow n = m$ für alle $n, m \in N$.

Ein Orbit mit den Eigenschaften (N0)-(N2) heisse **initial**.

Die Struktur $\mathbb{N} = (\omega, \mathsf{succ}, 0)$ ist ein initialer Orbit. Denn nach Definition von ω folgt aus $X \subseteq \omega$ und $\emptyset \in X$ und

$\mathsf{succ}^{\mathbb{N}}(x) \in X$ für alle $x \in X$ sofort $X = \omega$. Desweiteren ist $\mathsf{succ}^{\mathbb{N}}(n)$ immer eine Menge de Form $\{n, \{n\}\}$, also auf keinem Fall die leere Menge, $\emptyset = 0^{\mathbb{N}}$ und $\mathsf{succ}(m) = \mathsf{succ}(n)$ bedeutet $m \cup \{m\} = n \cup \{n\}$, also $m = n$.

Das Induktionsprinzip eröffnet uns die Möglichkeit, auf eine neue Art Eigenschaften initialer Orbits zu beweisen. Erfüllt 0 eine gewisse Eigenschaft P und mit $x \in N$ auch $\mathsf{succ}(x)$, dann erfüllt jedes Element $n \in N$ diese Eigenschaft.

Wir werden gleich Beispiele in Hülle und Fülle sehen. Neben dem Beweisen von Eigenschaften haben wir auch die Möglichkeit, neue Funktionen zu konstruieren; das erlaubt uns das

Satz 4.1 Rekursionsprinzip. *Sind ein initialer Orbit N, eine Menge M mit ausgezeichnetem Anfangswert $a \in M$ und eine Hilfsfunktion $h : M \to M$ gegeben, so gibt es genau eine Abbildung $f : N \to M$ mit $f(0) = a$ und*

$$f(\mathsf{succ}(n)) = h(f(n))$$

für alle $n \in N$.

Beweis. Schreiben wir der Einfachheit halber

$$1 = \mathsf{succ}(0) \text{ und } x + 1 = \mathsf{succ}(x),$$

so ergeben sich die Werte von f durch "Rechnungen" dieser Art:

$$
\begin{aligned}
0 \mapsto &\qquad a \\
1 \mapsto &\qquad h(a) \\
1+1 \mapsto &\qquad h(f(1)) = h(h(a)) \\
&\vdots \qquad\qquad \vdots \\
n+1 \mapsto &\qquad h(f(n)) = h(h(\ldots h(a)))
\end{aligned}
$$

Anders ausgedrückt, zu gegebenem N, M, Anfangswert a und Hilfsfunktion h ist die Menge der *Rechnungen* induktiv definiert durch

(i) $0 \mapsto a$ ist eine Rechnung

(ii) $0 \mapsto a$; $\mathsf{succ}(0) \mapsto h(a)$ ist eine Rechnung

(iii) Ist $R, n \mapsto b$ eine Rechung, so auch $R, n \mapsto b, \mathsf{succ}(n) \mapsto h(b)$

(iv) Nichts anderes ist eine Rechnung.

Wir haben nun durch Induktion zu zeigen, dass es zu jedem $n \in N$ genau eine Rechnung der Form $0 \mapsto b$ bzw. $R; n \mapsto b$ für $n \neq 0$ gibt. Ist das gezeigt, so haben wir mit $f(0) = a$ und

$$f(n) = b \Leftrightarrow \text{Es existiert eine Rechnung } R; n \mapsto b, n \neq 0$$

eine Abbildung $f : N \to M$, welche die gewünschten Eigenschaften besitzt. Da jede solche Funktion, wie oben demonstriert, durch Rechnungen eindeutig auszuwerten ist, gibt es auch nur ein solches f.

Die Existenz der Rechnungen folgt trivial, indem wir im Induktionsschritt an gegebenes $R; n \mapsto b$ einfach $\mathsf{succ}(n) \mapsto h(b)$ anhängen. Für die Eindeutigkeit müssen wir aber (N1) und (N2) bemühen. Eine Rechnung mit letzter Zeile $0 \mapsto b$ kann nicht nach (i) oder (ii) entstehen, weil sonst $0 = \mathsf{succ}(n)$, im Widerspruch zu (N1). Also muss sie nach (i) entstanden sein. Im Schluss von n auf $\mathsf{succ}(n)$ betrachten wir eine Rechnung mit letzter Zeile $\mathsf{succ}(n) \mapsto b$. Wieder wegen (N1) kann dies nur nach (ii) oder (iii) entstanden sein, hat also eine vorletzte Zeile der Form

$m \mapsto c$ mit $\mathsf{succ}(m) = \mathsf{succ}(n), b = h(c)$

Mit (N2) folgt $m = n$, nach der Induktionsannahme ist c eindeutig bestimmt und damit auch $b = h(c)$. □

Aus dem Rekursionsprinzip folgt, dass es nicht besonders viele initiale Orbits gibt:

Korollar 4.2 *Bis auf Isomorphie gibt es genau einen initialen Orbit.*

Beweis. Seien M, N initiale Orbits, $h = id_N$ und $a = 0^N$. Dann ist die durch das Rekursionsprinzip gegebene Funktion $f : M \to N$ ein Isomorphismus. □

In dem Beweis auf dem Anfang dieser Seite hatten wir die Formulierung "folgt trivial", was in den Ohren vieler Leser arrogant klingen mag. Mit "trivial" ist in mathematischen

Texten aber gemeint, dass die Aussage direkt aus der Definition abgeleitet werden kann. Arrogant war hingegen eher der Beweis unseres letzten Korollars. Anstelle eines Beweises wurde de facto nur eine kurze Beweisidee skizziert. Der Nachweis, dass es sich wirklich um einen Isomorphismus handelt, wird dann aber nicht erbracht. Solchen knappen Beweisen wirst du oft in der Mathematik begegnen. Die eine Hälfte der Leser ärgert sich, weil sie sich den Rest nun selber erarbeiten müssen, die andere Hälfte freut sich, dass ihnen die Idee mitgeteilt wird und sie sich nicht mit den technischen Details beschäftigen müssen.

Wenn wir eine natürliche Zahl m als Anfangswert und die Nachfolgerfunktion als Hilfsfunktion wählen, dann liefert das Rekursionsprinzip eine Funktion $f_m : \mathbb{N} \to \mathbb{N}$ mit der Abbildungsvorschrift $f_m(n) = m + n$. Definieren wir nun eine Funktion $\mathsf{plus} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch $\mathsf{plus}(m, n) = f_m(n)$, dann erhalten wir die Rekursionsgleichungen

$$\begin{aligned} \mathsf{plus}(m, 0) &= m \\ \mathsf{plus}(m, \mathsf{succ}(n)) &= \mathsf{succ}(\mathsf{plus}(m, n)) \end{aligned}$$

Für die Multiplikation gibt es ähnliche Gleichungen

$$\begin{aligned} \mathsf{mal}(m, 0) &= 0 \\ \mathsf{mal}(m, \mathsf{succ}(n)) &= \mathsf{plus}(\mathsf{mal}(m, n), m) \end{aligned}$$

und zur großen Freude können wir die grundlegenden Eigenschaften der Addition und Multiplikation mittels dieser rekursiven Definition und dem Induktionsprinzip beweisen, z. B. dass die Addition assoziativ ist, d.h. für alle natürlichen Zahlen m, n, p gilt

$$\mathsf{plus}(\mathsf{plus}(m, n), p) = \mathsf{plus}(m, \mathsf{plus}(n, p))$$

Gilt $p = 0$, dann ist

$$\mathsf{plus}(\mathsf{plus}(m, n), 0) = \mathsf{plus}(m, n) = \mathsf{plus}(m, \mathsf{plus}(n, 0))$$

Ist diese Aussage für p schon gezeigt, dann gilt

$$\begin{aligned} \mathsf{plus}(\mathsf{plus}(m, n), \mathsf{succ}(p)) &= \mathsf{succ}(\mathsf{plus}(\mathsf{plus}(m, n), p)) \\ &= \mathsf{succ}(\mathsf{plus}(m, \mathsf{plus}(n, p))) \\ &= \mathsf{plus}(m, \mathsf{succ}(\mathsf{plus}(n, p))) \\ &= \mathsf{plus}(m, \mathsf{plus}(n, \mathsf{succ}(p))) \end{aligned}$$

Nun wollen wir das Kommutativgesetz für die Addition beweisen. Dieses Gesetz besagt, dass für alle natürlichen Zahlen m, n folgendes gilt:

$$\mathsf{plus}(m, n) = \mathsf{plus}(n, m)$$

Dafür brauchen wir etwas Vorbereitung, und zwar zeigen wir zuerst die folgenden beiden Gesetze:

(4.1) Für alle m, n gilt

$$\mathsf{succ}(\mathsf{plus}(n, m)) = \mathsf{plus}(\mathsf{succ}(n), m)$$

(4.2) Für alle n gilt $\mathsf{plus}(n, 0) = \mathsf{plus}(0, n)$

Also zunächst (4.1) mittels Induktion über m:

Induktionsanfang $m = 0$:

$$\mathsf{succ}(\mathsf{plus}(n, 0)) = \mathsf{succ}(n) = \mathsf{plus}(\mathsf{succ}(n), 0)$$

Induktionsschritt von m nach $m + 1$:

$$\begin{aligned} \mathsf{succ}(\mathsf{plus}(n, \mathsf{succ}(m))) &= \mathsf{succ}(\mathsf{succ}(\mathsf{plus}(n, m)) \\ &= \mathsf{succ}(\mathsf{plus}(\mathsf{succ}(n), m)) \\ &= \mathsf{plus}(\mathsf{succ}(n), \mathsf{succ}(m)) \end{aligned}$$

Jetzt (4.2):

Induktionsanfang $n = 0$: $\mathsf{plus}(n, 0) = \mathsf{plus}(0, 0) = 0 = \mathsf{plus}(0, n)$

Induktionsschritt von n nach $n + 1$:

$$\begin{aligned} \mathsf{plus}(\mathsf{succ}(n), 0)) &= \mathsf{succ}(\mathsf{plus}(n, 0)) \\ &= \mathsf{succ}(\mathsf{plus}(0, n)) \\ &= \mathsf{plus}(0, \mathsf{succ}(n)) \end{aligned}$$

