Mathematik für Informatiker 1

Vorlesungsskriptum
Wintersemester 2011/2012

Gabriele Kern-Isberner
Bernhard Steffen
Oliver Rüthing

Fakultät für Informatik
Technische Universität Dortmund
2011

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Motivation

Ohne Zweifel ist die Mathematik neben der Elektrotechnik einer der Grundpfeiler der Informatik. So gab es z.B. noch bis in die neunziger Jahre hinein in Aachen einen Lehrstuhl mit der Bezeichnung "Praktische Mathematik, insbesondere Informatik". Inzwischen hat sich die Informatik jedoch emanzipiert und wird als eigenständiges Fach akzeptiert. Das bedeutet jedoch keinesfalls, dass ihre Wurzeln in der Mathematik dadurch irrelevant geworden sind. Vielmehr sind gerade die wohlverstandenen Grundlagen der Informatik durch einen starken mathematischen Kern gekennzeichnet, und viele konzeptuelle Vorgehensmuster (insbesondere, aber nicht nur) der theoretischen Informatik sind der Mathematik entlehnt. Auf der anderen Seite gibt es auch klassische mathematische Probleme, die am Ende nur mit Hilfe der Informatik gelöst werden konnten. Ein prominentes Beispiel ist das Vierfarbenproblem (`http://de.wikipedia.org/wiki/Vier-Farben-Satz`), dessen Lösung bis heute auf Hilfsmitteln der Informatik beruht. Durch diese enge Verzahnung hat die Informatik ihrerseits der Mathematik ihren Stempel aufgedrückt. Beispiele hier sind Bereiche der diskreten Mathematik, die konstruktive Logik und weite Teile der Numerik.

Ziel der Vorlesung ist es, den Wert dieser Verzahnung greifbar zu machen und ein Gefühl dafür zu vermitteln, wann welche mathematischen Vorgehensmuster vorteilhaft eingesetzt werden können. Gleichzeitig sollen die mathematischen Verfahrensmuster auch dazu dienen, die Natur der Informatik etwas besser zu verstehen: Was sind ihre Besonderheiten z.B. gegenüber der Mathematik.

Zu diesem Zweck werden insbesondere die folgenden fünf Beispiele im Einzelnen diskutiert werden:

Der Euklidische Algorithmus für Berechnung des GGT. Informell ausgedrückt, zieht der Euklidische Algorithmus (`http://de.wikipedia.org/wiki/Euklidischer_Algorithmus`) solange ein maximales Vielfaches der kleineren Zahl b von der größeren Zahl a ab, bis schließlich b Null wird. Der GGT ist dann a. Abbildung 1.1 illustriert dies mit $a = 65$, $b = 50$ worauf $a = 50$, $b = 15$ und schließlich $a = 15$ und $b = 5$ folgt. Der Wert von b passt nun dreimal in a worauf der

Algorithmus mit $b = 5$, dem größten gemeinsamen Teiler von 65 und 50, terminiert.

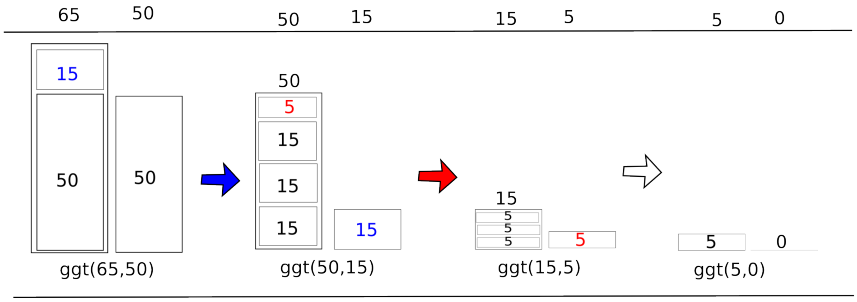


Abbildung 1.1: Illustration des GGT

Auf den ersten Blick ist hier keineswegs klar, warum dieser über 2200 Jahre alte Algorithmus tatsächlich den GGT seiner beiden Eingabeparameter berechnet. Klar wird dies, sobald man die dem Algorithmus unterliegende **Invariante** erkennt: Die Subtraktion ändert den zu berechnenden GGT nicht!

Invarianten sind der zentrale Schlüssel zum Verständnis von Programmschleifen und Rekursion. Diese Erkenntnis ist in vollem Einklang mit Archimedes Intuition: "Gebt mir einen Punkt auf dem ich still stehe, und ich werde die Welt aus den Angeln heben". Das Verständnis als Invarianten als archimedische Punkte (`http://de.wikipedia.org/wiki/Archimedischer_Punkt`) ist ein guter Leitfaden. Er hilft iterative und rekursive Programme zu beherrschen, Induktionsbeweise zu führen und und evolutionäre Programmentwicklung zu strukturieren, alles durch die Beantwortung der Frage "Was ist beständig im Wandel".

Türme von Hanoi. Ausgehend von drei unterschiedlich großen Scheiben auf dem ersten von drei Stapeln, sollen diese durch einzelne Bewegung in die gleiche Position auf dem dritten Stapel gebracht werden. Es dürfen dabei jedoch nur kleinere Scheiben auf größere gelegt werden (in der Ausgangsposition sind diese auch so angeordnet).

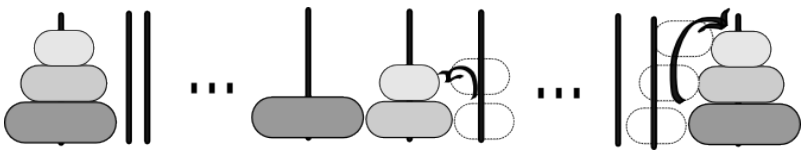


Abbildung 1.2: Türme von Hanoi

Frage: Wie viele Schritte benötigt man, um den Turm regelgerecht und vollständig zu 'verschieben'?

Während im vorigen Beispiel der Algorithmus vorgegeben war, kommt hier ein wesentliches Stück Informatik hinzu: Die **Entwicklung des Algorithmus**. Dabei ist darauf zu achten, dass dieser Algorithmus so strukturiert ist, dass er z.B. einer Analyse bzgl. der Schrittzahl zugänglich ist. Wie im vorigen Beispiel steht dabei der zugehörige archimedische Punkt (die Invariante) im Vordergrund.

Abbildung 1.3: Suchen eines Elements in einer Menge

Finden eines Objektes in einer Menge. Wie viele Objekte muss man im ungünstigsten Fall aus einer Menge herausnehmen, um nachzuprüfen, ob ein vorgegebenes Element in dieser Menge liegt? Ähnlich wie im vorigen Problem ist das Lösungsverfahren auch hier nicht vorgegeben.

Offensichtlich gibt es ein triviales Verfahren, das aber erfordert, dass man alle Elemente aus der Menge herausgenommen haben muss, bevor man entscheiden kann, dass das in Frage stehende Element nicht in der Menge liegt.

Geht das besser?

Das liegt an den Spielregeln. Darf ich mir die Menge selbst organisieren, d.h. darf ich die Art und Weise, wie die Elemente abgelegt werden, selbst bestimmen? Sofern das möglich ist, geht es viel besser. Als Anhaltspunkt denke man an ein Telefonbuch und überlege sich, wie es möglich ist, die gesuchte Telefonnummer unter Tausenden von Einträgen schnell finden zu können.

Dieses Beispiel illustriert einen wesentlichen Informatik-typischen Aspekt: Das Ausnutzen von **Modellierungsspielräumen**: Man kann (in Grenzen) seine Aufgabenstellung so (um)strukturieren, dass effiziente/elegante Lösungen möglich sind. Tatsächlich ist die adäquate (Um-)Strukturierung eine Kunst, die den guten Informatiker auszeichnet.

Im Folgenden werden wir entsprechende Vorgehensmuster behandeln, die insbesondere die mathematische Beherrschbarkeit und die damit verbunden Zuverlässigkeit von Systemen in den Vordergrund stellen. Spezifisch auf Laufzeiteffizienz zielende Muster werden typischer Weise unter dem Thema Algorithmen und Datenstrukturen vertieft.

Umgang mit beschränkten Ressourcen. Es ist modern, komplexe Aufgaben zu verteilen, und zwar zum Teil auf sehr, sehr viele Problemlöser (Crowd Sourcing). Ein von der Verteilung her noch moderateres Beispiel der Verteilung ist die in Abbildung 1.4 skizzierte ANTS Mission der NASA. Hier soll ein Schwarm von etwa 2000 notebookgroßen Raumschiffe durch den Asteroidengürtel geschifft werden, um irgendwelche Missionen zu erfüllen, wie Probennahmen, Fotografien, Analyse, usw.. Wegen ihrer eingeschränkten Größe und Kapazität muss dazu eine klare Rollenverteilung vorgenommen werden: jedes dieser Raumschiffe erfüllt Teilaufgaben, deren Ergebnisse dann

anschließend zusammengeführt werden müssen. Es ist im allgemeinen sehr schwierig, eine derartige Zusammenarbeit effizient zu organisieren. Wir wollen uns daher hier auf ein sehr einfaches Beispielproblem beschränken:

Abbildung 1.4: ANTS

Angenommen wir haben einen Schwarm von Minirechnern, die jeder die ganzen Zahlen bis zu einem Byte beherrschen. D.h. sie können die üblichen Rechenarten wie +, *, - und /, wobei / nur für glatt aufgehende Divisionen definiert ist.

Frage 1: Ist es möglich, trotz des Überlaufproblems zu garantieren, dass alle Ergebnisse, die sich mit einem Byte darstellen lassen, präzise sind?

Im Rahmen der Behandlung von Faktorstrukturen werden wir sehen, dass es genügt, nur auf den Resten nach Division mit einer geeigneten Menge von Primzahlen zu rechnen. Wie und warum das möglich ist, gehört zu den elementaren Grundlagen der Algebra.

Frage 2: Inwieweit lässt sich solch ein Vorgehen auch auf rationale Zahlen generalisieren?

Ideen hierzu werden wir hauptsächlich im Rahmen von Sonderaufgaben behandeln.

Faktorstrukturen haben viele Anwendungen in der Informatik, insbesondere bei der Modellbildung und der automatischen Programmanalyse (Stichwort: abstrakte Interpretation).

Eigenfaces Ein besonders aktuelles Anwendungsfeld des zweiten Vorlesungsteils ist die Gesichtserkennung: Wie charakterisiert man individuelle Gesichter möglichst einfach? Die Idee hier ist es, Gesichter (approximativ) aus einem kleinen Repräsentantensystem zusammen zu setzen/zu überlagern. Das geht auf die aus der Linearen Algebra bekannten Eigenraumzerlegung zurück (daher auch der Name Eigenfaces).

Das linke Bild zeigt ein Mittelwertgesicht (das ganz oben links) und 19 Eigenfaces. Mittelwertgesichter entstehen durch Überlagerung aller zugrundeliegenden Gesichter und sind daher ein guter

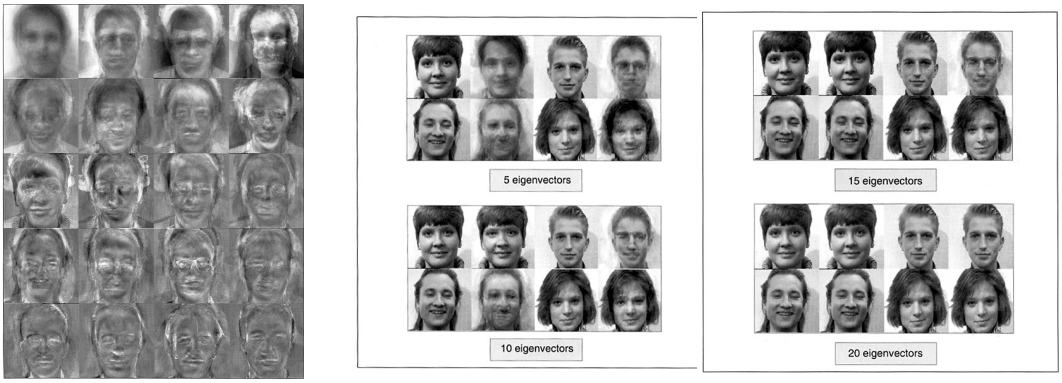


Abbildung 1.5: Eigenfaces

Ausgangspunkt von dem aus man spezifische Variantengesichter durch Hinzufügen von Eigengesichtern unterschiedlicher Intensität konstruieren kann. Mittelwertgesichter bilden damit den Ursprung des vollen 'Gesichtsraumes'. Weitere Gesichter werden dann durch sogenannte Linearkombinationen von Eigenfaces gebildet. Die Qualität dieser Bilder hängt von der Dimension dieses Raumes ab. Abbildung 1.5 zeigt Varianten für die Dimensionen 5, 10, 15, 20.

Im zweiten Teil der Vorlesung werden die mathematischen Grundlagen für derartige Konstruktionen gelegt. Details sind Thema weiterführender Vorlesungen wie Computergraphik.

Das Zusammenspiel von Syntax und Semantik Traditionell wird in der Mathematik präzise aber großenteils informell natürlichsprachlich argumentiert. Ein klare (formale) Abgrenzung zwischen der Argumentationsebene, auf der über das Problem geredet wird und der Problemebene selbst ist unüblich. Insbesondere trennen Mathematiker typischer Weise konzeptuell nicht zwischen der sogenannten Darstellungsebene/Repräsentation (Syntax) und der intendierten Bedeutung (Semantik). In der Informatik ist diese Trennung dagegen essentiell.

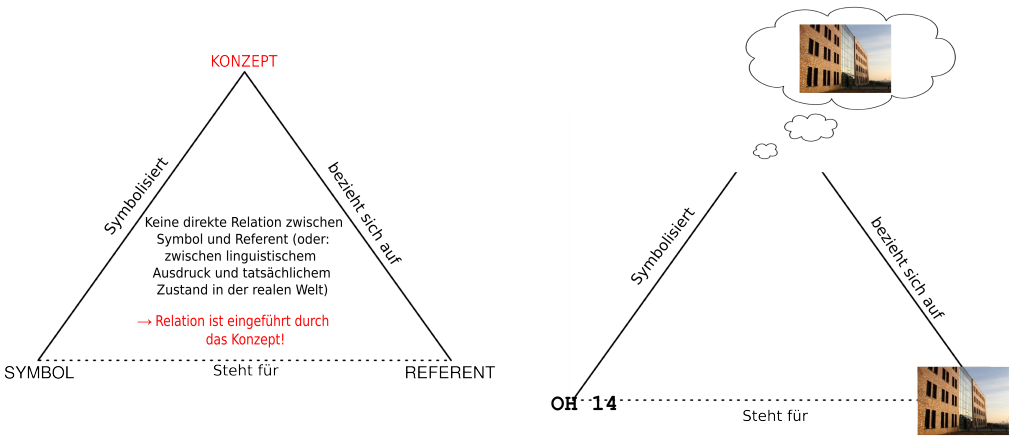


Abbildung 1.6: Semiotisches Dreieck

Im Rahmen der Vorlesung sollen zwei Vorteile dieser Trennung klar werden

- Die unzweideutige Präzision. Sie ist Grundlage für die Computer-gestützte Bearbeitung von Problemen, wie z.B. Theorembeweisen, Compiler-Generierung, und vieles mehr.
- Der kreative Spielraum, der durch diese Trennung ermöglicht wird: Das intuitiv vorgegebene Problem kann auch in der Informatik, wie z.B. in der Physik als 'naturgegeben' angesehen werden. Wir haben aber Spielraum bei der Art, wie dieses Problem formal beschrieben (repräsentiert) wird:

  Beispiel: Natürliche Zahlen: Wir sind an die Dezimaldarstellung gewöhnt, ihre logarithmische Prägnanz, und die elegante Weise wie man im Dezimalsystem stellenbezogen rechnet. Man vergleiche dies einmal mit der Darstellung als römische Zahlen und mit dem Unärsystem.

  Ein weiteres Beispiel, das bis heute Relevanz hat ist er Vergleich zwischen dem metrischen System und dem angelsächsischen System mit Fuß, Yard und Meile.

Das war jetzt ein Feuerwerk von Eindrücken, die nicht alle auf einmal vollständig verstanden und verarbeitet werden können. Seien Sie deswegen jetzt nicht beunruhigt. Der Weg liegt ja noch vor ihnen. Doch auch hier kann man auf Euklid zurückgreifen, der gesagt hat: "Es gibt keinen Königsweg zur Mathematik!" Das bedeutet aber nicht, dass der Weg zur Mathematik unattraktiv ist. Vielmehr genießt man den "Ausblick" von der Höhe des besseren Verständnisses besonders, wenn man ihn sich hart erarbeitet hat.

Sorgen machen müssen Sie sich erst, wenn Sie das hier vorgestellte Anliegen am Ende der Vorlesung immer noch nicht begreifen. Wenn Sie das Anliegen aber verinnerlicht haben, werden Sie auch dann zurecht kommen, wenn sie etwaige Details vergessen haben. Denn wenn Sie die Prinzipien/Verfahrensmuster verinnerlicht haben, dann werden Sie in der Lage sein, fehlende Details zu ermitteln. Google und Wikipedia wird Sie dabei unterstützen.

1.2 Lernziele zusammengefasst

Zweifelfreies Verstehen:

- mathematische Präzision,
- dazugehörige Formalismen, sowie
- mathematische Denkmuster und
- Beweismuster

Einsatz wiederverwendbarer Muster:

- Beschreibungsmuster
- Strukturierungsmuster
- Beweismuster
- algorithmische Muster

Prinzipielles Vorgehen:

- Was ist der Kern des Problems? (Dialog)
- Was sind angemessene Lösungsmuster? (Dialog, Google)
- Wie kann man diese Muster gezielt zur Problemlösung einsetzen? (Dialog, Kernkompetenz)

Beherrschung von Modellierungsspielräumen:

I Trennung von Syntax/Semantik: WIE vs. WAS

II (Induktives) Strukturieren

III Generalisierung und Abstraktion

als Grundlage für 'teile und herrsche'-Prinzipien wie:

IV Invarianz

V Kompositionalität

mit dem Ziel:

VI Korrektheit (z.B.(induktive) Beweisbarkeit)

VII Effizienz

Kapitel 2

Aussagen und Mengen

2.1 Aussagen

In der Mathematik ist es von essentieller Bedeutung wissenschaftliche Erkenntnisse in (schrift)sprachlicher Form abzufassen. Da umgangssprachliche Formulierungen die Gefahr von Missverständlichkeiten in sich tragen, hat sich eine formalisierte Verwendung sprachlicher Konstrukte durchgesetzt. Zentral dabei ist der Begriff der *Aussage* (engl. *proposition*).

Definition 2.1 (Aussagen) *Aussagen sind (schrift)sprachliche Gebilde, denen ein Wahrheitswert* wahr *(w) oder* falsch *(f) zugeordnet werden kann.*

Beispiele für Aussagen im Sinne dieser Definition sind:

Beispiel 2.2 (Aussagen)

1. *Borussia Dortmund ist Deutscher Fußballmeister 2011. (w)*
2. *Delfine sind Fische. (f)*
3. *5 ist eine Primzahl. (w)*
4. *Es gibt nur endlich viele Primzahlen. (f)*
5. *Jede natürliche Zahl größer als zwei ist Summe zweier Primzahlen. (?)*

Aussage (4) ist falsch, denn der Satz von Euklid impliziert, dass es unendliche viele Primzahlen gibt. Bei Aussage (5) hingegen handelt es sich um die sogenannte *Goldbachsche Vermutung*, deren Gültigkeit bis heute unbewiesen ist. Es liegt hier aber dennoch eine Aussage vor, da man davon ausgehen kann, dass die Vermutung entweder durch einen Beweis nachgewiesen oder durch ein Gegenbeispiel widerlegt werden kann.

Keine Aussagen im mathematischen Sinne sind:

Beispiel 2.3 (Keine Aussagen)

1. *Wie spät ist es?*
2. *Kommt her!*
3. *Verdi hat die bedeutendsten Opern komponiert.*
4. *Diese Aussage ist falsch.*

Während es sich bei (1) und (2) um eine Frage beziehungsweise Anweisung handelt, hat (3) zumindest die äußere Form einer Aussage. Allerdings kann man dem Satz keinen eindeutig bestimmten Wahrheitswert zuordnen, da unterschiedliche Personen -auch Experten- hier zu unterschiedlichen Urteilen kommen werden. Bei (4) handelt es sich um ein logisches Paradoxon. Nehmen wir an (4) wäre eine Aussage, dann steht jede Zuordnung eines Wahrheitswertes im Widerspruch mit dem Inhalt des Satzes.

2.1.1 Aussagenlogik

In der Aussagenlogik ist die innere Form einer elementaren Aussage nicht relevant. Vielmehr ist es von Interesse, wie Aussagen zu größeren Gebilden kombiniert werden können. Der Wahrheitswert der kombinierten Aussagen soll sich eindeutig aus dem Wahrheitswert der Teilaussagen ergeben (Prinzip der *Extensionalität*). Wir werden in den Kapiteln 4 und 5 diese Sichtweise formal präzisieren, indem wir aussagenlogische Formeln (*Syntax*) induktiv definieren und diesen dann induktiv eine Bedeutung (*Semantik*) zuweisen. Zunächst aber betrachten wir hier einen etwas weniger formalen Zugang:

Definition 2.4 (Verknüpfung von Aussagen) *Seien $\mathcal{A}$ und $\mathcal{B}$ beliebige Aussagen, dann auch die*

Negation *von $\mathcal{A}$: $(\neg\mathcal{A})$. Der Wahrheitswert von $\mathcal{A}$ wird invertiert.*[a]

Disjunktion *von $\mathcal{A}$ und $\mathcal{B}$: $(\mathcal{A} \vee \mathcal{B})$. Wahr genau dann, wenn mindestens eine der beiden Aussagen wahr ist.*

Konjunktion *von $\mathcal{A}$ und $\mathcal{B}$: $(\mathcal{A} \wedge \mathcal{B})$. Wahr genau dann, wenn beide Aussagen wahr sind.*

Implikation *von $\mathcal{A}$ und $\mathcal{B}$: $(\mathcal{A} \Rightarrow \mathcal{B})$: Wahr genau dann, wenn falls $\mathcal{A}$ wahr ist auch $\mathcal{B}$ wahr ist.*[b]

Äquivalenz *von $\mathcal{A}$ und $\mathcal{B}$: $(\mathcal{A} \Leftrightarrow \mathcal{B})$. Wahr genau dann, wenn beide Aussagen den gleichen Wahrheitswert besitzen.*

[a] Gelegentlich wird die Negation auch durch einen Überstrich ausgedrückt $\overline{\mathcal{A}}$.
[b] $\mathcal{A}$ ist die *Prämisse* und $\mathcal{B}$ die *Konklusion* der Implikation.

Bei der Implikation ist zu bedenken, dass diese im Falle einer nicht erfüllten Prämisse wahr ist. So ist die Aussage:

$$10 \text{ ist eine Primzahl } \Rightarrow \text{ Elefanten können fliegen}$$

eine wahre Aussage.

Die Verknüpfungssymbole $\neg, \vee, \wedge, \Rightarrow$ und $\Leftrightarrow$ werden auch *Junktoren* genannt. Um Klammern einzusparen vereinbart man, dass $\neg$ stärker bindet als $\wedge$, $\wedge$ stärker bindet als $\vee$ und $\vee$ stärker bindet als $\Rightarrow$ und $\Leftrightarrow$. Die folgende Tabelle fasst die in Definition 2.4 eingeführten Verknüpfungen in einer *Wahrheitstafel* zusammen:

$\mathcal{A}$	$\mathcal{B}$	$\neg\mathcal{A}$	$\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	$\mathcal{A} \Rightarrow B$	$\mathcal{A} \Leftrightarrow \mathcal{B}$
f	f	w	f	f	w	w
f	w	w	w	f	w	f
w	f	f	w	f	f	f
w	w	f	w	w	w	w

Aussagen $\mathcal{A}$ und $\mathcal{B}$, deren Wahrheitstafeleinträge gleich sind, werden als *(semantisch) äquivalent* bezeichnet (in Zeichen $\mathcal{A} \equiv \mathcal{B}$). Zum Beispiel kann die Konjunktion, die Implikation und die Äquivalenz durch alleinige Verwendung der Junktoren $\neg$ und $\vee$ ausgedrückt werden.

$$\mathcal{A} \wedge \mathcal{B} \equiv \neg(\neg\mathcal{A} \vee \neg\mathcal{B}) \tag{2.1}$$

$$\mathcal{A} \Rightarrow \mathcal{B} \equiv \neg A \vee \mathcal{B} \tag{2.2}$$

$$\mathcal{A} \Leftrightarrow \mathcal{B} \equiv \neg(\neg(\neg\mathcal{A} \vee \mathcal{B}) \vee \neg(\neg\mathcal{B} \vee \mathcal{A}))) \tag{2.3}$$

Die Äquivalenzen 2.1 und 2.2 sind exemplarisch in der folgenden Wahrheitstafel bewiesen:

$\mathcal{A}$	$\mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{B}$	$\neg\mathcal{A} \vee \neg\mathcal{B}$	$\neg(\neg\mathcal{A} \vee \neg\mathcal{B})$	$\mathcal{A} \wedge \mathcal{B}$	$\neg\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$
f	f	w	w	w	f	f	w	w
f	w	w	f	w	f	f	w	w
w	f	f	w	w	f	f	f	f
w	w	f	f	f	w	w	w	w

Zeigen die Gleichungen (2.1) - (2.3) noch, dass die Negation und Disjunktion ausreichen um alle Aussagenverknüfungen auszudrücken, so kommt man tatsächlich nur mit einem einzigen Operator aus. Definiert man die "Nicht-Und"-Verknüpfung (auch *Nand-Verknüpfung* genannt), durch $\mathcal{A} \barwedge \mathcal{B} \ =_{df} \ \neg(\mathcal{A} \wedge \mathcal{B})$, so lässt sich die Negation ausdrücken durch $\neg\mathcal{A} \ = \ \mathcal{A} \barwedge \mathcal{A}$ und die Disjunktion durch $\mathcal{A} \vee \mathcal{B} \ = \ \neg\mathcal{A} \barwedge \neg\mathcal{B} \ \equiv \ (\mathcal{A} \barwedge \mathcal{A}) \barwedge (\mathcal{B} \barwedge \mathcal{B})$.

Es sei darauf hingewiesen, dass die semantische Äquivalenz $\equiv$ nicht etwa Junktor der Aussagenlogik ist, sondern Metasymbol um Aussagen über Aussagen zu formulieren. Es gilt jedoch, dass für äquivalente Aussagen $\mathcal{A} \equiv \mathcal{B}$ die Aussage $\mathcal{A} \Leftrightarrow \mathcal{B}$ eine *Tautologie*, sprich eine immer wahre Aussage ist.

Im Folgenden stehen T und F als Symbole für eine immer wahre bzw. immer falsche Aussage. Dann können folgende semantische Äquivalenzen ebenfalls leicht mit Wahrheitstafeln nachgewiesen werden:

Lemma 2.5 (Semantische Äquivalenzen) *Es gelten für beliebige Aussagen $\mathcal{A}, \mathcal{B}, \mathcal{C}$ die folgenden Äquivalenzen:*

$$
\begin{array}{rcll}
\mathcal{A} \wedge \mathcal{B} & \equiv & \mathcal{B} \wedge \mathcal{A} & \textit{(Kommutativität)} \\
\mathcal{A} \vee \mathcal{B} & \equiv & \mathcal{B} \vee \mathcal{A} & \\
\\
(\mathcal{A} \wedge \mathcal{B}) \wedge C & \equiv & \mathcal{A} \wedge (\mathcal{B} \wedge \mathcal{C}) & \textit{(Assoziativität)} \\
(\mathcal{A} \vee \mathcal{B}) \vee \mathcal{C} & \equiv & \mathcal{A} \vee (\mathcal{B} \vee \mathcal{C}) & \\
\\
\mathcal{A} \wedge (\mathcal{A} \vee \mathcal{B}) & \equiv & \mathcal{A} & \textit{(Absorption)} \\
\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B}) & \equiv & \mathcal{A} & \\
\\
\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) & \equiv & (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C}) & \textit{(Distributivität)} \\
\mathcal{A} \vee (\mathcal{B} \wedge \mathcal{C}) & \equiv & (\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{A} \vee \mathcal{C}) & \\
\\
A \wedge \neg\mathcal{A} & \equiv & \mathsf{F} & \textit{(Negation)} \\
A \vee \neg\mathcal{A} & \equiv & \mathsf{T} & \\
\hline
\mathcal{A} \wedge \mathcal{A} & \equiv & \mathcal{A} & \textit{(Idempotenz)} \\
\mathcal{A} \vee \mathcal{A} & \equiv & \mathcal{A} & \\
\\
\neg\neg\mathcal{A} & \equiv & \mathcal{A} & \textit{(Doppelnegation)} \\
\\
\neg(\mathcal{A} \wedge \mathcal{B}) & \equiv & \neg\mathcal{A} \vee \neg\mathcal{B} & \textit{(deMorgansche Regeln)} \\
\neg(\mathcal{A} \vee \mathcal{B}) & \equiv & \neg\mathcal{A} \wedge \neg\mathcal{B} & \\
\\
\mathsf{T} \wedge \mathcal{A} & \equiv & \mathcal{A} & \textit{(Neutralität)} \\
\mathsf{F} \vee \mathcal{A} & \equiv & \mathcal{A} &
\end{array}
$$

2.1.2 Anwendung: Digitale Schaltkreise

In der bisher betrachteten Aussagenlogik liegt der Fokus auf der Kombination elementarer Aussagen zu größeren Konstrukten. Die Struktur elementarer Aussagen ist nicht relevant. Die Aussagenlogik ist daher in Szenarien adäquat, wo nicht näher untersuchte Basisobjekte genau zwei Werte annehmen können. Dieses ist zum Beispiel in der Theorie digitaler Schaltkreise der Fall. Dort geht es um die Verarbeitung binärer Signale, die durch zwei unterschiedliche Spannungspotentiale, etwa 0 V und 5 V, realisiert werden.

Wir betrachten hier zunächst die Funktionalität eines Halbaddierers. Dieser addiert die an zwei Eingängen A und B anliegende Signale und erzeugt dabei gegebenenfalls einen Überlauf, der von einem nachgeschalteten Halbaddierer abgegriffen werden kann. Liegt an einem der Eingänge eine

1 an, so ist das Signal an Ausgang Z ebenfalls 1.[1] Falls an beiden Eingängen eine 1 anliegt wird zusätzlich das Überlaufsignal an Ausgang Ü auch auf 1 gesetzt.

Abbildung 2.1 zeigt das Schaltbild eines Halbaddieres.

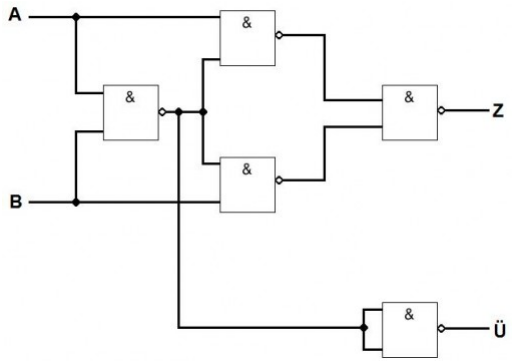


Abbildung 2.1: Halbaddierer aus NAND-Bausteinen

In diesem Schaltbild sind ausschließlich Nand-Bausteine verwendet, die eine Nicht-Und-Verknüpfung der Eingangssignale vornehmen. Das heißt, das Ausgangssignal ist genau dann 0, wenn an beiden Eingängen eine 1 anliegt. Die Wahrheitstafel für die Gesamtfunktionalität des Halbaddieres ist in Tabelle 2.1 zu finden.

A	B	C $\overbrace{A \barwedge B}$	D $\overbrace{A \barwedge C}$	E $\overbrace{C \barwedge B}$	Z $\overbrace{D \barwedge E}$	Ü $\overbrace{C \barwedge C}$
0	0	1	1	1	0	0
0	1	1	1	0	1	0
1	0	1	0	1	1	0
1	1	0	1	1	1	1

Tabelle 2.1: Wahrheitstafel zu Schaltung aus Abbildung 2.1

Wir werden digitale Schaltkreise an dieser Stelle nicht weiter vertiefen. Diese werden ausführlich in der Vorlesung Rechnerstrukturen oder Elektrotechnik-Vorlesungen (wie z.B. Elektrotechnik und Nachrichtentechnik) behandelt.

[1] Traditionell verwendet man statt den Wahrheitswerten w und f im Kontext digitaler Schaltkreise die Symbole 0 und 1 für das anliegende niedrige bzw. hohe Potential.

2.1.3 Prädikatenlogik

Im Gegensatz zur Theorie digitaler Schaltkreise ist Aussagenlogik für die Behandlung allgemeiner mathematischer Theorien zu eingeschränkt, da die innere Struktur der elementaren Aussagen dort eine Rolle spielt. Beispielsweise folgen die Aussagen

$$\begin{aligned} 1+2 &= 2+1 \\ 2+3 &= 3+2 \\ 6+14 &= 14+6 \\ &\vdots \end{aligned}$$

alle demselben Muster. Sie drücken nämlich die Kommutativität der Addition natürlicher Zahlen aus. Diesem wird durch die Einführung quantifizierter Ausdrucksformen wie "*für alle*" und "*es gibt*" in der *Prädikatenlogik* Rechnung getragen. Im vorangehenden Beispiel würde die prädikatenlogische Formel

$$\forall\, x \in \mathbb{N}.\ \forall\, y \in N.\ x + y = y + x$$

den Tatbestand der Kommutativität ausdrücken.

Wir verzichten in dieser Vorlesung auf eine formal fundierte Einführung der Prädikatenlogik und verweisen auf vertiefende Vorlesungen wie *Logik für Informatiker*. Wesentlicher Bestandteil der Prädikatenlogik ist eine zugrundliegende Struktur. Hierunter versteht man eine nichtleere Menge von Individuen mit zugehörigen Operationen und Relationen (siehe Kapitel 3.1). Beispielsweise kann man hier an die natürlichen Zahlen mit der Operationen Addition und Multiplikation und der Gleichheits- und $\leq$-Relation denken. Die Prädikatenlogik über den natürlichen Zahlen erweitert die Aussagenlogik in folgender Weise:

1. Die Junktoren der Aussagenlogik dürfen wie gewohnt zum Kombinieren von Aussagen verwendet werden.
2. Zusätzlich dürfen relationale Ausdrücke mit freien Variablen über natürlichen Zahlen, wie z.B. $n + 1 \leq 3$, verwendet werden. Man spricht hier von *Prädikaten* oder *Aussageformen*.[2]
3. Aussageformen können unter Verwendung des *All-* und *Existenzquantors* in Aussagen überführt werden. Für eine Aussageform $A(n)$ mit freier Variable n bilden wir die:

   ***Allaussage*:** $\forall\, n.\ A(n)$. Diese ist genau dann wahr, wenn $A(n)$ für alle Werte $n \in \mathbb{N}$ wahr ist.