Jetzt beweisen wir das Kommutativgesetz per Induktion über m. Der Induktionsanfang war gerade (4.2) und den Induktionsschritt sehen wir so ein:

$$\begin{aligned}\mathsf{plus}(n, \mathsf{succ}(m)) &= \mathsf{succ}(\mathsf{plus}(n, m)) \\ &= \mathsf{succ}(\mathsf{plus}(m, n)) \\ &= \mathsf{plus}(\mathsf{succ}(m), n)\end{aligned}$$

Auf ähnliche Weise können Assoziativ- und Kommutativgesetz für die Multiplikation bewiesen werden und ein Gesetz, das das Zusammenspiel von Addition und Multiplikation beschreibt, das sogennante **Distributivgesetz:** Für alle $k, m, n \in \mathbb{N}$

$$\mathsf{mal}(k, \mathsf{plus}(m, n)) = \mathsf{plus}(\mathsf{mal}(k, m), \mathsf{mal}(k, n))$$

Entsprechend gibt es Gesetze, die das Zusammenspiel zwischen Ordnung, Multiplikation und Addition erklären, wobei folgende rekursive Definition der Ordnung benutzt wird:

$$\neg m < 0, m < \mathsf{succ}(n) \Leftrightarrow m < n \vee m = n$$

Wenn wir wieder zur gewohnten Infixnotation übergehen, so erhalten wir die folgende Liste von Gesetzen:

Assoziativgesetz der Addition	$\forall x \forall y \forall z.(x + y) + z = x + (y + z)$
Assoziativgesetz der Multiplikation	$\forall x \forall y \forall z.(xy)z = x(yz)$
Kommutativgesetz der Addition	$\forall x \forall y.x + y = y + x$
Kommutativgesetz der Multiplikation	$\forall x \forall y.xy = yx$
Distributivgesetz	$\forall x \forall y \forall z.x(y + z) = xy + xz$
Additivität der Ordnung	$\forall x \forall y \forall z.x < y \rightarrow x + z < y + z$
Multiplikativität der Ordnung	$\forall x \forall y \forall z.x < y \wedge z > 0 \rightarrow xz < yz$

Weitere Operationen, die wir rekursiv definieren können, sind die Exponentiation

$$\begin{aligned} \mathsf{hoch}(m, 0) &= 1 \\ \mathsf{hoch}(m, \mathsf{succ}(n)) &= \mathsf{mal}(\mathsf{hoch}(m, n), m) \end{aligned}$$

die n-fache Summe

$$\sum_{i=0}^{0} a_i = a_0, \ \sum_{i=0}^{n+1} a_i = \mathsf{plus}(\sum_{i=0}^{n} a_i, a_{n+1})$$

und das n-fache Produkt

$$\prod_{i=0}^{0} a_i = a_0, \ \prod_{i=0}^{n+1} a_i = \mathsf{mal}(a_{n+1}, \prod_{i=0}^{n} a_i)$$

Anstelle von $\mathsf{hoch}(m, n)$ schreiben wir abkürzend m^n.

Nun können wir wieder per Induktion etliche Eigenschaften dieser Operationen beweisen. Eine der bekanntesten ist z. B. folgende Summationsformel:

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

Diese Gleichung gilt für $n = 0$, weil dann auf beiden Seiten 0 steht und folgendermaßen funktioniert der Induktionsschritt von n nach $n + 1$:

$$\begin{aligned}\sum_{k=0}^{n+1} k &= \sum_{k=0}^{n} k + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2n+2}{2} \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

Wir betrachten die Ausdrücke $\sum_{i=0}^{n} a_i$ und $\prod_{i=0}^{n} a_i$ nocheinmal genauer. Die Variable i wird in diesem Zusammenhang der **Laufindex** genannt. Dieser muss nicht unbedingt bei 0 starten, jeder andere Wert ist auch zulässig, zum Beispiel

$$\sum_{i=3}^{12} a_i \text{ oder } \prod_{i=3}^{2} a_i.$$

Ist $n < j$, dann soll $\sum_{i=j}^{n} a_n$ den Wert 0 und $\prod_{i=j}^{n} a_i$ den Wert 1 haben; das ist einfach eine Konvention, die sich als nützlich erwiesen hat. Eine weitere Schreibweise für $\sum_{i=3}^{12} a_i$ ist

$$\sum_{3 \le i \le 12} a_i.$$

Allgemeiner können wir unter das Summen- bzw. Produktzeichen eine Bedingung B schreiben, die nur von endlich vielen natürlichen Zahlen erfüllt wird. Dann ist $\sum_{B(i)} a_i$ die

Summe aller a_i, bei denen i die Eigenschaft B erfüllt. Zum Beispiel werden wir im nächsten Satz eine Summe der Form

$$\sum_{i+j=k} a_i a'_j$$

antreffen. Das ist so zu lesen: k ist eine feste Zahl und wir betrachten alle Paare natürlicher Zahlen (i, j) mit $i + j = k$, also

$$\sum_{i+j=k} a_i a'_j = a_0 a'_k + a_1 a'_{k-1} + \cdots + a_k a'_0.$$

Satz 4.3 *Sei $b > 0$ eine feste aber beliebige natürliche Zahl. Dann existiert zu jeder natürlichen Zahl $n \geq 1$ eine eindeutige natürliche Zahl m und eindeutige Zahlen a_0 bis a_m mit $0 \leq a_i < b$ für $0 \leq i \leq m$ und $a_m \neq 0$, so dass*

$$n = \sum_{k=0}^{m} a_k b^k$$

gilt. Für Addition und Multiplikation zweier natürlicher Zahlen folgt daraus: gilt

$$n' = \sum_{k=0}^{m'} a'_k b^k,$$

dann ist die Summe

$$n + n' = \sum_{k=0}^{\max\{m,m'\}} (a_k + a'_k)b^k,$$

wobei $a_{m+1} = \cdots = a_{m'} = 0$, *falls* $m' > m$ *bzw.* $a'_{m'+1} = \cdots = a'_m = 0$, *falls* $m > m'$, *und das Produkt ist*

$$n \cdot n' = \sum_{k=0}^{m+m'} c_k b^k \text{ mit } c_k = \sum_{k=i+j} a_i a'_j$$

Beweis. Es folgen mehrere Induktionsbeweise. Wir beweisen zunächst folgende Gleichung per Induktion über k:

(4.3) $\sum_{i=0}^{k}(b-1)\cdot b^i + 1 = b^{k+1}$

Für $k = 0$ haben wir

$$\sum_{i=0}^{0}(b-1)\cdot b^i + 1 = (b-1)\cdot b^0 + 1 = b - 1 + 1 = b^1$$

Der Schritt von k nach $k+1$:

$$\begin{aligned}\sum_{i=0}^{k+1}(b-1)\cdot b^i + 1 &= \sum_{i=0}^{k}(b-1)\cdot b^i + 1 + (b-1) * b^{k+1} \\ &= b^{k+1} + (b-1) * b^{k+1} = b^{k+2}\end{aligned}$$

Nun widmen wir uns der eindeutigen Darstellung von n. Für $n = 1$ erhalten wir

$$1 = \sum_{k=0}^{0} 1 \cdot b^0.$$

Sei nun n beliebig, aber wir wüssten schon, dass $n = \sum_{k=0}^{m} a_k b^k$ gilt. Dann sei $j = \min\{k \leq m : a_k \neq b-1\}$, falls so ein Minimum existiert, und wir erhalten die eindeutige Darstellung von $n+1$ mit Hilfe von (4.3):

$$n + 1 = \sum_{k=0}^{m} a_k \cdot b^k + 1 = \sum_{k=j+1}^{m} a_k b^k + (a_j + 1)b^j.$$

Wenn es ein solches Minimum j nicht gibt, dann ist $n+1 = 100...$ (mit m Nullen). Jetzt zum zweiten Teil des Beweises. Hierbei beschränken wir uns auf einen Beweis für die Darstellung der Multiplikation, der Beweis für die Addition ist einfacher. Wir führen einen Induktionsbeweis über m'. Gilt $m' = 0$, dann ist $n' = a'_0$ und

$$n \cdot n' = \left(\sum_{i=0}^{m} a_i b^i \right) \cdot a'_0 = \sum_{i=0}^{m} a'_0 a_i b^i = \sum_{k=0}^{m+m'} c_k b^k$$

mit $c_k = a'_0 \cdot a_k = \sum_{k=i+j} a'_0 a_j$. Sei nun die Aussage für m' bewiesen und

$$n' = \sum_{i=0}^{m'+1} a'_i b^i$$

gegeben. Dann können wir $n \cdot \left(\sum_{i=0}^{m'} a'_{i+1} b^i \right)$ eine eindeutige Darstellung $\sum c_i b^i$ mit $c_k = \sum_{k=i+j} a_i a'_{j+1}$ zuordnen. Es gilt

$$n \cdot \left(\sum_{i=1}^{m'+1} a'_i b^i \right) = \sum_{i=1}^{m+m'+1} c_i b^i$$

Zu dieser Darstellung müssen wir nur noch a'_0 so wie oben dazuaddieren. □

So eine eindeutige Darstellung einer natürlichen Zahl nennen wir ihre *b*-**ale** Darstellung. Dieser Satz erlaubt eine Rechtfertigung des Algorithmus für schriftliche Addition und Multiplikation des ersten Kapitels. Betrachten wir nocheinmal, was passiert, wenn wir n und n' wie im Satz oben addieren. Wir schreiben die beiden b-alen Darstellungen untereinander, ziehen einen Strich

$$\begin{array}{cccccc} & \ldots & a_m & \ldots & a_1 & a_0 \\ a'_{m'} & & & \ldots & a'_1 & a'_0 \\ \hline \end{array}$$

und bilden zuerst die Summe $a_0 + a'_0$. Dann gilt entweder $a_0 + a'_0 < b$ oder $a_0 + a'_0 = b + a''_0$ mit $a''_0 < b$. Entsprechend ist die Notation unter dem Strich und wir wiederholen dann eine Stelle weiter links... Das Vorgehen bei der Multiplikation ist auch naheliegend. Beachte, dass eine Multiplikation mit b einer Verschiebung nach links entspricht. Deshalb können wir mit einer Ziffer multiplizieren und das Ergebnis so oft nach links schieben, wie es der Position der Ziffer entspricht.