   ***Existenzaussage*:** $\exists\, n.\ A(n)$. Diese ist genau dann wahr, wenn $A(n)$ für mindestens einen Wert $n \in \mathbb{N}$ wahr ist.

   Ist die zugrundeliegende Struktur der natürlichen Zahlen nicht aus dem Kontext ersichtlich, schreiben wir auch $\forall\, n \in \mathbb{N}.\ A(n)$ bzw. $\exists\, n \in \mathbb{N}.\ A(n)$. In der quantifizierten Formel ist die Variable n an den Quantor *gebunden* und kann somit nicht durch äußere quantifizierte Formeln referenziert werden.

[2] Der Begriff Aussageform bringt zum Ausdruck, dass eine solche erst durch das Zuordnen von Werten für die Variablen zur Aussage wird. Beispielsweise ergibt $n + 1 \leq 3$ für $n \mapsto 2$ eine wahre für $n \mapsto 3$ eine falsche Aussage.

Prädikatenlogik über anderen Strukturen als den natürlichen Zahlen ist entsprechend aufgebaut. Um Klammern einzusparen vereinbart man, dass Quantoren schwächer binden als alle Junktoren. Soll eine engere Bindung zum Ausdruck gebracht werden, müssen quantifizierte Aussagen entsprechend geklammert werden. Statt $\neg(\forall\, n.\ A(n))$ und $\neg(\exists\, n.\ A(n))$ schreiben wir kurz $\not\forall\, n.\ A(n)$ und $\nexists\, n.\ A(n)$. Geschachtelte quantifizierte Aussagen mit demselben Quantor, etwa $\forall\, x_1.\ \forall\, x_2.\ \ldots \forall\, x_n.\ A(x_1, \ldots, x_n)$, können abgekürzt durch $\forall\, x_1, \ldots, x_n.\ A(x_1, \ldots, x_n)$ dargestellt werden.

Oft führt man in der Prädikatenlogik auch Relationen als Abkürzungen für komplexere Teilformeln mit freien Variablen ein. Wir demonstrieren dieses für die Eigenschaft des größten gemeinsamen Teilers. Zunächst definieren wir die Teilbarkeitsrelation:

$$n|m \ =_{df}\ \exists\, k \in \mathbb{N}.\ \ n \cdot k = m.$$

In Worten: n teilt m, falls es eine natürliche Zahl k gibt, so dass das k-fache von n die Zahl m ergibt. Darauf aufbauend definieren wir eine dreistellige Relation ggT, die ausdrückt, wann eine natürliche Zahl x größter gemeinsamer Teiler der natürlichen Zahlen n und m ist:

$$ggT(n, m, x) \ =_{df}\ \ x|n\ \wedge\ x|m\ \wedge\ \forall\, y \in \mathbb{N}.\ (y|n\ \wedge\ y|m)\ \Rightarrow\ y \leq x.$$

Durch $x|n\ \wedge\ x|m$ wird zunächst die Forderung ausgedrückt, dass x ein gemeinsamer Teiler von n und m ist. Die dann folgende Allaussage drückt die Forderung aus, dass x größer oder gleich zu jedem anderen gemeinsamen Teiler ist. Da die ggT-Relation auch als Funktion (siehe Kapitel 3.2) $ggT : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ angesehen werden kann, schreibt man statt $ggT(n, m, x)$ auch $x = ggT(n, m)$.

Für die Negation von quantifizierten Formeln gilt folgender Zusammenhang:

Lemma 2.6

1. $\neg(\forall\, x.\ \mathcal{A}(x)) \ \equiv\ \exists\, x.\ \neg\mathcal{A}(x)$
2. $\neg(\exists\, x.\ \mathcal{A}(x)) \ \equiv\ \forall\, x.\ \neg\mathcal{A}(x)$

Beweis Wir zeigen exemplarisch die erste Eigenschaft, wobei wir die Struktur natürlicher Zahlen zugrunde legen.

$\neg(\forall\, x.\ \mathcal{A}(x))$ ist wahr	*gdw.*	$\forall\, x.\ \mathcal{A}(x)$ ist falsch	(Auswertung $\neg$)
	gdw.	$\mathcal{A}(x)$ ist falsch für mindestens ein x	(Auswertung $\forall$)
	gdw.	$\neg\mathcal{A}(x)$ ist wahr für mindestens ein x	(Auswertung $\neg$)
	gdw.	$\exists\, x.\ \neg\mathcal{A}(x)$ ist wahr	(Auswertung $\exists$)

□

2.1.4 Logische Beweisprinzipien

Während Wahrheitstafeln ausreichend sind beliebige Sätze der Aussagenlogik zu beweisen, kann ein tabellarischer Ansatz in der Prädikatenlogik wegen der meist unendlich großen zugrundeliegenden Strukturen nicht mehr zielführend sein. Prinzipiell gibt es beim Beweisen zwei unterschiedliche Ansätze. Zum einen kann ein Beweis *semantisch* vorgehen, sprich sich direkt an der Definition der Semantik der logischen Konstrukte (Junktoren und Quantoren) orientieren. Ein Beispiel für eine solches Vorgehen ist der Beweis zu Lemma 2.6.[3] Zum anderen können als gültig nachgewiesene Regeln verwendet werden, um die zu beweisende Behauptung *syntaktisch* zu transformieren. Auf diesem Vorgehen basieren insbesondere automatische Beweiser. Ein Beweis für die semantische Äquivalenz $\mathsf{T} \vee \mathcal{A} \equiv \mathsf{T}$, der sich ausschließlich auf die Regeln aus Tabelle 2.5 stützt ist:

$$
\begin{array}{lcll}
\mathsf{T} \vee \mathcal{A} & \equiv & (\mathcal{A} \vee \neg\mathcal{A}) \vee \mathcal{A} & \text{(Negation)} \\
& \equiv & \mathcal{A} \vee (\neg\mathcal{A} \vee \mathcal{A}) & \text{(Assoziativität)} \\
& \equiv & \mathcal{A} \vee (\mathcal{A} \vee \neg\mathcal{A}) & \text{(Kommutativität)} \\
& \equiv & (\mathcal{A} \vee \mathcal{A}) \vee \neg\mathcal{A} & \text{(Assoziativität)} \\
& \equiv & \mathcal{A} \vee \neg\mathcal{A} & \text{(Idempotenz)} \\
& \equiv & \mathsf{T} & \text{(Negation)}
\end{array}
$$

In der mathematischen Praxis verwendet man meist ein gemischtes Vorgehen. Im Skript werden wir einige pragmatisch besonders relevante Beweismuster, immer dann wenn diese erstmalig eingesetzt werden, vorstellen.

2.2 Mengen

Die Mengenlehre als eigenständige mathematische Disziplin geht zurück auf Arbeiten von Georg Cantor aus dem späten 19. Jahrhunderts. In diesem Rahmen formulierte er folgende Mengendefinition:

Definition 2.7 *Unter einer* Menge *verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die* Elemente *von M genannt werden) zu einem Ganzen.*

Für eine Menge M kennzeichnet die Aussage $m \in M$, dass m ein Element von M ist. Für die negierte Aussage $\neg(m \in M)$ wird abkürzend auch $m \notin M$ geschrieben.

Mengen lassen sich in unterschiedlicher Weise beschreiben. Endliche Mengen lassen sich durch *Aufzählung* ihrer Elemente beschreiben. So stellt $M_1 = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ die Menge der Kartenfarben von Spielkarten und $M_2 = \{Sonntag, Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag\}$ die Menge der Wochentage dar. Auch für unendliche Mengen ist eine solche Beschreibung

[3] Da die Semantik von Prädikatenlogik in diesem Kapitel nicht vollständig formal ausgeführt ist, sollte man genau genommen von einem *intuitiv semantischen* Beweis sprechen. In Kapitel 5 werden wir anhand der formalen Semantik genauer argumentieren.

prinzipiell möglich, wenn die Beschreibung unmissverständlich ist. So kann man die aus der Schulmathematik bekannte Menge der natürlichen Zahlen aufzählend beschreiben als $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ und die Menge der geraden natürlichen Zahlen als $\mathbb{N}_{ger} = \{0, 2, 4, 6 \ldots\}$.[4]

Die *beschreibende* Form charakterisiert Mengen, indem die enthaltenen Elemente durch ein Prädikat charakterisiert werden. So kann die Menge der Primzahlen beschrieben werden durch

$$Prim = \{p \mid p \in \mathbb{N}\backslash\{0,1\} \wedge \forall n \in \mathbb{N}.\ n \,|\, p \ \Rightarrow\ n \in \{1, p\}\}.$$

Allgemein hat die beschreibende Form einer Menge M die Gestalt

$$M = \{m \mid \mathcal{A}(m)\},$$

wobei $\mathcal{A}(m)$ Prädikat über m, also eine Aussageform mit freier Variablen m ist. Sind die Elemente von m aus einer in $\mathcal{A}(m)$ beschriebenen Grundmenge, so kann diese Information auch der Variablenangabe zugeschlagen werden. Im Falle der Primzahlen hätten wir also:

$$Prim = \{p \in \mathbb{N}\backslash\{0,1\} \mid \forall n \in \mathbb{N}.\ n|p \ \Rightarrow\ n \in \{1, p\}\}.$$

Ist $\mathcal{A}(m)$ ein unerfüllbares Prädikat so wird dadurch die leere Menge $\emptyset$ beschrieben, also $\emptyset = \{x \mid \mathsf{F}\}$.

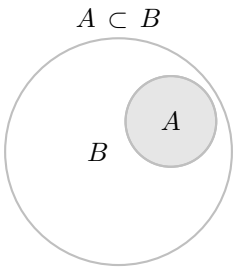
2.2.1 Mengenbeziehungen

Auf Mengen werden die Teilmengenbeziehung, echte Teilmengenbeziehung und die Gleichheit definiert durch:[5]

Definition 2.8 (Mengenbeziehungen) *Seien A und B Mengen.*

1. $A \subseteq B$ *(sprich A ist* Teilmenge *von B)* $\Leftrightarrow_{df}$ $(\forall x.\ x \in A \Rightarrow x \in B)$
2. $A = B$ *(sprich A ist* gleich *B)* $\Leftrightarrow_{df}$ $A \subseteq B \wedge B \subseteq A$.
3. $A \subset B$ *(sprich A ist* echte Teilmenge *von B)* $\Leftrightarrow_{df}$ $A \subseteq B \wedge A \neq B$.

Per Definition ist die leere Menge Teilmenge jeder anderen Menge. Die (echte) Teilmengenbeziehung von Mengen lässt sich anschaulich gut in einem sogenannten *Venn-Diagramm* darstellen:



[4] In Kapitel 4 wird das Konzept des induktiven Definierens als Formalisierung der ".."-Notation eingeführt.

[5] Es sei darauf hingewiesen, dass es sich bei der Teilmengenbeziehung um eine partielle Ordnung (siehe Kapitel 6.1) und bei der Gleichheitsrelation um eine Äquivalenzrelation (siehe Kapitel 3.3) handelt.

Potenzmenge

Mengen, deren Elemente selbst Mengen über einer Grundmenge M sind bezeichnet man als *Mengensysteme* über M. Ein besonders wichtiges Mengensystem ist die Menge aller Teilmengen von M:

Definition 2.9 (Potenzmenge) *Sei M eine Menge. Die* Potenzmenge *von M ist definiert durch* $\mathfrak{P}(M) =_{df} \{M' \mid M' \subseteq M\}$.

Beispiel 2.10 *Für* $M = \{1, 2, 3\}$ *gilt* $\mathfrak{P}(M) = \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, M \,\}$.

2.2.2 Mengenverknüpfungen

Ähnlich wie bei Aussagen sind auch auf Mengen Verknüpfungen definiert:

Definition 2.11 (Verknüpfung von Mengen) *Seien A und B Mengen. Dann sind folgende Mengenverknüpfungen definiert:*

Vereinigung $A \cup B =_{df} \{x \mid x \in A \vee x \in B\}$

Schnitt $A \cap B =_{df} \{x \mid x \in A \wedge x \in B\}$

Differenz $A \setminus B =_{df} \{x \mid x \in A \wedge x \notin B\}$

Symmetrische Differenz $A \,\Delta\, B =_{df} (A \cup B) \setminus (A \cap B)$

Falls $A \cap B = \emptyset$ gilt, so nennt man A und B *disjunkt*. Für eine gegebene Grundmenge M mit Teilmenge $A \subseteq M$ ist weiterhin das Komplement von A definiert als $A^{\complement} =_{df} M \setminus A$.

Im Venn-Diagramm sind die Verknüpfungen in Abbildung 2.2 illustriert.

Beispiel 2.12 *Seien $Prim$ und $\mathbb{N}_{ger}$ die Menge der Primzahlen und der geraden natürlichen Zahlen wie auf Seite 19 definiert. Es gilt:*

- $Prim \cap \mathbb{N}_{ger} = \{2\}$
- $Prim \cup \mathbb{N}_{ger} = \{0, 2, 3, 4, 5, 6, 7, 8, 10, \ldots\}$ *Beachte:* $9 \notin Prim \cup M_{ger}$
- $Prim \setminus \mathbb{N}_{ger} = \{3, 5, 7, 11, 13, \ldots\}$
- $\mathbb{N}_{ger} \setminus Prim = \{0, 4, 6, 8, 10, \ldots\}$
- $\mathbb{N}_{ger} \,\Delta\, Prim = \{0, 3, 4, 5, 6, 7, 8, 10, \ldots\}$

Korrespondierend zu den Gesetzen der Aussagenlogik (siehe Lemma 2.5) gelten folgende Gleichheitsgesetze auf Mengen:

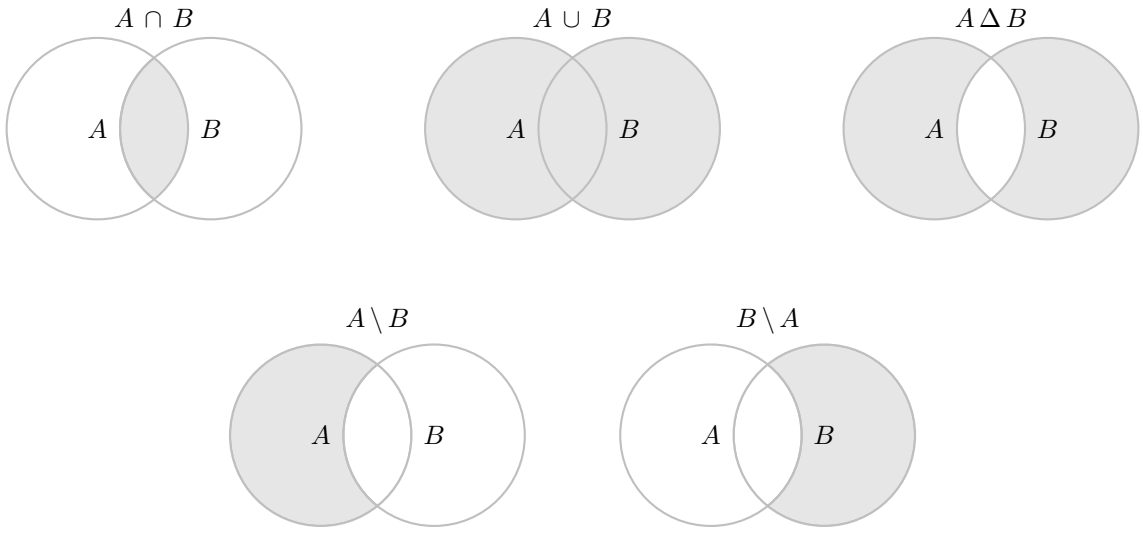


Abbildung 2.2: Venn-Diagramme

Lemma 2.13 (Mengengesetze) *Seien A, B, C Teilmengen einer gemeinsamen Grundmenge M. Dann gilt:*[a]

$$
\begin{array}{rcll}
A \cap B & = & B \cap A & \textit{(Kommutativität)} \\
A \cup B & = & B \cup A & \\
\\
(A \cap B) \cap C & = & A \cap (B \cap C) & \textit{(Assoziativität)} \\
(A \cup B) \cup C & = & A \cup (B \cup C) & \\
\\
A \cap (A \cup B) & = & A & \textit{(Absorption)} \\
A \cup (A \cap B) & = & A & \\
\\
A \cap (B \cup C) & = & (A \cap B) \cup (A \cap C) & \textit{(Distributivität)} \\
A \cup (B \cap C) & = & (A \cup B) \cap (A \cup C) & \\
\\
A \cap A^{\complement} & = & \emptyset & \textit{(Komplement)} \\
A \cup A^{\complement} & = & M & \\
\hline
A \cap A & = & A & \textit{(Idempotenz)} \\
A \cup A & = & A & \\
\\
A^{\complement\complement} & = & A & \textit{(Doppelkomplement)} \\
\\
(A \cap B)^{\complement} & = & A^{\complement} \cup B^{\complement} & \textit{(De Morganschen Gesetze)} \\
(A \cup B)^{\complement} & = & A^{\complement} \cap B^{\complement} & \\
\\
M \cap A & = & A & \textit{(Neutralität)} \\
\emptyset \cup A & = & A &
\end{array}
$$

[a] Die Voraussetzung der gemeinsamen Grundmenge M ist nur für Gesetze erforderlich, die M selbst oder die Komplementoperation $^{\complement}$ enthalten.

Die Vereinigung und der Schnitt von Mengen können verallgemeinert werden auf beliebige Mengensysteme, indem man definiert:

Definition 2.14 (Erweiterte Vereinigungen und Schnitte)
Sei $\mathfrak{M}$ ein Mengensystem über einer Grundmenge M. Dann gilt:

1. $\bigcup_{M' \in \mathfrak{M}} M' =_{df} \{m \in M \mid \exists\, M' \in \mathfrak{M}.\ m \in M'\}$
2. $\bigcap_{M' \in \mathfrak{M}} M' =_{df} \{m \in M \mid \forall\, M' \in \mathfrak{M}.\ m \in M'\}$

2.2.3 Mächtigkeit endlicher Mengen

Mit der *Mächtigkeit* einer Menge M mit endlich vielen Elementen bezeichnen wir die Anzahl ihrer Elemente und verwenden die Notation $|M|$. Die Mächtigkeit der leeren Menge beträgt 0, d.h.: $|\emptyset| = 0$. Es gelten folgende Eigenschaften:

Satz 2.15 *Seien M_1 und M_2 endliche Mengen.*

1. $|A \backslash B| = |A| - |A \cap B|$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \Delta B| = |A| + |B| - 2|A \cap B|$

Beweis

1. $A \backslash B = A \backslash (A \cap B)$. Da $(A \cap B) \subseteq A$ gilt $|A \backslash B| = |A| - |A \cap B|$
2. Sei $A \cap B = \emptyset$, dann $|A \cup B| = |A| + |B|$ was offensichtlich korrekt ist. Anderenfalls gilt jedoch wegen $A \cup B = A \cup (B \backslash A)$ auch $|A \cup B| = |A \cup (B \backslash A)| = |A| + |B \backslash A| \stackrel{(1)}{=} |A| + |B| - |A \cap B|$.
3. Wegen $A \Delta B = (A \cup B) \backslash (A \cap B)$ folgt $|A \Delta B| \stackrel{(1)}{=} |A \cup B| - |A \cap B| \stackrel{(2)}{=} |A| + |B| - 2|A \cap B|$.

□

Wir werden den Mächtigkeitsbegriff in Kapitel 3.2.2 auf beliebige Mengen verallgemeinern, benötigen dafür aber noch Begriffe, die erst im weiteren Verlauf eingeführt werden.

2.2.4 Antinomien

Die Cantorsche Mengenlehre stößt bei naiver Anwendung des Mengenbegriffes an ihre Grenzen. Bekannt unter dem Namen *Russelsche Antinomie* ist zum Beispiel die "Menge" aller Mengen, die sich nicht selbst als Element enthalten:

$$R =_{df} \{M \mid M \notin M\}.$$

Fragt man sich jetzt, ob R in R enthalten ist, so gilt:

$$R \in R \;\Leftrightarrow\; R \notin R,$$

was offensichtlich logisch widersprüchlich ist.

Grundlegend für die Russelsche Antinomie ist die selbstreferentielle Konstruktion von R. Ein verwandtes Phänomen war uns bereits im Zusammenhang paradoxer "Aussagen" wie in Beispiel 2.3(4) begegnet. Ähnlich wie man in der Aussagenlogik "paradoxe Aussagen" als Aussagen im mathematischen Sinne ausschließt, bildet die auf Zermelo-Fraenkel zurückgehende *axiomatische Mengenlehre* einen formalen Rahmen, der es verhindert, Konstrukte wie R als Mengen zu klassifizieren. Zentral dabei ist die Unterscheidung von *Klassen* und Mengen. Während Klassen beliebige Zusammenstellungen von Elementen zulassen, erfordert die Mengeneigenschaft das Einhalten zusätzlicher Konsistenzanforderungen.

Eine weitere bekannte Antinomie wurden von Cantor selbst, der sich sehr wohl der Antinomie-Problematik bewusst war, offengelegt. So ist die *Allmenge* $\mathfrak{A}$, das heißt die "Menge" aller "Mengen" widersprüchlich. Weil jede Teilmenge von $\mathfrak{A}$ in $\mathfrak{A}$ läge, müsste auch die Potenzmenge $\mathfrak{P}(\mathfrak{A})$ Teilmenge von $\mathfrak{P}(\mathfrak{A})$ sein. Dieses kann aber nicht sein, weil die Potenzmenge einer Menge echt mächtiger als die zugrundeliegende Grundmenge ist (Theorem 3.18).

Die Russelsche Antinomie hat auch einen unmittelbaren Bezug zur Informatik. Eine fundamentale Fragestellung der theoretischen Informatik ist, ob alle Probleme prinzipiell durch den Einsatz von programmierbaren Rechenmaschinen gelöst werden können. Die Antwort hierauf lautet "Nein" und eine konkrete Fragestellung, die nicht durch ein Computerprogramm beantwortet werden kann, ist das sogenannte *Halteproblem*. Dabei geht es um die Frage, ob ein Programm, das den Quelltext und die Eingabe eines anderen Programmes kennt, entscheiden kann ob dieses Programm unter der gegebenen Eingabe hält oder nicht. Das Halteproblem wird in weiterführenden Vorlesungen wie "Grundbegriffe der Theoretischen Informatik (GTI)" ausführlich behandelt. An dieser Stelle verweisen wir interessierte Leser auf einen in `http://lwb.mi.fu-berlin.de/personen/Halt.pdf` vorgestellten didaktisch sehr gelungener Brückenschlag zwischen Halteproblem und Russelscher Antinomie.

2.3 Abschließende Betrachtungen

Dem aufmerksamen Leser ist sicher nicht die ähnliche Struktur der Aussagen- und Mengengesetze in Lemma 2.5 und 2.13 entgangen. In der Tat liegt hier ein erstes Szenario vor, das die in Kapitel 7 ausführlich diskutierten *algebraischen Strukturen* motiviert. Abstrahiert man nämlich von den konkret vorliegenden Objekten und Verknüpfungen so lassen sich Gesetzmäßigkeiten unabhängig davon studieren. Tatsächlich sind sogar nur die jeweiligen Gesetze überhalb des Striches erforderlich, denn alle anderen Gesetze sind jeweils aus diesen herleitbar. Der Vollständigkeit halber sei erwähnt, dass mit den 5 Gesetzen eine sogenannte *Boolesche Algebra* (oder auch *Boolescher Verband*) vorliegt, eine Struktur mit herausragender Bedeutung in der Informatik.

Obwohl Sätze der Aussagenlogik anhand von endlichen Wahrheitstafeln semantisch überprüft werden können, stößt ein solches Vorgehen rasch an seine Grenzen, da die Tabellen exponentiell groß in der Anzahl der Aussagevariablen werden. Dagegen bietet das syntaktische Beweisen mit Hilfe der Gesetze aus Lemma 2.5 die Möglichkeit den Beweis kompositionell zu organisieren. Das Regelsystem erfüllt dabei zwei zentrale Zielsetzungen, die allgemein bei Axiomatisierung von Regel- bzw. Gleichungssystemen wichtig sind:

Korrektheit: Es können nur gültige Aussagen durch das Ersetzen von "Gleichem durch Gleiches" abgeleitet werden.

Vollständigkeit: Alle gültigen Aussagen können durch das Ersetzen von "Gleichem durch Gleiches" auch hergeleitet werden.

Für die Prädikatenlogik stellt sich die Situation allerdings schon etwas schwieriger dar. Zwar ist die Korrektheit in allen üblichen Regelsystemen gegeben, aber die Vollständigkeit hängt stark von den betrachteten Strukturen ab. Für die Struktur der natürlichen Zahlen wurde durch Gödel in seinem berühmten *1. Unvollständigkeitssatz* nachgewiesen, dass es kein vollständiges und korrektes Regelsystem geben kann. Einfache Strukturen wie Gruppen (siehe Kapitel 8) sind dagegen vollständig axiomatisierbar. Das bedeutet hier aber nur, dass genau die gültigen Aussagen im Regelsystem hergeleitet werden können. Dennoch gibt es hier kein Verfahren, das *e*ntscheiden kann, ob eine Aussage gültig ist oder nicht.

Kapitel 3

Relationen und Funktionen

3.1 Relationen

Relationen stellen Beziehungen zwischen den Elementen von Mengen her. Grundlegend für den Relationenbegriff ist die Konstruktion des *kartesischen Produktes*.

3.1.1 Kartesisches Produkt

Intuitiv ist das *Kartesische Produkt (auch Kreuzprodukt)* zweier Mengen A und B das Resultat, wenn man jedes Element aus A mit jedem aus B kombiniert.

Definition 3.1 (Kartesisches Produkt) *Seien A und B Mengen. Das* Kartesische Produkt *von A und B ist definiert durch:*

$$A \times B \;=_{df}\; \{(a,b) \mid a \in A \wedge b \in B\}$$

Elemente $(a,b) \in A \times B$ heißen *geordnete Paare*. Auf diesen ist die Gleichheit definiert durch:

$$(a,b) = (a',b') \;\Leftrightarrow_{df}\; a = a' \wedge b = b'.$$

Geordnete Paare sind von zweielementigen Mengen zu unterscheiden, denn bei letzteren spielt die Reihenfolge der Elemente keine Rolle. So gilt $\{1,2\} = \{2,1\}$, aber $(1,2) \neq (2,1)$. Dennoch kann man geordnete Paare auch als zweielementige Mengen auffassen. Hierzu definiert man:

$$(a,b) \;=_{df}\; \{\{a\},\{a,b\}\}.$$

Diese Festlegung ist im Einklang mit der strengeren Gleichheitheitsanforderung geordneter Paare, denn es gilt z.B. $(1,2) = \{\{1\},\{1,2\}\} \neq \{\{2\},\{1,2\}\} = (2,1)$.

Beispiel 3.2 (Kartesisches Produkt) *Betrachten wir* $A = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ *und* $B = \{As, König, Dame, Bube, 10, 9, 8, 7\}$ *so ist das kartesische Produkt die Menge der 32 Spielkarten in einem Skat-Spiel:*

$$\begin{aligned} A \times B \;=\; \{\, &(\clubsuit, As), \ldots, (\clubsuit, 7), \\ &(\spadesuit, As), \ldots, (\spadesuit, 7), \\ &(\heartsuit, As), \ldots, (\heartsuit, 7), \\ &(\diamondsuit, As), \ldots, (\diamondsuit, 7)\,\} \end{aligned}$$

Sofern $A = B$ gilt, schreiben wir statt $A \times A$ auch A^2. Das kartesische Produkt lässt sich auf mehr als zwei Mengen verallgemeinern durch:

$$M_1 \times M_2 \times \ldots \times M_n \;=_{df}\; ((\ldots(M_1 \times M_2) \times \ldots) \times M_n).$$

Wir schreiben $(m_1, m_2, \ldots, m_n)$ statt $((..(m_1, m_2), \ldots), m_n)$ und bezeichnen diese als *Tupel* der Länge n. Analog zur Notation A^2 schreiben wir kurz A^n an Stelle von $\underbrace{A \times \ldots \times A}_{n \text{ mal}}$.

Beispiel 3.3 (Endliche Bitvektoren) *Ein wichtiges Beispiel eines n-fachen kartesischen Produktes ist* $\{0,1\}^n$. *Die Tupel aus* $\{0,1\}^n$ *werden auch* Bitvektoren *der Länge n genannt. Sie haben eine besondere Rolle bei der Repräsentation von Teilmengen einer n-elementigen Menge* $M = \{m_1, \ldots, m_n\}$. *Denn* $A \subseteq M$ *kann durch einen* charakteristischen Bitvektor $(b_1, \ldots, b_n) \in \{0,1\}^n$ *repräsentiert werden mit:*

$$b_i = 1 \;\Leftrightarrow_{df}\; m_i \in A.$$

Betrachtet man aus der Grundmenge der Monate $M =_{df} \{Januar, \ldots, Dezember\}$ *die Teilmenge* M_{31} *der Monate mit 31 Kalendertagen, so können diese durch den Bitvektor*

$$(1,0,1,0,1,0,1,1,0,1,0,1)$$

beschrieben werden. Diese Sichtweise als Bitvektor ist versteckt auch in der bekannten Merkregel zu finden, die die Monate mit 31 Tagen anhand der Fingerknöchel beschreibt. Hier stehen die Knöchelerhebungen für die 1- *und die Knöchelvertiefungen für die* 0-*Einträge.*

Die Teilmenge der Monate M_r, *die den Buchstaben r enthalten, werden durch den Bitvektor*

$$(1,1,1,1,0,0,0,0,1,1,1,1)$$

charakterisiert.

3.1.2 n-stellige Relationen

Formal ist eine n-stellige Relation definiert durch:

Definition 3.4 (n-stellige Relation) *Sei $n \geq 1$ und $M_1, \ldots, M_n$ Mengen. Eine Teilmenge $R \subseteq M_1 \times \ldots \times M_n$ heißt n-stellige Relation auf $M_1 \times \ldots \times M_n$.*

Relationen spielen in der Informatik an verschiedenen Stellen eine bedeutende Rolle. Abbildung 3.1 illustriert eine Relation, die Dozenten und Kurse miteinander in Beziehung setzt.

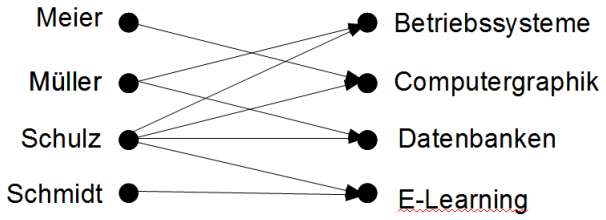


Abbildung 3.1: Relation zwischen Dozenten und Kursen.

Es fällt auf, dass in Definition 3.4 im Fall $n = 1$ auch einstellige Relationen zugelassen sind. In der Tat sind einstellige Relationen $R \subseteq M$ nichts anderes als Teilmengen von M. In Beispiel 3.3 hatten wir bereits Bitvektoren, sprich Elemente von $\{0,1\}^{|M|}$ als eine andere Darstellung von Teilmengen kennengelernt. Gehen wir hier zu den Relationen über, also Teilmengen von $\{0,1\}^{|M|}$, so sind dieses Mengensysteme. Anders ausgedrückt charakterisiert $R \subseteq \{0,1\}^{|M|}$ also eine Menge von Teilmengen von M.

3.1.3 Binäre Relationen

Im folgenden werden wir uns im wesentlichen auf *binäre* (oder auch *zweistellig* genannte) Relationen beschränken. Wir verwenden hier typischerweise die Notation $R \subseteq A \times B$. In diesem Fall heißt A *Argumentbereich* und B *Bildbereich* der Relation. Vertauscht man deren Rollen kommt man zum Begriff der Umkehrrelation.

Definition 3.5 (Umkehrrelation) *Sei $R \subseteq A \times B$ eine binäre Relation. Die Umkehrrelation $R^{-1} \subseteq B \times A$ ist definiert durch $R^{-1} =_{df} \{(b,a) \mid (a,b) \in R\}$.*

Binäre Relationen können komponiert werden, wenn der Zielbereich der ersten Relation mit dem Argumentbereich der zweiten Relation übereinstimmt. In diesem Fall definiert man:

Definition 3.6 (Produktrelation) *Seien $R_1 \subseteq A \times B$ und $R_2 \subseteq B \times C$ Relationen. Die* Produktrelation *$R_1 \odot R_2 \subseteq A \times C$ ist definiert durch $R_1 \odot R_2 =_{df} \{(a,c) \mid \exists b \in B.\ (a,b) \in R_1 \wedge (b,c) \in R_2\}$.*

Die Konstruktion ist illustriert in Abbildung 3.2.

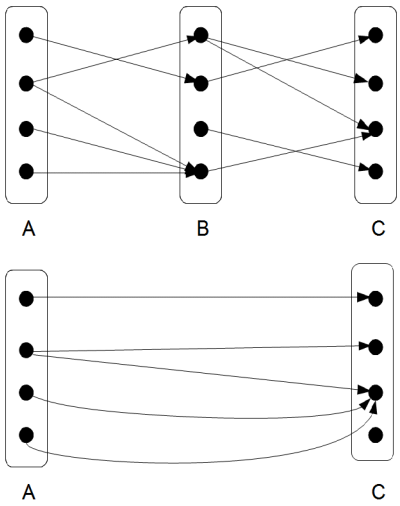


Abbildung 3.2: Produktrelation

Konventionen: Statt $(a, b) \in R$ wird oft auch die *Infixnotation* $a\,R\,b$ verwendet. Dieses ist insbesondere bei Relationen wie "$=, \leq, <, \ldots$" der Fall, wo die Infixschreibweise üblich ist. Mit $R(a) = \{b \mid (a, b) \in R\}$ wird die Menge der Bilder eines Elementes aus dem Argumentbereich bezeichnet. Man beachte, dass $R(a)$ auch leer sein kann. Entsprechend ist $R^{-1}(b)$ die Menge der Urbilder eines Elementes aus dem Bildbereich.

Eine Sonderrolle spielen Relationen der Art $R \subseteq A \times A$, also solche bei denen Argument- und Bildbereich übereinstimmen. Diese werden als *homogene* Relationen bezeichnet. Die *identische Relation* auf A ist definiert als $I_A =_{df} \{(a, a) \mid a \in A\}$.[1]

3.2 Funktionen

Wie aus der Schulmathematik bekannt sind Funktionen eindeutige Zuordnungen von Elementen eines Argumentbereiches zu Elementen eines Zielbereiches. Dieses wird im Folgenden präzisiert, indem wir Funktionen als binäre Relationen mit speziellen Zuordnungseigenschaften beschreiben. Hierfür betrachten wir zwei symmetrisch aufgebaute Eindeutigkeits- und Totalitätseigenschaften.

[1] Wenn A aus dem Kontext klar hervorgeht, kann der Index A auch wegfallen.