Hier ist auch eine gute Stelle um einen Beweis für Lemma 2.10 nachzuholen: Sei also $|X| = |Y| = n$ und $f : X \to Y$ injektiv. Ist $n = 1$, dann gibt es sowieso nur eine solche Funktion f, die das einzige Element aus X auf das einzige Element aus Y abbildet. Ist $n = m + 1$, und $a \in X$, dann ist auch $f' : X \setminus \{a\} \to Y \setminus \{f(a)\}$ injektiv, $|X \setminus \{a\}| = |Y \setminus \{f(a)\}| = m$, also ist nach Induktionsvoraussetzung f' bijektiv. Dann ist aber auch f bijektiv. □

Nachdem wir das Assoziativgesetz für die Addition und Multiplikation der natürlichen Zahlen gezeigt haben, folgen dieselben Eigenschaften für die ganzen und rationalen Zahlen sehr einfach, denn

$$\begin{aligned}(m,n) + (m',n') &= (m + m', n + n') \\ &= (m' + m, n' + n) \\ &= (m',n') + (m,n)\end{aligned}$$

liefert zum Beispiel das Kommutativgesetz für die Addition ganzer Zahlen und

$$\frac{r}{s}(\frac{a}{b}+\frac{c}{d}) = \frac{r}{s}\cdot\frac{ad+bc}{bd} = \frac{r(ad+bc)}{sbd} = \frac{rad+rbc}{sbd} = \frac{r}{s}\frac{a}{b}+\frac{r}{s}\frac{c}{d}$$

das Distributivgesetz für die rationalen Zahlen. Außerdem gelten neue Aussagen: wegen $z + (-z) = 0$ gilt

$$\mathbb{Z} \models \forall x \exists y . x + y = 0$$

oder, wenn wir $x \mapsto -x$ als neue einstellige Operation auffassen,

$$\mathbb{Z} \models \forall x.x + (-x) = 0$$

Für die rationalen Zahen haben wir zum Beispiel

$$\mathbb{Q} \models \forall x.x \neq 0 \to \exists y.xy = 1$$

Wir versuchen Ordnung in diese Ansammlung von Aussagen zu bekommen: Eine **Gruppe** ist eine Struktur mit Signatur $(\cdot, ^{-1}, e)$, die folgende Aussagen erfüllt:

$$\begin{aligned} \forall x \forall y \forall z.(x \cdot y) \cdot z &= x \cdot (y \cdot z) \\ \forall x.e \cdot x &= x \\ \forall x.x^{-1} \cdot x &= e \end{aligned}$$

Beispiele sind $(\mathbb{Z}, +, -, 0), (\mathbb{Q}, +, -, 0)$ und $(\mathbb{Q}\backslash\{0\}, \cdot, ^{-1}, 1)$. Das ist so zu lesen, dass $\cdot^{\mathbb{Z}} = +$, $^{-1^{\mathbb{Z}}} = -$ und $e^{\mathbb{Z}} = 0$ gilt.

Eine Gruppe ist **abelsch**, falls

$$\forall x \forall y.x \cdot y = y \cdot x$$

erfüllt ist. Die drei Beispiele oben sind alle abelsch.

Ein **Ring** R hat Signatur $(+, \cdot, -, 0, 1)$; dabei ist $(R, +, -, 0)$ eine abelsche Gruppe und weiterhin gilt

$$\begin{aligned} \forall x \forall y \forall z.(x \cdot y) \cdot z &= x \cdot (y \cdot z) \\ \forall x.1 \cdot x &= x \\ \forall x \forall y \forall z.(x + y) \cdot z &= x \cdot z + y \cdot z \\ \forall x \forall y \forall z.x \cdot (y + z) &= x \cdot y + x \cdot z \end{aligned}$$

Beispiele sind $(\mathbb{Z}, +, \cdot, -, 0, 1)$ und $(\mathbb{Q}, +, \cdot, -, 0, 1)$. Schließlich ist ein **Körper** ein Ring, der die zusätzlichen Axiome

$$\forall x.x \neq 0 \rightarrow \exists y.x \cdot y = 1,\ \forall x \forall y.x \cdot y = y \cdot x$$

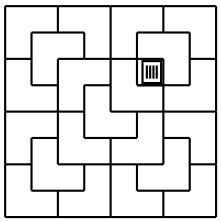
erfüllt. Einziges bis jetzt bekanntes Beispiel ist der Körper der rationalen Zahlen.

Aufgaben

1. Welche der folgenden Abbildungen sind Homomorphismen?

   - $\phi : \mathbb{Z} \to \mathbb{Q}$ mit $\phi(z) = z^2$ bzgl. der Signatur $(+, -, 0)$,
   - $\phi : \mathbb{Z} \to \mathbb{Z}$ mit $\phi(z) = -z$ bzgl. der Signatur $(+, -, 0)$ bzw. $(<)$,
   - $\psi : \mathbb{Z}_2 \to \mathbb{Z}_2$ mit $\psi(z) = z^2$ bzgl. der Signatur $(+, -, 0)$.

2. Betrachte ein quadratisches Badezimmer mit Seitenlänge 2^n. Eines seiner $(2^n)^2$ Einheitsquadrate ist für einen Abfluß vorgesehen. Zeige durch vollständige Induktion, dass sich die verbleibenden $(2^n)^2 - 1$ Felder mit Fliesen von der Form ⧉ kacheln lassen. Hier ist der Fall $n = 3$ dargestellt:



3. Zeige, dass für den Orbit A auf Seite 69 das Rekursionsprinzip nicht gilt.

5 Rechnen

Wir untersuchen die Struktur des Rings der ganzen Zahlen und kommen somit zur Theorie der "Teilbarkeit". Nebenbei werden wir viele neue Beispiele für Ringe und Körper kennenlernen. Ist a eine ganze Zahl, dann sei $|a| = a$, falls $a \geq 0$, ansonsten sei $|a| = -a$.

Wir sagen, die ganze Zahl a **teilt** die ganze Zahl b, falls wir eine dritte ganze Zahl c finden, so dass $b = ac$ gilt; wir schreiben $a|b$. Teilbarkeit ist somit eine zweistellige Relation auf der Menge der ganzen Zahlen. Sie erfüllt die folgenden Regeln:

- $a|0$
- $0|a \Rightarrow a = 0$
- $a|b \Rightarrow (ac)|(bc)$
- $a|b$ und $a|c \Rightarrow a|(b+c)$

Satz 5.1 Division mit Rest. *In $\mathbb{Z}$ gibt es zu allen a und b, beide ungleich 0, eindeutig bestimmte Zahlen r und q mit*

$$a = bq + r,\ 0 \leq r < |b|.$$

Die eindeutige Zahl r wird der **Rest** der Division von a mit b genannt.

Beweis. Wir beweisen zunächst die Existenz einer solchen Darstellung und beschränken uns auf den Fall $a \geq b > 0$.

Jetzt können wir einen Induktionsbeweis über a führen: Ist $a = 1$, dann muss auch $b = 1$ sein und wir haben $a = b \cdot 1 + 0$. Nehmen wir nun an, dass wir für ein beliebiges a natürliche Zahlen q, r mit $a = b \cdot q + r$ und $r < b$ haben. Falls $r + 1 < b$ gilt, dann ist $a + 1 = b \cdot q + (r + 1)$ auch wieder eine passende Darstellung. Ansonsten ist $r + 1 = b$ und

$$\begin{aligned} a + 1 &= b \cdot q + r + 1 \\ &= b \cdot q + b \\ &= b \cdot (q + 1) + 0 \end{aligned}$$

Wir müssen nun noch die Annahmen, die wir gemacht haben, abschwächen. Im Fall $b > a > 0$ können wir einfach $q = 0$ und $r = a$ setzen. Ist eine der beiden Zahlen negativ, dann muss q durch $-q$ ersetzt werden. Sind beide Zahlen negativ, sagen wir $a < b < 0$, dann finden wir q, r mit $-a = -bq + r$. Daraus folgt $-a = -b(q + 1) + r + b$ bzw. $a = b(q + 1) + (-b - r)$ und $0 \geq -b - r < |b|$.

Schließlich zur Eindeutigkeit der Darstellung: Ist nun $a = bq + r = bq' + r'$ und z.B. $r' \geq r$, so folgt $b(q - q') = r' - r$. Also $q - q' = 0$, da sonst $|b| \leq |r' - r| < |b|$. Und es folgt $r = r'$. □

Das Teilen durch b mit Rest liefert einen Algorithmus zur Bestimmung der b-alen Darstellung einer Zahl.

Teilen wir $\sum_{i=0}^{m} a_i b^i$ durch b, dann erhalten wir $\sum_{i=1}^{m} a_i b^{i-1}$ mit Rest a_0. Teilen wir dann wieder durch b, ist das Ergebnis $\sum_{i=2}^{m} a_i b^{i-2}$ mit Rest a_1. Nach m Schritten bleibt a_m mit Rest a_{m-1} übrig.

Beispiel. Wir bestimmen die Binärdarstellung von 124 (in Dezimaldarstellung).

$$\begin{array}{rcrcrl} 124 & : & 2 & = & 62 & \text{Rest } 0 \\ 62 & : & 2 & = & 31 & \text{Rest } 0 \\ 31 & : & 2 & = & 15 & \text{Rest } 1 \\ 15 & : & 2 & = & 7 & \text{Rest } 1 \\ 7 & : & 2 & = & 3 & \text{Rest } 1 \\ 3 & : & 2 & = & 1 & \text{Rest } 1 \end{array}$$

Wir erhalten die Binärdarstellung 1111100.

Die Zahl t ist ein **gemeinsamer Teiler** von a und b, falls $t|a$ und $t|b$ gilt. Ein gemeinsamer Teiler d von a und b ist ein **größter gemeinsamer Teiler**, falls jeder andere gemeinsame Teiler t von a, b auch Teiler von d ist. Es folgt, dass es zu a, b bis auf das Vorzeichen höchstens einen größten gemeinsamen Teiler gibt, wir schreiben $ggT(a, b) = d$ mit $d \geq 0$, falls es so einen gibt.