Definition 3.7 (Rechts-,Linkseindeutigkeit) *Eine binäre Relation $R \subseteq A \times B$ heißt*

1. rechtseindeutig $\Leftrightarrow_{df}$
   $\forall\, a \in A,\, b_1, b_2 \in B.\ (a, b_1) \in R \wedge (a, b_2) \in R \ \Rightarrow\ (b_1 = b_2)$
2. linkseindeutig $\Leftrightarrow_{df}$
   $\forall\, a_1, a_2 \in A,\, b \in B.\ (a_1, b) \in R \wedge (a_2, b) \in R \ \Rightarrow\ (a_1 = a_2)$

Rechtseindeutige Relationen zeichnen sich dadurch aus, dass kein Element des Argumentbereiches verschiedene Elemente des Bildbereiches erreicht. Abbildung 3.3(a) zeigt eine Relation, die nicht rechtseindeutig ist. Entsprechend sind linkseindeutige Relationen solche, bei denen Elemente des Zielbereiches nicht von verschiedenen Elementen des Argumentbereiches getroffen werden dürfen. Abbildung 3.3(b) zeigt eine Relation, die zwar rechts- aber nicht linksseindeutig ist.

Abbildung 3.3: a) Nicht rechtseindeutige Relation b) Nicht linkseindeutige Relation

Eine Relation, die allen Elementen des Argumentbereiches Bilder zuordnet heißt linkstotal. Werden alle Elemente des Bildbereiches getroffen, so spricht man von einer rechtstotalen Relation.

Definition 3.8 (Links-,Rechtstotalität) *Eine binäre Relation $R \subseteq A \times B$ heißt*

1. linkstotal $\Leftrightarrow_{df}\ \forall\, a \in A.\ \exists\, b \in B.\ (a, b) \in R$
2. rechtstotal, $\Leftrightarrow_{df}\ \forall\, b \in B.\ \exists\, a \in A.\ (a, b) \in R$

Die Relation aus Abbildung 3.3(a) ist offensichtlich rechts- aber nicht linkstotal, während die Relation aus Abbildung 3.3(b) links- aber nicht rechtstotal ist.

Definition 3.9 (Funktion) *Eine rechtseindeutige, linkstotale Relation heißt Funktion.*

Funktionen werden auch *Abbildungen* genannt. Ist $f \subseteq A \times B$ eine Funktion, so sind die Bildmengen $f(a)$ wegen der Rechtseindeutigkeit höchstens und wegen der Linkstotalität mindestens einelementig. Statt $f(a) = \{b\}$ schreibt man dann kurz $f(a) = b$. Anstelle $f \subseteq A \times B$ benutzt man die Notation $f : A \to B$ und beschreibt die Zuordnung der Funktionswerte in der Form $a \mapsto f(a)$. Für die Menge aller Funktionen von A nach B schreiben wir auch kurz B^A. Die Komposition von Funktionen $f : A \to B$ und $g : B \to C$ entspricht ihrer Produktrelation bei Sichtweise als Relationen. Man beachte, dass Linkstotalität und Rechtseindeutigkeit durch das Relationenprodukt erhalten

bleiben. Historisch hat sich allerdings bei der Komposition von Funktionen eine gegenüber dem Relationenprodukt umgekehrte Reihenfolge der Argumente durchgesetzt. Die zuerst angewandte Funktion steht rechts. Es gilt also:

$$g \circ f \;=_{df}\; f \odot g$$

wobei $\circ$ das Symbol für die Funktionskomposition ist. Der Vorteil der geänderten Reihenfolge ist, dass die Komposition von Funktionen so kompatibel mit der argumentweisen Anwendung ist. Es gilt nämlich für ein Argument $a \in A$:

$$(g \circ f)(a) = g(f(a)).$$

Die identischen Relationen I_A sind per Konstruktion auch Funktionen von A nach A. Im Funktionskontext benutzen wir gleichbedeutend die Notation id_A.

3.2.1 Eigenschaften von Funktionen

Linkstotalität und Rechtseindeutigkeit sind die essentiellen Eigenschaften von Funktionen. Rechtstotalität und Linkseindeutigkeit bestimmen besondere zusätzliche Funktionseigenschaften.

Definition 3.10 (Injektivität, Surjektivität) *Eine Funktion $f : A \to B$ heißt:*

1. injektiv $\Leftrightarrow_{df}$ *f ist linkseindeutig*
2. surjektiv $\Leftrightarrow_{df}$ *f ist rechtstotal*
3. bijektiv $\Leftrightarrow_{df}$ *f ist injektiv und surjektiv*

Wir betrachten einige Beispiele für diese Eigenschaften:

Beispiel 3.11

1. *Die Funktion $f_1 : \mathbb{N} \to \mathbb{N}$ mit $n \mapsto 2\,n$ ist injektiv, denn für $n, m \in \mathbb{N}$ mit $n \neq m$ folgt $f_1(n) \neq f_1(m)$. Andererseits ist f_1 nicht surjektiv, denn es gibt kein $n \in \mathbb{N}$ mit $f_1(n) = 1$.*
2. *Die Funktion $f_2 : \mathbb{Z} \to \mathbb{N}$ mit $z \mapsto |z|$ ist surjektiv,[a] denn jedes $n \in \mathbb{N}$ ist Bild der entsprechenden Zahl aus $\mathbb{Z}$. Allerdings ist f_2 nicht injektiv, denn es gilt $f_2(-1) = f_2(1) = 1$. Das bedeutet, dass die Eins von verschiedenen Elementen aus $\mathbb{Z}$ getroffen wird.*
3. *Die Funktion $f_3 : \mathbb{Q} \to \mathbb{Q}$ mit $q \mapsto 2\,q$ ist bijektiv. Die Injektivität folgt analog wie für f_1. Die Surjektivität ergibt sich aus der Tatsache, dass jede Zahl $q \in \mathbb{Q}$ von $\frac{q}{2} \in \mathbb{Q}$ getroffen wird.*

[a] $|z|$ bezeichnet den Absolutbetrag von z definiert durch $|z| \;=_{df}\; \begin{cases} z & \text{falls } z \geq 0 \\ -z & \text{sonst} \end{cases}$.

Beim Beweis der Injektivität von f_1 wurde nicht direkt mit der Definition der Linkseindeutigkeit argumentiert. Vielmehr wurde statt der Implikation $f_1(a_1) = f_1(a_2) \Rightarrow a_1 = a_2$ die Implikation $a_1 \neq a_2 \Rightarrow f_1(a_1) \neq f_1(a_2)$ gezeigt. Dieses Vorgehen ist allgemein als Prinzip der Kontraposition bekannt:

Beweisprinzip 3.12 (Kontraposition)

Seien $\mathcal{A}, \mathcal{B}$ Aussagen. Dann gilt:

$$(\mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow (\neg\mathcal{B} \Rightarrow \neg\mathcal{A}).$$

In Worten: Eine Implikation $\mathcal{A} \Rightarrow \mathcal{B}$ kann man beweisen, indem man die umgekehrte Implikation über den negierten Aussagen beweist.

Die Gültigkeit des Prinzip der Kontraposition kann leicht anhand von einer Wahrheitstafel gezeigt werden.

Offensichtlich ist die Umkehrrelation einer Funktion im Allgemeinen keine Funktion (man betrachte etwa die Funktion f_2 aus Beispiel 3.11). Injektive Funktionen haben wegen der Linkseindeutigkeit zumindest partiell definierte Umkehrfunktionen (siehe Kapitel 3.2.3). Eine bijektive Funktionen f hat allerdings eine Umkehrfunktion, die wir mit f^{-1} bezeichnen.

Es gilt der folgende hilfreiche Zusammenhang:

Satz 3.13 *Seien $f : A \to B$ und $g : B \to A$ Funktionen mit $g \circ f = id_A$ und $f \circ g = id_B$. Dann sind f und g bijektiv und es gilt weiter $f^{-1} = g$ bzw. $g^{-1} = f$.*

Beweis Wegen der symmetrischen Rollen von f und g genügt es die Bijektivität von f zu zeigen sowie die Eigenschaft, dass g Umkehrfunktion von f ist.

Wir zeigen zunächst die Injektivität von f und betrachten dazu $a, a' \in A$. Dann gilt:

$$\begin{array}{lll} f(a) = f(a') & \Rightarrow & g(f(a)) = g(f(a')) \qquad (g \text{ ist Funktion}) \\ & \Rightarrow & (g \circ f)(a) = (g \circ f)(a') \qquad (\text{Def. } \circ) \\ & \Rightarrow & id_A(a) = id_A(a') \qquad (g \circ f = id_A) \\ & \Rightarrow & a = a' \qquad (\text{Def. } id_A) \end{array}$$

Für die Surjektivität haben wir zu zeigen, dass jedes $b \in B$ ein Urbild $a \in A$ besitzt. Sei also $b \in B$. Dann setze $a =_{df} g(b)$. Es gilt:

$$f(a) \overset{\text{Def. } a}{=} f(g(b)) = (f \circ g)(b) \overset{f \circ g = id_B}{=} id_B(b) = b$$

Schließlich zeigen wir noch, dass g Umkehrfunktion von f ist, also $f^{-1} = g$ gilt. Seien $a \in A,\ b \in B$. Dann gilt:

$$\begin{array}{lll} f(a) = b & \Rightarrow & g(f(a)) = g(b) \qquad (g \text{ ist Funktion}) \\ & \Rightarrow & (g \circ f)(a) = g(b) \qquad (\text{Def. } \circ) \\ & \Rightarrow & id_A(a) = g(b) \qquad (g \circ f = id_A) \\ & \Rightarrow & a = g(b) \qquad (\text{Def. } id_A) \\ & \Rightarrow & f^{-1}(b) = g(b) \qquad (\text{Def. } f^{-1}) \end{array}$$

□

Obwohl wir schon mit quantifizierten Aussagen umgegangen sind, möchten wir an dieser Stelle noch einmal ein prinzipielles Vorgehen beim Beweisen aufgreifen. Dieses machen wir anhand der Surjektivitätseigenschaft im vorangegangenen Beweis klar. Formal betrachtet ist hier eine geschachtelte All- und Existenzaussage zu zeigen, nämlich:

$$\forall\, b \in B.\ \exists\, a \in A.\ f(a) = b.$$

Der Beweis benutzt dabei folgendes Prinzip zu Elimination der Quantoren:

Beweisprinzip 3.14 (Auflösung Quantoren)

- *Der Allquantor einer Allaussage $\forall\, x.\ A(x)$ wird aufgelöst, indem die Variable x* **beliebig** *aus der Struktur gewählt wird und dann $A(x)$ bewiesen wird. Im Beweis verwendet man dann eine Formulierung wie "Sei x beliebig gewählt".*
- *Der Existenzquantor einer Existenzaussage $\exists\, y.\ A(y)$ wird aufgelöst, indem die Variable y* **geeignet** *aus der Struktur gewählt wird und dann $A(y)$ bewiesen wird. Im Beweis verwendet man dann eine Formulierung wie "Wähle y als .." oder "Setze $y = ..$" .*

3.2.2 Mächtigkeit von Mengen

Injektive und bijektive Funktionen spielen eine wichtige Rolle bei der Entwicklung eines formal fundierten Mächtigkeitsbegriffes von Mengen (vergl. Kapitel 2.2), der auch für unendliche Mengen trägt. Hier definiert man nämlich zunächst:

Definition 3.15 (Mächtigkeitsbeziehungen von Mengen) *Seien A und B Mengen.*

1. *A und B heißen* gleichmächtig*, in Zeichen $A \cong B$, falls es eine bijektive Funktion $f : A \to B$ gibt.*
2. *A ist* weniger mächtig *als B,*[a] *in Zeichen $A \leqq B$, falls es eine injektive Funktion $f : A \to B$ gibt.*

[a] Der Begriff "weniger mächtig" schließt gleichmächtig ein.

Offensichtlich sind gemäß dieser Definition die endlichen Mengen $\{1, 2, 3, 4\}$ und $\{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ gleichmächtig, die Mengen $\{2, 3, 4, 5\}$ und $\{gelb, rot, blau\}$ aber nicht. In diesem Fall ist $\{gelb, rot, blau\}$ echt weniger mächtig als $\{2, 3, 4, 5\}$.

Es gilt folgender Zusammenhang:

Satz 3.16 *Seien A und B Mengen. Dann gilt:*

$$A \cong B \quad \Leftrightarrow \quad A \leqq B \ \wedge \ B \leqq A.$$

Obwohl dieser Zusammenhang intuitiv naheliegend ist, ist der Beweis keinesfalls trivial. Das Resultat ist als Satz von Cantor-Bernstein-Schröder bekannt.

Interessant werden Mächtigkeitsbetrachtungen im Falle unendlicher Mengen. Diese können wir zunächst einmal formal charakterisieren:

Definition 3.17 (Endliche und unendliche Mengen) *Eine Menge M heißt* unendlich *genau dann, wenn*

$$\exists\, M' \subset M.\ M' \cong M.$$

Andererseits ist M endlich.

Die natürlichen Zahlen sind unendlich, denn es ist $\mathbb{N}\backslash\{0\} \subset \mathbb{N}$ und die Funktion

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}\backslash\{0\} \\ n &\mapsto n+1 \end{aligned}$$

ist bijektiv.

Bei den natürlichen Zahlen sagt man auch, dass diese *abzählbar unendlich* sind. Im folgenden werden wir weitere wichtige abzählbar unendliche Mengen kennenlernen, also solche, die mit den natürlichen Zahlen gleichmächtig sind. Die erste dieser Mengen sind die ganzen Zahlen $\mathbb{Z}$. Um einzusehen, dass diese gleichmächtig zu den natürlichen Zahlen sind, betrachten wir die Funktion:

$$\begin{aligned} f_{\mathbb{Z}} : \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade} \\ -\frac{n+1}{2} & \text{falls } n \text{ ungerade} \end{cases} \end{aligned}$$

Dann bildet $f_{\mathbb{Z}}$ natürliche Zahlen in folgender Weise auf ganze Zahlen ab:

$$0 \mapsto 0,\ 1 \mapsto -1,\ 2 \mapsto 1,\ 3 \mapsto -2,\ 4 \mapsto 2, \ldots.$$

Offensichtlich ist f surjektiv, denn jede negative ganze Zahl z wird durch die natürliche Zahl $-(2z+1)$, jede andere ganze Zahl durch $2z$ getroffen. Zusätzlich ist $f_{\mathbb{Z}}$ auch injektiv, denn für unterschiedliche natürliche Zahlen ist deren Bild unterschiedlich.

Etwas erstaunlicher ist, dass $\mathbb{N} \times \mathbb{N}$ gleichmächtig zu $\mathbb{N}$ ist. Die Konstruktion der bijektiven Abbildung $d : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist bekannt als *Cantorsches Diagonalverfahren* und illustriert in Abbildung 3.4.

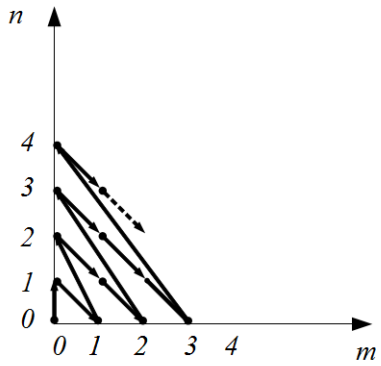


Abbildung 3.4: Cantorsches Diagonalverfahren: Aufzählung der Elemente aus $\mathbb{N} \times \mathbb{N}$ entlang der markierten Linie durch $d(0,0) = 0,\ d(0,1) = 1,\ d(1,0) = 2,\ d(0,2) = 3,\ d(1,1) = 4 \ldots$

Die dem Diagonalverfahren zugrunde liegende Funktion d kann auch explizit angegeben werden durch:[2]

$$d(m,n) =_{df} \frac{1}{2}(n+m)(n+m+1) + m.$$

Die Gleichmächtigkeit von $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ ist auch deshalb von besonderer Bedeutung, da die rationalen Zahlen $\mathbb{Q}$ durch Brüche, also Paare ganzer Zahlen, repräsentiert werden können. Da verschiedene Brüche allerdings dieselbe rationale Zahl darstellen können, etwa $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$ liefert die Funktion d hier nur eine Injektion $d_Q : \mathbb{Q} \to \mathbb{N}$. Dabei wird eine rationale Zahl repräsentiert durch einen vollständig gekürzten Bruch $\frac{p}{q}$ mit $p \in Z$ und $q \in \mathbb{N}\backslash\{0\}$. In der Diagonalfunktion lesen wir den Wert für $(f_{\mathbb{Z}}^{-1}(p), q)$ ab, also:

$$d_Q(\frac{p}{q}) \ =_{df} \ d(f_{\mathbb{Z}}^{-1}(p), q).$$

Da es die triviale Injektion von $\mathbb{N}$ nach $\mathbb{Q}$ gibt, sind nach Satz 3.16 die Mengen $\mathbb{N}$ und $\mathbb{Q}$ gleichmächtig.

Fassen wir die bisherigen Erkenntnisse zusammen, so gilt also:

$$\mathbb{N} \ \cong \ \mathbb{Z} \ \cong \ \mathbb{N} \times \mathbb{N} \ \cong \ \mathbb{Q}.$$

Dass nicht jede unendliche Menge gleichmächtig zu $\mathbb{N}$ ist, es also *überabzählbar unendliche* Mengen gibt, ergibt sich aus folgendem sehr weitreichenden Resultat.

Satz 3.18 *Sei M eine nichtleere Menge. Dann gilt $M \ncong \{0,1\}^M$.*

Beweis Angenommen es gäbe eine bijektive, also insbesondere surjektive, Funktion

$$g : M \to \underbrace{\{f \mid f : M \to \{0,1\}\}}_{\{0,1\}^M}.$$

[2] Der Term $\frac{1}{2}(n+m)(n+m+1)$ entspricht $\sum_{i=0}^{n+m-1}(i+1) \ = \ \sum_{i=0}^{n+m} i$. Das sind die aufgezählten Elemente auf den vollständig durchlaufenen Diagonalen. In der letzten Diagonalen kommen dann noch m Schritte hinzu.

Dann definieren wir folgende Funktion $h : M \to \{0,1\}$

$$h(m) \;=_{df}\; 1 - g(m)(m) \;\text{ für alle } m \in M.$$

Da g surjektiv ist, existiert ein $m_0 \in M$:

$$g(m_0) \;=\; h \tag{3.1}$$

Nach Konstruktion gilt aber $g(m_0)(m_0) \;\neq\; h(m_0)$, also $g(m_0) \;\neq\; h$ im Widerspruch zu Gleichung 3.1. □

Die Konstruktion aus dem vorherigen Beweis ist für $M = \mathbb{N}$ als Diagonalargument graphisch in Abbildung 3.5 veranschaulicht. Hier sind die Funktionen $g(i) : \mathbb{N} \to \{0,1\}$ reihenweise in der Form $g(i) = g(i)(0)\; g(i)(1)\; g(i)(2)\ldots$ dargestellt. Auf der Diagonalen gibt es immer eine Nichtübereinstimmung zur Funktion h.

$$\begin{array}{lcccccc}
g(0) & = & \underbrace{g(0)(0)}_{\neq h(0)} & g(0)(1) & g(0)(2) & g(0)(3) & \ldots \\
g(1) & = & g(1)(0) & \underbrace{g(1)(1)}_{\neq h(1)} & g(1)(2) & g(1)(3) & \ldots \\
g(2) & = & g(2)(0) & g(2)(1) & \underbrace{g(2)(2)}_{\neq h(2)} & g(2)(3) & \ldots \\
 & : & & & & : &
\end{array}$$

Abbildung 3.5: Diagonalargument für die Nichtsurjektivität von Funktion g aus dem Beweis von Satz 3.18. Funktion h wird nicht von g erreicht.

Beim Beweis von Theorem 3.18 haben wir ein weiteres wichtiges Beweisprinzip kennengelernt, nämlich das des Widerspruchsbeweises.

Beweisprinzip 3.19 (Widerspruchsbeweis)

Sei $\mathcal{A}$ eine zu beweisende Aussage. Gelingt es aus der Annahme $\neg\mathcal{A}$ auf eine Aussage $\mathcal{B}$ zu schließen, für die $\neg\mathcal{B}$ gilt, so muss $\mathcal{A}$ gelten. Kurz:

$$\big((\neg\mathcal{A} \;\Rightarrow\; \mathcal{B}) \;\wedge\; \neg\mathcal{B}\big) \Rightarrow\; \mathcal{A}.$$

Auch dieses Beweismuster lässt leicht sich anhand einer Wahrheitstafel als gültig nachweisen.

Satz 3.18 hat deshalb besondere Bedeutung, da zwischen der Potenzmenge einer Menge und den Funktionen vom M in die Menge $\{0,1\}$ eine bijektive Beziehung besteht. Eine Teilmenge A von

M kann nämlich durch ihre *charakteristische Funktion*

$$\chi_A : M \to \{0,1\}$$
$$\chi_A(m) \ =_{df} \begin{cases} 1 & \text{falls } m \in A \\ 0 & \text{sonst} \end{cases}$$

beschrieben werden. Die charakteristische Funktion ist also ein (u.U. auch unendlicher) Bitvektor, der durch seine 1-Einträge genau die in A enthaltenen Elemente markiert. Es ist leicht zu sehen, dass

$$f_M : \mathfrak{P}(M) \to \{0,1\}^M$$
$$f_M(A) \ =_{df} \ \chi_A$$

bijektiv ist. Unmittelbare Folge von Satz 3.18 ist daher, dass die Potenzmenge einer Menge M echt mächtiger als die Menge selbst ist. Dieses offenbart auch die Vielschichtigkeit unendlicher Mengen. Offensichtlich liegt mit $\mathbb{N}, \mathfrak{P}(\mathbb{N}), \mathfrak{P}(\mathfrak{P}(N)), \ldots$ eine Folge von Mengen vor, deren Mächtigkeit in jedem Schritt echt ansteigt. In der Mathematik trägt man dieser Tatsache durch den Begriff der *Kardinalzahlen* (siehe Kapitel 3.3.2) Rechnung.

Nachdem wir bereits typische abzählbar unendliche Mengen kennengelernt haben, wollen wir $\mathfrak{P}(\mathbb{N})$ als nächste Ebene noch näher beleuchten. Auch hier gibt es interessante gleichmächtige Mengen, denn es gilt:

$$\{0,1\}^{\mathbb{N}} \ \cong \ \mathfrak{P}(\mathbb{N}) \ \cong \ (0,1) \ \cong \ \mathbb{R}$$

wobei $(0,1) \ =_{df} \ \{x \in \mathbb{R} \mid 0 < x < 1\}$ das offene Intervall der reellen Zahlen zwischen 0 und 1 bezeichnet.

Die erste $\cong$-Beziehung haben wir bereits gezeigt. Die dritte $\cong$-Beziehung ist unmittelbar durch die Bijektion $f_{\mathbb{R}} : (0,1) \to \mathbb{R}$ mit $x \mapsto \frac{x-\frac{1}{2}}{x\,(x-1)}$ gerechtfertigt.

Die zweite $\cong$-Beziehung basiert auf der Idee, dass jede reelle Zahl im Intervall zwischen 0 und 1 als Binärbruchentwicklung, also als abzählbar unendlicher Bitvekor, geschrieben werden kann. So wird etwa der periodische Binärbruch $0,0010\overline{01}$ durch den entsprechenden unendlichen Bitvektor $0010010101\ldots$ repräsentiert. Da diese Repräsentation aber nur eindeutig ist, wenn keine Binärbrüche mit endständiger Periode 1 vorliegen,[3] ist die dadurch definierte Abbildung $f : (0,1) \to \{0,1\}^{\mathbb{N}}$ nur injektiv aber nicht surjektiv. Umgekehrt kann man alle unendlichen Bitvektoren, die nicht ab einer Position dauerhaft 1 sind, auf ihre Binärbruchentwicklung im Intervall $(0,1)$ abbilden, die anderen auf ihre Binärbruchentwicklung plus 1. Damit hat man eine injektive Funktion von $\{0,1\}^{\mathbb{N}}$ nach $\mathbb{R}$. Schaltet man nun die injektive Funktion $f_{\mathbb{R}}^{-1} : \mathbb{R} \to (0,1)$ dahinter, hat man auch eine injektive Funktion von $\{0,1\}^{\mathbb{N}}$ nach $(0,1)$. Aus Satz 3.16 folgt schließlich die Gleichmächtigkeit von $(0,1)$ und $\{0,1\}^{\mathbb{N}}$.

[3] Man beachte, dass z.B. der periodische Binärbruch $0,010\bar{1}$ und der Binärbruch $0,011$ dieselbe reelle Zahl repräsentieren.

3.2.3 Partiell definierte Funktionen

In der Informatik hat man es oft auch mit Abbildungen zu tun, die zwar rechtseindeutig, aber nicht linkstotal sind. Man denke zum Beispiel an ein Programm, das eine ganzzahlige Eingabe erwartet und eine ganzzahlige Ausgabe zurückliefert. Diese Ein-Ausgabe-Relation ist rechtseindeutig, denn falls ein Ergebnis zurückgeliefert wird, so ist dieses eindeutig bestimmt. Falls die Berechnung allerdings fehlschlägt, sich etwa in einer Endlosschleife verfängt, so existiert keine Ausgabe. Die Ein-Ausgabe-Relation ist also nicht linkstotal. Im Falle von rechtseindeutigen Relationen spricht man daher auch von *partiell definierten* Funktionen. Wir verwenden die Notation $f : A \dashrightarrow B$. Der *Definitionsbereich* von f (in Zeichen: $Def(f)$) ist die Menge aller Elemente aus A, die ein Bildelement besitzen. Die Komposition partiell definierter Funktionen kann analog zu der totaler Funktionen definiert werden.

3.3 Äquivalenzrelationen

Äquivalenzrelationen formalisieren mathematisch das Konzept des Identifizierens ähnlicher Objekte. Sie sind daher zentrales Instrument für den Prozess der Abstraktion. So lassen sich zum Beispiel wertegleiche arithmetische Ausdrücke wie $x + x$ und $2x$ identifizieren. Auch bei der mathematisch fundierten Konstruktion der Zahlbereiche spielen Äquivalenzrelationen eine entscheidende Rolle. Da die Brüche $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \ldots$ allesamt dieselbe rationale Zahl repräsentieren, liegt es in der Tat nahe, die rationalen Zahlen $\mathbb{Q}$ über eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ zu definieren. Formal sind Äquivalenzrelationen homogene Relationen mit folgenden Eigenschaften:

Definition 3.20 (Äquivalenzrelation) *Eine Relation* $\sim \subseteq A \times A$ *heißt* Äquivalenzrelation $\Leftrightarrow_{df}$

1. $\sim$ *ist* reflexiv, *d.h.:* $\forall\, a \in A.\ a \sim a$
2. $\sim$ *ist* symmetrisch, *d.h.:* $\forall\, a_1, a_2 \in A.\ a_1 \sim a_2 \ \Rightarrow a_2 \sim a_1$
3. $\sim$ *ist* transitiv, *d.h.:* $\forall\, a_1, a_2, a_3 \in A.\ a_1 \sim a_2 \ \wedge\ a_2 \sim a_3 \ \Rightarrow\ a_1 \sim a_3$

Beispiel 3.21 *Wir betrachten hier einige Verwandtschaftsbeziehungen unter einer Menge von Personen.*

1. *Die Geschwisterbeziehung ist eine Äquivalenzrelation.*[a]
2. *Die Freundschaftsbeziehung ist im Allgemeinen keine Äquivalenzrelation, da diese nicht transitiv ist. Wenn Anna mit Bob befreundet ist und Bob mit Charlotte, so müssen Anna und Charlotte nicht unbedingt befreundet sein.*
3. *Die Bruderbeziehung ist keine Äquivalenzrelation, da diese nicht symmetrisch ist. Andreas ist zwar Bruder von Beate, aber natürlich nicht umgekehrt.*

[a] Wir nehmen dabei an, dass eine Person Geschwister von sich selbst ist. Ferner haben Geschwister ein gemeinsames Elternpaar, was Halbgeschwister ausschließt.

Äquivalenzrelationen über einer Grundmenge A legen *Äquivalenzklassen* auf A fest.

Für $a \in A$ ist die zugehörige $\sim$-Äquivalenzklasse:

$$[a]_\sim \ =_{df} \ \{a' \in A \mid a \sim a'\}$$

Die Äquivalenzklassen sind also Teilmengen von A, die nur äquivalente Elemente enthalten. Die Menge der Äquivalenzklassen bilden ein besonderes Mengensystem, dessen Typ wir im folgenden näher betrachten.

3.3.1 Partitionen

Partitionen sind Mengensysteme, die eine Grundmenge in eine disjunkte Menge von Teilmengen, auch *Partitionsklassen* genannt, zerlegen. Formal:

Definition 3.22 (Partition) *Sei M eine Menge. $P \subseteq \mathfrak{P}(M)$ heißt* Partition $\Leftrightarrow_{df}$

1. $\emptyset \notin P$ *(Die Partitionsklassen sind nichtleer)*
2. $\bigcup_{M' \in P} M' \ = \ M$ *(Die Partitionsklassen überdecken M)*
3. $\forall\, M_1, M_2 \in P.\ M_1 \neq M_2 \ \Rightarrow \ M_1 \cap M_2 = \emptyset$ *(Die Partitionsklassen sind paarweise disjunkt)*

Beispiel 3.23 *Für $M = \{1,2,3\}$ sind $P_1 =_{df} \{\{1\},\{2\},\{3\}\}$ und $P_2 =_{df} \{\{1,2\},\{3\}\}$ Partitionen. $P_3 =_{df} \{\{1,2\},\{2\}\}$ ist keine Partition, da das Element 3 nicht überdeckt wird. Ebenso ist $P_4 =_{df} \{\{1,2\},\{2,3\}\}$ keine Partition, denn die beiden Partitionsklassen sind nicht disjunkt.*

Partitionen und Äquivalenzrelationen stehen in enger Beziehung. Es gilt nämlich:

Lemma 3.24 *Sei $\sim \subseteq \ A \times A$ eine Äquivalenzrelation. Dann bildet die Menge aller Äquivalenzklassen*

$$A/\sim \ =_{df} \ \{[a]_\sim \mid a \in A\}$$

eine Partition auf A.

Beweis Wegen $a \in [a]_\sim$ für alle $a \in A$ sind die Äquivalenzklassen offensichtlich nicht leer. Außerdem gilt $\bigcup_{a \in A}[a]_\sim = A$. Es bleibt zu zeigen, dass die Äquivalenzklassen paarweise disjunkt sind. Dieses zeigen wir per Kontraposition. Sei $[a_1]_\sim \cap [a_2]_\sim \neq \emptyset$ für $a_1, a_2 \in A$. Dann existiert $a' \in [a_1]_\sim$ und $a' \in [a_2]_\sim$. Also gilt $a' \sim a_1$ und $a' \sim a_2$. Mit der Symmetrie und Transitivität von $\sim$ folgt $a_1 \sim a_2$ und somit auch $[a_1]_\sim = [a_2]_\sim$. □

Umgekehrt induziert auch jede Partition auf A eine Äquivalenzrelation, nämlich:

Lemma 3.25 *Sei $P \subseteq \mathfrak{P}(A)$ eine Partition auf A. Dann ist*

$$\sim_P =_{df} \{(a_1, a_2) \in A \times A \mid \exists\, A' \in P.\ a_1, a_2 \in A'\}$$

eine Äquivalenzrelation.

Beweis Wir zeigen zuerst, dass $\sim_P$ reflexiv ist. Sei $a \in A$. Weil P ganz A überdeckt, existiert eine Partitionsklasse A', die a enthält. Per Definition gilt dann $a \sim_P a$. Um die Symmetrie von $\sim_P$ zu zeigen, nehmen wir an es gelte $a_1 \sim_P a_2$ für Elemente $a_1, a_2 \in A$. Per Definition liegen a_1 und a_2 in einer gemeinsamen Partitionsklasse A' und es folgt dann auch $a_2 \sim_P a_1$. Der Beweis der Transitivität ist analog. □

Insbesondere induziert jede Funktion $f : A \to B$ eine Äquivalenzrelation $\sim_f$ auf A:

$$a_1 \sim_f a_2 \ \Leftrightarrow_{df} \ f(a_1) = f(a_2).$$

Die zugehörige Partition wird als *Urbildpartition* bezeichnet, denn ihre Partitionsklassen sind die Urbilder der Elemente aus $f(A)$, also der Gestalt $f^{-1}(b)$ mit $b \in f(A)$.

Beispiel 3.26 *Wir betrachten eine Menge von Studierenden $S =_{df}$ {Adam, Barbie, Conan, Dana, Eric, Fred, Gia, Hannah, Ken, Iris, Jan}, die an einer Klausur teilgenommen haben. Die erzielte Klausurnote kann als Funktion $n : S \to \{1, 2, 3, 4, 5\}$ wie angesehen werden und sei hier etwa:*

$$\text{Adam} \mapsto 2, \text{Barbie} \mapsto 5, \text{Conan} \mapsto 1, \text{Dana} \mapsto 2, \text{Eric} \mapsto 3, \text{Fred} \mapsto 3,$$
$$\text{Gia} \mapsto 3, \text{Hannah} \mapsto 2, \text{Ken} \mapsto 5, \text{Iris} \mapsto 1, \text{Jan} \mapsto 2$$

Die zugehörige Äquivalenzrelation identifiziert Studierende mit derselben Klausurnote. Die Partitionsklasse der Einserresultate ist:

$$n^{-1}(1) \ = \ \{s \in S \mid n(s) = 1\} \ = \ \{\text{Conan}, \text{Iris}\}.$$

Die gesamte Urbildpartition ist:

$$\{\{\text{Conan}, \text{Iris}\}, \{\text{Adam}, \text{Dana}, \text{Hannah}, \text{Jan}\}, \{\text{Eric}, \text{Fred}, \text{Gia}\}, \{\text{Barbie}, \text{Ken}\}\}.$$

Man beachte, dass die Note 4 nicht vergeben wurde und daher die leere Urbildmenge nicht Bestandteil der Partition ist.

3.3.2 Kardinalzahlen

Man kann sich leicht überlegen, dass die Gleichmächtigkeit von Mengen, wie sie in Kapitel 3.2.2 definiert wurde, eine Äquivalenzrelation auf Mengen ist.[4] Die Äquivalenzklassen dieser Relation werden als *Mächtigkeit* oder *Kardinalzahlen* bezeichnet. Wir verwenden wie im Falle endlicher

[4] Wegen der Antinomie der Allmenge muss der Begriff streng genommen auf der Klasse der Mengen oder relativ zu einem zugrundeliegenden Mengenuniversum gesehen werden.

Mengen die Notation $|M|$. Die kleinste unendliche Kardinalzahl ist $\aleph_0 =_{df} |\mathbb{N}|$. Die Kontinuumshypothese besagt, dass die nächst größere unendliche Kardinalzahl $\aleph_1 =_{df} |\mathbb{R}|$ ist.