Lemma 5.2 *Für beliebige ganze Zahlen a, b gelten folgende Regeln:*

(i) $ggT(a,b) = ggT(a-qb, b)$
(ii) $ggT(a,b) = ggT(b,a)$
(iii) $ggT(a,b) = ggT(|a|,|b|)$
(iv) $a|b \Leftrightarrow ggT(a,b) = |a|$
(v) *Für jede rationale Zahl q gibt es ganze Zahlen a, b mit $q = \frac{a}{b}$ und $ggT(a,b) = 1$*

Beweis. Sei $d = ggT(a,b)$. Dann ist d ein Teiler von a und b, damit aber auch einer von qb bzw. $a - qb$. Wenn e ein weiterer Teiler von b und $a - qb$ ist, dann teilt e auch $a = a - qb + qb$. Nach Definition des größten gemeinsamen Teilers ist somit e auch ein Teiler von d. Das beweist (i). Wenn t ein Teiler von a, b ist, dann auch von b, a und $|a|, |b|$. Daraus lassen sich die Gleichungen

$$ggT(a,b) = ggT(b,a) = ggT(|a|,|b|)$$

sofort herleiten. Auch (iv) ist leicht zu zeigen, und wir überlassen dem Leser den Beweis. Bleibt noch (v): Wenn wir zu q eine Darstellung als Bruch $q = \frac{z}{n}$ haben, dann setzen wir $a = z/ggT(z,n)$ und $b = n/ggT(z,n)$. Dann gilt

$$\frac{a}{b} = \frac{\frac{z}{ggT(z,n)}}{\frac{n}{ggT(z,n)}} = \frac{z}{n}$$

und der größte gemeinsame Teiler von a und b ist 1. □

Satz 5.3 (Euklid+Bezout) *Zu je zwei ganzen Zahlen a, b gibt es den größten gemeinsamen Teiler und ganze Zahlen x und y mit*

$$ggT(a, b) = ax + by.$$

Beweis. Zur Berechnung des größten gemeinsamen Teilers benutzen wir die Regeln des vorherigen Lemmas: Wir nehmen an, dass $0 < b < a$ gilt (ansonsten vertauschen wir gegebenenfalls die Rollen von a und b oder ersetzen a durch $|a|$ oder b durch $|b|$). Ist b ein Teiler von a, dann ist $ggT(a, b) = b$. Wenn nicht, dann finden wir eine ganze Zahl q mit $a - qb < b$ und $ggT(a - qb, b) = ggT(a, b)$.

Wir setzen $b_1 = a - qb$ und $a_1 = b, q_1 = q$. Dann gilt $b_1 < a_1$ und wir wiederholen das Prozedere mit den Zahlen a_1 und b_1. Bei jedem Schritt nimmt der Betrag einer der beiden Zahlen ab und irgendwann erhalten wir Zahlen a_m, b_m mit der Eigenschaft $b_m | a_m$; spätestens, wenn eine der beiden Zahlen gleich 1 ist. Nun gilt $a_m = q_m b_m$ und $ggT(a, b) = b_m$. Daraus folgt

$$\begin{aligned} ggT(a, b) &= b_m \\ &= a_{m-1} - q_{m-1} b_{m-1} \\ &= b_{m-2} - q_{m-1}(a_{m-2} - q_{m-2} b_{m-2}) \\ &\vdots \\ &= xa + yb \end{aligned}$$

□

Wir schauen uns ein Beispiel an: $a = 101,\ b = 43$ und

$$\begin{aligned} ggT(101, 43) = ggT(101 - 2 \cdot 43, 43) &= ggT(15, 43) = \\ ggT(43, 15) = ggT(43 - 2 \cdot 15, 15) &= ggT(13, 15) = \\ ggT(15, 13) = ggT(15 - 13, 13) &= ggT(2, 13) = \\ ggT(13, 2) = ggT(13 - 6 \cdot 2, 2) &= ggT(1, 2) = 1. \end{aligned}$$

Also

$$\begin{aligned} 1 = 2 - 1 = 2 - 13 + 6 \cdot 2 = 7 \cdot 2 - 13 = 7(15 - 13) - 13 \\ = 7 \cdot 15 - 8 \cdot 13 = 7 \cdot 15 - 8(43 - 2 \cdot 15) = 23 \cdot 15 - 8 \cdot 43 \\ = 23(101 - 2 \cdot 43) - 8 \cdot 43 = 23 \cdot 101 - 54 \cdot 43 \end{aligned}$$

Ein Teiler d von a ist **echt**, falls $|d| \neq 1$ und $|d| \neq |a|$. Eine Zahl a mit $|a| > 1$ ist **unzerlegbar**, falls sie keine echten Teiler besitzt.

Satz 5.4 *Jede natürliche Zahl $n > 1$ ist ein Produkt von unzerlegbaren Zahlen.*

Beweis. Wenn es ein Gegenbeispiel gibt, dann auch ein kleinstes Gegenbeispiel n. Insbesondere ist n selbst zerlegbar. Also $n = a \cdot b$ mit $1 < a, b < n$. Da a kein Gegenbeispiel ist, ist es ein Produkt $a = p_1 \cdot \ldots \cdot p_k$ von unzerlegbaren Zahlen und $b = q_1 \cdot \ldots \cdot q_l$ ebenfalls. Also ist $n = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l$ auch ein Produkt von unzerlegbaren Zahlen, Widerspruch.

□

Eine Zahl p mit $|p| > 1$ ist eine **Primzahl**, falls für alle $x, y \in \mathbb{Z}$ aus $p|x \cdot y$ folgt, dass $p|x$ oder $p|y$ gilt.

Satz 5.5 *In $\mathbb{Z}$ sind die unzerlegbaren Zahlen genau die Primzahlen.*

Beweis. Sei p prim und $p = a \cdot b$, so o. B. d. A. $p|a$, also $|p| \leq |a|$. Andererseits $|a| \leq |p|$, also $|a| = |p|$. Es folgt $|b| = 1$.

Sei umgekehrt p unzerlegbar und ein Teiler von ab. Ist p kein Teiler von a, so gilt $\mathrm{ggT}(p, a) = 1$; also existieren nach Satz 5.3 ganze Zahlen x und y mit $1 = ax+py$ bzw. $b = abx+bpy$. Nun teilt p das Produkt ab, also auch abx, aber auch sich selbst und damit bpy und damit letztendlich $abx + bpy = b$.

□

"*o. B. d. A.*" ist übrigens die Abkürzung für "ohne Beschränkung der Allgemeinheit", was soviel bedeutet wie "Wir schauen uns nur einen Fall an. Wenn wir uns aber die anderen Fälle anschauen, dann läuft der Beweis analog".

Satz 5.6 *Jede ganze Zahl a mit $|a| > 1$ hat eine Zerlegung*

$$a = p_1 \cdot \ldots \cdot p_n \text{ in Primzahlen } p_1, \ldots, p_n, \ n \geq 1.$$

Die p_i sind bis auf Vorzeichen und Reihenfolge eindeutig bestimmt.

Beweis. Die Existenz haben wir schon gezeigt. Die Eindeutigkeit folgt mit Induktion über n. Ist $n = 1$, dann ist a unzerlegbar, und es gilt $a = a$. Ist $a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$ so teilt p_n eines der q_j nach Umsortieren etwa q_m. Es folgt $|p_n| = |q_m|$ und durch Kürzen $\prod_{i=1}^{n-1} |p_i| = \prod_{j=1}^{m-1} |q_j|$. Mit Induktion folgt $n = m$ und der Rest der Behauptung. □

Satz 5.7 (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, dies wäre nicht der Fall. Dann gäbe es ja nur endlich viele Primzahlen, sagen wir die Zahlen p_1 bis p_r. Die Zahl $n = p_1 \cdot p_2 \cdots p_r + 1$ ist weder durch p_1 noch durch p_2 noch durch eine andere Zahl der Form p_i teilbar. Also muss n einen Primteiler q haben, der sich von den Primzahlen p_1 bis p_r unterscheidet, Widerspruch. Es muss daher unendlich viele Primzahlen geben. □

Modulare Arithmetik

Sei n eine feste ganze Zahl. Wir definieren eine binäre Relation auf $\mathbb{Z}$

$$a \equiv b \mod n \quad \Leftrightarrow \quad n \mid (a - b) \quad \Leftrightarrow \quad n \mid (b - a)$$

und lesen: a ist **kongruent** zu b **modulo** n. Das bedeutet, dass a und b denselben Rest bei Division durch n haben.

Sei nämlich (in $\mathbb{Z}$)

$$a = q_1 n + r_1 \quad b = q_2 n + r_2$$

mit $0 \leq r_1, r_2 < n$ und o. B. d. A. $r_2 \leq r_1$, so gilt $a - b = qn + r$ mit $q = q_1 - q_2$, $0 \leq r = r_1 - r_2 < n$, also

$$n|(a-b) \quad \Leftrightarrow \quad r = 0 \quad \Leftrightarrow \quad r_1 = r_2$$

Somit ist $\equiv \mod n$ eine Äquivalenzrelation auf $\mathbb{Z}$. Man darf aber mit $\equiv \mod n$ weitgehend wie mit dem Gleichheitszeichen rechnen:

Lemma 5.8

$$\begin{aligned} a \equiv b \mod n,\ c \equiv d \mod n &\Rightarrow a + c \equiv b + d \mod n \\ a \equiv b \mod n &\Rightarrow -a \equiv -b \mod n \\ a \equiv b \mod n,\ c \equiv d \mod n &\Rightarrow ac \equiv bd \mod n \end{aligned}$$

Beweis. Gelte $n \mid (a-b)$ und $n \mid (c-d)$. Dann $n \mid (a-b+c-d) = (a+c) - (b+d)$ und $n \mid -(a-b) = -a - (-b)$ und $n \mid a(c-d) + (a-b)d = ac - bd$. □

Mit Hilfe dieses Lemmas können leicht die aus der Schule bekannten Teilbarkeitsregeln abgeleitet werden. Wir betrachten zum Beispiel die Regel, dass eine Zahl durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. Denn sei n eine natürliche Zahl und $\sum_{i=0}^{k} a_i \cdot 10^i$ ihre Darstellung im Dezimalsystem, dann gilt wegen $10 \equiv 1 \mod 3$

$$\sum_{i=0}^{k} a_i \cdot 1^i \equiv 0 \mod 3 \Rightarrow \sum_{i=0}^{k} a_i \cdot 10^i \equiv 0 \mod 3$$

Dabei steht links gerade die Quersumme.