Basierend auf den Mächtigkeitsgesetzen endlicher Mengen definiert man folgende Rechenoperationen auf Kardinalzahlen:

Definition 3.27 (Operationen auf Kardinalzahlen)

1. $|A| + |B| \ =_{df} \ |A \cup B|$, *falls* $A \cap B = \emptyset$
2. $|A| * |B| \ =_{df} \ |A \times B|$
3. $|A|^{|B|} \ =_{df} \ |A^B|$

Kardinalzahlen sind durch $\leqq$ partiell geordnet (siehe Kapitel 6.1).[5] Für unendliche Mengen A und B mit $|A| \leq |B|$ gilt:

$$|A| + |B| = |A| * |B| = |B|.$$

[5] Die Antisymmetrie ist hier Konsequenz von Satz 3.16.

Kapitel 4

Induktives Definieren

Induktiv aufgebaute Strukturen sind in der Informatik von zentraler Bedeutung. Klassisch sind hier die natürlichen Zahlen zu nennen, die durch Peano's Axiomatisierung aus dem Atom Null und der Nachfolgefunktion konstruiert werden. Die überragende Bedeutung des induktiven Prinzips kommt aber erst durch eine Vielzahl anderer Anwendungsbereiche zum Ausdruck. So sind Zahldarstellungen, Ausdrücke, Datenstrukturen, Programmier- und Prozessspachen großteils induktiv aufgebaut. Algorithmen, Funktionen und Prädikate sind induktiv über den Aufbau der Strukturen definiert. Induktives Beweisen (siehe Kapitel 6) bedeutet "Beweisen entlang der induktiven Struktur" der zugrundeliegenden Objekte. Induktionsbeweise erlauben es, Eigenschaften für unendlich viele Objekte auf einen repräsentativen Induktionsschluss zurückzuführen.

4.1 Natürliche Zahlen

Der intuitive Umgang mit natürlichen Zahlen ist dem Leser seit früher Kindheit vertraut. Etwas genauer betrachtet lassen sich natürliche Zahlen als das Resultat eines Abstraktionsprozesses verstehen, bei dem gleichmächtige endliche Mengen identifiziert werden. Die natürlichen Zahlen sind dann Modell der Äquivalenzklassen dieser Abstraktion.

4.1.1 Peano-Axiome

Eine formale Grundlage für die Definition natürlicher Zahlen sind die Peano-Axiome: Grundidee dabei ist, dass jede natürliche Zahl durch eine endliche Anwendung der Nachfolgefunktion $\mathfrak{s}(\cdot)$ entsteht.

Definition 4.1 (Peano-Axiome)

P1 0 *ist eine natürliche Zahl:* $0 \in \mathbb{N}$.

P2 *Jede natürliche Zahl* n *besitzt eine eindeutig bestimmte natürliche Zahl* $\mathfrak{s}(n)$ *als Nachfolger:*

$\forall\, n \in \mathbb{N}.\ \exists\, m \in \mathbb{N}.\ m = \mathfrak{s}(n)$

P3 *0 ist nicht Nachfolger einer natürlichen Zahl:*

$\nexists\, n \in \mathbb{N}.\ 0 = \mathfrak{s}(n)$

P4 *Verschiedene natürliche Zahlen haben verschiedene Nachfolger:*

$\forall\, m, n \in \mathbb{N}.\ n \neq m \ \Rightarrow\ \mathfrak{s}(n) \neq \mathfrak{s}(m)$

P5 Induktionsaxiom*: Ist* $M \subseteq \mathbb{N}$ *mit* $0 \in M$ *und der Eigenschaft, dass aus* $n \in M$ *auch* $\mathfrak{s}(n) \in M$ *folgt, so muss* $M = \mathbb{N}$ *gelten.*

$(\forall\, M \subseteq \mathbb{N}.\ 0 \in M\ \wedge\ \forall\, n \in \mathbb{N}.\ n \in M \Rightarrow \mathfrak{s}(n) \in M)\ \Rightarrow\ (M = \mathbb{N})$.

Die Axiome (P1) und (P3) beschreiben die Sonderrolle der Null. Die Axiome (P2) und (P4) drücken aus, dass die Nachfolgerelation $\mathfrak{s}(\cdot)$ linkstotal und rechtseindeutig, mithin also eine Funktion ist. Axiom (P5) ist Grundlage des später in Theorem 6.14 eingeführten Beweisprinzips der vollständigen Induktion.

An dieser Stelle sei darauf hingewiesen, dass im Induktionsaxiom (P5) erstmals eine sogenannte prädikatenlogische Formel 2. Stufe vorliegt. Der äußere Allquantor bezieht sich nämlich nicht auf Individuen der Struktur natürlicher Zahlen, sondern auf Mengen solcher Individuen. Allgemein spricht man von Prädikatenlogik 2. Stufe, wenn dort auch über Relationen quantifiziert werden darf. Lässt man auch Relationen über Relationen zu so kommt man zur Prädikatenlogik 3. Stufe usw.

4.1.2 Operationen auf natürlichen Zahlen

Es fällt auf, dass Operationen wie Addition und Multiplikation nicht Bestandteil der Peano-Axiome sind. Diese können aber leicht auf der axiomatischen Grundlage aufbauend definiert werden. Betrachten wir zunächst die Addition und definieren:

Definition 4.2 (Addition natürlicher Zahlen) *Die Addition zweier Zahlen aus* $\mathbb{N}$ *ist induktiv definiert durch*

$$\begin{aligned} 0 + m &=_{df} m \\ \mathfrak{s}(n) + m &=_{df} \mathfrak{s}(n + m) \end{aligned}$$

Auf der Addition basierend kann die Multiplikation definiert werden:

Definition 4.3 (Multiplikation natürlicher Zahlen) *Die Multiplikation zweier Zahlen aus* $\mathbb{N}$ *ist induktiv definiert durch*

$$\begin{aligned} 0 \cdot m &=_{df} 0 \\ \mathfrak{s}(n) \cdot m &=_{df} m + (n \cdot m) \end{aligned}$$

Summen und Produkte können k-stellig ($k \in \mathbb{N}$) erweitert werden durch folgende induktive Definition:

$$\sum_{i=1}^{k} n_i =_{df} \begin{cases} 0 & \text{falls } k = 0 \\ (\sum_{i=1}^{k-1} n_i) + n_k & \text{sonst} \end{cases}$$

$$\prod_{i=1}^{k} n_i =_{df} \begin{cases} 1 & \text{falls } k = 0 \\ (\prod_{i=1}^{k-1} n_i) \cdot n_k & \text{sonst} \end{cases}$$

wobei $n_i \in \mathbb{N}$ für alle $i \in \{1, \ldots, k\}$.

$\prod_{i=1}^{n} i = (..(1 \cdot 2) \ldots) \cdot n)$ wird auch *Fakultät* von n genannt, in Zeichen $n!$.

$\prod_{i=1}^{n} m = \underbrace{(..(m \cdot m) \ldots) \cdot m)}_{n \text{ mal}}$ ist die n-te Potenz von m, in Zeichen m^n.

4.1.3 Induktiv definierte Algorithmen

Basierend auf der induktiven Definition natürlicher Zahlen können eine Vielzahl weiterer Funktionen definiert werden. Etwas weniger offensichtlich, aber mindestens so bedeutend sind induktiv definierte Algorithmen. In der Einleitung haben wir bereits das Problem der Türme von Hanoi kennengelernt.

Die algorithmische Lösung für das Problem n Scheiben von einem Ausgangsstab A unter Verwendung eines Hilfsstabes B auf einen Zielstapel C zu verschieben läßt sich induktiv über die Anzahl n definieren:

- Für $n = 0$ ist nichts zu tun.
- Für $n > 0$
  - Verschiebe $n - 1$ Scheiben von Stapel A nach B, wobei C als Hilfsstapel dient.
  - Verschiebe die n-te Scheibe von Stapel A nach C.
  - Verschiebe $n - 1$ Scheiben von Stapel B nach C, wobei A als Hilfsstapel dient.

4.2 Induktive definierte Mengen

Natürliche Zahlen sind nur eine spezielle sehr einfache induktiv definierte Struktur. Allgemeiner können wir defieren:

Definition 4.4 (Induktiv definierte Menge) *Sei*

1. *G eine hinreichend große Grundmenge,*[a]
2. *$A \subseteq G$ eine Menge* elementarer *oder* atomarer *Bausteine und*
3. *O eine Menge von* Operatoren *mit zugehöriger Stelligkeit, die es erlauben, kleinere Bausteine zu größeren Einheiten zusammenzusetzen.*
   Formal ist $O =_{df} \bigcup_{n\in\mathbb{N}} O_n$, wobei $O_n \subseteq \{o \mid o : G^n \to G\}$.

Die durch G, A, O induktiv beschriebene Menge ist die kleinste Menge $M \subseteq G$ mit

1. *$A \subseteq M$,*
2. *Falls $o \in O_n$ und $m_1, \ldots, m_n \in M$ sind, so ist auch $o(m_1, \ldots, m_n) \in M$.*

[a] Die Grundmenge an sich ist nicht von Interesse. Sie muss nur hinreichend groß sein, um die induktiv zu beschreibenden Objekte zu enthalten. Formal wird G benötigt, um die Operatoren Op als Funktionen aufzufassen.

Induktiv definierte Mengen spielen in der Informatik eine entscheidende Rolle. Wir betrachten im folgenden einige Beispiele:

Beispiel 4.5 (Binäre Bäume) *Binäre Bäume sind die kleinste Menge mit*

1. *Der* leere Binärbaum *$-$ ist ein atomarer Binärbaum und*
2. *Falls T_1 und T_2 Binärbaume sind, so ist auch $[T_1, T_2]$ ein Binärbaum. T_1 ist linker und T_2 rechter Teilbaum von diesem.*

Der induktiv konstruierte Binärbaum $[[[-,-],[[-,-],-]],[-,-]]$ ist in Abbildung graphisch in Baumform dargestellt.

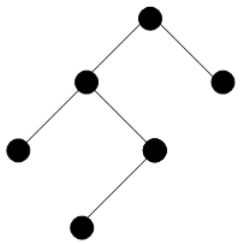


Abbildung 4.1: Graphische Darstellung eines Binärbaumes

Boolesche Terme

Im folgenden betrachten wir eine weitere induktiv definierte Menge, nämlich die der *Booleschen Terme*. Diese sind letztlich nichts anderes als ein induktiv definiertes Model für die in Kapitel 2.1 eingeführte Aussagenlogik.

Definition 4.6 (Boolesche Terme) *Sei $\mathcal{V}$ eine Menge von Booleschen Variablen, z.B. $\mathcal{V} = \{X, Y, Z, ...\}$. Die Menge $\mathcal{BT}$ aller* Booleschen Terme *über $\mathcal{V}$ ist die kleinste Menge mit:*

1. T, F *und Boolesche Variablen aus $\mathcal{V}$ sind atomare Boolesche Terme.*
2. *Sind t_1 und t_2 Boolesche Terme, so sind auch*
   - $\neg t_1$, *die* Negation *von t_1,*
   - $(\, t_1 \wedge t_2\,)$, *die* Konjunktion *von t_1 und t_2 und*
   - $(\, t_1 \vee t_2\,)$, *die* Disjunktion *von t_1 und t_2*

   Boolesche Terme.

Wir werden Booleschen Termen in Kapitel 5.4 eine Semantik zuordnen. Vorerst führen wir in diesem Kapitel aber noch eine induktive Definition ein, die Transformationen auf Booleschen Termen beschreibt:

Definition 4.7 (Syntaktische Substitution) *Die Substitution ist eine dreistellige Abbildung*

$$\cdot[\cdot/\cdot] : \mathcal{BT} \times \mathcal{BT} \times \mathcal{V} \;\rightarrow\; \mathcal{BT}.$$

Intuitiv ist $t_1[t_2/X]$ der Term, der entsteht, wenn wir in t_1 die Variable X an allen Stellen durch den Term t_2 ersetzen.

Formal ist die Substitution für Boolesche Terme $t, t_1, t_2 \in \mathcal{BT}$ und Variablen $X, Y \in \mathcal{V}$ induktiv über den Aufbau von t_1 wie folgt definiert:

- $\mathsf{T}[t/X] =_{df} \mathsf{T}$
- $\mathsf{F}[t/X] =_{df} \mathsf{F}$
- $Y[t/X] =_{df} \begin{cases} t & \text{falls } Y = X \\ Y & \text{sonst} \end{cases}$
- $(\neg t_1)[t/X] =_{df} \neg(t_1[t/X])$
- $(t_1 \wedge t_2)[t/X] =_{df} (t_1[t/X] \wedge t_2[t/X])$
- $(t_1 \vee t_2)[t/X] =_{df} (t_1[t/X] \vee t_2[t/X])$

Im folgenden ist der Substitutionsbegriff anhand zweier Beispiele illustiert. Im Falle der ersten Substitution sind die Zwischenschritte gemäß der induktiven Definition explizit ausgeführt:

Beispiel 4.8

- $\neg(Y \wedge X)[t/X] \;=\; \neg((Y \wedge X)[t/X]) \;=\; \neg(Y[t/X] \wedge X[t/X]) \;=\; \neg(Y \wedge t)$
- $(X \vee (Y \wedge X))[t/X] \;=\; (t \vee (Y \wedge t))$

Kapitel 5

Darstellung und deren Bedeutung

Grundsätzlich beschäftigt sich die Informatik mit der systematischen Verarbeitung von Informationen, insbesondere deren automatischen Verarbeitung mit Hilfe von Rechenanlagen. Unter *Information* versteht man dabei den abstrakten Bedeutungsgehalt eines Begriffs der realen Welt. Damit wir Information kommunizieren und Rechenanlagen diese verarbeiten können, wird eine schematische, formalisierte *Darstellung* benötigt: die *Repräsentation*. Eine Information kann allerdings auf verschiedene Weisen repräsentiert werden. Beispielsweise sind gebräuchliche Repräsentanten der natürliche Zahl "vier":

- Dezimal: **4**
- Binär: **100**
- Unär: ||||
- Römisch: **IV**

Umgekehrt können auch Repräsentationen unterschiedlich interpretiert werden. Zum Beispiel kann **IV** entweder eine Buchstabenfolge oder eine Darstellung der natürlichen Zahl "vier" sein.

Die Festlegung oder Konzeption eines geeigneten Repräsentationssystems (*Sprache*) zusammen mit einer adäquaten Begriffsbildung ist eine zentrale Aufgabe der Informatik, die wir als Definition eines *Semantikschemas* bezeichnen wollen. Die *Interpretation* (Deutung) liefert zu jeder Repräsentation ihre *Semantik* (Bedeutung). Ohne Interpretation sind alle Repräsentationen bedeutungsleer. Erst die Zuordnung von Bedeutungen macht die Repräsentation zur Information.

Im täglichen Leben wird zwischen Repräsentation und Information oft nicht explizit unterschieden. Vielmehr unterstellt man implizit oft eine *Standardinterpretation*. In der Informatik gibt es a priori keine Standardinterpretation. Das erhöht den Spielraum beim Design der Semantikschemata, macht aber eine explizite begriffliche Trennung zwischen dem abstrakten Informationsgehalt und der äußeren Form unbedingt notwendig.

5.1 Zeichreihen

Syntaktische Repräsentationen sind in der Regel Sequenzen von Alphabetzeichen, sogenannte *Zeichenreihen* oder *Worte*. Mathematisch gesehen sind Zeichenreihen endliche Folgen, d.h. Funktionen deren Argumentbereich ein Anfangsstück der positiven natürlichen Zahlen ist.

Definition 5.1 (Zeichenreihe)
Sei A eine endliche Menge von Zeichen (auch Alphabet *genannt). Eine Zeichenreihe (auch* Wort*) w der Länge $n \in \mathbb{N}$ über A ist eine Funktion*

$$w : \{1, \ldots, n\} \to A.$$

Für $n = 0$ ist $\{1, \ldots, n\}$ leer. Man bezeichnet die Zeichenreihe als das leere Wort ϵ.

Die Mengen aller Zeichenreihen über A mit Länge n wird mit A^n bezeichnet. Die Menge aller endlichen Zeichenreihen ist:

$$A^* \ =_{df} \ \bigcup_{n \in \mathbb{N}} A^n.$$

Offensichtlich enthält A^* auch das das leere Wort ϵ. Beschränkt man sich auf nichtleere Worte so schreiben wir $A^+ \ =_{df} \ A^* \backslash \{\epsilon\}$.

Endliche Zeichenreihen können aneinandergereiht (konkateniert) werden.

Definition 5.2 (Konkatenation von Zeichenreihen)
Seien w_1 und w_2 Zeichenreihen der Länge n und m über A. Dann ist die Konkatenation *von w_1 und w_2 definiert durch:*

$$w_1\, w_2 : \{1, \ldots, n+m\} \to A$$
$$w_1\, w_2(i) = \begin{cases} w_1(i) & \textit{falls } 1 \leq i \leq n \\ w_2(i) & \textit{falls } n+1 \leq i \leq m \end{cases}$$

An dieser Stelle wollen wir noch auf eine die Informatik folgenreiche Beobachtung hinweisen. Die Menge der endlichen Zeichenreihen A^* ist abzählbar unendlich. Für den Spezialfall der endlichen Bitvektoren, also $\{0, 1\}^*$ wurde dieses im Rahmen der Übungen behandelt. Für mehr als zweielementige Alphabete lässt sich die Konstruktion leicht verallgemeinern. Programme in einer beliebigen Programmiersprache sind durch ihre textuelle Darstellung gegeben. Folglich kann es nur abzählbar unendlich viele unterschiedliche Programme geben. Andererseits ist die Menge der Funktionen von $\mathbb{N}$ nach $\mathbb{N}$ überabzählbar unendlich. Also kann nicht jede Funktion $f : \mathbb{N} \to \mathbb{N}$ durch auf Computern ausführbare Programme berechnet werden. Diese Überlegung ist allerdings nicht konstruktiv. Im Rahmen der Vorlesung Grundbegriffe der Theoretischen Informatik (GTI) werden Sie tatsächlich Funktionen kennenlernen, die nicht berechnet werden können.

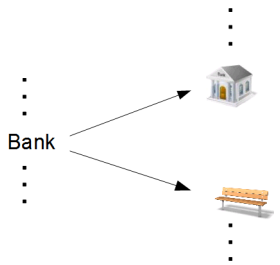
5.2 Semantikschemata

Formal wird der Zusammenhang zwischen Information und Repräsentation durch den Begriff des *Semantikschemas* erfasst.

Definition 5.3 (Semantikschema) *Ein* Semantikschema *ist ein Tripel* $(\mathcal{R}, \mathcal{I}, [\![\cdot]\!])$ *mit*

- $\mathcal{R}$*: Menge der Repräsentationen,*
- $\mathcal{I}$*: Menge der Informationen,*
- $[\![\cdot]\!] \subseteq \mathcal{R} \times \mathcal{I}$*: Semantikrelation oder Interpretation. Statt* $[\![\cdot]\!](r)$ *schreibt man* $[\![r]\!]$*.*

Bei der überwiegenden Anzahl von Semantikschemata in der Informatik liegen Sematikfunktionen oder zumindestens partiell definierte Semantikfunktionen vor. In Umfeld natürlicher Sprachen ist dieses meist nicht der Fall. So steht das Wort *Bank* in der deutschen Sprache für unterschiedliche Gegenstandskategorien unseres täglichen Lebens.



Die folgenden Semantikschemata für die Darstellung natürlicher Zahlen verdeutlichen den Unterschied zwischen der Information und ihrer Repräsentation. Wir beginnen mit der einfachsten Repräsentation, der Unärdarstellung, die sich bei Verwendung des einelementigen Strichalphabetes ergibt:

Beispiel 5.4 (Unärdarstellung natürlicher Zahlen)

- $\mathcal{R}_u =_{df} \{|\}^* = \{|, ||, |||, \ldots\}$
- $\mathcal{I}_u =_{df} \mathbb{N} = \{1, 2, \ldots\}$*: Natürliche Zahlen*
  (als Information, nicht als ihre Darstellung im Dezimalsystem!)
- $[\![\cdot]\!]_u$ *ist definiert durch* $[\![\underbrace{||\ldots|}_{n}]\!]_u =_{df} n$

  Die Semantik einer Nachricht aus n Strichen ist also die natürliche Zahl n.

Im dem täglichen Umgang gebräuchlich ist die Verwendung der Dezimaldarstellung:

Beispiel 5.5 (Dezimaldarstellung natürlicher Zahlen)

- $\mathcal{R}_d \ =_{df} \ \{\mathbf{0},\ldots,\mathbf{9}\}^+$
- $\mathcal{I}_d \ =_{df} \ \mathbb{N}$
- $[\![\cdot]\!]_d$ *ist definiert durch* $[\![w]\!]_d \ =_{df} \ \sum_{i=1}^{n} 10^{n-i} \cdot [\![w(i)]\!]_z$

  Dabei bezeichnet $[\![\cdot]\!]_z$ *den Wert einer Dezimalziffer, also* $[\![\mathbf{0}]\!]_z \ =_{df} \ 0, \ldots, [\![\mathbf{9}]\!]_z \ =_{df} \ 9.$

Die Darstellung aus Definition 5.5 hat den Nachteil, dass $[\![\cdot]\!]_d$ nicht injektiv ist. Das Problem liegt im Zulassen führender Nullen von Repräsentanten. So gilt:

$$[\![\mathbf{1}]\!]_d \ = \ [\![\mathbf{01}]\!]_d \ = \ [\![\mathbf{001}]\!]_d \ = \ \ldots = 1.$$

Führende Nullen können aber vermieden werden, indem man die Menge der Repäsentanten einschränkt auf:

$$\mathcal{R}_d \ =_{df} \ \{\mathbf{0}\} \cup \{z\,w \mid z \in \{\mathbf{1},\ldots,\mathbf{9}\}, w \in \{\mathbf{0},\ldots,\mathbf{9}\}^*\}$$

Wir betrachten nun noch als weitere Darstellung natürlicher Zahlen deren Binärdarstellung:

Beispiel 5.6 (Binärdarstellung natürlicher Zahlen)

- $\mathcal{R}_b \ =_{df} \ \{\mathbf{0}\} \cup \{\mathbf{1}\,w \mid w \in \{\mathbf{0},\mathbf{1}\}^*\}$
- $\mathcal{I}_b \ =_{df} \ \mathbb{N}$
- $[\![\cdot]\!]_b$ *ist*

  definiert durch $[\![w]\!]_b \ =_{df} \ \sum_{i=1}^{n} 2^{n-i} \cdot [\![w(i)]\!]_{bz}$

  Dabei bezeichnet $[\![\cdot]\!]_{bz}$ *den Wert einer Binärziffer, also* $[\![\mathbf{0}]\!]_{bz} \ =_{df} \ 0$ *und* $[\![\mathbf{1}]\!]_{bz} \ =_{df} \ 1.$

Interessanterweise eröffnet sich für Binärzahlen auch eine völlig andere Möglichkeit der Interpretation. Diese können nämlich auch als endliche Mengen natürlicher Zahlen interpretiert werden (vergleiche Beispiel 3.3). Eine $\mathbf{1}$ steht für ein vorhandenes, eine $\mathbf{0}$ für ein nicht vorhandenes Element. Bei Binärzahlen ohne führende Nullen liegt es nahe das größte vorhandene Element durch die führende Eins zu repräsentieren. Also haben wir folgendes Semantikschema:

Beispiel 5.7 (Binärdarstellung endlicher Mengen natürlicher Zahlen)

- $\mathcal{R}_{bs} \ =_{df} \ \{\mathbf{0}\} \cup \{\mathbf{1}\,w \mid w \in \{\mathbf{0},\mathbf{1}\}^*\}$
- $\mathcal{I}_{bs} \ =_{df} \ \mathfrak{P}(\mathbb{N})$
- $[\![\cdot]\!]_{bs}$ *ist definiert durch* $[\![w]\!]_{bs} \ =_{df} \ \{|w| - i \mid i \in \{1,\ldots,|w|\} \wedge w(i) = \mathbf{1}\}$

Offensichtlich ist $[\![\cdot]\!]_{bs}$ injektiv, aber nicht surjektiv, denn unendliche Teilmengen von $\mathbb{N}$ können nicht durch endliche Binärworte beschrieben werden. Wir kommen in Kapitel 5.4 auf Semantikschemata im Kontext induktiven Definierens zurück.

5.3 Backus-Naur-Form

Die bislang in den Semantikschemata auftretenden Zeichenreihen waren sehr einfach. Oft sind aber syntakische Strukturen komplizierter aufgebaut. In der Informatik hat sich ein spezielles Format zur induktiven Definition syntaktischer Strukturen (Sprachen) durchgesetzt, die Backus-Naur-Form (BNF).

Eine BNF besteht aus endlich vielen Regeln der Form $< N > ::= w$. Die linke Regelseite besteht aus einem sogenannten *Nichtterminalsymbol*, die rechte Regelseite besteht aus einer ggf. auch leeren Zeichenreihe, die sowohl Nichtteminalsybole als auch Terminalsymbole enthalten kann. Zum Zweck der Unterscheidung werden Nichtterminalsymbole hier in spitzen Klammern dargestellt. Nichtterminalsymbole sind Hilfssymbole, die im Rahmen eines Ableitungsprozesses ersetzt werden. Am Ende dieses Prozesses sollen Nichtterminalsymbole vollständig eliminiert werden und eine Zeichenreihe hervorgehen, die allein aus Terminalsymbolen besteht.

Enthält eine BNF mehrere Regeln mit identischen linken Seiten, etwa

$$\begin{aligned} <N> &::= w_1 \\ &\dots \\ <N> &::= w_n \end{aligned}$$

so schreiben wir für diese Regeln auch kurz

$$<N> ::= w_1 \mid \dots \mid w_n$$

Beispiel 5.8 (BNF für natürliche Zahlen) *Die natürlichen Zahlen sind durch die folgende BNF definiert:*

$$<Nat> ::= 0 \mid \mathfrak{s}(<Nat>)$$

In der BNF für natürliche Zahlen sind "0","$\mathfrak{s}$", "(" und ")" Terminalzeichen, während $<Nat>$ das einzige Nichtterminalzeichen ist.

Intuitiv benutzt man BNF's um Zeichenreihen, die nur aus Terminalzeichen bestehen, zu erzeugen. Dafür startet man mit einem ausgezeichneten Nichtterminalzeichen (dem *Startsymbol*), hier etwa $<Nat>$, das man durch die rechte Seite einer Regel, etwa $\mathfrak{s}(<Nat>)$, ersetzt. In dieser rechten Seite kann dann ein beliebiges Vorkommen eines Nichtterminalzeichens ebenso ersetzt werden. Dieser Prozess wird solange fortgesetzt, bis nur noch Terminalzeichen vorhanden sind. Zum Beispiel kann

die natürliche Zahl 3 durch folgende Ableitung erzeugt werden:

$$\begin{aligned} <Nat> &\implies \mathfrak{s}(<Nat>) \\ &\implies \mathfrak{s}(\mathfrak{s}(<Nat>)) \\ &\implies \mathfrak{s}(\mathfrak{s}(\mathfrak{s}(<Nat>))) \\ &\implies \mathfrak{s}(\mathfrak{s}(\mathfrak{s}(0))) \end{aligned}$$

Das Konzept der Ableitung wird durch den Begriff der *Ableitungsrelation* formalisiert. Seien $\mathbf{T}$ die Terminalzeichen, $\mathbf{N}$ die Nichtterminalzeichen und $\mathbf{R}$ die Regeln einer BNF, so ist die *Ableitungsrelation* $\implies \subseteq (\mathbf{N} \cup \mathbf{T})^* \times (\mathbf{N} \cup \mathbf{T})^*$ definiert wie folgt:

$$\begin{aligned} & w \implies w' \Leftrightarrow_{df} \\ & \quad \exists\, w_1, w_2 \in (\mathbf{N} \cup \mathbf{T})^*,\ A ::= \tilde{w} \in \mathbf{R}.\ w = w_1\, A\, w_2 \wedge w' = w_1\, \tilde{w}\, w_2 \end{aligned}$$

In einem Ableitungsschritt, in dem man eine Regel $A ::= \tilde{w}$ anwendet, ersetzt man also in einem Wort w ein Vorkommen von A durch $\tilde{w}$. Dabei bleibt alles, was in w links oder rechts von dem ersetzten Vorkommen von A steht, unverändert. Die oben angegebene Definition von $\implies$ schreibt man auch kürzer als

$$w_1\, A\, w_2 \implies w_1\, \tilde{w}\, w_2$$

Eine Folge $w_1, \ldots, w_k$ von Worten über $(\mathbf{N} \cup \mathbf{T})^*$ (d.h. $w_1, \ldots, w_k \in (\mathbf{N} \cup \mathbf{T})^*$) heißt *Ableitungsfolge*, wenn $w_i \implies w_{i+1}$ für alle $i \in \{1, \ldots, k-1\}$ gilt. Man sagt, ein Wort $w' \in (\mathbf{N} \cup \mathbf{T})^*$ lässt sich aus einem Wort $w \in (\mathbf{N} \cup \mathbf{T})^*$ *ableiten*, wenn es eine Ableitungsfolge $w_1, \ldots, w_k$ mit $w = w_1$ und $w' = w_k$ gibt. Für ein gegebenes Nichtterminalsymbol A besteht die *von A generierte Sprache* aus genau den Worten w über $\mathbf{T}$ (d.h. $w \in \mathbf{T}^*$), die sich aus A ableiten lassen. Beachte, dass die Worte in der von A abgeleiteten Sprache keine Nichtterminalsymbole enthalten dürfen.

Wir werden Eigenschaften der Backus-Naur-Form hier nicht weiter verfolgen, da diese uns hier in erster Linie als Werkzeug induktiven Definierens interessieren. Für eine umfassende Behandlung sei auf Vorlesungen wie Datenstrukturen, Algorithmen und Programmierung (DAP) oder Grundbegriffe der Theoretischen Informatik (GTI) verwiesen.

Betrachten wir nun eine BNF für Dezimalzahlen.

Beispiel 5.9 (BNF für Dezimalzahlen)

$$\begin{aligned} <DezimalZahl> &::= <Ziffer> \mid <DezimalZahl><Ziffer> \\ <Ziffer> &::= \mathsf{0} \mid \ldots \mid \mathsf{9} \end{aligned}$$

Die Booleschen Terme (siehe Definition 4.6) sind durch die folgende BNF definiert:

Beispiel 5.10 (BNF für Boolesche Terme)

$$\begin{aligned} <BT> &::= \mathsf{T} \mid \mathsf{F} \mid <V> \mid \neg <BT> \mid (<BT> \wedge <BT>) \mid (<BT> \vee <BT>) \\ <V> &::= X_0 \mid X_1 \mid \ldots \end{aligned}$$

Bei der BNF für Boolesche Terme fällt auf, dass eine unendliche Variablenmenge durch eine mit Punkten stilisierten Notation beschrieben wird. Streng genommen ist das bei einer BNF nicht erlaubt, denn Terminal- und Nichtterminalsymbole, sowie Regeln müssen endlich sein. Hier ist das aber kein Problem, da Variablen auch unter Verwendung der Produktionen für Dezimalzahlen nummerierbar wären. Dazu müssten nur die Regeln für $<V>$ abgeändert werden zu:

$<V> ::= X <DezimalZahl>$

Dann sind die Variablennamen wie $X\mathbf{0},\ X\mathbf{1},\ X\mathbf{2}, \ldots$ ableitbar.

5.4 Induktive Semantikschemata

Besondere Bedeutung haben Semantikschemata, bei denen die Repräsentationen induktiv beschrieben sind, etwa als induktive Menge oder über eine BNF. In dieser Situation bietet es sich an, dass auch die Semantikfunktion induktiv auf den Repräsentationen definiert ist.

Betrachten wir zunächst eine induktive Variante für das Semantikschmema aus Beispiel 5.5, die sich ergibt wenn wir die induktive Beschreibung der Repräsentationen aus Beispiel 5.9 zugrundelegen:

Beispiel 5.11 (Dezimaldarstellung natürlicher Zahlen)

- $\mathcal{R}_d \ =_{df}\ \{\mathbf{0}, \ldots, \mathbf{9}\}^+$,
- $\mathcal{I}_d \ =_{df}\ \mathbb{N}$
- $[\![\cdot]\!]_d$ *ist induktiv definiert durch*

$$\begin{aligned} [\![z]\!]_d &=_{df} [\![z]\!]_z \\ [\![w\, z]\!]_d &=_{df} 10 \cdot [\![w]\!]_d + [\![z]\!]_d \end{aligned}$$

Semantik Boolescher Terme

Boolesche Terme als syntaktische Konstrukte haben per se keine Semantik. Da diese Variablen enthalten, die den elementaren Aussagen in der Aussagenlogik entsprechen, kann ein Boolescher Term nur relativ zu dem Wahrheitswert der Variablen ausgewertet werden. Wir führen dazu den Begriff der Variablenbelegungen ein. Formal sind das Zuordnungen von Variablen zu Wahrheitswerten.

$$\mathcal{B}_{\mathcal{V}} \ =_{df}\ \{\beta \mid \beta : \mathcal{V} \to \{w, f\}\}.$$

Relativ zu einer Variablenbelegung kann nun Booleschen Termen eine Bedeutung (ein Wahrheitswert) zugeordnet werden:

Definition 5.12 (Semantikfunktion) *Die* Semantikfunktion *für Boolesche Terme ist eine Funktion* $[\![\cdot]\!]_B : \mathcal{BT} \to (\mathcal{B}_\mathcal{V} \to \{w, f\})$*, die einem Booleschen Term unter Zuhilfenahme einer Belegung einen Wahrheitswert zuordnet. Sie ist wie folgt induktiv definiert:*

- $[\![\mathsf{T}]\!]_B(\beta) =_{df} w$
- $[\![\mathsf{F}]\!]_B(\beta) =_{df} f$
- $[\![X]\!]_B(\beta) =_{df} \beta(X)$ *für alle* $X \in \mathcal{V}$
- $[\![(\neg t_1)]\!]_B(\beta) =_{df} \dot{\neg}([\![t_1]\!]_B(\beta))$
- $[\![(t_1 \wedge t_2)]\!]_B(\beta) =_{df} ([\![t_1]\!]_B(\beta) \mathbin{\dot{\wedge}} [\![t_2]\!]_B(\beta))$
- $[\![(t_1 \vee t_2)]\!]_B(\beta) =_{df} ([\![t_1]\!]_B(\beta) \mathbin{\dot{\vee}} [\![t_2]\!]_B(\beta))$

Dabei sind $\dot{\neg}$, $\dot{\wedge}$, $\dot{\vee}$ *semantische Operationen auf den Wahrheitswerten* $\{w, f\}$*, die durch folgende Wahrheitstafel beschrieben sind:*

b_1	b_2	$\dot{\neg} b_1$	$b_1 \mathbin{\dot{\vee}} b_2$	$b_1 \mathbin{\dot{\wedge}} b_2$
f	f	w	f	f
f	w	w	w	f
w	f	f	w	f
w	w	f	w	w

Folgendes Besipiel enthält eine schrittweise Anwendung der Semantikfuktion.

Beispiel 5.13 (Anwendung Semantikfunktion) *Sei* $\beta \in \mathcal{B}_\mathcal{V}$ *eine Variablenbelegung mit* $\beta(X) = f$*. Dann gilt:*

$$
\begin{array}{lcll}
[\![(\neg X \vee \mathsf{F})]\!]_B(\beta) & = & [\![\neg X]\!]_B(\beta) \mathbin{\dot{\vee}} [\![\mathsf{F}]\!]_B(\beta) & (\text{Def. } [\![\cdot]\!]_B \text{ für Disjunktion}) \\
& = & \dot{\neg}[\![X]\!]_B(\beta) \mathbin{\dot{\vee}} [\![\mathsf{F}]\!]_B(\beta) & (\text{Def. } [\![\cdot]\!]_B \text{ für Negation}) \\
& = & \dot{\neg}\beta(X) \mathbin{\dot{\vee}} [\![\mathsf{F}]\!]_B(\beta) & (\text{Def. } [\![\cdot]\!]_B \text{ für Variablen}) \\
& = & \dot{\neg}\beta(X) \mathbin{\dot{\vee}} f & (\text{Def. } [\![\cdot]\!]_B \text{ für Konstante } \mathsf{F}) \\
& = & \dot{\neg} f \mathbin{\dot{\vee}} f & (\text{Auswertung } \beta(X)) \\
& = & t & (\text{Auswertung mit Operatoren } \dot{\neg}, \dot{\vee})
\end{array}
$$

Boolesche Terme, die unabhängig von der Variablenbelegung, den gleichen Wert besitzen heißen *semantisch äquivalent*. Formal heißt das für $t_1, t_2 \in \mathcal{BT}$:

$$t_1 \equiv t_2 \Leftrightarrow_{df} \forall \beta \in \mathcal{B}_\mathcal{V}.\ [\![t_1]\!]_B(\beta) = [\![t_2]\!]_B(\beta).$$

Kapitel 6

Induktives Beweisen

In Kapitel 4 und 5 haben wir zahlreiche induktiv definierte Mengen, Funktionen und Algorithmen betrachtet. In diesem Kapitel werden wir das Werkzeug des induktiven Beweisens kennenlernen. Induktives Beweisen bedeutet "Beweisen entlang der induktiven Struktur" der zugrundeliegenden Objekte. Induktionsbeweise erlauben es, Eigenschaften für unendlich viele Objekte auf einen repräsentativen Induktionsschluss zurückzuführen.

In diesem Kapitel werden wir mehrere Induktionsprinzipien kennenlernen. Abweichend von der historisch geprägten Reihenfolge beginnen wir hier aber nicht mit den natürlichen Zahlen und dem Prinzip der vollständigen Induktion, sondern stellen in Kapitel ein universelles Induktionsprinzip vor, das auf rein ordnungsbegrifflichen Grundlagen fußt.

6.1 Ordnungsrelationen

Ordnungen sind von verschiedenen Mengen bekannt. So sind Zahlbereiche wie $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ mit einer Ordnung $\leq$ versehen, die es erlaubt Zahlen hinsichtlich ihrer Größe zu vergleichen. Für Potenzmengen stellt die Mengeninklusion $\subseteq$ eine Ordnung unter den Mengen her. Im Gegensatz zu den Ordnungen auf Zahlbereichen gibt es hier allerdings auch unvergeleichbare Elemente. So gilt zum Beispiel weder $\{1,2\} \subseteq \{1,3\}$ noch $\{1,3\} \subseteq \{1,2\}$. Man spricht daher hier von einer *partiellen Ordnung*. Die Verallgemeinerung der Inklusionsbeziehung führt zum Begriff der partiellen Ordnung.

Definition 6.1 (Partielle Ordnung) *Eine homogene Relation* $\preceq \subseteq A \times A$ *heißt* partielle Ordnungsrelation *oder auch* Halbordnungsrelation*, gdw.*

1. $\preceq$ *ist* reflexiv*:* $\forall\, a \in A.\ a \preceq a$
2. $\preceq$ *ist* antisymmetrisch*:* $\forall\, a_1, a_2 \in A.\ a_1 \preceq a_2 \ \wedge\ a_2 \preceq a_1 \Rightarrow a_1 = a_2$
3. $\preceq$ *ist* transitiv*:* $\forall\, a_1, a_2, a_3 \in A.\ a_1 \preceq a_2 \ \wedge\ a_2 \preceq a_3 \ \Rightarrow\ a_1 \preceq a_3$

Ist $\preceq$ partielle Ordnungsrelation auf A, so nennen wir $(A, \preceq)$ eine *partiell geordnete Menge* oder kurz *partielle Ordnung*. Falls A aus dem Kontext eindeutig hervorgeht, benutzen wir die Bezeichnung auch für die Ordnungsrelation $\preceq$ selbst. Es ist leicht nachzuweisen, dass $(\mathfrak{P}(A), \subseteq)$ für jede Grundmenge A eine partiell geordnete Menge ist. Ebenso sind die natürlichen Zahlen mit der Teilbarkeitsbeziehung partiell geordnet.

Auf den natürlichen Zahlen ist jedem die intuitive Ordnung $0 \leq 1 \leq 2 \leq \ldots$ klar. Allerdings ist diese nicht unmittelbarer Bestanteil der Peano-Axiome (siehe 4.1). Dennoch kann man die Ordnung auf natürlichen Zahlen wie folgt defineren:

Definition 6.2 (Ordnung auf $\mathbb{N}$) *Für $n, m \in \mathbb{N}$ definiere wir eine Relation $\leq$ durch*

$$n \leq m \;\Leftrightarrow_{df}\; \exists\, k \in \mathbb{N}.\; n + k = m.$$

Es gilt:

Satz 6.3 *$\leq$ ist eine partielle Ordnung auf $\mathbb{N}$.*

Beweis Wir zeigen die drei geforderten Eigenschaften:[1]

Reflexivität: Sei $n \in \mathbb{N}$. Mit $k = 0$ gilt dann $n + 0 = 0 + n = n$, also auch $n \leq n$.

Antisymmetrie: Seien $n, m \in \mathbb{N}$ mit $n \leq m$ und $m \leq n$. Dann existieren Zahlen $k_1, k_2 \in \mathbb{N}$ mit:

$$\begin{array}{lcl} n + k_1 & = & m \\ m + k_2 & = & n \end{array}$$

Setzt man m aus der ersten Gleichung in die Zweite ein, so erhält man $(n + k_1) + k_2 = n$. Wegen der Assoziativität und Kommutativität der Addition gilt $(k_1 + k_2) + n = n$ und somit auch

$$(k_1 + k_2) + n = 0 + n.$$

Daraus folgt mit der Rechtskürzungsregel $k_1 + k_2 = 0$, was wegen Peano-Axiom (**P3**) $k_1 = k_2 = 0$ impliziert. Also gilt schließlich auch $n = m$.

Transitivität: Seien $n, m, p \in \mathbb{N}$ mit $n \leq m$ und $m \leq p$. Dann existieren Zahlen $k_1, k_2 \in \mathbb{N}$ mit:

$$\begin{array}{lcl} n + k_1 & = & m \\ m + k_2 & = & p \end{array}$$

Setzt man m aus der ersten Gleichung in die Zweite ein, so erhält man $(n + k_1) + k_2 = p$. Mit der Assoziativität der Addition folgt

$$n + (k_1 + k_2) = p$$

und damit gilt $n \leq p$. □

Zu einer gegebenen partiellen Ordnung $\preceq$ lässt sich eine zughörige strikte partielle Ordnung $\prec$ definieren durch:

$$a_1 \prec a_2 \;\Leftrightarrow_{df}\; a_1 \preceq a_2 \wedge a_1 \neq a_2\,.$$

[1] Hiefür benötigen wir allerdings formal noch die Assoziativität, Kommutativität und Rechtskürzungsregel der Addition natürlicher Zahlen, die wir erst an späterer Stelle zeigen (siehe Satz 6.15).

Offensichtlich ist $\prec$ transitiv und antisymmetrisch, wobei letztere Eigenschaft hier ohne Aussagekraft ist. Die Reflexivität geht hingegen verloren. Charakteristische Eigenschaften von $\prec$ sind:

Lemma 6.4

1. $\prec$ *ist* irreflexiv, *d.h.:* $\forall\, a \in A.\ a \not\prec a$
2. $\prec$ *ist* asymmetrisch, *d.h.:* $\forall\, a_1, a_2 \in A.\ a_1 \prec a_2 \ \Rightarrow\ a_2 \not\prec a_1$
3. $\prec$ *ist* transitiv, *d.h.:* $\forall\, a_1, a_2, a_3 \in A.\ a_1 \prec a_2 \ \wedge\ a_2 \prec a_3 \ \Rightarrow\ a_1 \prec a_3$

Umgekehrt induziert eine Relation $\prec$ mit den Eigenschaften aus Lemma 6.4 unmittelbar eine partielle Ordnung $\preceq$ durch:

$$a_1 \preceq a_2 \ \Leftrightarrow_{df}\ \ a_1 \prec a_2 \ \vee\ a_1 = a_2\,.$$

Reduziert man eine strikte partielle Ordnung auf die unmittelbar benachbarten Abhängigkeiten erhält man die Nachbarschaftsordnung $\prec_N$ definiert durch:

$$a_1 \prec_N a_2 \Leftrightarrow_{df}\ a_1 \prec a_2 \ \wedge\ \nexists\, a_3 \in A.\ a_1 \prec a_3 \prec a_2\,.$$

In $\prec_N$ sind transitive Beziehungen eliminiert. Abbildung 6.1 illustriert den Unterschied der Relationen $\preceq$, $\prec$ und $\prec_N$ anhand der Teilbarkeitsrelation auf der Menge der natürlichen Zahlen $\{1, 2, 3, 4, 6, 12\}$. Diese ist dabei wie üblich definiert durch $n|m \ \Leftrightarrow_{df}\ \exists\, k \in \mathbb{N}.\ n \cdot k = m$. Im Bild wird $n|m$ durch einen Pfeil von n nach m repräsentiert.

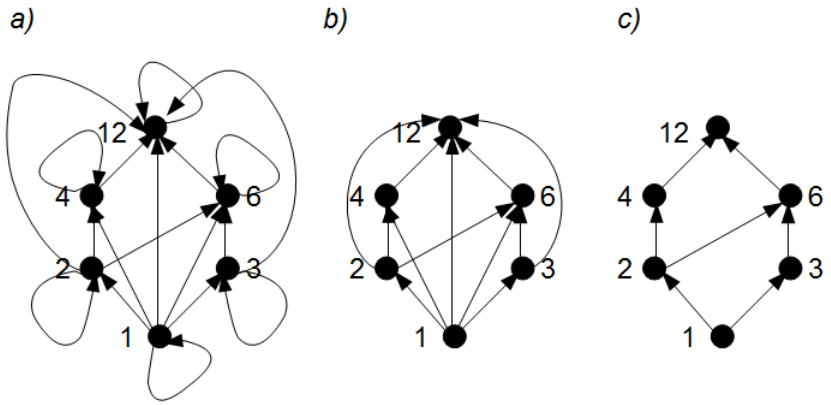


Abbildung 6.1: Teilbarkeitsrelation auf $\{1, 2, 3, 4, 6, 12\}$: a) Als partielle Ordnung, b) als strikte partielle Ordnung und c) als Nachbarschaftsordnung.

Konstruiert man $\prec_N$ ausgehend von einer partiellen Ordnung $\preceq$, so erhält man $\preceq$ aus $\prec_N$ zurück, indem man deren *transitiv reflexive Hülle* bildet. Allgemein ist die transitiv reflexive Hülle R^* einer

Relation $R \subseteq A \times A$ die kleinste R umfassende transitive und reflexive Relation. Das ist:[2]

$$R^* =_{df} \bigcap\{R' | R \subseteq R' \wedge R' \text{ reflexiv} \wedge R' \text{ transitiv}\}.$$

Wir haben dann zwischen $\preceq$ und $\prec_N$ folgenden Zusammenhang:

$$\prec_N^* = \preceq .$$

Wegen $\prec_N \subseteq \prec \subset \preceq$ ist $\prec_N$ für die kompakte Respräsentation von $\preceq$ von besonderer Bedeutung. Die graphische Darstellung von $\prec_N$ ist auch unter dem Begriff *Hasse-Diagramm* von $\preceq$ bekannt. Bei dieser Darstellung wird $\prec_N$ durch Verbindungen dargestellt, wobei kleinere Elemente unten angeordnet sind. Abbildung 6.2 zeigt die Hasse-Digramme einiger partieller Ordnungen.

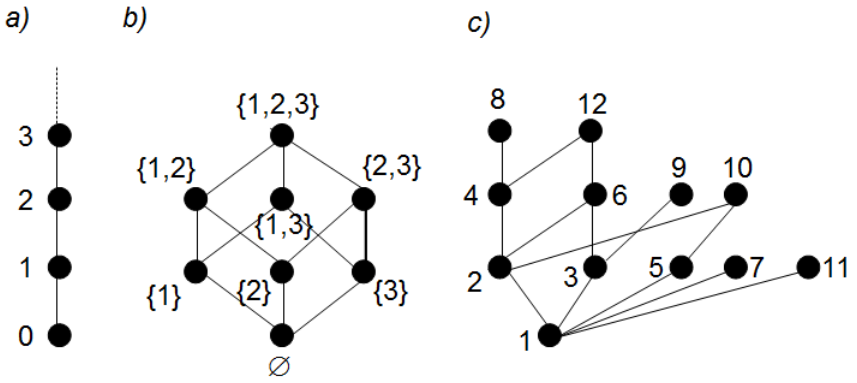


Abbildung 6.2: Hasse Diagramme zu a) $\leq$-Ordnung auf $\mathbb{N}$, b) $\subseteq$-Ordnung auf $\mathfrak{P}(\{1,2,3\})$, c) der Teilbarkeitsrelation $|$ auf $\{1,\ldots,12\}$.

Weitere Ordnungsbegriffe

In manchen Situationen ist die Antisymmetrie eine zu restriktive Forderung. Besagt sie doch, dass wechselweise in Ordnungsrelation stehende Elemente schon identisch sein müssen. Will man aber beispielsweise Personen nach ihrer Körpergröße ordnen, so existieren durchaus verschiedene Personen, die gleichgroß sind. Verzichtet man in Definition 6.1 auf die Antisymmetrie, so spricht man von einer *Präordunungsrelation* oder auch *Quasi-Ordnungsrelation*. Die Implikation auf Booleschen Termen ist ein weiteres gutes Beispiel einer Präordnung. Offensichtlich ist hier Reflexivität und Transitivität gegeben, die Antisymmetrie aber verletzt, denn verschiedene semantisch äquivalente Terme stehen in beidseitiger Implikationsbeziehung. Betrachtet man die Implikation auf den Äquivalenzklassen semantisch äquivalenter Terme liegt hingegen eine partielle Ordnung vor. Im Allgemeinen wird für eine Präordnung $\preceq \subseteq A \times A$ durch

$$a_1 \sim_\preceq a_2 \Leftrightarrow_{df} a_1 \preceq a_2 \wedge a_2 \preceq a_1$$

[2]Da transitive und relexive Relationen gegen Schnittbildung abgeschlossen sind, ist $\bigcap\{R' | R \subseteq R' \wedge R' \text{ reflexiv} \wedge R' \text{ transitiv}\}$ ebenfalls relexiv und transitiv.

eine Äquivalenzrelation auf A definiert. Man spricht hier auch vom *Kern* der Präordnung.

Eine partielle Ordnung $\preceq \subseteq A \times A$ in der alle Elemente vergleichbar sind, d.h. für die gilt

$$\forall\, a_1, a_2 \in A.\ a_1 \preceq a_2 \vee a_2 \preceq a_1$$

heißt *totale* oder auch *lineare* Ordnung.

So sind die natürlichen Zahlen mit der $\leq$-Ordnung (siehe Abbildung 6.2(a)) total geordnet.

Teilstrukturen

Betrachtet man eine partielle Ordnung $\preceq \subseteq A \times A$ und eine Teilmenge $B \subseteq A$ so existieren in B spezielle Elemente. Die folgende Definition klassifiziert solche B-Elemente, die nicht echt von anderen dominiert werden.

Definition 6.5 (Minimale, maximale Elemente)
Sei $\preceq \subseteq A \times A$ partielle Ordnung und $B \subseteq A$. Ein Element $b \in B$ heißt

1. minimales *Element in B* $\Leftrightarrow_{df}$ $\nexists\, b' \in B.\ b' \prec b$ *und*
2. maximales *Element in B* $\Leftrightarrow_{df}$ $\nexists\, b' \in B.\ b \prec b'$.

Man beachte, dass es in B mehrere verschiedene minimale bzw. maximale Elemente geben kann.

Beispiel 6.6 *Betrachten wir in Abbildung 6.2(c) die Teilmenge $B = \{2, 3, 4, 6\}$, so sind 2 und 3 minimale Elemente, während 4 und 6 maximale Elemente sind.*

Wirklich dominierende Elemente werden durch folgende strengere Definition erfasst:

Definition 6.7 (Kleinstes, größtes Element) *Sei $\preceq \subseteq A \times A$ partielle Ordnung und $B \subseteq A$. Ein Element $b \in B$ heißt*

1. kleinstes *Element in B* $\Leftrightarrow_{df}$ $\forall\, b' \in B.\ b \preceq b'$ *und*
2. größtes *Element in B* $\Leftrightarrow_{df}$ $\forall\, b' \in B.\ b' \preceq b$.

Offensichtlich ist ein kleinstes Element insbesondere minimal und ein größtes Element auch maximal. Für totale Ordungen gilt umgekehrt auch, dass minimale Elemente schon kleinste Elemente sind, beziehungsweise maximale Elemente größte Elemente sind.

Beispiel 6.8 *Betrachten wir in Abbildung 6.2(c) die gesamte Menge der Elemente $\{1, \ldots, 12\}$, so sind $7, 8, 9, 10, 11$ und 12 maximale Elemente, aber es existiert kein größtes Element. Andererseits ist die 1 minimales und hier auch kleinstes Element.*

6.2 Noethersche Induktion

Das Prinzip der Noetherschen Induktion ist das universelle Instrument, um Aussagen über induktiv aufgebaute Strukturen (siehe Kapitel 4) zu beweisen. Generell müssen nur schwache ordnungstheoretische Voraussetzungen für die Anwendbarkeit dieses Induktionsprinzips vorliegen, nämlich die Struktur einer *Noethersch geordneten* Menge.

Definition 6.9 (Noethersch geordnete Menge) *Eine partielle Ordnung $\preceq \subseteq A \times A$ heißt* Noethersch geordnete Menge *genau dann, wenn jede nichtleere Teilmenge von M ein minimales Element besitzt.*

Anschaulich verhindert diese Definition, dass es bezüglich $\prec$ unendliche echt absteigende Ketten in A gibt. Damit stößt man beim Zerlegen einer Struktur immer in endlich vielen Schritten auf atomare Bestandteile. Insbesondere ist so jede gemäß Definiton 4.4 induktiv definierte Menge Noethersch geordnet. Die induktive Definition selbst legt die Nachbarschaftsordnung $\prec_N$ einer partiellen Ordnung fest. Die atomaren Elemente erzwingen die Existenz minimaler Elemente.

Weitere Beispiele Nothersch geordneter Mengen enthält folgendes Beispiel:

Beispiel 6.10 (Noethersche geordnete Mengen)

1. *Die durch $\leq$ geordneten natürlichen Zahlen $\mathbb{N}$ sind Noethersch geordnet, denn jede nichtleere Teilmenge enthält sogar ein kleinstes Element.*
2. *Die durch die Teilwortbeziehung geordnete Menge der endlichen Zeichenreihen $A*$ ist Noethersch geordnet. Jede echt absteigende Kette von Zeichenreihen wird in jedem Schritt echt kürzer.*
3. *Die Potenzmenge jeder endlichen Menge M ist durch $\subseteq$ Noethersch geordnet. Jede echt absteigende Kette von Mengen enthält in jedem Schritt mindestens ein Element weniger.*

Beispiele nicht Nothersch geordneter Mengen sind:

Beispiel 6.11 (Nicht Noethersch geordnete Mengen)

1. *Die durch $\leq$ geordneten ganzen Zahlen $\mathbb{Z}$ sind nicht Noethersch geordnet, denn die nichtleere Teilmenge $\mathbb{Z}$ besitzt kein minimales Element.*
2. *Die durch $\leq$ geordneten nichtnegativen rationalen Zahlen $\mathbb{Q}_{\geq 0}$ sind nicht Noethersch geordnet, denn die nichtleere Teilmenge $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$ besitzt kein minimales Element.*
3. *$\mathfrak{P}(\mathbb{N})$ ist durch $\subseteq$ nicht Noethersch geordnet, denn die nichtleere Teilmenge $\{\mathbb{N}, \mathbb{N}\backslash\{0\}, \mathbb{N}\backslash\{0,1\}, \mathbb{N}\backslash\{0,1,2\}, \ldots\}$ besitzt kein minimales Element.*

Es gilt nun:

Beweisprinzip 6.12 (Prinzip der Noetherschen Induktion)

Sei $\preceq \subseteq M \times M$ eine Noethersch geordnete Menge. Lässt sich eine Aussage $\mathcal{A}$ über M für jede Struktur $m \in M$ aus der Gültigkeit der Aussage für alle echt kleineren Strukturen ableiten, dann ist sie für jede Struktur m wahr.

$$\Big(\forall\, m \in M.\ \big(\forall\, m' \in M.\ m' \prec m \Rightarrow \mathcal{A}(m')\big) \Rightarrow \mathcal{A}(m)\Big) \Rightarrow \forall\, m \in M.\ \mathcal{A}(m).$$

Beweis Wir zeigen die Behauptung per Kontraposition. Falls $\forall\, m \in M.\ \mathcal{A}(m)$ nicht gilt, gibt es eine nichtleere Menge $G \subseteq M$ von Gegenbeispielen definiert durch $G =_{df} \{g \in M \mid \neg\mathcal{A}(g)\}$. Weil $\preceq$ Noethersch ist, existiert ein minimales Gegenbeipiel $g_{min} \in G$. Wegen der Minimalität von g_{min} gilt $\forall\, m' \in M.\ m' \prec g_{min} \Rightarrow \mathcal{A}(m')$. Damit ist aber der Induktionsschritt, d.h. die Implikation

$$\Big(\forall\, m \in M.\ \big(\forall\, m' \in M.\ m' \prec m \Rightarrow \mathcal{A}(m')\big) \Rightarrow \mathcal{A}(m)\Big),$$

verletzt, denn $\forall\, m' \in M.\ m' \prec g_{min} \Rightarrow \mathcal{A}(m')$ gilt, aber nicht $\mathcal{A}(g_{min})$. □

Eine Hauptanwendung des Beweisprinzips der Northerschen Induktion sind Beweise für induktiv definierte Mengen (siehe Definition 4.4). Wie bereits ausgeführt liegt hier eine Noethersche Ordnung vor und das Prinzip der Noetherschen Induktion ist anwendbar. In diesem Kontext spricht man auch vom Prinzip der *strukturellen Induktion*.

Anwendung: Boolesche Terme

Gleichheitsbeweise durch algebraisches Umformen basieren auf einer Reihe von bewiesenen elementaren Gleichheiten zwischen Termen. Beweisidee ist, den einen Term solange durch 'Ersetzen von Gleichem durch Gleiches' umzuformen, bis der zweite Term erreicht wird. Die elementaren Gleichheiten nennt man auch *Axiome* und die beschriebene Vorgehensweise *axiomatisch*.

Grundvoraussetzung für die Axiomatisierbarkeit eines Gleichheitsbegriffs ist, daß er eine *Kongruenz* definiert, das heißt dass das Prinzip 'Ersetzen von Gleichem durch Gleiches" gültig ist. Wir sehen, dass im Falle der semantischen Äquivalenz für Boolesche Terme die Welt in Ordnung ist. Dieses ist in dem folgendem Kompositionalitätssatz festgehalten.

Satz 6.13 (Kompositionalität von $[\![\cdot]\!]_B$) *Seien $t, t', t'' \in \mathcal{BT}$ mit $t' \equiv t''$ und $X \in \mathcal{V}$. Dann gilt*

$$t[t'/X] \equiv t[t''/X].$$

Das heißt, man darf (simultan) Gleiches durch (semantisch) Gleiches ersetzen.

Beweis Seien $t, t', t'' \in \mathcal{BT}$ beliebig mit $t' \equiv t''$ und $X \in \mathcal{V}$. Nach Definition der semantischen Äquivalenz ist für eine beliebige Belegung $\beta \in \mathcal{B}_{\mathcal{V}}$ zu zeigen:

$$(*) \qquad [\![t[t'/X]]\!]_B(\beta) \;=\; [\![t[t''/X]]\!]_B(\beta).$$

Wir zeigen $(*)$ mittels struktureller Induktion über den Termaufbau von t:

1. Fall: $t \in \{\mathsf{T}, \mathsf{F}, Y\}$ für $Y \in \mathcal{V}$ mit $Y \neq X$.
   Dann folgt $(*)$ wegen $t[t'/X] \;=\; t \;=\; t[t''/X]$.

2. Fall: $t \;=\; X$
   Hier folgt $(*)$ mit der Voraussetzung $t' \equiv t''$:
   $$X[t'/X] \;=\; t' \equiv t'' \;=\; X[t''/X].$$

3. Fall: $t \;=\; \neg t_1$
   $$\begin{array}{rcll} [\![\,(\neg t_1)[t'/X]\,]\!]_B(\beta) & = & [\![\,(\neg(t_1[t'/X]))\,]\!]_B(\beta) & \text{(Def. } [\cdot/\cdot]) \\ & = & \dot{\neg}([\![\,t_1[t'/X]\,]\!]_B)(\beta)) & \text{(Def. } [\![\,\cdot\,]\!]_B) \\ & = & \dot{\neg}([\![\,t_1[t''/X]\,]\!]_B)(\beta)) & \text{(Ind.Annahme)} \\ & = & [\![\,(\neg(t_1[t''/X]))\,]\!]_B(\beta) & \text{((Def. } [\![\,\cdot\,]\!]_B) \\ & = & [\![\,(\neg t_1)[t''/X]\,]\!](\beta) & \text{(Def. } [\cdot/\cdot]) \end{array}$$

4. Fall: $t \;=\; (t_1 \vee t_2)$
   $$\begin{array}{rcll} [\![\,(t_1 \vee t_2)[t'/X]\,]\!]_B(\beta) & = & [\![\,t_1[t'/X] \;\vee\; t_2[t'/X]\,]\!]_B(\beta) & \text{(Def. } [\cdot/\cdot]) \\ & = & [\![\,t_1[t'/X]\,]\!]_B(\beta) \;\dot{\vee}\; [\![\,t_2[t'/X]\,]\!]_B(\beta) & \text{(Def. } [\![\,\cdot\,]\!]_B) \\ & = & [\![\,t_1[t''/X]\,]\!]_B(\beta) \;\dot{\vee}\; [\![\,t_2[t''/X]\,]\!]_B(\beta) & \text{(Ind.Annahme)} \\ & = & [\![\,t_1[t''/X] \;\vee\; t_2[t''/X]\,]\!]_B(\beta) & \text{(Def. } [\![\,\cdot\,]\!]_B) \\ & = & [\![\,(t_1 \vee t_2)[t''/X]\,]\!]_B(\beta) & \text{(Def. } [\cdot/\cdot]) \end{array}$$

5. Fall: $t \;=\; (t_1 \wedge t_2)$ ist analog zu Fall 4)

□

6.3 Vollständige Induktion

Traditionell ist induktives Beweisen sehr stark mit dem Beweisprinzip der vollständigen Induktion verknüpft. In der Tat lässt sich diese unmittelbar aus dem Induktionsaxiom (P5) der Peanoaxiome ableiten. Es gilt:

Beweisprinzip 6.14 (Induktionsprinzip der vollständigen Induktion)

Ist eine Aussage $\mathcal{A}$ über natürliche Zahlen für 0 wahr und lässt sich ihre Gültigkeit für jede größere natürliche Zahl aus der Gültigkeit der Aussage für ihren Vorgänger ableiten, dann ist sie für jede natürliche Zahl wahr.

$$\big(\,\mathcal{A}(0) \;\wedge\; \forall\, n \in \mathbb{N}.\; \mathcal{A}(n) \;\Rightarrow\; \mathcal{A}(n+1)\,\big) \;\Rightarrow\; \forall\, n \in \mathbb{N}.\; \mathcal{A}(n).$$

Das Beweisprinzip der vollständigen Induktion kann zunächst dazu verwendendet werden zahlreiche Eigenschaften der induktiv definierten Addition und Multiplikation zu beweisen:

Satz 6.15 *Seien $n, m, k \in \mathbb{N}$. Dann gilt:*

Assoziativität:

$(n+m)+k \;=\; n+(m+k)$ $\qquad$ $(n \cdot m) \cdot k \;=\; n \cdot (m \cdot k)$

Kommutativität:

$n+m \;=\; m+n$ $\qquad$ $n \cdot m \;=\; m \cdot n$

Neutrale Elemente:

$n+0 \;=\; n$ $\qquad$ $n \cdot 1 \;=\; n$

Rechtskürzungsregeln:

$(n+k \;=\; m+k) \;\Rightarrow\; (n=m)$ $\qquad$ $(n \cdot k \;=\; m \cdot k) \;\Rightarrow\; (n=m)$ $\qquad$ falls $k \neq 0$

Distributivität:

$(n+m) \cdot k \;=\; n \cdot k + m \cdot k$

Beweis Wir beweisen exemplarisch die Assoziativität der Addition per vollständiger Induktion über das Argument n. Dabei verwenden wir die Definition der Addition natürlicher Zahlen aus Definition 4.2. Alle anderen Eigenschaften von Satz 6.15 können im wesentlichen analog bewiesen werden.

Induktionsanfang: $n = 0$. Dann gilt: $(0+m)+k \overset{\text{Def.}+}{=} m+k \overset{\text{Def.}+}{=} 0+(m+k)$

Induktionsschluss: Sei die Behauptung bereits für ein beliebiges, aber festes $n \in \mathbb{N}$ gezeigt (Induktionsannahme). Dann zeigen wir, dass die Behauptung auch für $n+1$ gilt:

$$\begin{aligned}((n+1)+m)+k &\overset{\text{Def.}+1}{=} (\mathfrak{s}(n)+m)+k \overset{\text{Def.}+}{=} \mathfrak{s}(n+m)+k \overset{\text{Def.}+}{=} \mathfrak{s}((n+m)+k) \\ &\overset{IA}{=} \mathfrak{s}(n+(m+k)) \overset{\text{Def.}+}{=} \mathfrak{s}(n)+(m+k) \overset{\text{Def.}+1}{=} (n+1)+(m+k)\end{aligned}$$

□

In der durch (IA) gekennzeichneten Gleichung im Induktionsschluss geht die Induktionsannahme ein. Dieses ist in einem sauber ausgeführten Induktionsbeweis immer irgendwo der Fall und sollte auch entsprechend gekennzeichnet werden.

Das Beweisprinzip der vollständigen Induktion kann in Kombination mit den induktiv definierten Operationen auf natürlichen Zahlen auch für anpruchsvolle Aussagen verwendet werden:

Beispiel 6.16 (Beispiele zur vollständigen Induktion)
Für alle $n \in \mathbb{N}$ gilt:

1. *Es gibt 2^n Teilmengen von n–elementigen Mengen.*
2. $\sum_{i=1}^{n} i = \frac{n*(n+1)}{2}$, *Summe der ersten n natürlichen Zahlen.*
3. $\sum_{i=1}^{n} (2i-1) = n^2$, *Summe der ersten n ungeraden Zahlen.*

Beweis Wir beweisen hier nur die erste Aussage.

Induktionsanfang: $n = 0$. Eine 0-elementige Menge ist die leere Menge und diese hat genau $2^0 = 1$ Teilmengen, nämlich die leere Mange selbst.

Induktionsschluss: Sei die Behauptung bereits für ein beliebiges aber festes $n \in \mathbb{N}$ gezeigt (Induktionsannahme). Sei M eine $n+1$-elementige Menge. Wir wählen ein beliebiges $m \in M$. Sei $A \subseteq M$. Dann gibt es zwei Fälle:

- $m \notin A$. Also A liegt voll in der n-elementigen Menge $M\backslash\{m\}$, d.h.: $A \subseteq M\backslash\{m\}$. Nach Induktionsannahme gibt es 2^n solche Teilmengen.
- $m \in A$. Dann liegt die Restteilmenge $A\backslash\{m\}$ voll in der n-elementigen Menge $M\backslash\{m\}$. Da jede der Teilmengen in $M\backslash\{m\}$ auch zu einer Teilmenge mit m beitragen kann, gibt es nach Induktionsannahme wiederum 2^n solche Teilmengen.

Insgesamt hat man $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ Teilmengen.

□

6.4 Verallgemeinerte Induktion

Das Beweisprinzip der vollständigen Induktion ist in der Anwendung oft zu unflexibel. Als Beispiel dazu wollen wir eine Aussage über die Folge der Fibonacci–Zahlen betrachten. Diese sind wie folgt induktiv definiert:

Definition 6.17 (Fibonacci-Zahlen)

$$\begin{array}{lll} fib(0) & =_{df} & 0 \\ fib(1) & =_{df} & 1 \\ fib(n+1) & =_{df} & fib(n) + fib(n-1) \end{array}$$

Die zu beweisende Aussage lautet:

$$\forall\, n \in \mathbb{N}.\ fib(n) < 2^n.$$

Offensichtlich lässt sich der Beweis mittels vollständiger Induktion nicht unmittelbar führen, da im Induktionsschluss nicht nur die Induktionsvoraussetzung für den Vorgänger $n-1$ von n, sondern auch für den Vorvorgänger $n-2$ von n benötigt wird. Allerdings erhalten wir ein allgemeineres Beweisprinzip auf natürlichen Zahlen, wenn wir das Prinzip der Noetherschen Induktion (siehe Beweisschema 6.12) auf die spezielle Situation der natürlichen Zahlen mit der in Definition 6.2 eingeführten Noetherschen Ordnung übertragen. Dieses Beweisprinzip ist auch unter dem Namen *Verallgemeinerte Induktion* bekannt.

Beweisprinzip 6.18 (Prinzip der verallgemeinerten Induktion)

Lässt sich eine Aussage $\mathcal{A}$ über natürliche Zahlen für jede natürliche Zahl aus der Gültigkeit der Aussage für alle kleineren natürlichen Zahlen ableiten, dann ist sie für jede natürliche Zahl wahr.

$$\Big(\forall\, n \in \mathbb{N}.\ (\forall\, m \in \mathbb{N}.\ m < n\ \Rightarrow\ \mathcal{A}(m))\ \Rightarrow\ \mathcal{A}(n)\Big)\ \Rightarrow\ \forall\, n \in \mathbb{N}.\ \mathcal{A}(n).$$

Es ist auffällig, dass im Gegensatz zum Prinzip der vollständigen Induktion bei der verallgemeinerten Induktion vermeintlich auf einen Induktionsbeginn für die Null verzichtet wird. Allerdings ist dieser implizit im Induktionsschritt verborgen. Weil es keine kleineren natürlichen Zahlen als die Null gibt, ist die Eigenschaft $\forall\, m < 0.\ \mathcal{A}(m)$ trivialerweise erfüllt. Weil die gesamte Implikation $\forall\, m < 0.\ \mathcal{A}(m)\ \Rightarrow\ \mathcal{A}(0)$ im Induktionsschluss gelten muss, ist $\mathcal{A}(0)$ als gültig nachzuweisen.