Satz 5.9 *Ist eine Abstraktion $\mathbb{Z} \to \mathbb{Z}_n$ nach der Äquivalenzrelation $\equiv \mod n$ vorgegeben, d.h. eine surjektive Abbildung $a \mapsto \tilde{a} \in \mathbb{Z}_n$ mit*

$$\tilde{a} = \tilde{b} \quad \Leftrightarrow \quad a \equiv b \mod n$$

so wird $\mathbb{Z}_n$ zu einem kommutativen Ring, wenn die Operationen **repräsentantenweise** *erklärt sind.*

$$\tilde{a} + \tilde{c} = \widetilde{a+c},\ -\tilde{a} = \widetilde{-a},\ \tilde{a} \cdot \tilde{c} = \widetilde{a \cdot c}$$

Insbesondere sind $\tilde{0}$ und $\tilde{1}$ die neutralen Elemente bzgl. Addition und Multiplikation; $\mathbb{Z}_p$ ist ein Körper, wenn p eine Primzahl ist.

Beweis. Alle Ringeigenschaften von $\mathbb{Z}_n$ folgen aus den entsprechenden Eigenschaften von $\mathbb{Z}$, z. B. das Kommutativgesetz folgendermaßen:

$$\tilde{a} + \tilde{b} = \widetilde{a+b} = \widetilde{b+a} = \tilde{b} + \tilde{a},$$

oder dass $\tilde{0}$ das neutrale Element der Addition ist:

$$\tilde{a} + \tilde{0} = \widetilde{a+0} = \tilde{a}.$$

Sei nun $n = p$ prim. Jedes Element $\tilde{a} \neq \tilde{0}$ von $\mathbb{Z}_p$ erhält man mit einem a mit $0 < a < p$, insbesondere sind p und a teilerfremd. Nach Satz 5.3 gibt es ganze Zahlen x, y mit $ax + py = 1$, also $ax \equiv 1 \mod n$ und $\tilde{a} \cdot \tilde{x} = \widetilde{ax} = \tilde{1}$. □

Betrachten wir zwei Beispiele, den Ring $\mathbb{Z}_{12}$ und den Körper $\mathbb{Z}_7$. In $\mathbb{Z}_{12}$ haben wir die Elemente $\tilde{0}$ bis $\widetilde{11}$, der Bequemlichkeit halber schreiben wir 0 bis 11. Dann gilt

$$1 + 1 = 2,\ 3 + 4 = 7,\ 8 + 5 = 1, 4 \cdot 4 = 4, 3 \cdot 5 = 3$$

Ist das Ergebnis von Summe und Produkt kleiner als 12, dann rechnen wir also wie mit ganzen Zahlen. Wenn das Ergebnis größer ist, dann ermitteln wir den ganzzahligen Rest beim Teilen durch 12. Wir rechnen also wie mit den Stunden auf dem Ziffernblatt. In $\mathbb{Z}_{12}$ kann es passieren, dass wir zwei Elemente ungleich Null nehmen, deren Produkt gleich Null ist,

$$6 \cdot 2 = 0,$$

solche Elemente nennen wir **Nullteiler**. In einem Körper kann es keine Nullteiler geben, also auch nicht in $\mathbb{Z}_7$, weil dort jedes Element ungleich Null invertierbar ist, ein Inverses finden wir mit Hilfe von Satz 5.3. Was ist z. B. 4^{-1}?

$$ggT(7, 4) = ggT(7 - 4, 4) = ggT(4, 3) = ggT(4 - 3, 3) = 1$$

und $1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7$ (das hätte man auch raten können), also gilt $4^{-1} = 2$.

Aufgaben

1. Bestimme die Darstellung von 121 (in Dezimaldarstellung) zur Basis $2, 4$ und 5.
2. Berechne im Körper $\mathbb{Z}_7$ die Elemente $-4, 5 + 8, 5^{-1}$ und 3^4.
3. Zeige, dass es in einem Körper keine Nullteiler geben kann. Gib ein Beispiel eines Rings an, der zwar keine Nullteiler hat und das Gesetz $\forall xy.xy = yx$ erfüllt, aber doch kein Körper ist. So einen Ring nennen wir **Integritätsbereich**.

6 Konstruieren

Wir haben nun einige Methoden kennengelernt, um Eigenschaften von Strukturen zu beschreiben. Aber außer den natürlichen, ganzen und rationalen Zahlen kennen wir kaum Strukturen. Deshalb wollen wir in diesem Kapitel eine Konstruktion besprechen. Dabei greifen wir auf einen Trick zurück, der tief im zwanzigsten Jahrhundert verwurzelt ist, und der Mathematikern früherer Generationen nicht in den Sinn gekommen wäre: Wir benutzen die formale Sprache, die der Beschreibung unserer Struktur dient, als Grundbaustein unserer Konstruktion.

Wir wollen nun einige Konstruktionen durchführen, in der Tat sogar unendlich viele. Alle Konstruktionen laufen aber nach demselben Muster: Die Sprache L enthält zumindest die beiden binären Operationen $+, \cdot$, die einstellige Operation $-$ sowie die Konstanten 0 und 1.

Jetzt unterscheiden wir die folgenden drei Fälle:

1. Wir haben keine weiteren Symbole in L und betrachten die Menge aller Terme T der Signatur L mit der freien Variablen x. Wir definieren eine zweistellige Relation $\sim$ auf diesen Termen durch

$$r(x) \sim s(x) \Leftrightarrow \mathbb{Z} \models \forall x.r(x) = s(x)$$

   Zu T gehören zum Beispiel die Terme $r(x) = x \cdot x + x + x - x$, $s(x) = x \cdot x + x$, $t(x) = x + 1$ und es gilt

$r(x) \sim s(x)$ weil für jede ganze Zahl z die Gleichung $z \cdot z + z + z - z = z \cdot z + z$ erfüllt ist; andereseits gilt $r(x) \not\sim t(x)$, weil zum Beispiel für $x = 0$ dann $0 \cdot 0 + 0 + 0 - 0 = 0 < 0 + 1$ gilt.

2. Wir definieren L und T genau wie im esten Fall, definieren aber die Relation $\sim$ so, dass für ein vorgegebenes n

$$r(x) \sim s(x) \Leftrightarrow \mathbb{Z}_n \models \forall x.r(x) = s(x)$$

erfüllt ist. Damit stehen jetzt mehr Terme zueinander in Relation, zum Beispiel gilt nun:

$$\underbrace{1 + \cdots + 1}_{n-mal} = 0$$

3. Wir nehmen für jede rationale Zahl eine Konstante dazu; der Bequemlichkeit wegen benutzen wir dasselbe Symbol für eine rationale Zahl und die Konstante, die diese Zahl benennt (das ist übrigens das erste Beispiel für eine Signatur mit unendlich vielen Symbolen). Damit sind L und T festgelegt. Analog zu den beiden Fällen oben definieren wir $\sim$ durch

$$r(x) \sim s(x) \Leftrightarrow \mathbb{Q} \models \forall x.r(x) = s(x)$$

Wir haben zum Beispiel

$$(q + r) \cdot x \ \sim \ q \cdot x + r \cdot x$$

$$(q \cdot r) \cdot x \ \sim \ q \cdot r \cdot x$$

wobei q, r alle rationalen Zahlen durchlaufen.

Auch wenn die Definition der Relation $\sim$ in alle drei Fällen unterschiedlich war, sehen wir wegen

$$\begin{aligned} R &\models \forall x.s(x) = s(x) \\ R &\models \forall x.s(x) = t(x) \to t(x) = s(x) \\ R &\models \forall x.r(x) = s(x) \wedge s(x) = t(x) \to r(x) = t(x), \end{aligned}$$

dass $\sim$ eine Äquivalenzrelation ist; dabei ist R eine der Strukturen $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{Z}_n$ für eine natürliche Zahl $n > 1$. Damit können wir die Menge X der Äquivalenzklassen von T nach $\sim$ bilden, und wir erstellen nun eine neue Struktur A der Signatur L, deren Grundmenge gerade X ist und bei der wir die Operationen und Konstanten über die Repräsentanten definieren:

$$\begin{aligned} s(x)/\sim +^A t(x)/\sim &= (s(x) + t(x))/\sim \\ s(x)/\sim \cdot^A t(x)/\sim &= (s(x) \cdot t(x))/\sim \\ -^A(s(x)/\sim) &= -s(x)/\sim \\ 0^A &= 0/\sim \\ 1^A &= 1/\sim \\ q^A &= q/\sim \end{aligned}$$

Dabei ist q in der letzten Zeile eine beliebige rationale Zahl (diese Definition benötigen wir nur im dritten Fall). Wir

müssen zeigen, dass diese Definitionen wohldefiniert sind, also unabhängig von der Wahl eines Repräsentanten. Für die Addition gilt zum Beispiel: Seien Terme $s_0(x), s_1(x), t_0(x), t_1(x)$ gegeben und es gilt außerdem $s_0(x) \sim s_1(x)$ bzw. $t_0(x) \sim t_1(x)$, dann ist

$$\begin{aligned} s_0(x)/\sim +^A t_0(x)/\sim &= (s_0(x) + t_0(x))/\sim \\ &= (s_1(x) + t_1(x))/\sim \\ &= s_0(x)/\sim +^A t_0(x)/\sim . \end{aligned}$$

Für die Multiplikation und das Rechnen mit den Konstanten ist der Nachweis der Wohldefiniertheit analog.

Wir wollen unserer Konstruktion nun entsprechend einem der drei Fälle jeweils einen Namen geben:

1. der **Polynomring** $\mathbb{Z}[x]$ in der freien Variablen x über dem Ring der ganzen Zahlen,
2. der **Polynomring** $\mathbb{Z}_n[x]$ in der freien Variablen x über dem Ring der ganzen Zahlen modulo n,
3. der **Polynomring** $\mathbb{Q}[x]$ in der freien Variablen x über dem Körper der rationalen Zahlen.

Meinen wir eine dieser Strukturen, dann schreiben wir $R[x]$. Das Symbol R steht dann für einen der Ringe $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}$, den wir dann auch den **Koeffizientenring** und seine Elemente entsprechend **Koeffizienten** nennen. Ein **Polynom** ist ein Element eines Polynomrings. Wir schreiben in der Regel

Polynome in der Form $p(x), q(x), \ldots$ Wir geben also einen Hinweis auf den Namen der freien Variablen.

Ist der Koeefizientenring sogar ein Körper, das ist der Fall bei den rationalen Zahlen und den endlichen Körpern $\mathbb{Z}_p$ mit p einer Primzahl, dann schreiben wir auch gerne $K[x]$ anstelle von $R[x]$. Diese Strukturen wollen wir jetzt näher untersuchen:

Lemma 6.1 *Jedes Polynom $p(x) \in R[x]$ hat eine eindeutige Darstellung in* **Normalform**

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

mit $a_i \in R$. Die eindeutige Zahl n wird der **Grad** *des Polynoms p genannt.*

Beweis. Zwei Dinge müssen wir beweisen:

1. Eine solche Darstellung existiert.
2. Eine solche Darstellung ist eindeutig.

Den ersten Teil beweisen wir mit Hilfe von *Induktion über den Aufbau der Terme*; das klingt hochgestochen, besagt aber nichts anderes, als dass wir diese Eigenschaft für Variable und Konstanten und dann für zusammengesetzte Terme nachprüfen: Die Terme $0, 1, x$ bzw. q mit $q \in \mathbb{Q}$ sind schon in

Normalform. Angenommen, die Terme $s(x), t(x)$ sind schon in Normalform, also etwa

$$s(x) = \sum_{i=0}^{n} a_i x^i \text{ und } t(x) = \sum_{i=0}^{m} b_i x^i.$$

O. B. d. A. nehmen wir an, dass $n \geq m$ gilt. Wir vereinbaren, dass $b_{m+1} = \cdots = b_n = 0$, falls $n > m$, dann gilt für die Summe

$$s(x) + t(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i \sim \sum_{i=0}^{n} (a_i + b_i) x^i$$

und für das Produkt

$$s(x) \cdot t(x) = \left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{i=0}^{m} b_i x^i \right) \sim \sum_{j=0}^{n+m} c_j x^j$$

mit $c_j = \sum_{i+k=j} a_i b_k$. Das sollte jeden an den Beweis über die eindeutige b-ale Entwicklung einer natürlichen Zahl erinnern, was es uns erlaubt, hier knapp zu sein.

Nun zur Eindeutigkeit: Zunächst bemerken wir, dass es ausreichend ist, die Eindeutigkeit der Darstellung des Nullpolynoms zu zeigen. Denn hätten wir zwei Darstellungen

$$\sum a_i x^i \neq \sum b_j x^j$$

eines Polynoms, dann sind 0 und $\sum(a_i - b_i)x^i$ zwei Darstellungen des Nullpolynoms. Wir zeigen zunächst $x^n \not\sim 0$. Wie zeigt man, dass zwei Terme nicht äquivalent sind? Wir geben einen weiteren Ring an, in dem alle vorgegebenen Gleichungen gelten, aber eben nicht $x^n \sim 0$. Dieser Ring ist R selbst, wobei $x^R = 1$ sein soll. Damit haben wir $1^n = 1 \not\sim 0$. Analog sehen wir $r \cdot x^n \not\sim 0$ für jedes Element $r \neq 0$ aus R oder $x^n - x^m \not\sim 0$ für $n > m$; ansonsten wäre $x^n \sim x^m$ und $x^{n-m} \sim 1$ (was wir diesmal mit der Interpretation $x^R = 0$ widerlegen können). Letztendlich erhalten wir $\sum_{i=0}^{n} a_i x^i \not\sim 0$, wenn nur ein Koeffizient ungleich Null ist. □

Das eben bewiesene Lemma erschließt uns nun folgenden Satz:

Satz 6.2 *Der Polynomring $R[x]$ ist, wie der Name schon verrät, ein kommutativer Ring. Für einen Körper K ist $K[x]$ sogar ein Integritätsbereich, das heißt, der Ring hat keine Nullteiler.*

Beweis. Die eindeutige Darstellung erlaubt es, alle Ringeigenschaften von R auf $R[x]$ zu übertragen; Zum Beispiel die Kommutativität der Addition:

$$\begin{aligned}\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i &= \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i \\ &= \sum_{i=0}^{\max\{m,n\}} (b_i + a_i) x^i \\ &= \sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{n} a_i x^i.\end{aligned}$$

Ist K ein Körper und $p, q \in K[x]$ ungleich dem Nullpolynom, dann zeigt die Formel für die Multiplikation, dass auch mindestens einer der Koeffizienten ungleich Null sein muss. Das zeigt, dass wir einen Integritätsbereich haben. □

Korollar 6.3 *Ist K ein Körper, sind $p(x), q(x)$ Polynome aus $K[x]$ und ist der Grad von p kleiner gleich dem Grad von q, dann existieren eindeutige Polynome $r, s \in K[x]$, sodass $q = sp + r$ und r einen kleineren Grad als p hat.*

Beweis. Im Gegensatz zu dem analogen Beweis für die Teilbarkeit mit Rest bei den ganzen Zahlen können wir hier den Rest explizit angeben. Die Idee ist recht einfach: Das Polynom mit dem kleineren Grad multiplizieren wir jeweils mit Potenzen von x und passend gewählten Koeffizienten und ziehen diese sukzessive von dem Polynom mit dem größeren Grad ab. Im konkreten Fall sieht das so aus: Sei $q(x) = \sum_{i=0}^{n} a_i x^i$ und $p(x) = \sum_{i=0}^{m} b_i x^i$ mit $m < n$. Dann ist

$$r = \sum_{i=0}^{n} a_i x^i - \frac{a_n}{b_m} x^{n-m} \sum_{i=0}^{m} b_i x^i - \frac{b_m a_{n-1}}{a_n b_{m-1}} x^{n-m-1} \sum_{i=0}^{m} b_i x^i - \cdots - \frac{b_m \dots a_m}{a_n \dots b_k} \sum_{i=0}^{m} b_i x^i$$

ein Polynom vom Grade kleiner m. Dabei haben wir stillschweigend vorausgesetzt, dass die Koeffizienten $a_n, b_m, \dots$ alle ungleich Null sind. Sollte einer dieser Koeffizienten gleich Null sein, dann kann der entsprechende Summand weggelassen werden. □

Teilen mit Rest ist also wie bei den ganzen Zahlen möglich.

Beispiel. Wir berechnen in $\mathbb{Q}[x]$ den Teiler mit Rest von $x^4 + x^3 + x$ durch $x^2 - 1$:

$$\begin{aligned} x^4 + x^3 + x &= x^2(x^2 - 1) + x^3 + x^2 + x \\ &= x^2(x^2 - 1) + x(x^2 - 1) + x^2 + 2x \\ &= x^2(x^2 - 1) + x(x^2 - 1) + (x^2 - 1) + 2x + 1 \end{aligned}$$

Damit $x^4 + x^3 + x = (x^2 - 1)(x^2 + x + 1) + 2x + 1$ oder anders ausgedrückt, $x^4 + x^3 + x$ geteilt durch $x^2 - 1$ ergibt $x^2 + x + 1$ mit Rest $2x + 1$.

Für ein Polynom $p \in R[x]$ nennen wir ein Element $a \in R$ mit $R[x] \models p[a] = 0$ eine **Nullstelle** von p.

Korollar 6.4 (Abspaltung) *Ist $p(x)$ ein Polynom vom Grad $n > 0$ und $a \in K$ eine Nullstelle, so gibt es ein (eindeutig bestimmtes) Polynom $q(x) \in K[x]$ vom Grad $n - 1$ so, dass $p(x) = q(x)(x - a)$.*

Beweis. Division in $K[x]$ ergibt $p(x) = q(x)(x-a)+b$ mit konstantem $b \in K$. Einsetzen ergibt

$$0 = p[a] = q[a](a-a) + b = b. \quad \square$$

$x - a$ heißt der **Linearfaktor** zur Nullstelle a. Hat man $p(x) = q(x)(x-a)^k$ mit $q[a] \neq 0$ (und das ist eindeutig bestimmt), so ist a eine k-**fache Nullstelle** von $p(x)$.

Lemma 6.5 *Ein Polynom von Grad $n > 0$ hat höchstens n verschiedene Nullstellen.*

Beweis. Nach $n-1$ Abspaltungen kann nur noch ein Linearfaktor übrigbleiben. Daraus folgt die Behauptung. $\square$

Wie bei ganzen Zahlen folgt (der Grad übernimmt die Rolle des Betrags):

Satz 6.6 (Bezout) *Zu $p(x), q(x) \in K[x]$ gibt es bis auf Multiplikation mit einem Element aus $K \setminus \{0\}$ genau einen größten gemeinsamen Teiler und $r(x), s(x) \in K[x]$ mit*

$$ggT(p(x), q(x)) = p(x)r(x) + q(x)s(x)$$

und r hat einen kleineren Grad als q sowie s einen kleineren Grad als p. Diese bestimmt man mit dem Euklidischen Algorithmus für Polynome.

Beispiel. Wir berechnen den größten gemeinsamen Teiler von x^4+1 und x^3+x in $\mathbb{Q}[x]$:

$$\begin{aligned} ggT(x^4+1, x^3+x) &= ggT(x^4+1-x^4-x^2, x^3+x) \\ &= ggT(x^3+x, -x^2+1) \\ &= ggT(x^3+x-x^3+x, -x^2+1) \\ &= ggT(-x^2+1, 2x) \\ &= ggT(-x^2+1+x^2, 2x) \\ &= 1 \end{aligned}$$

also

$$\begin{aligned} 1 &= 1-x^2+x^2 \\ &= (1-x^2)+\frac{1}{2}x(x^3+x-x^3+x) \\ &= (1+\frac{1}{2}x^2)(1-x^2)+\frac{1}{2}x(x^3+x) \\ &= (1+\frac{1}{2}x^2)((x^4+1)-x(x^3+x))+\frac{1}{2}x(x^3+x) \\ &= (1+\frac{1}{2}x^2)(x^4+1)-\frac{1}{2}(x^3+x)(x^3+x) \end{aligned}$$

Ein nicht konstantes Polynom $p(x)$ heißt **unzerlegbar** oder **irreduzibel**, wenn in jeder Zerlegung $p(x)=q(x)r(x)$ einer der Faktoren konstant ist. Ein nicht konstantes Polynom $p(x)$ ist ein **Primpolynom**, wenn

$$p(x)|(q(x)r(x)) \;\Rightarrow\; p(x)|q(x) \text{ oder } p(x)|r(x)$$

Wie bei den ganzen Zahlen folgt:

Satz 6.7 *Die unzerlegbaren Polynome sind gerade die Primpolynome. Jedes nichtkonstante Polynom $f(x)$ hat eine Darstellung*

$$f(x) = p_1(x) \cdot \cdots \cdot p_n(x).$$

Diese Darstellung ist bis auf die Reihenfolge und Multiplikation mit Elementen aus $K \setminus \{0\}$ eindeutig.