Greifen wir noch einmal die Abschätzung der Fibonacci-Zahlen auf

$$\forall\, n \in \mathbb{N}.\ fib(n) < 2^n.$$

Dann kann die Behauptung mit verallgemeinerter Induktion bewiesen werden:

Beweis Sei $n \in \mathbb{N}$ und die Behauptung bewiesen für alle $m < n$ (Induktionsannahme). Wir unterscheiden dann folgende 3 Fälle:

- $n = 0$. Dann gilt $fib(0) \stackrel{\text{Def.}}{=} 0 < 1 = 2^0$.
- $n = 1$. Dann gilt $fib(1) \stackrel{\text{Def.}}{=} 1 < 2 = 2^1$.
- $n \geq 2$. Dann gilt:

$$fib(n) \stackrel{\text{Def.}}{=} fib(n-2) + fib(n-1) \stackrel{IA}{<} 2^{n-2} + 2^{n-1} \leq 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.$$

□

Kapitel 7

Ordnungsstrukturen

In Kapitel 6.1 haben wir den Begriff der partiellen Ordnungen kennengelernt, motiviert durch das Induktionsprinzip der Noetherschen Induktion. Auf der anderen Seite haben wir zahlreiche Beispiele partieller Ordnungen kennengelernt, die von großer Bedeutung sind, etwa:

- $(\mathfrak{P}(M), \subseteq)$: Potenzmengen mit Inklusionsbeziehung
- $(\mathcal{BT}|_{\equiv}, \Rightarrow)$: Klassen semantisch äquivalenter Boolesche Terme mit der Implikationsbeziehung
- $(\mathbb{N}, |)$: Natürliche Zahlen mit der Teilbarkeitsbeziehung

Die Definition partieller Ordnungen stellt an sich nur schwache Anforderungen, die den strukturellen Eigenschaften der obigen Beispiele nicht voll gerecht werden. So besitzen zum Beispiel zwei Teilmengen immer eine kleinste diese enthaltende Obermenge, die Vereinigung der beiden Mengen. Dass dieses in partiellen Ordnungen allgemein, selbst in solchen mit kleinstem und größtem Element, keineswegs der Fall sein muss, illustriert Abbildung 7.1. Hier werden die Elemente 2 und 3 zwar von $4, 5$ und 6 nach oben übertroffen, aber in $\{4, 5, 6\}$ gibt es kein kleinstes Element.

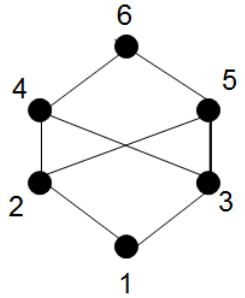


Abbildung 7.1: Partielle Ordnung mit kleinstem und größtem Element, die kein Verband ist.

7.1 Verbände

Will man Strukturen, wie in Abbildung 7.1 ausschließen, betrachtet man partielle Ordnungen mit zusätzlichen strukturellen Eigenschaften, die sogenannten *Verbände*. Bevor wir diese formal definieren, benötigen wir aber noch einige Begriffe.

Definition 7.1 (Obere und untere Schranken) *Sei* $(M, \preceq)$ *eine partielle Ordnung und* $X \subseteq M$.

1. (a) $y \in M$ *heißt* obere Schranke *von* $X \Leftrightarrow_{df} \forall x \in X.\ x \preceq y$.
   Wir schreiben auch kurz $X \preceq y$.
   (b) *Die Menge der oberen Schranken von* X *ist* $\mathcal{O}_X =_{df} \{y \in M \mid X \preceq y\}$.
   (c) *Besitzt* $\mathcal{O}_X$ *ein kleinstes Element, die kleinste obere Schranke (oder* Supremum*) von* X*, so wird dieses mit* $\sup(X)$ *bezeichnet.*
2. (a) $y \in M$ *heißt* untere Schranke *von* $X \Leftrightarrow_{df} \forall x \in X.\ y \preceq x$.
   Wir schreiben auch kurz $y \preceq X$.
   (b) *Die Menge der unteren Schranken von* X *ist* $\mathcal{U}_X =_{df} \{y \in M \mid y \preceq X\}$.
   (c) *Besitzt* $\mathcal{U}_X$ *ein größtes Element, die größte untere Schranke (oder* Infimum*) von* X*, so wird dieses mit* $\inf(X)$ *bezeichnet.*

Im Allgemeinen kann die Menge der oberen und unteren Schranken leer sein. So hat in Abbildung 6.2 die Menge $\{8, 12\}$ keine gemeinsamen oberen Schranken, d.h. $\mathcal{O}_{\{8,12\}} = \emptyset$. Selbst wenn etwa obere Schranken existieren, müssen diese kein kleinstes Element besitzen. Wie bereits diskutiert hat in Abbildung 7.1 die Knotenmenge $\{2, 3\}$ die oberen Schranken $4, 5$ und 6, d.h. $\mathcal{O}_{\{2,3\}} = \{4, 5, 6\}$, aber es gibt keine kleinste obere Schranke.

Infimum und Supremum, sofern existent, sind eindeutig bestimmt. Dieses führen wir hier für das Infimum näher aus. Seien $y_1, y_2 \in M$ zwei Infima von $X \subseteq M$. Dann gilt $y_2 \preceq y_1$, denn y_2 ist untere Schranke von X und y_1 ist größte untere Schranke von X. Mit vertauschten Rollen von y_1 und y_2 folgt ebenso $y_1 \preceq y_2$. Wegen der Antisymmetrie von $\preceq$ impliziert $y_2 \preceq y_1$ zusammen mit $y_1 \preceq y_2$ dann $y_1 = y_2$.

Offensichtlich ist ein kleinstes Element von X, sofern ein solches existiert, das Infimum von X und ein größtes Element von X das Supremum. Im Allgemeinen sind Infima und Suprema aber nicht notwendig kleinste bzw. größte Elemente der Teilmenge X, ja nicht einmal in X selbst enthalten. Dieses gilt selbst dann, wenn X total geordnet ist. Betrachten wir die Potenzmenge der natürlichen Zahlen, also $(\mathfrak{P}(\mathbb{N}), \subseteq)$ und $X \subseteq \mathfrak{P}(\mathbb{N})$ mit $X =_{df} \{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\}$. Offensichtlich gilt $\sup(X) = \mathbb{N}$, aber $\mathbb{N}$ ist nicht größtes Element von X, da $\mathbb{N}$ nicht in X enthalten ist.

Mit dem Begriff der Infima und Suprema definiert man:

Definition 7.2 (Verband) *Eine partielle Ordnung* $(V, \preceq)$ *heißt* Verband $\Leftrightarrow_{df}$

$$\forall x, y \in V.\ \inf(\{x, y\}) \text{ existiert } \wedge\ \sup(\{x, y\}) \text{ existiert}$$

Betrachten wir erneut die Potenzmenge als Ordnung $(\mathfrak{P}(M), \subseteq)$ so liegt offensichtlich ein Verband vor mit $\sup(\{A, B\}) = A \cup B$ und $\inf(\{A, B\}) = A \cap B$. Ebenso ist $(\mathbb{N}, |)$ ein Verband mit $\sup(\{n, m\}) = KgV(n, m)$, dem kleinsten gemeinsamen Vielfachen von n und m, und $\inf(\{n, m\}) = GgT(n, m)$, dem größten gemeinsamen Teiler von n und m. Verbände spielen eine wichtige Rolle im Zusammenhang mit der Repräsentation von konkreter und abstrakter Information. So ist in Abbildung 7.2(a) ein Verband zu sehen, der als starke Abstraktion von $\mathfrak{P}(\mathbb{Z}, \subseteq)$ angesehen werden kann. Hier sind Mengen ganzer Zahlen auf ihre Vorzeicheninformationen reduziert. So steht das mit ">=0" annotierte Element für die Vorzeicheninformation "nicht negativ". Drunter fallen solche Mengen ganzer Zahlen, deren Elemente alle größer oder gleich 0 sind. Eine genauere Vorzeicheninformation als ">=0" hat man mit ">0" oder "=0". Das größte Element "any" steht für die total unspezifische Vorzeicheninformation, also Mengen, die sowohl positive als auch negative ganze Zahlen enthalten. Das kleinste Element "none" steht für das Fehlen von Vorzeicheninformation und abstrahiert damit allein die leere Menge. Abbildung 7.2(b) zeigt den sogenannten *flachen Verband* ganzer Zahlen. Hier wird die übliche Ordnungsbeziehung zwischen den Zahlen völlig ignoriert und alle Zahlen unabhängig nebeneinander angeordnet. Damit gilt aber für verschiedene Zahlen wie 2 und 3 nicht etwa $\sup(2, 3) = \max(2, 3) = 3$, wie es bezüglich der üblichen $\leq$-Beziehung der Fall ist, sondern $\sup(2, 3) =$ any. Andererseits besitzt der flache Verband den Vorteil, dass es keine echt unendlich absteigenden Folgen von Elementen gibt. In der Tat sind alle echt absteigenden Folgen in ihrer Länge durch 3 beschränkt.

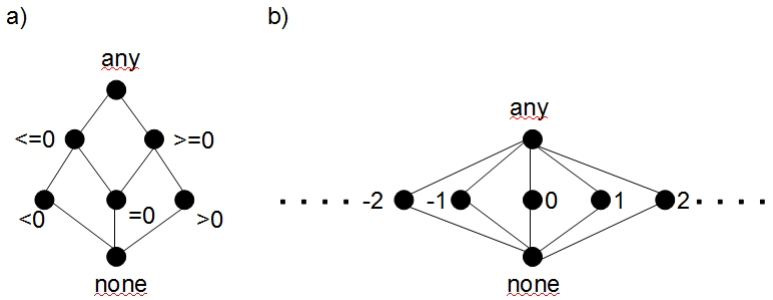


Abbildung 7.2: a) Verband der Vorzeicheninformationen ganzer Zahlen, b) Flacher Verband ganzer Zahlen

Auf endlichen Verbände, also solchen mit endlicher Trägermenge $V =_{df} \{x_1, \ldots, x_n\}$, existieren die Infima und Suprema auch für beliebige nichtleere Teilmengen. Das Infimum von $X \subseteq M$ bestimmt sich nämlich induktiv durch:

$$\inf(\{x_1, \ldots, x_k\}) = \begin{cases} x_1 & \text{falls } k = 1 \\ \inf(\{\inf(\{x_1, \ldots, x_{k-1}\}), x_k\}) & \text{sonst} \end{cases}$$

Das Supremum kann analog beschrieben werden. Endliche Verbände besitzen folglich auch ein kleinstes und ein größtes Element, nämlich $\inf(V)$ bzw. $\sup(V)$. In unendlichen Verbänden gilt dieses nicht unbedingt. Betrachten wir etwa die Teilbarkeit auf positiven natürlichen Zahlen, also $(\mathbb{N}\backslash\{0\}, |)$, so liegt ein Verband ohne größtes Element vor.

7.1.1 Verbände als algebraische Strukturen

Die Definition eines Verbandes erlaubt es, inf und sup als binäre Operatoren aufzufassen. Daher definieren wir:

$$\begin{aligned} x \curlywedge y &=_{df} \inf(\{x, y\}) \\ x \curlyvee y &=_{df} \sup(\{x, y\}) \end{aligned}$$

Es gilt dann:

Satz 7.3 *Sei $(V, \preceq)$ ein Verband. Dann gilt für alle $x, y, z \in V$:*

1. *Assoziativität:*
   (a) $(x \curlywedge y) \curlywedge z = x \curlywedge (y \curlywedge z)$
   (b) $(x \curlyvee y) \curlyvee z = x \curlyvee (y \curlyvee z)$
2. *Kommutativität:*
   (a) $x \curlywedge y = y \curlywedge x$
   (b) $x \curlyvee y = y \curlyvee x$
3. *Absorption:*
   (a) $x \curlywedge (x \curlyvee y) = x$
   (b) $x \curlyvee (x \curlywedge y) = x$

Beweis Die Kommutativität ist offensichtlich trivial. Für die Assoziativität betrachten wir Eigenschaft 1(a). Es bezeichne $u_1 =_{df} (x \curlywedge y) \curlywedge z = \inf(\{\inf(\{x, y\}), z\})$ und $u_2 =_{df} x \curlywedge (y \curlywedge z) = \inf(\{x, \inf(\{y, z\})\})$. Offensichtlich ist u_1 untere Schranke von x, y und z. Also gilt $u_1 \preceq \inf(\{y, z\})$ und weiter $u_1 \preceq \inf(\{x, \inf(\{y, z\})\}) = u_2$. Analog haben wir $u_2 \preceq u_1$ und mit der Antisymmetrie von $\preceq$ schließlich $u_1 = u_2$. Eigenschaft 1(b) beweist man dual. Für Absorptionseigenschaft 3(a) stellen wir zunächst fest $x \curlyvee y = \sup(\{x, y\}) \succeq x$. Offensichtlich gilt dann $x \curlywedge (x \curlyvee y) = \inf(\{x, \underbrace{\sup(\{x, y\})}_{\succeq x}\}) = x$. Letztere Gleichheit folgt trivial aus der Tatsache, dass das Infimum einer zweielementigen linear geordneten Menge deren kleinstes Element ist. Eigenschaft 3(b) beweist man wiederum dual. □

Eine Menge V mit zwei Operationen $\curlywedge$ und $\curlyvee$, die die Eigenschaften aus Satz 7.3 erfüllen, wird als *algebraischer Verband* bezeichnet. Die erwähnten Eigenschaften (Assoziativität, Kommutativität und Absorption) sind uns bereits an früherer Stelle begegnet. In der Tat sind die Mengen- und Aussagengesetze in Tabelle 2.13 und 2.5 Ausdruck einer zugrundeliegenden algebraischen Verbandsstruktur.

Aus Gründen der Abgrenzung zu algebraischen Verbänden bezeichnen wie Verbände im Sinne von Definition 7.2 auch als *ordnungsstrukturelle Verbände*. Mit Satz 7.3 haben wir bereits gesehen, dass jeder ordnungsstrukturelle Verband einen algebraischen Verband induziert. Dass auch die Umkehrung gilt, wird in Satz 7.5 gezeigt. Zuvor zeigen wir aber die Idempotenzeigschaften in algebraischen Verbänden.

Lemma 7.4 (Idempotenz) *Sei $(V, \curlywedge, \curlyvee)$ ein algbraischer Verband und $x \in V$. Dann gilt:*

1. $x = x \curlywedge x$
2. $x = x \curlyvee x$

Beweis

$$\begin{array}{lcll} x & = & x \curlywedge (x \curlyvee (x \curlywedge x)) & \text{(Absorption)} \\ & = & x \curlywedge x & \text{(Absorption)} \end{array}$$

$$\begin{array}{lcll} x & = & x \curlyvee (x \curlywedge (x \curlyvee x)) & \text{(Absorption)} \\ & = & x \curlyvee x & \text{(Absorption)} \end{array}$$

□

Lemma 7.4 geht unmittelbar in den Beweis des bereits ankündigten folgenden Resultates ein:

Satz 7.5 *Sei $(V, \curlywedge, \curlyvee)$ ein algebraischer Verband. Definiert man eine binäre Relation $\preceq \subseteq V \times V$ durch:*

$$x \preceq y \;\Leftrightarrow_{df}\; x = x \curlywedge y,$$

so ist $(V, \preceq)$ ein ordnungsstruktureller Verband.

Beweis Zunächst müssen wir zeigen, dass $\preceq$ überhaupt eine partielle Ordnung ist.

- Reflexivität: Folgt unmittelbar aus der Idempotenz von $\curlywedge$ (Lemma 7.4).
- Antisymmetrie: Seien $x, y \in V$ mit $x \preceq y$ und $y \preceq x$. Das heißt nach Definition $x = x \curlywedge y$ und $y = y \curlywedge x$. Wegen der Kommutativität von $\curlywedge$ impliziert das $x = y$.
- Transitivität: Es gelte $x \preceq y$ und $y \preceq z$.

  $$\begin{array}{lcll} x & = & x \curlywedge y & (x \preceq y) \\ & = & (x \curlywedge y) \curlywedge (y \curlywedge z) & (x \preceq y, y \preceq z) \\ & = & (x \curlywedge (y \curlywedge y)) \curlywedge z & \text{(Assoziativität)} \\ & = & (x \curlywedge y) \curlywedge z & \text{(Idempotenz)} \\ & = & x \curlywedge z & (x \preceq y) \end{array}$$

  Das heißt nach Definition $x \preceq z$.

Es bleibt zu zeigen, dass je zwei Elemente aus V ein Infimum und Supremum besitzen. Aus Dualitätsgründen beschränken wir uns hier auf die Infimumseigenschaft. Seien $x, y \in V$. Wir behaupten, dass $x \curlywedge y$ Infimum von $\{x, y\}$ ist. Wegen $x \curlywedge y \overset{Idemp.}{=} (x \curlywedge x) \curlywedge y \overset{Assoz.}{=} x \curlywedge (x \curlywedge y) \overset{Komm.}{=} x \curlywedge (y \curlywedge x) \overset{Assoz.}{=} (x \curlywedge y) \curlywedge x$ gilt $x \curlywedge y \preceq x$. Ebenso kann $x \curlywedge y \preceq y$ gezeigt werden. $x \curlywedge y$ ist also untere Schranke von $\{x, y\}$. Um zu zeigen, dass es auch die größte untere Schranke ist, nehmen wir an $z \in V$ sei eine beliebige untere Schranke von $\{x, y\}$. Dann gilt:

$$\begin{array}{lcll} z & = & z \curlywedge y & (z \preceq y) \\ & = & (z \curlywedge x) \curlywedge y & (z \preceq x) \\ & = & z \curlywedge (x \curlywedge y) & (\text{Assoziativität}) \end{array}$$

Also ist $z \preceq x \curlywedge y$. □

7.2 Spezielle Verbände

Nachdem wir nun Verbände sowohl in der Sicht als Ordnungsstrukturen, als auch als algebraische Strukturen kennengelernt haben, wollen wir noch einige wichtige spezielle Verbände untersuchen. Diese ergeben sich durch zusätzliche Anforderungen an die betrachteten Strukturen.

7.2.1 Vollständige Verbände

Betrachten wir die ordnungsstrukturelle Sicht von Verbänden aus Definition 7.2, so haben wir gesehen, dass in endlichen Verbänden beliebige nichtleere Teilmengen ein Infimum und Supremum besitzen. Es liegt also nahe diese Forderung auf unendliche Verbände zu übertragen. Man kommt so zum Begriff vollständiger Verbände:

Definition 7.6 (Vollständiger Verband) *Eine partielle Ordnung* $(V, \preceq)$ *heißt* vollständiger Verband $\Leftrightarrow_{df}$

$$\forall\, X \subseteq V.\ \inf(X) \text{ existiert } \wedge\ \sup(X) \text{ existiert}$$

Beispiel 7.7 (Vollständiger Verband)

1. $(\mathbb{N}, \leq)$ *ist Verband, aber kein vollständiger Verband, denn* $\sup(\mathbb{N})$ *existiert nicht.*
2. $(\mathbb{N} \cup \{\infty\}, \leq)$ *mit* $n \leq \infty$ *für alle* $n \in \mathbb{N} \cup \{\infty\}$ *ist ein vollständiger Verband.*
3. $(\mathfrak{P}(M), \subseteq)$ *ist vollständiger Verband für jede Menge* M*.*
4. $(\mathbb{N}, |)$ *ist vollständiger Verband mit* $\inf(X) = GgT(X)$*, dem größten gemeinsamen Teiler aller Elemente in* X*. Das Supremum ist analog* $\sup(X) = KgV(X)$*, das kleinste gemeinsame Vielfache aller Elemente in* X*. Man beachte, dass dieses für unendliche Teilmengen die* 0 *ist.*
5. $(\mathbb{N}\backslash\{0\}, |)$ *ist kein vollständiger Verband denn für unendliche Teilmengen wie z.B.* $\mathbb{N}$ *existiert kein Supremum.*

Definition 7.6 ist eigentlich unnötig restriktiv definiert. Es reicht nämlich die Existenz von Infima oder Suprema allein zu fordern, da die jeweils andere Eigenschaft dann automatisch sichergestellt ist. Es gilt nämlich:

Lemma 7.8 (Vollständiger Verband)

1. *Sei* $(V, \preceq)$ *eine partielle Ordnung, in der Infima generell existieren, also*

$$\forall\, X \subseteq V.\ \inf(X) \text{ existiert.}$$

Dann ist $(V, \preceq)$ *vollständiger Verband, d.h. auch Suprema existieren generell, also*

$$\forall\, X \subseteq V.\ \sup(X) \text{ existiert.}$$

2. *Sei* $(V, \preceq)$ *eine partielle Ordnung, in der Suprema generell existieren, also*

$$\forall\, X \subseteq V.\ \sup(X) \text{ existiert.}$$

Dann ist $(V, \preceq)$ *vollständiger Verband, d.h. auch Infima existieren generell, also*

$$\forall\, X \subseteq V.\ \inf(X) \text{ existiert.}$$

Beweis Aus Dualitätsgründen beschränken wir uns auf Teil (1) und nehmen an, dass für alle Teilmengen $X \subseteq V$ das Infimum $\inf(X)$ existiert. Sei $X \subseteq V$. Wir betrachten die Menge der oberen Schranken $\mathcal{O}_X$ von X und zeigen:

$$\sup(X) \;=\; \inf(\mathcal{O}_X).$$

Hierfür zeigen wir zwei Ordunungsbeziehungen, wodurch die Behauptung aus der Antisymmetrie folgt.

- $\sup(X) \;\preceq\; \inf(\mathcal{O}_X)$: Per Definition ist $\sup(X)$ kleinste obere Schranke von X. Also gilt $\sup(X) \;\preceq\; \mathcal{O}_X$. Damit ist $\sup(X)$ untere Schranke von $\mathcal{O}_X$ und somit $\sup(X) \;\preceq\; \inf(\mathcal{O}_X)$, da ja $\inf(\mathcal{O}_X)$ die größte untere Schranke von $\mathcal{O}_X$ ist.
- $\sup(X) \;\succeq\; \inf(\mathcal{O}_X)$: Per Definition ist $\sup(X)$ insbesondere obere Schranke von X. Somit ist $\sup(X) \in \mathcal{O}_X$ und es gilt $\inf(\mathcal{O}_X) \;\preceq\; \sup(X)$, denn $\inf(\mathcal{O}_X)$ ist ja insbesondere untere Schranke von $\mathcal{O}_X$.

□

In einem vollständigen Verband $(V, \preceq)$ existiert immer ein kleinstes Element $\bot_V$ (sprich *bottom* von V) und ein größtes Element $\top_V$ (sprich *top* von V), nämlich:

$$\begin{array}{lcllcl} \bot_V & = & \inf(V) & = & \sup(\emptyset) \\ \top_V & = & \sup(V) & = & \inf(\emptyset) \end{array}$$

Nach den Ausführungen auf Seite 69 ist in endlichen Verbänden die Existenz der Infima und Suprema nichtleerer Teilmengen sichergestellt. Mit der vorangegangenen Betrachtung über größte und kleinste Elemente existiert auch $\inf(\emptyset)$ und $\sup(\emptyset)$ und wir haben:

Satz 7.9 *Jeder endliche Verband ist vollständig.*

7.2.2 Boolesche Verbände

Während vollständige Verbände ausschließlich über die Erweiterung der ordnungsstrukturellen Eigenschaften definiert sind, können auch algebraische Verbände über zusätzliche Eigenschaften erweitert werden. In der Tat enthalten die Mengen- und Aussagengesetze in Tabelle 2.13 und 2.5 zwei zusätzliche Gesetze. Eines davon ist die Distributivität, die in folgenden Weise verallgemeinert werden kann.

Definition 7.10 (Distributiver Verband) *Ein algbraischer Verband* $(V, \curlywedge, \curlyvee)$ *heißt* distributiv*, genau dann wenn für alle* $x, y, z \in V$ *gilt:*

1. $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$
2. $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$

Genau genommen reicht es in Definition 7.10 eine der beiden Eigeschaften zu fordern. Es gilt:

Lemma 7.11 (Distributiver Verband) *Die Bedingungen in Definition 7.10 sind äquivalent. Das heißt, eine der Eigenschaften stellt bereits sicher, dass ein distributiver Verband vorliegt.*

Beweis Nehmen wir an, dass Eigenschaft (1) erfüllt ist. Dann gilt

$$
\begin{array}{lcll}
x \curlywedge (y \curlyvee z) & = & \big(x \curlywedge (x \curlyvee z)\big) \curlywedge (y \curlyvee z) & \text{(Absorption)} \\
& = & x \curlywedge \big((x \curlyvee z) \curlywedge (y \curlyvee z)\big) & \text{(Assoziativität)} \\
& = & x \curlywedge \big((z \curlyvee x) \curlywedge (z \curlyvee y)\big) & \text{(Kommutativität)} \\
& = & x \curlywedge \big(z \curlyvee (x \curlywedge y)\big) & \text{(Distributivität Eig. (1))} \\
& = & \big(x \curlyvee (x \curlywedge y)\big) \curlywedge \big(z \curlyvee (x \curlywedge y)\big) & \text{(Absorption)} \\
& = & \big((x \curlywedge y) \curlyvee x\big) \curlywedge \big((x \curlywedge y) \curlyvee z\big) & \text{(Kommutativität)} \\
& = & (x \curlywedge y) \curlyvee (x \curlywedge z) & \text{(Distributivität Eig. (1))}
\end{array}
$$

□

Abbildung 7.3 zeigt einen Verband, der nicht distributiv ist, denn es gilt zum einen $a \curlyvee (b \curlywedge c) = a \curlyvee 0 = a \curlyvee 0 = a$, zum anderen $(a \curlyvee b) \curlywedge (a \curlyvee c) = 1 \curlywedge 1 = 1$.

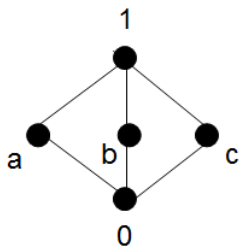


Abbildung 7.3: Nichtdistributiver Verband.

Ausgehend von dieser Definition führen wir Boolesche Verbände ein als ein abstraktes Model für Strukturen wie sie und in der Mengenlehre oder Aussagenlogik begegnet sind.

Definition 7.12 (Boolescher Verband) *Ein distributiver algebraischer Verband* $(V, \curlywedge, \curlyvee)$ *heißt* Boolescher Verband*, genau dann wenn es zwei verschiedene Elemente 0 und 1 in* V *gibt und für jedes* $x \in V$ *ein komplementäres Element* $\bar{x} \in V$ *existiert, so dass gilt:*

1. $x \curlyvee \bar{x} = 1$
2. $x \curlywedge \bar{x} = 0$

Satz 7.13 (Boolescher Verband) *Sei* $(V, \curlywedge, \curlyvee)$ *ein* Boolescher Verband*. Dann gilt für jedes* $x, y \in V$*:*

1. $\bar{x}$ *ist eindeutig bestimmt.*
2. *Neutralität:*
   (a) $x \curlyvee 0 = x$
   (b) $x \curlywedge 1 = x$
3. *Extremalgesetze:*
   (a) $x \curlyvee 1 = 1$
   (b) $x \curlywedge 0 = 0$
4. *Doppelkomplement:* $\bar{\bar{x}} = x$
5. *De Morgansche Gesetze:*
   (a) $\overline{x \curlyvee y} = \bar{x} \curlywedge \bar{y}$
   (b) $\overline{x \curlywedge y} = \bar{x} \curlyvee \bar{y}$

Beweis Wir beweisen zunächst (2), da dieses für den Beweis von (1) vorteilhaft ist. Hier beschränken wir uns auf Teil 1(a). Es gilt:

$$x \curlyvee 0 \overset{Kompl.}{=} x \curlyvee (x \curlywedge \bar{x}) \overset{Absorp.}{=} x.$$

Für die Eindeutigkeit von $\bar{x}$ nehmen wir an, y und z wären zwei Komplemente von x. Dann gilt:

$$y \overset{\text{Neutr.}}{=} y \curlywedge 1 \overset{\text{Def.z}}{=} y \curlywedge (x \curlyvee z) \overset{\text{Distr.}}{=} (y \curlywedge x) \curlyvee (y \curlywedge z)$$
$$\overset{\text{Komm.}}{=} (x \curlywedge y) \curlyvee (y \curlywedge z) \overset{\text{Def.y}}{=} 0 \curlyvee (y \curlywedge z) \overset{\text{Neutr.}}{=} (y \curlywedge z)$$

Analog zeigt man $z = (y \curlywedge z)$, was dann $y = z$ beweist.

Für die Extremalgesetze beschränken wir uns wieder auf Eigenschaft 3(1). Hier gilt:

$$x \curlyvee 1 \overset{\text{Kompl.}}{=} x \curlyvee (x \curlyvee \bar{x}) \overset{\text{Assoz.}}{=} (x \curlyvee x) \curlyvee \bar{x} \overset{\text{Idemp.}}{=} x \curlyvee \bar{x} \overset{\text{Kompl.}}{=} 1$$

Für die Eigenschaft des Doppelkomplementes haben wir zunächst:

(A) $x \curlywedge \bar{x} = 0$

(B) $\bar{x} \curlywedge \bar{\bar{x}} = 0$

Nun gilt:

$$x \overset{\text{Neutr.}}{=} x \curlyvee 0 \overset{\text{(B)}}{=} x \curlyvee (\bar{x} \curlywedge \bar{\bar{x}}) \overset{\text{Distr.}}{=} (x \curlyvee \bar{x}) \curlywedge (x \curlyvee \bar{\bar{x}}) \overset{\text{Kompl.}}{=} 1 \curlywedge (x \curlyvee \bar{\bar{x}}) \overset{\text{Neutr.}}{=} x \curlyvee \bar{\bar{x}}$$

Analog zeigt man unter Benutzung von (A) $\bar{\bar{x}} = x \curlyvee \bar{\bar{x}}$. Zusammen haben wir dann $\bar{\bar{x}} = x$.

Beweis de Morgan folgt.

□

7.3 Konstruktionsprinzipien

Im folgenden gehen wir noch auf einige besonders wichtige Konstruktionsprinzipien ein, um Verbände zu größeren Verbänden zu kombinieren. Zunächst betrachten wir das kartesische Produkt der den Verbänden zugrundeliegenden Mengen:

Satz 7.14 (Produktverband) *Seien $(A, \preceq_A)$ und $(B, \preceq_B)$ Verbände. Dann ist*

$$(A \times B, \preceq_{A\times B})$$

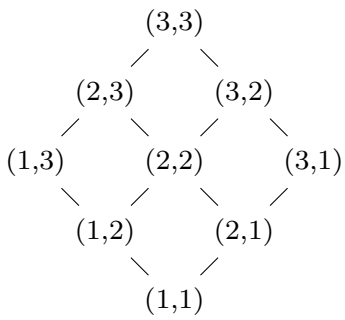
ein Verband, wobei

$$(a, b) \preceq_{A\times B} (a', b') \Leftrightarrow_{df} a \preceq_A a' \wedge b \preceq_B b'.$$

Sind $(A, \preceq_A)$ und $(B, \preceq_B)$ vollständig, so ist auch der Produktverband vollständig.

Beweis Folgt □

Das folgende Bild zeigt den Produktverband von $(\{1, 2, 3\}, \leq)$ mit sich selbst, wobei $\leq$ die übliche Ordnung auf natürlichen Zahlen ist.



Ein praktisch relevantes Beispiel eines Produktverbandes ist z.B. das Produkt der Verbände $(\mathbb{R}, \geq)$ und $(\mathbb{R}, \leq)$. Die Paare charakterisieren Intervalle reeller Zahlen. Hier kann man etwa an ein Zeitfenster denken, in dem eine Steuerungsschaltung eine bestimmte Reaktion auslösen muss. Betrachten wir nun das Infimum zweier Intervalle, so gilt:

$$\inf((l_1, u_1), (l_2, u_2)) \;=\; (\inf_{\geq}(l_1, l_2), \inf_{\leq}(u_1, u_2)) \;=\; (\max(\{l_1, l_2\}), \min(\{u_1, u_2\})).$$

Konkret ist etwa $\inf((3.5, 7.2), (2.9, 5.7)) \;=\; (3.5, 5.7)$. Damit wird zum Ausdruck gebracht, dass das Zeitfenster $(3.5, 5.7)$ das größte ist, welches in den beiden Zeitfenstern $(3.5, 7.2)$ und $(2.9, 5.7)$ enthalten ist. Dual dazu ist das Supremum zweier Intervalle definiert.

Betrachtet man Funktionen, deren Zielbereich Verbandseigenschaft hat, so kommt man zum Begriff des *Funktionenverbandes*.

Satz 7.15 (Funktionenverband) *Sei $(A, \preceq_A)$ ein Verband und M eine Menge. Dann ist*

$$(A^M, \preceq_{A^M})$$

ein Verband, wobei die Funktionsordnung $\preceq_{A^M}$ definiert ist durch:

$$f \preceq_{A^M} g \;\Leftrightarrow_{df}\; \forall\, m \in M.\; f(m) \;\preceq_A\; g(m).$$

Beweis Folgt □

7.4 Strukturverträgliche Abbildungen

Im folgenden untersuchen wir Funktionen zwischen (vollständigen) Verbänden. Verbände haben wir bislang sowohl in der Sichtweise als Ordnungsstrukturen als auch in der Sichtweise als algebraische Strukturen kennengelernt. Funktionen, die in besonderer Weise verträglich mit Operatoren oder Ordnungen sind, werden allgemein als *Homomorphismen* bezeichnet. Diese spielen insbesondere im Zusammenhang mit algebraischen Strukturen eine wichtige Rolle und werden uns daher auch in Kapitel 8 immer wieder begegnen.

Wir betrachten hier zunächst den relativ schwachen Begriff des *Ordnungshomomorphismus*:

Definition 7.16 (Ordnungshomomorphismus) *Seien $(A, \preceq_A)$ und $(B, \preceq_B)$ Verbände und $f : A \to B$ eine Funktion. f heißt* Ordnungshomomorphismus *genau dann, wenn für alle $a_1, a_2 \in A$ gilt:*

$$a_1 \;\preceq_A\; a_2 \;\Rightarrow\; f(a_1) \;\preceq_B\; f(b).$$

Man nennt f dann auch monoton *oder* isoton.