Konstruktion von Körpern

Im Körper $\mathbb{Q}$ gibt es keine Lösung für die Gleichung

$$x^2 = 2.$$

Das wusste schon Euklid. Denn hätten wir eine solche Lösung q, dann könnten wir schreiben

$$q = \frac{m}{n} \text{ mit } m, n \in \mathbb{Z} \text{ und } ggT(m, n) = 1.$$

Daraus folgt $m^2 = 2n^2$. Damit wären m^2 und auch m gerade Zahlen, also $m = 2m'$. Es folgt $4m'^2 = 2n^2$ und daraus, dass auch n gerade wäre. Also $ggT(m, n) \geq 2$, ein Widerspruch.

Trotzdem wäre es nett, einen Körper L zu finden, in dem diese Gleichung eine Lösung hat und in dem $\mathbb{Q}$ steckt, das heißt, wir haben eine Einbettung $\phi : \mathbb{Q} \to L$. So einen Körper konstruieren wir uns nun.

Satz 6.8 *Ist $p(x)$ in $K[x]$ fest gewählt, so erhält man eine Kongruenzrelation auf $K[x]$ mit*

$$f(x) \sim_{p(x)} g(x) \;\Leftrightarrow\; p(x)|(f(x) - g(x))$$

Eine Abstraktion $K[x] \xrightarrow{\pi} K[x]/p(x)$ liefert auf $K[x]/p(x)$ die Struktur eines Integritätsbereichs, wenn die Operationen repräsentantenweise erklärt werden, also

$$\pi(p) + \pi(q) = \pi(p + q),\ \pi(p) \cdot \pi(q) = \pi(p \cdot q).$$

Das Element $a = \pi(x)$ ist eine Nullstelle von $p(x)$ in $K[x]/p(x)$. Die Elemente dieser Struktur haben eine eindeutige Darstellung

$$b_{n-1}a^{n-1} + \ldots b_1 a + b_0,$$

wobei n der Grad von p ist und $b_i \in K$. Der Körper K wird durch $k \mapsto \pi(k)$ eingebettet. Der Ring $K[x]/p(x)$ ist ein Körper genau dann, wenn $p(x)$ Primpolynom ist.

Beweis. Dass man eine Kongruenzrelation hat, sieht man wie in dem Beispiel der Kongruenzen auf $\mathbb{Z}$. Analog folgt auch die Tatsache, dass $K[x]/p(x)$ ein Integritätsbereich ist.

Um zu zeigen, dass K in $K[x]/p(x)$ eingebettet ist, müssen wir nachweisen, dass π eingeschränkt auf K injektiv ist: Sind aber k, b zwei Elemente von K bzw. die entsprechenden konstanten Polynome, dann kann $\pi(k) = \pi(b)$ nur dann gelten, wenn $\pi(k - b) = \pi(0)$ ist. Das Polynom $p(x)$ kann

aber nur dann das konstante Polynom $k - b$ teilen kann, wenn $k - b = 0$ ist.

Als nächstes widmen wir uns der eindeutigen Darstellung der Elemente von $K[x]/p(x)$. Dafür zeigen wir durch Induktion über den Grad, dass es für jedes Polynom $f(x)$ ein $g(x)$ von Grad kleiner n gibt mit $\pi(f(x)) = \pi(g(x))$. Es gibt eine Darstellung $f(x) = h(x)x + c$, wobei h einen kleineren Grad als f hat und c konstant ist. Also gibt es $k(x) = \sum_{i=0}^{n-1} c_i x_i$ von Grad $< n$ mit $\pi(h(x)) = \pi(k(x))$. Aus $p(x) = \sum_{i=0}^{n} a_i x^i$ folgt $x^n = a_n^{-1} \sum_{i=0}^{n-1} a_i x^i$, also

$$k(x)x + c = c_{n-1}a_n^{-1} \sum_{i=0}^{n-1} a_i x^i + \sum_{i=1}^{n-1} c_{i-1} x^i + c$$

was wegen $\pi(f(x)) = \pi(k(x)x + c)$ die Behauptung beweist. Eindeutigkeit: Weil f, g einen Grad kleiner n haben und $\pi(f) = \pi(g)$ folgt $p|(f - g)$ und $f - g$ hat auch einen Grad kleiner n, also $f - g = 0$. Ist $p(x)$ prim und $p(x) \not| f(x)$, so erhält man man das Inverse von $\pi(f(x))$ nach Bezout. □

Zum Beispiel ist $\mathbb{Q}[x]/x^2 - 2$ ein Körper, weil wir uns oben überlegt haben, dass die Gleichung $x^2 = 2$ keine Lösung in $\mathbb{Q}$ hat und damit das Polynom $x^2 - 2$ irreduzibel ist. Nach Satz 6.8 können wir uns die Elemente dieses Körpers als Polynome $q + rx$ mit $q, r \in \mathbb{Q}$ auffassen, wobei wir modulo $x^2 - 2$ rechnen. Das Element $\pi(x)$ ist nun aber eine Lösung der Gleichung $x^2 - 2$, und wir definieren deswegen $\sqrt{2} = \pi(x)$. Damit bekommen die Elemente des Körpers die Gestalt $q + r\sqrt{2}$.

Wir haben somit die Möglichkeit, die rationalen Zahlen um Wurzeln anzureichern. Was wir hier gemacht haben, ist, wie schon gesagt, eine Idee des zwanzigsten Jahrhunderts. Anstatt eine Lösung zu *suchen*, *konstruieren* wir eine solche.

Wenn wir nur einen Integritätsbereich R als Koeffizientenring haben, geht das meiste noch durch, wir erhalten aber im allgemeinen keinen Körper. Zum Beispiel ist $\mathbb{Z}[x]/(x^2+1)$ ein Ring aber kein Körper.Wir schreiben i für $\pi(x)$ und schreiben auch entsprechend $\mathbb{Z}[i]$ für diesen Ring und nennen ihn den Ring der ganzen **Gaußschen Zahlen**. In diesem Ring hat ein Element der Form $x^2 + y^2$ plötzlich eine Zerlegung der Form

$$x^2 + y^2 = (x + iy)(x - iy)$$

Zum Beispiel gilt

$$5 = 4 + 1 = (2 + i)(2 - i),$$

5 ist damit in diesem Ring keine Primzahl mehr.

Aufgaben

1. Bestimme die Normalform von $(x-1)^4$ in $\mathbb{Z}[x], \mathbb{Q}[x]$ und $\mathbb{Z}_2[x]$.
2. Zeige, dass die Gleichung $x^2 = -1$ in $\mathbb{Q}$ keine Lösung hat. Daraus folgt, dass $\mathbb{Q}(x)/(x^2+1)$ ein Körper ist.
3. Bestimme das Inverse von x^2 im Polynomring $\mathbb{Q}[x]/(x^3+x+1)$.
4. Zeige, dass $\mathbb{Z}_2[x]/x^2+x+1$ ein Körper ist. Wieviele Elemente hat er?
5. Zerlege die Zahl 6 im Ring $R = \mathbb{Z}[x]/(x^2+5)$. Wieviele Möglichkeiten gibt es?

7 Lösungen und weitere Literatur

Lösungen zu den Übungsaufgaben

Zählen

1. In beiden Tabellen sind verschiedene Symmetrien zu finden: Zum Beispiel steht in Zeile i, Spalte j dasselbe wie in Zeile j, Spalte i. Dies gilt, weil Addition und Multiplikation *kommutativ* sind. In der Additionstabelle stehen auf einer Diagonalen von links unten nach rechts oben immer dieselben Einträge, denn $n + m = (n - 1) + (m + 1)$.

2. Wir haben die folgenden beiden Rechnungen:

$$\begin{array}{cccc} & * & @ & ! \\ & & @ & @ \\ \hline & * & \% & \# \end{array} \qquad \begin{array}{cccccccc} & & & ! & @ & ! & \times & ! & @ & ! \\ \hline & & & ! & @ & ! & & & & \\ & & @ & \% & @ & & & & & \\ & ! & @_! & ! & & & & & & \\ \hline & ! & * & \square & \% & ! & & & & \end{array}$$

3. Das Einmaleins und Einspluseins:

+	b	c	d
b	c	d	ba
c	d	ba	bb
d	ba	bb	bc

×	b	c	d
b	b	c	d
c	c	ba	bc
d	d	bc	cb

4. Eine wiederholte Multiplikation entspricht dem Potenzieren. Eine genaue Definition dieser Operation wird im vierten Kapitel gegeben.

Strukturieren

1. Während $\{1, 2, 3\}$ die Menge mit den Elementen $1, 2$ und 3 ist, ist $[1, 2, 3]$ die Liste mit den Einträgen $1, 2$ und 3, also eine Abbildung $f : 3 \to \{1, 2, 3\}$. Die Listen $[1, 2]$, $[1, 2, 2]$ und $[2, 2, 1]$ sind alle voneinander verschieden, aber $[\{1, 2\}, 2] = [\{2, 1\}, 2]$, da $\{1, 2\} = \{2, 1\}$ und $2 = 2$. Letztendlich gilt $[a_1, \ldots, a_n] = [b_1, \ldots, b_m]$, falls $m = n$ und $a_i = b_i$ für $1 \leq i \leq m$.

2. (a) Ist $a \in X \setminus (A \cup B)$, dann gilt $a \in X$ und $a \notin A \cup B$, also $a \in X$ und $a \notin A$ und $a \notin B$. Daraus folgt $a \in (X \setminus A) \cap (X \setminus B)$. Ist b ein Element der letzteren Menge, dann liegt b in X aber weder in A noch in B, also nicht in der Vereinigung $A \cup B$. Also $b \in X \setminus (A \cup B)$.

   (b) Liegt $a \in A$, dann liegt a nicht in $X \setminus A$, damit aber wiederum in $X \setminus (X \setminus A)$. Liegt b in $X \setminus (X \setminus A)$, dann nicht in $X \setminus A$, dann aber in A. Damit folgt die gegebene Gleichung.

3. Die Relation "x ist Bruder von y" ist weder reflexiv noch symmetrisch, aber immerhin transitiv. Die Relation "x und y haben die gleichen Vorfahren" ist tatsächlich eine Äquivalenzrelation. Diese hat übrigens eine einzige Äquivalenzklasse unter der Voraussetzung, dass wir alle von Adam und Eva abstammen. Die Relation "x liebt y" ist nicht transitiv, tragischerweise oft nicht symmetrisch und nicht reflexiv.