Im Folgenden betrachten wir einige Beispiele:

Beispiel 7.17 (Ordnungshomomorphismus)

1. *Für* $(\mathbb{N}, \leq)$ *ist jede konstante Funktion* $\mathbb{N} \to k$ *mit festem* $k \in \mathbb{N}$ *ein Ordnungshomomorphismus.*
2. *Für* $(\mathbb{N}, |)$ *ist* $f_7 : \mathbb{N} \to \mathbb{N}$ *mit* $f_7(n) =_{df} 7 \cdot n$ *ein Ordnungshomomorphismus, denn aus* $n \mid m$ *folgt* $n \cdot k = m$ *für ein geeignetes* $k \in \mathbb{N}$*. Dann gilt aber auch* $7 \cdot (n \cdot k) = (7 \cdot n) \cdot k = 7 \cdot m$*, also* $f_7(n) \mid f_7(m)$*.*
3. *Für* $(\mathbb{N}, \leq)$ *ist die Funktion* qs*, die einer Zahl ihre Quersumme zuordnet kein Ordnungshomomorphismus, denn* $99 \leq 100$*, aber* $qs(99) = 18 > 1 = qs(100)$*.*

In der Sichtweise algebraischer Verbände stellt sich die Homomorphieeigenschaft als Verträglichkeit mit den binären Operatoren $\curlyvee$ und $\curlywedge$ dar.

Definition 7.18 ($\curlyvee-$ und $\curlywedge$-homomorphismus) *Seien* $(A, \curlyvee_A, \curlywedge_A)$ *und* $(B, \curlyvee_B, \curlywedge_B)$ *algebraische Verbände und* $f : A \to B$ *eine Funktion.*

1. f *heißt* $\curlyvee$-Homomorphismus *genau dann, wenn für alle* $a_1, a_2 \in A$ *gilt:*
$$f(a_1 \curlyvee_A a_2) = f(a_1) \curlyvee_B f(a_2).$$
2. f *heißt* $\curlywedge$-Homomorphismus *genau dann, wenn für alle* $a_1, a_2 \in A$ *gilt:*
$$f(a_1 \curlywedge_A a_2) = f(a_1) \curlywedge_B f(a_2).$$

Die algebraischen Homomorphieeigenschaften implizieren Ordnungshomomorhie, wie das folgende Resultat ausführt:

Satz 7.19 *Seien* $(A, \curlyvee_A, \curlywedge_A)$ *und* $(B, \curlyvee_B, \curlywedge_B)$ *algebraische Verbände und* $f : A \to B$ *eine Funktion. Wir betrachten weiter die zugehörigen ordnungsstrukturellen Verbände* $(A, \preceq_A)$ *und* $(B, \preceq_B)$ *(siehe Satz 7.5). Dann gilt:*

1. *Falls* f *ein* $\curlyvee$*-Homomorphismus ist, so ist* f *ein Ordnungshomomorphismus.*
2. *Falls* f *ein* $\curlywedge$*-Homomorphismus ist, so ist* f *ein Ordnungshomomorphismus.*

Beweis Wir zeigen zunächst (2). Seien $a_1, a_2 \in A$. Dann gilt:

$$\begin{array}{lll} a_1 \preceq_A a_2 & \Leftrightarrow & a_1 \curlywedge_A a_2 = a_1 \qquad \text{Def. } \preceq_A \\ & \Rightarrow & f(a_1 \curlywedge_A a_2) = f(a_1) \\ & \Rightarrow & f(a_1) \curlywedge_B f(a_2) = f(a_1) \qquad f \text{ ist } \curlywedge_A\text{-Homomorphismus} \\ & \Leftrightarrow & f(a_1) \preceq_B f(a_2) \qquad \text{Def. } \preceq_B \end{array}$$

(1) folgt analog, wenn wir folgende allgemein in Verbänden geltende Beziehung ausnutzen:

$$x \curlywedge y = x \Leftrightarrow x \curlyvee y = y.$$

Für die "⇒"-Richtung betrachten wir die aus der Absorption folgende Gleichheit $y = y \curlyvee (y \curlywedge x)$. Ausnutzen der Voraussetzung $x \curlywedge y = x$ liefert $y = y \curlyvee x$ und damit auch $x \curlyvee y = y$. Die "⇐"-Richtung ist analog. □

Dass $\curlyvee$- und $\curlywedge$-Homomorphismen echt strengere Eigenschaften als Ordungshomomorphismen sind, können wir anhand des folgenden Beispiels einsehen. Wir betrachten den gewöhnlichen Verband natürlicher Zahlen $(\mathbb{N}, \leq)$ und $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definiert durch $f((n, m)) = n + m$. Offensichtlich ist f ein Ordnungshomomorphismus. Allerdings liegt kein $\curlyvee$-Homomorphismus vor, denn es gilt zum einen

$$f((1,4) \curlyvee_{\mathbb{N}\times\mathbb{N}} (3,2)) = f((\min(\{1,3\}), \min(\{4,2\}))) = f((1,2)) = 3,$$

zum anderen aber

$$f((1,4)) \curlyvee_{\mathbb{N}} f((3,2)) = \min(\{f((1,4)), f((3,2))\}) = \min(\{5,5\}) = 5.$$

Ebenso liegt auch kein $\curlywedge$-Homomorphismus vor, denn zum einen haben wir

$$f((1,4) \curlywedge_{\mathbb{N}\times\mathbb{N}} (3,2)) = f((\max(\{1,3\}), \max(\{4,2\}))) = f((3,4)) = 7,$$

zum anderen

$$f((1,4)) \curlywedge_{\mathbb{N}} f((3,2)) = \max(\{f((1,4)), f((3,2))\}) = \max(\{5,5\}) = 5.$$

Kapitel 8

Algebraische Strukturen

In Kapitel 7.1.1 haben wir bereits Verbände in der Sichtweise algebraischer Strukturen betrachtet. In diesem Kapitel werden wir weitere wichtige algebraische Strukturen kennenlernen. Die Untersuchung algebraischer Strukturen ist Ergebnis eines für die moderne Mathematik prägenden Abstraktionsprozesses. Statt ähnliche Resultate für unterschiedliche mathematische Disziplien unabhängig nebeneinander zu entwickeln, versucht man gemeinsame Grundstrukturen zu identifizieren und Resultate anhand einer rein axiomatischen Basis herzuleiten.

8.1 Mengen mit einer Verknüpfung

Wir betrachten zunächst Mengen G, auf denen eine Verknüpfung $\oplus : G \times G \to G$ definiert ist. G bildet mit $\oplus$ eine algebraische Struktur, für die wir üblicherweise die Schreibweise $\langle G, \oplus \rangle$ verwenden.

8.1.1 Halbgruppen und Monoide

Setzen wir als minimale Eigenschaft die Assoziativität der Verknüfung voraus, wird die Struktur zur Halbgruppe:

Definition 8.1 (Halbgruppe) $\langle G, \oplus \rangle$ *heißt* Halbgruppe $\Leftrightarrow_{df}$ $\oplus$ *ist assoziativ, d.h.:*

$$\forall\, a, b, c \in G.\ (a \oplus b) \oplus c \ = \ a \oplus (b \oplus c)$$

Betrachten wir die ganzen Zahlen $\mathbb{Z}$ mit der Addition, so handelt es sich bei $\langle \mathbb{Z}, + \rangle$ um eine Halbgruppe, denn die Addition in $\mathbb{Z}$ ist bekanntlich assoziativ. Wenn wir anstatt der Addition allerdings die Subtraktion als Verknüpfung betrachten, so liegt keine Halbgruppe vor, denn die Eigenschaft der Assoziativität ist hier verletzt. Zeichenreihen (siehe Kapitel 5.1) mit der zugehörigen Konkatenation, also $\langle A^+, \cdot \rangle$, sind ein weiteres Beispiel für eine Halbgruppe.

Eine Halbgruppe $\langle G, \oplus \rangle$, deren Operation $\oplus$ kommutativ ist, wird *kommutative* oder auch *abelsche Halbgruppe* genannt. Ein algebraischer Verband besteht folglich aus zwei kommutativen Halbgruppen, die über das Absorptionsaxiom gekoppelt sind.

Ein Element $e \in G$ heißt *neutrales Element* genau dann, wenn

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

Natürlich muss es kein solches Element geben, z.B. sind $\langle \mathbb{N}\backslash\{1\}, \cdot \rangle$ oder $\langle \mathbb{N}\backslash\{0\}, + \rangle$ Halbgruppen ohne neutrale Elemente. Es kann aber höchstens ein neutrales Element geben:

Lemma 8.2 (Eindeutigkeit von neutralen Elementen) *Neutrale Elemente in einer Halbgruppe sind eindeutig bestimmt.*

Beweis Seien e, e' neutrale Elemente. Dann gilt: $e = e \oplus e' = e'$. □

Eine Halbgruppe mit neutralem Element heißt *Monoid*.

Beispiel 8.3 (Halbgruppen/Monoide)

- $\langle A^+, \cdot \rangle$ *ist Halbgruppe, aber kein Monoid, da kein neutrales Element existiert.*
- $\langle A^*, \cdot \rangle$ *ist Monoid mit neutralem Element* $\epsilon \in A^*$.
- $\langle \mathbb{N}, + \rangle$ *ist Monoid mit neutralem Element* 0.
- $\langle \mathbb{N}, \cdot \rangle$ *ist Monoid mit neutralem Element* 1.
- $\langle A^A, \circ \rangle$ *(Funktionen* $f : A \to A$*, Komposition) ist Monoid mit der identischen Abbildung* id_A *als neutralem Element.*

8.1.2 Gruppen

Betrachtet man $\langle \mathbb{Z}, + \rangle$, so liegt hier zwar wie bei $\langle \mathbb{N}, + \rangle$ auch ein Monoid vor, dieses besitzt aber eine zusätzliche wichtige Eigenschaft, nämlich das Vorhandensein inverser Elemente. Allgemein definiert man:

Definition 8.4 (Inverses Element) *Sei* $\langle G, \oplus \rangle$ *ein Monoid mit neutralem Element* e *und* $a \in G$. *Ein Element* $a^{-1} \in G$ *mit* $a \oplus a^{-1} = a^{-1} \oplus a = e$ *heißt* inverses Element *zu* a.

Inverse Elemente sind ebenfalls eindeutig bestimmt.

Lemma 8.5 (Eindeutigkeit von inversen Elementen) *Inverse Elemente in einer Halbgruppe sind eindeutig bestimmt.*

Beweis Sei a^{-1} und $\widetilde{a^{-1}}$ inverse Elemente zu a. Dann gilt:

$$a^{-1} \overset{\text{Neut.}}{=} e \oplus a^{-1} \overset{\text{Inv.}}{=} (\widetilde{a^{-1}} \oplus a) \oplus a^{-1} \overset{\text{Ass.}}{=} \widetilde{a^{-1}} \oplus (a \oplus a^{-1}) \overset{\text{Inv.}}{=} \widetilde{a^{-1}} \oplus e \overset{\text{Neut.}}{=} \widetilde{a^{-1}}$$

□

Monoide, die inverse Elemente besitzen, kennzeichnen eine außerordentlich wichtige algebraische Struktur.

Definition 8.6 (Gruppe) *Ein Monoid $\langle G, \oplus \rangle$, bei dem zu jedem Element $a \in G$ ein inverses Element $a^{-1} \in G$ existiert, heißt* Gruppe.

Liegt sogar ein kommutives Monoid zugrunde, so spricht man einer *kommutativen* bzw. *abelschen* Gruppe.

Beispiel 8.7 (Gruppen)

- $\langle \mathbb{R}\backslash\{0\}, \cdot \rangle$ *ist eine kommutative Gruppe mit neutralem Element 1. Das zu x inverse Element ist $\frac{1}{x}$.*
- $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{Z}, + \rangle$ *sind kommutative Gruppen. Neutrales Element ist die 0 und inverses Element zu x ist $-x$.*
- $\langle A^+, \cdot \rangle$ *ist keine Gruppe, da Worte aus A^+ keine inversen Elemente besitzen.*
- $\langle \mathbb{Z}, \cdot \rangle$ *ist keine Gruppe, da ganze Zahlen i.A. keine multiplikativ inversen Elemente besitzen.*
- $\langle \{-1, 1\}, \cdot \rangle$ *ist kommutative Gruppe.*

Endliche algebraische Strukturen wie Letztere aus Beispiel 8.7 lassen sich über Strukturtafeln darstellen. Im diesem Falle ist das einfach:

$\cdot$	-1	1
-1	1	-1
1	-1	1

Sei $\mathbb{Z}_n =_{df} \{0, \ldots, n-1\}$ $(n \geq 1)$. Dann definieren wir für $a, b \in \mathbb{Z}_n$:

$$\begin{aligned} a +_n b &=_{df} (a + b) \mod n \\ a \cdot_n b &=_{df} (a \cdot b) \mod n \end{aligned}$$

In Abbildung 8.1 wird die Addition $+_n$ und Multiplikation $\cdot_n$ exemplarisch für $\mathbb{Z}_6$ dargestellt.

Es gilt:

Satz 8.8 $\langle \mathbb{Z}_n, +_n \rangle$ *ist kommutative Gruppe.*

Beweis Übungen □

$+_n$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_n$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Abbildung 8.1: Additions- und Multiplikationstafeln für $\mathbb{Z}_6$

Allgemein gelten in Gruppen die folgenden Rechenregeln:

Lemma 8.9 (Rechenregeln in Gruppen) *Sei $\langle G, \oplus\rangle$ eine Gruppe. Dann gilt:*

1. $\forall a, b, c \in G.\ a \oplus b = c \oplus b \Rightarrow a = c$ *(Rechtskürzungsregel[a])*
2. $\forall a, b \in G.\ (a \oplus b)^{-1} = b^{-1} \oplus a^{-1}$ *(Invertierungsregel)*

[a] Es sei bemerkt, dass die Rechtskürzungsregel auch etwa in den Monoiden $\langle \mathbb{N}, +\rangle$ und $\langle \mathbb{N}\backslash\{0\}, \cdot\rangle$ gilt. Diese muss dann allerdings explizit unter Verwendung der Peano-Axiome bewiesen werden (siehe Satz 6.15).

Beweis

1. Wir folgern die Konklusion unter Anwendung der Prämisse:

$$\begin{aligned} a &\overset{\text{Neut.}}{=} a \oplus e \overset{\text{Inv.}}{=} a \oplus (b \oplus b^{-1}) \overset{\text{Assoz.}}{=} (a \oplus b) \oplus b^{-1} \\ &\overset{\text{Präm.}}{=} (c \oplus b) \oplus b^{-1} \overset{\text{Assoz.}}{=} c \oplus (b \oplus b^{-1}) \overset{\text{Inv.}}{=} c \oplus e \\ &\overset{\text{Neut.}}{=} c \end{aligned}$$

2. Übungen

□

8.1.3 Untergruppen

Für eine gegebene Gruppe lassen sich interessante Teilstrukturen, die sogenannten *Untergruppen*, identifizieren und näher untersuchen.

Definition 8.10 (Untergruppen) Ist $\langle G, \oplus\rangle$ eine Gruppe und $H \neq \emptyset$ eine Teilmenge von G, so dass $\langle H, \oplus\rangle$ auch eine Gruppe ist, so nennen wir $\langle H, \oplus\rangle$ Untergruppe von $\langle G, \oplus\rangle$.

Analoge Unterstrukturen lassen sich für Halbgruppen und Monoide definieren. Unterstrukturen müssen insbesondere mit derselben Operation wie in der Oberstruktur versehen sein. So ist zum Beispiel die Gruppe $\langle \mathbb{Z}, -\rangle$ keine Untergruppe der Gruppe $\langle \mathbb{R}, +\rangle$, obwohl $\mathbb{Z} \subseteq \mathbb{R}$ gilt.

Beispiel 8.11 $\langle \mathbb{Z}, + \rangle$ *ist Untergruppe von* $\langle \mathbb{R}, + \rangle$.

Dass das neutrale Element in einem Monoid eindeutig ist, wurde in Satz 8.2 bereits gezeigt. Man könnte jetzt vermuten, dass Untermonoide auch dasselbe neutrale Element wie in der übergeordneten Struktur besitzen. Dies gilt jedoch nicht der Fall:

Beispiel 8.12 *Bei einem Monoid mit Untermonoid müssen die neutralen Elemente nicht notwendig übereinstimmen. Gegeben sei das Monoid* $\langle G, \oplus \rangle$ *gemäß der folgenden Verknüpfungstabelle:*

$\oplus$	a	b
a	a	b
b	b	b

$\langle G, \oplus \rangle$ *besitzt als neutrales Element* a*. Im Untermonoid* $\langle \{b\}, \oplus \rangle$ *ist* b *jedoch neutrales Element.*

Diese Situation ändert sich aber, wenn wir es mit Gruppen zu tun haben.

Satz 8.13 *Eine Untergruppe* $\langle H, \oplus \rangle$ *von* $\langle G, \oplus \rangle$ *besitzt das gleiche neutrale Element wie* $\langle G, \oplus \rangle$.

Beweis Seien e_G und e_H die neutralen Elemente von G bzw. H und $a \in H$ (beachte $H \neq \emptyset$). Dann gilt $a = e_G \oplus a = e_H \oplus a$. Mit der Rechtskürzungsregel (Satz 8.9(1)) folgt sofort $e_G = e_H$. □

Satz 8.13 stellt insbesondere sicher, dass $\{e\}$ die einzige einelemenige Untergruppe ist. Jede Gruppe hat damit zwei *triviale Untergruppen*, nämlich $\{e\}$ und die Gruppe selbst.

Definition 8.14 (Symmetrische Gruppe)
Für $n \geq 2$ *bildet* $S_n =_{df} \{f \mid f : \{1, \ldots, n\} \to \{1, \ldots, n\}, f \text{ bijektiv}\}$ *mit der Komposition als Operation eine Gruppe, die sogenannte* symmetrische Gruppe*. Die Elemente in* S_n*, sprich die bijektiven Abbildungen, werden auch als* Permutationen *bezeichnet.*

Permutationen sind umkehrbar und gegenüber Komposition abgeschlossen. Die identische Abbildung ist Permutation und dient als neutrales Element. Weil die Hintereinanderausführung von Funktionen assoziativ ist, hat S_n offensichtlich Gruppeneigenschaften. Wir werden später sehen, dass die S_n (außer für $n = 2$) nicht kommutativ sind.

Permutationen lassen sich Matrixschreibweise darstellen. So repräsentiert die Schreibweise

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

eine Permutation aus S_3 mit $f(1) = 3$, $f(2) = 2$ und $f(3) = 1$. Damit ist ganz S_3 darstellbar als:

$$S_3 = \left\{ \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix} \right\}$$

Alternativ können Permutationen auch in der kompakten Zyklenschreibweise angegeben werden. Im obigen Beispiel etwa $f = (1\,3)$, was bedeutet, dass das erste und dritte Element vertauscht werden. Ein 3-Zyklus wie $(1\,2\,3)$ steht für die Permutation

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Allgemein steht $(c_1\,c_2\,c_3\,\ldots\,c_{k-1}\,c_k)$ für $c_1 \mapsto c_2$, $c_2 \mapsto c_3$,...,$c_{k-1} \mapsto c_k$, $c_k \mapsto c_1$. Kommt ein c_i nicht vor so bedeutet dies $c_i \mapsto c_i$. Die identische Abbildung ist folglich durch den leeren Zyklus () repräsentiert. In dieser Schreibweise liest sich die S_3-Darstellung wie folgt:

$$S_3 = \{(), (23), (12), (123), (132), (13)\}.$$

Zu einer Gruppe $\langle G, \oplus \rangle$ bildet die Menge aller Untergruppen einen vollständigen Verband (siehe Abbildung 8.2). Die Infimumsoperation ist dabei der Schnitt der Untergruppen, die trivialen Untergruppen bilden das kleinste und größte Element.

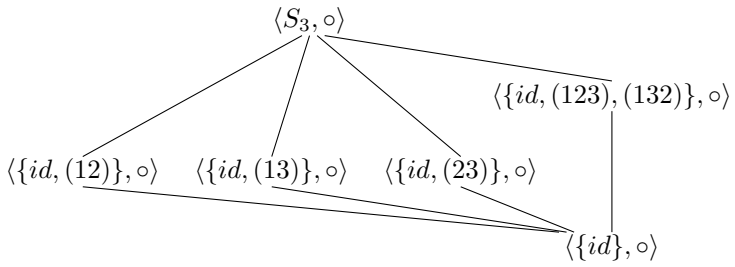


Abbildung 8.2: Untergruppenverband zu $\langle S_3, \circ \rangle$

8.1.4 Nebenklassen und Normalteiler

Untergruppen induzieren auf der zugrundliegenden Gruppe eine Zerlegung in sogenannte Nebenklassen. Betrachtet man beispielsweise die Gruppe $\langle \mathbb{Z}, + \rangle$ und deren Untergruppe der durch 3 teilbaren Zahlen $3\mathbb{Z}$, so kann man sich $\mathbb{Z}$ zerlegt vorstellen in

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ 3\mathbb{Z}+1 &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ 3\mathbb{Z}+2 &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

Dieses kann verallgemeinert werden durch den Begriff der Nebenklassen:

Definition 8.15 (Nebenklassen) *Sei $\langle H, \oplus\rangle$ eine Untergruppe von $\langle G, \oplus\rangle$ und $a \in G$. Dann bezeichne*

$$\begin{aligned} aH &=_{df} \{a \oplus h \mid h \in H\} \\ Ha &=_{df} \{h \oplus a \mid h \in H\} \end{aligned}$$

die Links- *und* Rechtsnebenklasse *von H zu a.*

Offensichtlich stimmen in kommutativen Gruppen Links- und Rechtsnebenklassen überein. Im allgemeinen ist dieses aber nicht so, wie das folgende Beispiel zeigt:

Beispiel 8.16 *Betrachten wir die Untergruppe $H = \langle\{id, (1,2)\}, \circ\rangle$ von $\langle S_3, \circ\rangle$ und das Element $a = (23) \in G$, dann gilt*

$$\begin{aligned} aH &= \{(23) \circ id, (23) \circ (12)\} = \{(23), (132)\} \\ Ha &= \{id \circ (23), (12) \circ (23)\} = \{(23), (123)\} \end{aligned}$$

Folgendes wichtiges Resultat setzt die Mächtigkeiten von Gruppen und deren Untergruppen in Beziehung:

Satz 8.17 (Satz von Lagrange) *Sei $\langle G, \oplus\rangle$ eine endliche Gruppe und $\langle H, \oplus\rangle$ eine Untergruppe von G. Dann gilt*

$$|H| \Big| |G|$$

Beweis Wir zeigen: Die Menge der Rechtsnebenklassen bildet eine Partition mit gleichgroßen Klassen. Im Detail:

1. $\forall a \in G.\ aH \neq \emptyset$. Klar, da H nicht leer ist.
2. $\bigcup_{g \in G} gH = G$. Klar, da $e \in H$ (H ist Untergruppe).
3. $\forall a, a' \in G.\ \ aH \cap a'H \neq \emptyset \ \Rightarrow\ aH = a'H$.
   Seien $a, a' \in G$ mit $aH \cap a'H \neq \emptyset$. Dann gibt es $h, h' \in H$ mit $a \oplus h = a' \oplus h'$, also
   $$a \ = \ a' \oplus h' \oplus h^{-1} \tag{8.1}$$
   Zeige o.B.d.A. $aH \subseteq a'H$ (Antisymmetrie-Beweisprinzip). Sei $g \in aH$. Dann gibt es ein $h'' \in H$ mit $g = a \oplus h''$. Also folgt:
   $$g \ = \ a \oplus h'' \ \overset{(8.1)}{=}\ \overbrace{a' \oplus \underbrace{h' \oplus h^{-1}}_{\in H} \oplus h''}^{a} \in a'H$$
   Beachte: $h' \oplus h^{-1} \oplus h'' \in H$, da H eine Untergruppe ist.
4. $\forall a, a' \in G.\ |aH| = |a'H|$.
   Sei $f : aH \to G$ mit $b \mapsto a' \oplus a^{-1} \oplus b$. Zu zeigen

(a) $\forall b \in aH.\ f(b) \in a'H$
Wegen $b \in aH$ gibt es ein $h \in H$ mit $b = a \oplus h \in aH$. Es gilt:

$$\begin{aligned} f(b) &= f(a \oplus h) \\ &= a' \oplus \underbrace{a^{-1} \oplus a}_{e} \oplus h \\ &= a' \oplus h \in a'H. \end{aligned}$$

(b) f ist injektiv. Seien $b_1 = a \oplus h_1$, $b_2 = a \oplus h_2$ und $f(b_1) = f(b_2)$. Dann gilt:

$$\begin{aligned} b_1 &= a \oplus h_1 = \underbrace{a \oplus \overbrace{a'^{-1} \oplus a'}^{e} \oplus a^{-1}}_{e} \oplus \overbrace{a \oplus h_1}^{b_1} = a \oplus a'^{-1} \oplus \underbrace{a' \oplus a^{-1} \oplus a \oplus h_1}_{f(b_1)} \\ &\overset{Vor.}{=} a \oplus a'^{-1} \oplus f(b_2) = a \oplus a'^{-1} \oplus \overbrace{a' \oplus a^{-1} \oplus a \oplus h_2}^{f(b_2)} \\ &= \underbrace{a \oplus \overbrace{a'^{-1} \oplus a'}^{e} \oplus a^{-1}}_{e} \oplus \overbrace{a \oplus h_2}^{b_2} = a \oplus h_2 = b_2 \end{aligned}$$

□

Aus Satz 8.17 folgt zum Beispiel, dass es in S_3 keine Untergruppen mit 4 Elementen geben kann. Ebenso kann eine Gruppe, deren Mächtigkeit eine Primzahl ist, nur triviale Untergruppen haben. Weitere bekannte Resultate, die auf dem Satz von Lagrange aufbauen, sind der kleine Satz von Fermat und dessen Generalisierung, Eulers Theorem.

Wie bereits erwähnt, stimmen für kommutative Gruppen Rechts- und Linksnebenklassen generell, d.h. für alle Untergruppen, überein. Allgemein nehmen Untergruppen mit dieser Eigenschaft eine besondere Rolle ein.

Definition 8.18 (Normalteiler) *Sei $\langle H, \oplus \rangle$ eine Untergruppe von $\langle G, \oplus \rangle$. Wenn die Rechts- und Linksnebenklassen für alle $a \in G$ übereinstimmen ($Ha = aH$), wird H ein Normalteiler von G genannt (Notation: $H \triangleleft G$).*

Wie bereits ausgeführt ist in kommutativen Gruppen jede Untergruppe Normalteiler. Für die nichtkommutative Gruppe S_3 haben wir aber auch Normalteiler:

Beispiel 8.19 *Es gilt* $\langle \underbrace{\{id, (123), (132)\}}_{N}, \circ\rangle \triangleleft \langle S_3, \circ\rangle$. *Wähle z.B.* $a = (23) \in S_3$. *Dann gilt*

$$\begin{aligned}(23) \circ N &= \{(23) \circ id, (23) \circ (123), (23) \circ (132)\} = \{(23), (13), (12)\}\\ N \circ (23) &= \{id \circ (23), (123) \circ (23), (132) \circ (23)\} = \{(23), (12), (13)\} = (23) \circ N\end{aligned}$$

$\langle\{id, (123), (132)\}, \circ\rangle$ *wird auch als* A_3 *(alternierende Gruppe) bezeichnet.* $\langle A_3, \circ\rangle \cong \langle \mathbb{Z}_3, +_3\rangle$ *(Isomorphie: später formal)*

$\circ$	*id*	*(123)*	*(132)*
id	*id*	*(123)*	*(132)*
(123)	*(123)*	*(132)*	*id*
(132)	*(132)*	*id*	*(123)*

$+_3$	*0*	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

Die Bedeutung der Normalteiler liegt darin, dass sie eine Gruppenstruktur auf die Nebenklassen übertragen. So ist es quasi möglich direkt auf den Nebenklassen zu "rechnen". Betrachten wir beispielsweise den Normalteiler $3\mathbb{Z}$ von $\mathbb{Z}$ auf Seite 86 erneut, so haben wir etwa:

$$(1 + 3\mathbb{Z}) +_{3\mathbb{Z}} (2 + 3\mathbb{Z}) \;=\; (1 + 2) + 3\mathbb{Z} \;=\; 3 + 3\mathbb{Z} \;=\; 3\mathbb{Z}.$$

Allgemein definieren wir:

Lemma 8.20 (Faktorgruppe) *Sei* $\langle G, \oplus\rangle$ *eine Gruppe und* N *ein Normalteiler von* G. *Dann ist* $\langle G/N, \oplus_N\rangle$ *mit*

$$G/N =_{df} \{aN \mid a \in G\}$$

eine Gruppe, wobei $\oplus_N$ *wie folgt definiert ist:*

$$aN \oplus_N bN = (a \oplus b)N$$

Wir nennen $\langle G/N, \oplus_N\rangle$ *die* Faktorgruppe *von* G *bezüglich* N.

Beweis

Zu zeigen:

1. Wohldefiniertheit (Representantenunabhängigkeit), d.h.

   $$\forall a, a', b, b' \in G.$$

   $$aN = a'N \wedge bN = b'N \quad \Rightarrow \quad aN \oplus_N bN = a'N \oplus_N b'N$$

   Seien a, a', b, b' gegeben mit $aN = a'N \wedge bN = b'N$. Zunächst gilt: $\exists n, n' \in N.$ mit $a' = a \oplus n'$, $b' = b \oplus n''$. Weil N Normalteiler ist, stimmen die Links- und Rechtsnebenklassen überein

und es gilt insbesondere $n' \oplus b = b \oplus n'''$ für ein geeignetes $n''' \in N$. Dann gilt:

$$\begin{aligned} a'N \oplus_N b'N &= (a' \oplus b')N \\ &= ((a \oplus n') \oplus (b \oplus n''))N \\ &= (a \oplus (n' \oplus b) \oplus n'')N \\ &= (a \oplus (b \oplus n''') \oplus n'')N \\ &= ((a \oplus b) \oplus \underbrace{n''' \oplus n''}_{n''''})N \\ &= (a \oplus b)N \\ &= aN \oplus_N bN \end{aligned}$$

2. G/N hat ein neutrales Element e_N.
   Sei e das neutrale Element von G. Dann zeigen wir:

   $$eN = N = Ne \text{ ist neutrales Element von } G/N.$$

   Sei $a \in G$. Dann gilt:

   $$aN \oplus_N eN = (a \oplus e)N = aN$$

3. G/N hat inverse Elemente:

   $$\forall a \in G\ \exists a^{-1} \in G.\ \ aN \oplus_N a^{-1}N = e_N$$

   Sei $N' \in G/N$. Dann ist zu zeigen: $\exists\, N''.\ N' \oplus_N N'' = N$.
   Zunächst gilt $\exists\, a \in G.\ N' = aN$ und damit:

   $$aN \oplus_N a^{-1}N = (a \oplus a^{-1})N = eN = N$$

□

Unmittelbare Folge des Satzes von Lagrange (genau genommen dessen Beweises) ist dann:

Korollar 8.21 (Korollar zum Satz von Lagrange) *Sei $\langle G, \oplus\rangle$ eine endliche Gruppe und H ein Normalteiler von G. Es gilt*

$$|G| = |H| \cdot |G/H|$$

8.1.5 Homomorphismen

Homomorphismen als *strukturverträgliche Abbildungen* wurden bereits in Kapitel 7.4 im Zusammenhang mit Verbänden betrachtet. Auch für die hier vorgestellten algebraischen Strukturen sind diese von großer Bedeutung. Einige solche strukturverträglichen Abbildungen sind bereits durch "Rechengesetze" der Schulmathematik bekannt, ohne explizit als Homomorhismen charakterisiert worden zu sein. So verbirgt sich beispielsweise hinter dem Gesetz zum Rechnen mit Logarithmen

$$\log(x \cdot y) = \log(x) + \log(y)$$

die Aussage, dass log ein Gruppenhomomorphismus von $\langle \mathbb{R}_{>0}, \cdot\rangle$ nach $\langle \mathbb{R}, +\rangle$ ist.

Definition 8.22 ((Gruppen-)Homomorphismus) *Seien $\langle G_1, \oplus_1 \rangle$ und $\langle G_2, \oplus_2 \rangle$ Gruppen und $f : G_1 \to G_2$ eine Abbildung. f heißt (Gruppen-)Homomorphismus, genau dann wenn*

$$\forall a, b \in G_1.\ f(a \oplus_1 b) = f(a) \oplus_2 f(b)$$

Die Abbildung heißt

- *Monomorphismus, wenn f zusätzlich **injektiv** ist.*
- *Epimorphismus, wenn f zusätzlich **surjektiv** ist.*
- *Isomorphismus, wenn f zusätzlich **bijektiv** ist.*

Bei Gleichheit der beiden Gruppen nennt man f ferner

- *Endomorphismus*
- *Automorphismus, wenn f auch **Isomorphismus** ist.*

Analoge Begriffe können für Halbgruppen und Monoide definiert werden. Bei Monoidhomomorphismen fordert man zusätzlich, dass das neutrale Element der Argumentmonoids auf das neutrale Element des Zielmonoids abbildet. Für Gruppenhomomorphismen muss dieses nicht explizit gefordert werden, denn wir haben folgendes Resultat:

Lemma 8.23 (Lemma) *Seien $\langle G_1, \oplus_1 \rangle$ und $\langle G_2, \oplus_2 \rangle$ Gruppen mit neutralen Elementen e_1 und e_2. Ferner sei $f : G_1 \to G_2$ ein Gruppenhomomorphismus. Dann gilt:*

1. $f(e_1) = e_2$
2. $\forall a \in G_1.\ f(a^{-1}) = (f(a))^{-1}$

Beweis

1. Sei $a \in G_1$. Dann gilt zum einen $f(a) = f(e_1 \oplus_1 a) = f(e_1) \oplus_2 f(a)$,
   zum anderen $f(a) = e_2 \oplus_2 f(a)$.

   Insgesamt haben wir also $f(e_1) \oplus_2 f(a) = e_2 \oplus_2 f(a)$ und mit der Rechtskürzungsregel (siehe Satz 8.9(1)) folgt $f(e_1) = e_2$.

2. Sei $a \in G_1$. Dann gilt zum einen $e_2 = (f(a))^{-1} \oplus_2 f(a)$,
   zum anderen $e_2 \overset{(1)}{=} f(e_1) = f(a^{-1} \oplus_1 a) = f(a^{-1}) \oplus_2 f(a)$.

   Insgesamt haben wir also $(f(a))^{-1} \oplus_2 f(a) = f(a^{-1}) \oplus_2 f(a)$. Wieder folgt mit der Rechtskürzungsregel $f(a^{-1}) = (f(a))^{-1}$.

□

Wir schreiben im Folgenden auch kurz $f : \langle G_1, \oplus_1 \rangle \to \langle G_2, \oplus_2 \rangle$, um die die zugrundliegenden Strukturen $\langle G_1, \oplus_1 \rangle$ und $\langle G_2, \oplus_2 \rangle$ und die Abbildung in einer Schribweise kompakt darzustellen. Betrachten wir nun einige Beispiele für Homomorphismen.