4. Sei $x \in X$, Dann $f(g(x)) = (f \circ g)(x) = (f \circ h)(x) = f(h(x))$ und wegen der Injektivität von f auch $g(x) = h(x)$.

   Die analoge Aussage für surjektive Funktionen: Ist $f : X \to Y$ surjektiv und sind $g : Y \to Z$ und $h : Y \to Z$ Abbildungen mit $g \circ f = h \circ f$, so folgt $g = h$.

   Beweis. Sei $y \in Y$. Wegen der Surjektivität von f gibt es $x \in X$ mit $f(x) = y$. Es folgt $g(y) = (g \circ f)(x) = (h \circ f)(x) = h(y)$. □

5. Die Abbildung $\phi : X \times X \to X^2$ definiert durch

$$\phi([a_1, a_2]) = (a_1, a_2)$$

   ist, wie leicht zu sehen ist, bijektiv.

Formalisieren

1. $L = \{a^n b^n c^n : n \in \mathbb{N}\}$
2. $(r+t)^{\mathbb{N}}[1,0] = 3,\ (r \cdot t)^{\mathbb{N}}[0,1] = 0,\ ((r+r) \cdot t)^{\mathbb{N}}[1,1] = 8$
3. Es gilt $\{x \in X : x \notin x\} = X$.

Abstrahieren

1. • Kein Homomorphismus, denn es gilt z. B.

$$\phi(2) = 4 \neq 2 = \phi(1) + \phi(1).$$

- Ein Homomorphismus bzgl. $(+, -, 0)$, denn für feste aber beliebige ganze Zahlen z, z' gilt

$$\begin{aligned} \phi(z + z') &= -(z + z') = -z + (-z') = \phi(z) + \phi(z') \\ \phi(-z) &= -(-z) = z = -\phi(z) \\ \phi(0) &= -0 = 0, \end{aligned}$$

  aber kein Homomorphismus bzgl. $<$ wegen $0 < 1$ und $-1 = \phi(1) < 0$.

- Ein Homomorphismus, denn

$$\psi(1 + 1) = \tilde{4} = \tilde{0} = \psi(1) + \psi(1)$$

  Analog folgen die restlichen Gleichungen.

2. Induktionsanfang: Ist $n = 1$, dann haben wir ein 2×2-Badezimmer mit einem Abfluss. Es ist offensichtlich, dass dort genau eine Fliese hereinpasst.

   Induktionsschritt von n nach $n + 1$. Unser Badezimmer der Seitenlänge 2^{n+1} kann in vier Quadrate der Seitenlänge 2^n zerlegt werden. In einem dieser Quadrate liegt der Abfluss, und wir können dieses Quadrat nach Induktionsannahme kacheln. Die restlichen drei Quadrate haben keinen Abfluss, aber wir können an der Stelle, an der alle vier Quadrate anstoßen an das schon gekachelte Quadrat eine Fliese anlegen, sodass in jedem der verbliebenen Quadrate genau ein Feld gekachelt ist. Jetzt können wir uns einbilden, dass dieses Feld jeweils ein Abfluss wäre, und nach Induktionsannahme diese drei Quadrate kacheln.

3. Sei $M = \mathbb{N}, h = \mathsf{succ}^{\mathbb{N}}$ und $a = 0^{\mathbb{N}}$. Wäre dadurch eine Funktion f eindeutig festgelegt, dann wäre

$$\begin{aligned} f(0) &= 0^{\mathbb{N}} \\ f(1) &= 1^{\mathbb{N}} \\ \vdots &\quad \vdots \\ f(\mathsf{succ}(7)) &= \mathsf{succ}^{\mathbb{N}}(7) = 8 \end{aligned}$$

Aber in A gilt $\mathsf{succ}(7) = 0$ und $f(0) = 0^{\mathbb{N}} \neq 8$, ein Widerspruch.

Rechnen

1. Zur Basis 2 haben wir die Darstellung 1111001, zur Basis 4 die Darstellung 1321 und zu 5 die Darstellung 441.

2. $-4 \equiv 3 \mod 7$, $5+8 = 13 \equiv 6 \mod 7$, $5 \cdot 3 = 15 \equiv 1 \mod 7$, also gilt $5^{-1} = 3$, $3^4 = 9 \cdot 9 \equiv 2 \cdot 2 \mod 7 = 4$.

3. Angenommen, $a \neq 0$ ist ein Nullteiler im Körper K, d. h., es existiert ein Element $b \neq 0$ mit $ab = 0$. dann gilt aber

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0,$$

ein Widerspruch. Der Ring der ganzen Zahlen ist ein Integritätsbereich aber kein Körper.

Konstruieren

1. Wir rechnen $(x-1)^4 = (x^2-2x+1)^2 = x^4+4x^2-1$. Damit haben wir die Normalform x^4+4x^2-1 in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ und wegen $4 \equiv 0 \mod 2$ bzw. $-1 \equiv 1 \mod 2$ die Normalform x^4+1 in $\mathbb{Z}_2[x]$.

2. Gäbe es eine Lösung a dieser Gleichung, dann wäre

$$a > 0, a < 0 \text{ oder } a = 0.$$

   In allen drei Fällen folgt $a^2 = -1 \geq 0$. Aber aus $0 < 1$ folgt $-1 < 1 + (-1) = 0$, ein Widerspruch.

3. Es gilt

$$x^3 + x + 1 = x(x^2+1) + 1,$$

   also $(x^2)^{-1} = x^2 + 1$.

4. Wäre x^2+x+1 zerlegbar, so ein Produkt zweier Linearfaktoren und es gäbe eine Nullstelle $a \in \mathbb{Z}_2$. Aber 0 und 1 sind beide keine. Nach Satz 6.8 erhalten wir einen Körper. Dessen Element sind $0, 1, x$ und $x+1$, und es wird modulo x^2+x+1 gerechnet.

5. Es gibt mindestens zwei Möglichkeiten:

$$6 = 3 \cdot 2 = (1+i\sqrt{5})(1-i\sqrt{5}),$$

   dabei ist i Nullstelle des Polynoms x^2+1 und $\sqrt{5}$ Nullstelle des Polynoms x^2-5.

Literatur

Für diejenigen, die bald ein Studium beginnen, möchte ich keine weitere Literatur empfehlen. In den nächsten Wochen werdet ihr mehr Empfehlungen, als euch lieb ist, bekommen.

Für diejenigen, die auf eigener Faust auf mathematischen Pfaden wandeln wollen, hier drei Empfehlungen:

Eine unterhaltsame Bettektüre:

> Der Zahlenteufel von Hans M. Enzensberger, Deutscher Taschenbuch Verlag, 1999.

Ein Einblick in die Geometrie, die wir hier vollkommen vernachlässigt haben, und viele interessante historische Anmerkungen:

> Matrizen, Geometrie, lineare Algebra von Peter Gabriel, Birkhäuser Verlag, Basel, 2012.

Tiefere Einsichten in Algebra und Zahlentheorie, für die man nun gerüstet sein sollte:

> Zahlentheorie: eine Einführung in die Algebra von Armin Leutbecher, Springer Verlag, Berlin, 2013.

Index

+, 10
$K[x]$, 98
$R[x]$, 98
$\cap$, 20
$\cup$, 21
$\emptyset$, 20
$\equiv$, 90
$\in$, 18
$\setminus$, 20
$\subset$, 19
$\subseteq$, 19
$\times$, 13
$\mathcal{P}(M)$, 34
Äquivalenzklasse, 23
Äquivalenzrelation, 23
Übertrag, 11

Abbildung, 25
  identische, 25
  partielle, 25
Ableitung
  direkte, 47
Abstraktion, 32
addieren, 10
Algorithmus, 12
Allrelation, 22
Alphabet, 45
Anzahl, 5, 35
Aussage, 56
Auswertung, 52
Axiom, 57
Axiomenschema, 58

Basis, 16
Bild, 25
Binärsystem, 17
Bindungsstärke, 54
Block, 6
Buchstabe, 46

Darstellung
  b-ale, 78
Definitionsbereich, 25
Dezimalsystem, 17
Division mit Rest, 83

Einbettung, 62
Einmaleins, 16
Einspluseins, 16
Element, 18
Elementbeziehung, 18
endlich, 35

falsch, 53

Formel, 54
    atomare, 52
Funktion, 25
funktional, 25

gleichmächtig, 33
Gleichung, 40
Glied einer Liste, 37
Grad, 99
Grammatik, 46
Grundmenge, 39
Gruppe, 80
    abelsche, 80

Homomorphismus, 62

induktiv, 34
Infixnotation, 51
injektiv, 29
Integritätsbereich, 94
Irreflexivität, 36
isomorph, 64
Isomorphismus, 64

Körper, 81
Koeffizienten, 98
Koeffizientenring, 98
Komplement, 20
Komponente
    erste, zweite, 22
kongruent, 91
Kongruenzrelation, 42
Konstante, 50
Korollar, 27

leere Menge, 20
Lemma, 27
Linearfaktor, 104
Liste, 37
    leere, 37

Mächtigkeit, 35
Menge, 18
modulo, 90
multiplizieren, 13

Nachfolgerfunktion, 38
Normalform, 99
Nullstelle, 103
    k-fache, 104
Nullteiler, 93

Operation
    n-stellige, 38
Ordnung
    lineare, 36

Paar, 22
Polynom, 98
Polynomring, 98
Potenzmenge, 34
Präfixnotation, 51

Primzahl, 89
Produkt, 13

Regel, 46
Relation, 22
  n-stellige, 38
Repräsentant, 32
Rest, 83
Ring, 81
Robinson-Arithmetik, 56

Satz, 27, 56
Schnitt, 20
Signatur, 57
Sprache, 46
  abgeleitete, 47
  formale, 45
Startzeichen, 46
Struktur, 38
Summe, 10
surjektiv, 30
Symbol, 7

teilen, 83
Teiler
  echter, 88
  gemeinsamer, 85
  gröster gemeinsamer, 85
Teilmenge, 19
  echte, 19
Terminalalphabet, 46
Theorem, 27

Unbekannte, 40
Ungleichung, 40
unzerlegbar, 88

Variable, 50
  der atomaren Formel, 52
  des Terms, 52
  freie, 55
Vereinigungsmenge, 21

wahr, 53
Wertebereich, 25
Wohldefiniertheit, 32
Wort, 45
  leeres, 46

Zahl
  Gaussche, 109
  natürliche, 39
  negative, 42
  positive, 42
Zielmenge, 25