Beispiel 8.24

1. $\varphi_1 : \langle A^*, \cdot\rangle \to \langle \mathbb{N}, +\rangle$ *mit* $w \mapsto |w|$ *ist ein Monoidepimorphismus, denn es gilt* $\varphi_1(\varepsilon) = |\varepsilon| = 0$ *und*
$$\varphi_1(w_1 \cdot w_2) = \varphi_1(w_1 w_2) = |w_1 w_2| = |w_1| + |w_2| = \varphi_1(w_1) + \varphi_1(w_2)$$
Surjektivität: Sei $a \in A$. $\forall n \in \mathbb{N} : \varphi_1(a^n) = n$.

Nichtinjektivität für $|A| \geq 2$*: Seien* $a, b \in A$ *verschieden. Dann ist* $\varphi_1(ab) = \varphi_1(ba) = 2$.

2. $\varphi_2 : \langle \mathbb{Z}, +\rangle \to \langle \mathbb{N}, +\rangle$ *mit* $\varphi_2(x) = x^2$ *ist kein Homomorphismus, denn*
$$\varphi_2(1+1) = (1+1)^2 = 2^2 = 4 \quad \neq \quad 2 = 1^2 + 1^2 = \varphi_2(1) + \varphi_2(1)$$

3. *Sei* G *eine Gruppe und* N *ein Normalteiler von* G*. Dann ist*
$$\varphi_3 : G \to G/N \quad \textit{mit} \quad \varphi_3(g) = gN$$
ein Gruppenepimorphismus.

4. *Sei* $\langle G, \oplus\rangle$ *eine Gruppe und* $b \in G$*. Dann ist*
$$\varphi_b : G \to G \quad \textit{mit} \quad \varphi_b(g) = b^{-1} \oplus g \oplus b$$
ein Gruppenautomorphismus.

Homomorphie: Seien $g_1, g_2 \in G$*. Dann gilt:*
$$\begin{aligned}
\varphi_b(g_1 \oplus g_2) &\overset{\text{Def. } \varphi_b}{=} b^{-1} \oplus (g_1 \oplus g_2) \oplus b \overset{\text{Ass.}}{=} (b^{-1} \oplus g_1) \oplus (g_2 \oplus b) \\
&\overset{\text{Neut.}}{=} (b^{-1} \oplus g_1) \oplus e \oplus (g_2 \oplus b) \overset{\text{Inv.}}{=} (b^{-1} \oplus g_1) \oplus (b \oplus b^{-1}) \oplus (g_2 \oplus b) \\
&\overset{\text{Ass.}}{=} (b^{-1} \oplus g_1 \oplus b) \oplus (b^{-1} \oplus g_2 \oplus b) \\
&\overset{\text{Def. } \varphi_b}{=} \varphi_b(g_1) \oplus \varphi_b(g_2)
\end{aligned}$$

Surjektivität: Sei $g \in G$*. Dann gilt mit* $g' =_{df} b \oplus g \oplus b^{-1}$*:*
$$\begin{aligned}
\varphi_b(g') &\overset{\text{Def. } g'}{=} b^{-1} \oplus (b \oplus g \oplus b^{-1}) \oplus b \overset{\text{Ass.}}{=} (b^{-1} \oplus b) \oplus g \oplus (b^{-1} \oplus b) \\
&\overset{\text{Inv.}}{=} e \oplus g \oplus e \overset{\text{Neut.}}{=} g
\end{aligned}$$

Injektivität: Seien $g_1, g_2 \in G$*. Dann gilt:*
$$\begin{aligned}
\varphi_b(g_1) = \varphi_b(g_2) &\overset{\text{Def. } \varphi_b}{\Rightarrow} b^{-1} \oplus g_1 \oplus b = b^{-1} \oplus g_2 \oplus b \\
&\overset{\textit{Rkürz}}{\Rightarrow} b^{-1} \oplus g_1 = b^{-1} \oplus g_2 \\
&\Rightarrow b \oplus (b^{-1} \oplus g_1) = b \oplus (b^{-1} \oplus g_2) \\
&\overset{\text{Ass.}}{\Rightarrow} (b \oplus b^{-1}) \oplus g_1 = (b \oplus b^{-1}) \oplus g_2 \\
&\overset{\text{Inv.}}{\Rightarrow} e \oplus g_1 = e \oplus g_2 \\
&\overset{\text{Neut.}}{\Rightarrow} g_1 = g_2
\end{aligned}$$

Abschließend wollen wir noch auf spezielle von Homomorphismen induzierte Gruppenstrukturen eingehen.

Definition 8.25 (Kern) *Seien $\langle G_1, \oplus_1\rangle$ und $\langle G_2, \oplus_2\rangle$ Gruppen mit neutralen Elementen e_1 und e_2. Für einen Gruppenhomomorphismus $\varphi : G_1 \to G_2$ ist der Kern von φ die Menge der Elemente, die auf das neutrale Element in G_2 abgebildet werden:*

$$Kern(\varphi) \ =_{df} \ \{x \in G_1 \mid \varphi(x) = e_2\}$$

Beispiel 8.26 (Kern) *$\varphi : \langle \mathbb{Z}_6, +_6\rangle \to \langle Z_6, +_6\rangle$ mit $\varphi(x) = 2x$ ist ein Gruppenhomomorphismus. Es gilt:*

$$Kern(\varphi) = \{0, 3\}$$

Allgemein gilt folgendes Resultat:

Satz 8.27 (Homomorphismen und Gruppenstrukturen) *Seien $\langle G_1, \oplus_1\rangle$ und $\langle G_2, \oplus_2\rangle$ Gruppen mir neutralen Elementen e_1 und e_2. Für einen Gruppenhomomorphismus $\varphi : G_1 \to G_2$ gilt:*

1. *$Kern(\varphi)$ bildet einen Normalteiler von G_1,*
2. *$Bild(\varphi) = \{y \in G_2 \mid \exists x \in G_1.\ \varphi(x) = y\}$ bildet eine Untergruppe von G_2.*

Beweis

1. Sei $K =_{df} Kern(\varphi)$. Wir zeigen zunächst, dass K Untergruppe von G_1 ist. Seien $a, b \in K$. Wegen $\varphi(a \oplus_1 b) = \varphi(a) \oplus_2 \varphi(b) = e_2 \oplus_2 e_2 = e_2$ ist K bezüglich $\oplus_1$ abgeschlossen. Wegen $\varphi(e_1) = e_2$ ist außerdem $e_1 \in K$. Mit Lemma 8.23(2) gilt auch $\varphi(a^{-1}) = (\varphi(a))^{-1} = e_2^{-1} = e_2$ und somit liegen auch die Inversen in K.

   Wir zeigen nun, dass K Normalteiler von G_1 ist. Zunächst überlegen wir uns dafür eine alternative Normalteilercharakterisierung. Für eine Gruppe $\langle G, \oplus\rangle$ und deren Untergruppe H gilt nämlich:

   $$(\forall\, a \in G.\ aHa^{-1} \subseteq H) \ \Leftrightarrow \ (\forall\, a \in G.\ aH = Ha) \qquad (*)$$

   Wir haben zum einen:

   $$(\forall\, a \in G.\ aHa^{-1} \subseteq H) \ \Rightarrow \ (\forall\, a \in G.\ aHa^{-1}a \subseteq Ha) \ \Rightarrow \ (\forall\, a \in G.\ aH \subseteq Ha)$$

   und zum anderen:

   $$\begin{aligned}(\forall\, a \in G.\ aHa^{-1} \subseteq H) \ &\Rightarrow \ (\forall\, a \in G.\ a^{-1}Ha \subseteq H) \ \Rightarrow \ (\forall\, a \in G.\ aa^{-1}Ha \subseteq aH)\\ &\Rightarrow \ (\forall\, a \in G.\ Ha \subseteq aH)\end{aligned}$$

Zusammen gilt $(\forall\, a \in G.\ aHa^{-1} \subseteq H) \ \Rightarrow\ (\forall\, a \in G.\ aH = Ha)$. Die umgekehrte Richtung ist einfach, denn es gilt

$$(\forall\, a \in G.\ aH = Ha) \ \Rightarrow\ (\forall\, a \in G.\ aHa^{-1} = Haa^{-1}) \ \Rightarrow\ (\forall\, a \in G.\ aHa^{-1} = H).$$

Um zu zeigen, dass K Normalteiler von G_1 ist, zeigen wir nun die allgemeinere Behauptung, dass jedes Urbild eines Normalteilers von G_2 ein Normalteiler von G_1 ist. Da $\{e_2\}$ trivialer Normalteiler von G_2 ist, impliziert das insbesondere die Behauptung. Sei also N_2 Normalteiler von G_2 und $N_1 =_{df} \varphi^{-1}(N_2)$ dessen Urbild. Dann gilt für $a \in G_1$:

$$\varphi(aN_1a^{-1}) \overset{\varphi \text{ Hom.}}{=} \varphi(a)\varphi(N_1)\varphi(a^{-1}) \overset{\text{Lem.8.23}}{=} \varphi(a)\varphi(N_1)(\varphi(a))^{-1} \overset{\text{Def.}N_1}{=} \varphi(a)N_2(\varphi(a))^{-1} \overset{(*)}{\subseteq} N_2$$

Da das Bild von aN_1a^{-1} in N_2 liegt, muss nach Definition von N_1 insbesondere $aN_1a^{-1} \subseteq N_1$ gelten. Gemäß Eigenschaft (*) folgt hieraus aber schon, dass N_1 Normateiler von G_1 ist.

2. Sei $B =_{df} Bild(\varphi)$. Wir zeigen, dass B Untergruppe von G_2 ist. Seien $b_1, b_2 \in B$. Dann existieren $a_1, a_2 \in G_1$ mit $b_1 = \varphi(a_1)$ und $b_2 = \varphi(a_2)$. Wegen $b_1 \oplus_2 b_2 = \varphi(a_1) \oplus_2 \varphi(a_1) = \varphi(a_1 \oplus_1 a_2)$ ist B bezüglich $\oplus_2$ abgeschlossen. Mit Lemma 8.23(2) gilt außerdem $b_1^{-1} = (\varphi(a_1))^{-1} = \varphi(a_1^{-1}) \in B$.

□

Gruppenhomomorphismen selbst können wieder Gruppenstuktur besitzen. Hier gilt:

Satz 8.28 (Automorphismengruppe) *Die Menge aller Automorphismen einer Gruppe ist zusammen mit der Komposition selbst eine Gruppe.*

Beweis Die Funktionskomposition ist offensichtlich assoziativ und die identische Abbildung neutrales Element. Die Umkehrfunktionen sind die inversen Elemente. Mit der Abgeschlossenheit bijektiver Funktionen und Homomorphismen bezüglich Funktionskomposition ist alles gezeigt. □

8.2 Mengen mit zwei Verknüpfungen

Der Zahlbereich der ganzen Zahlen war bislang gekennzeichnet durch eine additive kommutative Gruppe und ein multiplikatives Monoid. Der Zusammenhang zwischen Addition und Multiplikation bleibt dabei allerdings unberücksichtigt. Da in vielen Bereichen der Mathematik solche mit zwei Verknüfungen versehenen Objekte vorliegen, sind auch hier entsprechende algebraische Strukturen entstanden, die eine saubere axiomatische Grundlage schaffen.

8.2.1 Ringe

Die einfachste Struktur, nämlich die der *Ringe*, ist eine Verallgemeinerung der wesentlichen Eigenschaften der ganzen Zahlen. Die Theorie der Ringe liefert bereits weitreichende Resultate, die Anwendung auch in anderen Strukturen wie Polynomringen und quadratische Matrizen haben.

Definition 8.29 (Ring) *Eine Menge R mit Operationen $\oplus$ und $\odot$ heißt Ring* $\Leftrightarrow_{df}$

- $\langle R, \oplus\rangle$ *bildet eine kommutative Gruppe,*
- $\langle R, \odot\rangle$ *bildet eine Halbgruppe,*
- *Es gelten die Distributivgesetze:*

$$\begin{aligned} \forall a,b,c \in R.\ a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c) \\ \forall a,b,c \in R.\ (a \oplus b) \odot c &= (a \odot c) \oplus (b \odot c) \end{aligned}$$

Ein Ring $\langle R, \oplus, \odot\rangle$ heißt kommutativ genau dann, wenn auch $\langle R, \odot\rangle$ kommutativ ist.

Das neutrale Element bezüglich $\oplus$ bzeichnet man als *Nullelement* oder kurz 0, des Ringes. Existiert auch ein neutrales Element bezüglich $\odot$ so bezeichnet man dieses als *Einselement* oder kurz 1 des Ringes. In diesem Fall spricht man von einem "*Ring mit Einselement*". In einem Ring verwendet man für die Inversen der additiven Gruppe die Notation $-a$ statt a^{-1}. Für jedes Element a eines Ringes gilt $a \odot 0 \ = \ 0 \odot a \ = \ 0$, denn

$$0 \oplus (0 \odot a) \ = \ 0 \odot a \ = \ (0 \oplus 0) \odot a \ \stackrel{\text{Dist.}}{=} \ (0 \odot a) \oplus (0 \odot a).$$

Mit der Rechtkürzungsregel folgt dann $0 \ = \ 0 \odot a$. Analog gilt $0 \ = \ a \odot 0$.

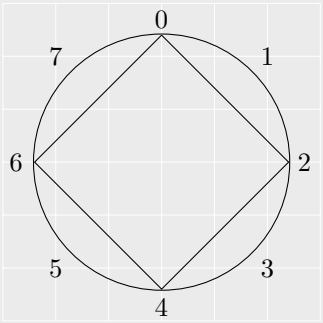
Beispiel 8.30 (Ringe)

- $\langle \mathbb{Z}, +, \cdot\rangle$ *ist ein kommutativer Ring mit Einselement 1.*
- $\langle m\mathbb{Z}, +, \cdot\rangle$ *mit* $m\mathbb{Z} =_{df} \{m \cdot z \mid z \in \mathbb{Z}\}$ *für* $m \in \mathbb{N}\backslash\{0\}$ *sind kommutative Ringe. Für* $m > 1$ *ist aber kein Einselement vorhanden.*
- $\langle \mathfrak{P}(M), \Delta, \cap\rangle$ *(Potenzmenge, symmetrische Differenz, Schnittmenge) ist kommutativer Ring mit Einselement.*[a] *Offenbar ist* $\langle \mathfrak{P}(M), \cap\rangle$ *kommutative Halbgruppe mit neutralem Element* M. $\langle \mathfrak{P}(M), \Delta\rangle$ *ist sogar kommutative Gruppe mit neutralem Element* $\emptyset$. *Die symmetrische Differenz ist offensichtlich kommutativ und* $\emptyset$ *neutrales Element. Mit* $A\Delta B \ = \ (A \cap B^{\complement}) \cup (A^{\complement} \cap B)$ *lässt sich die Assoziativität, wenn auch mit einigem Rechenaufwand, nachweisen. Schließlich ist jede Menge zu sich selbst invers, denn* $A \,\Delta\, A \ = \ \emptyset$.
- $\mathbb{R}[x] \ =_{df} \ \langle \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}, +, \cdot\rangle$ *(Polynome mit reellen Koeffizienten) ist ein kommutativer Ring. Hierbei bezeichnen* $+$ *und* $\cdot$ *die Polynomaddition und -multiplikation. Null- und Einselement sind die konstante 0- bzw. 1-Funktion.*
- *Die* $n \times n$*-Matrizen (*$n \in \mathbb{N}\backslash\{0\}$*) über* $\mathbb{R}$ *bilden einen nichtkommutativen Ring mit Einselement (siehe Satz 10.1.4).*

[a] Man beachte, dass $\langle \mathfrak{P}(M), \cup, \cap\rangle$ kein Ring ist. Zwar ist $\langle \mathfrak{P}(M), \cup\rangle$ kommutative Halbgruppe mit neutralem Element $\emptyset$ und $\langle \mathfrak{P}(M), \cap\rangle$ kommutative Halbgruppe mit neutralem Element M, aber die Mengenkomplemente sind keine geeigneten Inversen. Bzgl. der Vereinigung gilt $A \cup A^{\complement} = M$ und nicht etwa $A \cup A^{\complement} = \emptyset$. Ebenso gilt $A \cap A^{\complement} = \emptyset$ und nicht etwa $A \cap A^{\complement} = M$.

Analog zum Begriff der Untergruppe bildet eine nichtleere Teilmenge $R' \subseteq R$ eines Ringes $\langle R, \oplus, \odot \rangle$ einen *Unterring*, wenn $\langle R', \oplus, \odot \rangle$ ein Ring ist. Trivialerweise ist ein Unterring eines kommutativen Ringes wieder kommutativ. Wie das Beispiel $2\mathbb{Z} \subseteq \mathbb{Z}$ zeigt, muss ein Unterring aber nicht notwendig ein Einselement entalten, selbst wenn der Oberring ein Einselement besitzt.

Beispiel 8.31 *Ring $\mathbb{Z}_8$ mit Unterring $\{0, 2, 4, 6\}$.*



Weitere Unterringe: $\mathbb{Z}_8$ selbst und $\{0\}$ und $\{0, 4\}$.

8.2.2 Ideale

Für Ringe lässt sich eine zu den Nebenklassen für Gruppen analoge Konstruktion durchführen:

Definition 8.32 (Ideale) *Sei $\langle R, \oplus, \odot \rangle$ ein Ring. $I \subseteq R$ heißt Linksideal, genau dann wenn*

1. *$\langle I, \oplus \rangle$ ist Untergruppe von $\langle R, \oplus \rangle$*
2. *$\forall a \in I, r \in R.\ \ r \odot a \in I$*

Ersetzt man die zweite Bedingung durch

2'. $\forall a \in I, r \in R.\ \ a \odot r \in I$

erhält man analog den Begriff des Rechtsideals.

Die Bedingung aus Punkt 2) lässt sich auch kurz schreiben als $r \odot I \subseteq I$, wobei $r \odot I =_{df} \{r \odot a \mid a \in I\}$. Analoges gilt für Bedingung 2').

$I \subseteq R$ heißt Ideal *genau dann, wenn I Links- und Rechtsideal ist. Wir schreiben in Anlehnung an die Normalteilereigenschaft dann $I \lhd R$.*

Offensichtlich ist jedes Ideal ein Unterring.

Beispiel 8.33 (Ideale)

- *Die Unterringe $m\mathbb{Z}$ von $\mathbb{Z}$ mit $m \in \mathbb{N}\backslash\{0\}$ sind sämtlich Ideale.*
- *Die endlichen oder co-endlichen[a] Teilmengen von $\mathbb{N}$ sind ein Unterring von $\langle \mathfrak{P}(\mathbb{N}), \Delta, \cap \rangle$, denn die endlich/co-endlichen Teilmengen sind bezüglich Schnitten, Vereinigung und Komplementbildung abgeschlossen. Es liegt aber kein Ideal vor, denn der Schnitt der co-endlichen Menge $\mathbb{N}$ mit der Menge der geraden Zahlen $\mathbb{N}_{ger}$ ist $\mathbb{N}_{ger}$, welche weder endlich noch co-endlich ist.*
- *Polynome $p \in \mathbb{R}[x]$ mit $p(1) = 0$ sind ein Ideal der Menge der Polynome mit reelen Koeefizienten (siehe Beispiel 8.30).*

[a] Eine Teilmenge $A \subseteq \mathbb{N}$ heißt co-endlich genau dann, wenn $A^{\complement}$ endlich ist.

Wegen Definition 8.32(1) ist jedes Ideal insbesondere nicht leer, wegen der Kommutativität der additiven Gruppe sogar ein Normalteiler von $\langle R, \oplus \rangle$. Ist R kommutativ, so fallen die Begriffe Linksideal, Rechtsideal und Ideal zusammen. Ein Links- bzw. Rechtsideal, das das Einselement enthält, ist immer schon der ganze Ring. Sowohl das Nullelement als auch ganz R sind Ideale in jedem Ring R, die *trivialen Ideale*. Ein Ring, der nur triviale Ideale besitzt, heißt *einfach*.

Ideale besitzen ein Reihe von Abgeschlossenheitseigenschaften:

Satz 8.34 (Abgeschlossenheitseigenschaften von Idealen)
Sei $\langle R, \oplus, \odot \rangle$ ein Ring und $I, J \lhd R$ beliebige Ideale. Dann gilt:

1. $I \cap J \lhd R$
2. $I + J =_{df} \{a \oplus b \mid a \in I, b \in J\} \lhd R$
3. $IJ =_{df} \{a \odot b \mid a \in I, b \in J\} \lhd R$
4. $I : J =_{df} \{x \in R \mid x \odot J \subseteq I\} \lhd R$

Beweis Wir zeigen exemplarisch die Linksidealeigenschaft. Die Rechtsidealeigenschaft ist analog.

1. Seien $a, r \in R$ Dann gilt:
$$a \in I \cap J \;\Rightarrow\; a \in I \wedge a \in J \;\Rightarrow\; r \odot a \in I \wedge r \odot a \in J \;\Rightarrow\; r \odot a \in I \cap J.$$
2. Seien $a, b, r \in R$ Dann gilt:
$$\begin{aligned} a \oplus b \in I + J \;&\Rightarrow\; a \in I \wedge b \in J \;\Rightarrow\; r \odot a \in I \wedge r \odot b \in J \;\Rightarrow\; (r \odot a) \oplus (r \odot b) \in I + J \\ &\Rightarrow\; r \odot (a \oplus b) \in I + J. \end{aligned}$$
3. Seien $a, b, r \in R$ Dann gilt:
$$\begin{aligned} a \odot b \in IJ \;&\Rightarrow\; a \in I \wedge b \in J \;\Rightarrow\; r \odot a \in I \wedge b \in J \;\Rightarrow\; (r \odot a) \odot b \in IJ \\ &\Rightarrow\; r \odot (a \odot b) \in IJ. \end{aligned}$$

4. Sei $a \in R$. Dann gilt:

$$a \in I : J \;\Rightarrow\; a \odot J \subseteq I \;\Rightarrow\; r \odot (a \odot J) \subseteq \underbrace{r \odot I}_{\subseteq I} \;\Rightarrow\; (r \odot a) \odot J \subseteq I$$

□

Als Konsequenz von Satz 8.34 haben wir:

Satz 8.35 (Verband der Ideale) *Die Menge aller Ideale eines Ringes $\langle R, \oplus, \odot\rangle$ bildet einen algebraischen Verband, nämlich*

$$\langle \{I \mid I \lhd R\}, +, \cap\rangle$$

Beweis Die Abgeschlossenheit der Operationen + und ∩ wurde bereits in Satz 8.34 gezeigt. Offensichtlich sind beide Operationen auch assoziativ und kommutativ. Es bleiben die Absorptionseigenschaften $I + (I \cap J) = I$ und $I \cap (I + J) = I$ nachzuweisen. Betrachten wir zunächst die erste Eigenschaft. Hier gilt zunächtst die Inklusion $I \subseteq I + (I \cap J)$, weil $I \cap J$ das Nullelement enthält. Umgekehrt gilt $I + (I \cap J) \;=\; \{a \oplus b \mid a \in I \wedge b \in I \cap J\} \subseteq I$. Anderderseits gilt trivialerweise $I \cap (I + J) \subseteq I$. Umgekehrt impliziert, dass J das Nullelement enthält, $I + J \supseteq I$. Dann gilt auch $I \cap (I + J) \supseteq I$. □

Analog zum Konstruktion einer Faktorgruppe mittels eines Normateilers lassen sich Ringe gemäß ihrer Ideale faktorisieren.

Lemma 8.36 (Faktorring) *Sei $\langle R, \oplus, \odot\rangle$ ein Ring und I ein Ideal von R. Dann ist $\langle R/I, \oplus_I, \odot_I\rangle$ ein Ring, der sogenannte* Faktorring *von R bezüglich I.*

Dabei ist R/I und $\oplus_I$ definiert wie in Lemma 8.20 und $\odot_I$ durch:

$$(a \oplus I) \odot_I (b \oplus I) \quad =_{df} \quad (a \odot b) \oplus I$$

Beweis Weite Teile des Beweises sind bereits durch den Beweis zu Lemma 8.20 erledigt. Analog zum Beweis der Repräsentantenunabhängigkeit von $\oplus_I$ kann dieses auch für $\odot_I$ gezeigt werden. Die Assoziativität von $\odot_I$ und somit Halbgruppeneigenschaft von $\langle R/I, \odot_I\rangle$ ist hingegen trivial. □

8.2.3 Homomorphismen

Auch auf Strukturen mit 2 Operationen lässt sich der Homomorphiebegriff ausdehnen. Hier wird die Strukturverträglichkeit dann bezüglich beider Operationen gefordert. Exemplarisch für Ringe haben wir:

Definition 8.37 (Ringhomomorphismus)
Seien $\langle R, \oplus_R, \odot_R \rangle$ *und* $\langle S, \oplus_S, \odot_S \rangle$ *Ringe. Eine Funktion*

$$f : R \to S$$

heißt Ringhomomorphismus *genau dann, wenn für alle* $a, b \in R$ *gilt:*

1. $f(a \oplus_R b) = f(a) \oplus_S f(b)$ *und*
2. $f(a \odot_R b) = f(a) \odot_S f(b)$

Sind R *und* S *Ringe mit* 1*, also solche, für die* 1_R *und* 1_S *existieren, so gilt zusätzlich:*[a]

3) $f(1_R) = 1_S$.

[a] Diese Bedingung ist ohnehin erfüllt, wenn f surjektiv ist.

Beispiele für Ringhomomorphismen sind sind:

Beispiel 8.38

- *Die Abbildung ganzer Zahlen auf ihre Modulo-Restklassen:*

$$\begin{aligned} &\varphi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \text{ mit} \\ &z \;\mapsto\; (z \mod n)\mathbb{Z} \end{aligned}$$

- *Der Auswertungshomorphismus für Polynome mit reellen Koeeffizienten für festes* $r \in \mathbb{R}$*:*

$$\begin{aligned} &\alpha_r : \mathbb{R}[x] \to \langle \mathbb{R}, +, \cdot \rangle \text{ mit} \\ &\sum_{i=0}^{n} a_i x^i \;\mapsto\; \sum_{i=0}^{n} a_i r^i \end{aligned}$$

Als Verallgemeinerung des ersten Beispiels haben wir folgendes Resultat:

Satz 8.39 *Sei* $\langle R, \oplus, \odot \rangle$ *ein Ring und* I *ein Ideal von* R*. Dann bildet die Funktion*

$$\begin{aligned} &f : R \to R/I \quad \text{mit} \\ &a \;\mapsto\; a \oplus I \end{aligned}$$

einen Ringepimorphismus.

Beweis Für die $\oplus$-Strukturverträglichkeit haben wir:

$$f(a \oplus b) \;=\; (a \oplus b) \oplus I \;=\; (a \oplus I) \oplus_I (b \oplus I) \;=\; f(a) \oplus_I f(b).$$

Die $\odot$-Strukturverträglichkeit ist analog. Die Surjektivität ist offensichtlich. □

Die Ringe $\langle \mathbb{Z}_n, +, \cdot \rangle$ und die Faktorringen $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ sind sogar isomorph. Man kann leicht nachweisen, dass die Abbildung $z \mapsto z + \mathbb{Z}/n$ in der Tat ein Ringisomorphismus ist.

Analog zu Satz 8.27(1) haben wir außerdem:

Satz 8.40 *Sei $\langle R, \oplus, \odot \rangle$ ein Ring und $f : R \to R$ ein Ringhomomorphismus. Dann gilt:*

$$Kern(f) \ =_{df} \ \{a \in R \mid f(a) = 0\}$$

bildet ein Ideal.

Beweis Im Beweis zu Satz 8.27(1) wurde bereits gezeigt, dass $Kern(f)$ ein Normalteiler zu $\langle R, \oplus \rangle$ und damit insbesondere Untergruppe ist. Sei $a \in Kern(f)$ und $r \in R$. Dann gilt:

$$f(a \odot r) \ \overset{f \text{ Hom.}}{=} \ f(a) \odot f(r) \ \overset{a \in Kern(f)}{=} \ 0 \odot f(r) \ = \ 0.$$

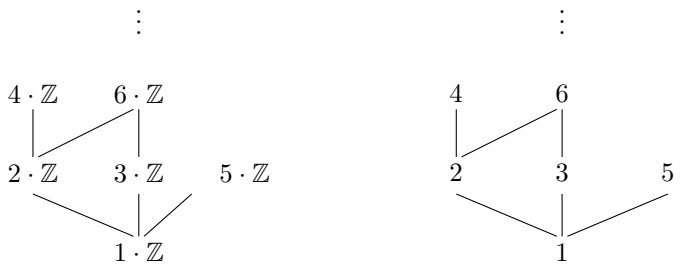
Analog folgt $f(r \odot a) \ = \ 0$. Also gilt $a \odot r \in Kern(f)$ und $r \odot a \in Kern(f)$. □

Schließlich sei noch auf einen interessanten Zusammenhang mit der Verbandsstruktur der Ideale (siehe Satz 8.35) hingewiesen, denn es gilt:

Lemma 8.41 *Die Abbildung aller Ideale $n\mathbb{Z} \subseteq \mathbb{Z}$ nach $\langle \mathbb{N}, | \rangle$ ist ein Ordnungshomomorphismus auf Verbänden*

$$\begin{aligned} f : \langle \{n\mathbb{Z} \mid n \in \mathbb{N} \backslash \{0\}\}, \supseteq \rangle &\to \langle \mathbb{N}, | \rangle \\ n\mathbb{Z} \ &\mapsto \ n \end{aligned}$$

Der Zusammenhang wird im der folgenden Abbildung graphisch veranschaulicht.



8.2.4 Integritätsbereiche und Körper

In Ringen sind noch nicht alle Eigenschaften ganzer Zahlen adäquat abgebildet. Insbesondere die besondere Rolle der 0 für die Multiplikation ist nicht berücksichtigt. Diesem wird durch die Definition der Integritätsbereiche Rechnung getragen. Zunächst einmal definiert man:

Definition 8.42 (Nullteiler) *Sei $\langle R, \oplus, \odot\rangle$ ein Ring. Ein Element $a \in R$ mit $a \neq 0$ heißt* Nullteiler *in R genau dann, wenn*

$$\exists b \in R.\ \ b \neq 0 \wedge (a \odot b = 0 \vee b \odot a = 0).$$

Existieren keine Nullteiler in R, so heißt er nullteilerfrei.

Beispiel 8.43 (Nullteiler)

- $\langle \mathbb{Z}, +, \cdot\rangle$ *ist nullteilerfrei*
- $\langle \mathbb{Z}_7, +_7, \cdot_7\rangle$ *ist nullteilerfrei.*
- $\langle \mathbb{Z}_6, +_6, \cdot_6\rangle$ *ist nicht nullteilerfrei. Nullteiler sind 2, 3 und 4, denn $2 \cdot_6 3 = 0$ und $3 \cdot_6 4 = 0$.*

Man definiert dann:

Definition 8.44 (Integritätsbereich) *Ist $\langle R, \oplus, \odot\rangle$ ein kommutativer Ring mit $1 \neq 0$, so heißt $\langle R, \oplus, \odot\rangle$* Integritätsbereich.

Man erkennt leicht, dass $\langle \mathbb{Z}_n, +_n, \cdot_n\rangle$ genau dann ein Integritätsbereich ist, wenn n eine Primzahl ist. Da $\mathbb{Z}_n$ isomorph zu $\mathbb{Z}/n\mathbb{Z}$ ist, bietet sich hier eine Verallgemeinerung an:

Definition 8.45 (Primideal) *Ist $\langle R, \oplus, \odot\rangle$ ein kommutativer Ring und $P \subset R$ ein Ideal von R, so heißt P* Primideal *genau dann, wenn*

$$\forall a, b \in P.\ \ a \odot b \in P \quad \Rightarrow \quad a \in P \vee b \in P$$

Dann gilt:

Satz 8.46 (Primideal) *Ist $\langle R, \oplus, \odot\rangle$ ein kommutativer Ring und $P \subset R$ ein Ideal von R. Dann gilt:*

$$R/P \text{ nullteilerfrei} \ \Leftrightarrow\ P \text{ Primideal.}$$

Beweis Wegen Satz 8.39 ist $f : R \to R/P$ Ringepimorphismus. Wie man sich leicht überlegt, gilt dabei insbesondere $Kern(f) = P$. Damit genügt es dann allgemein zu zeigen, dass für jeden Ringepimorphismus $\varphi : \langle R, \oplus_R, \odot_R\rangle \to \langle S, \oplus_S, \odot_S\rangle$ gilt:

$$S \text{ nullteilerfrei} \ \Leftrightarrow\ Kern(\varphi) \text{ Primideal}$$

Für die $\Rightarrow$-Richtung betrachten wir $r_1, r_2 \in R$ mit $r_1 \odot_R r_2 \in Kern(\varphi)$. Dann gilt:

$$\begin{aligned} \varphi(r_1 \odot_R r_2) = 0 \ &\Rightarrow\ \varphi(r_1) \odot_S \varphi(r_2) = 0 \ \overset{\text{Vor.}}{\Rightarrow}\ \varphi(r_1) = 0 \ \vee\ \varphi(r_2) = 0 \\ &\Rightarrow\ \varphi(r_1) \in Kern(\varphi) \ \vee\ \varphi(r_2) \in Kern(\varphi) \end{aligned}$$

Für die $\Leftarrow$-Richtung nehmen wir an, dass $Kern(\varphi)$ Primideal ist. Seien nun $s_1, s_2 \in S$ mit $s_1 \odot_S s_2 = 0$. Wegen der Surjektivität von φ existieren $r_1, r_2 \in R$ mit $\varphi(r_1) = s_1$ und $\varphi(r_2) = s_2$. Dann gilt:

$$\begin{aligned} s_1 \odot_S s_2 = 0 &\Rightarrow \varphi(r_1) \odot_S \varphi(r_2) = 0 \Rightarrow \varphi(r_1 \odot_R r_2) = 0 \Rightarrow r_1 \odot_R r_2 \in Kern(\varphi) \\ &\overset{\text{Vor.}}{\Rightarrow} r_1 \in Kern(\varphi) \vee r_2 \in Kern(\varphi) \Rightarrow \varphi(r_1) = 0 \vee \varphi(r_2) = 0 \\ &\Rightarrow s_1 = 0 \vee s_2 = 0 \end{aligned}$$

□

Unmittelbare Folge von Satz 8.47 ist:

Korollar 8.47 (Primideal) *Ist $\langle R, \oplus, \odot \rangle$ ein kommutativer Ring mit 1 und P Primideal von R, so ist R/P Integritätsbereich.*

Beweis Die Nullteilerfreiheit von R/P gilt nach Satz 8.47. Es bleibt nur zu zeigen, dass $0 \neq 1$ gilt. Wäre $0 = 1$, so würde $1 \in Kern(f)$ gelten, wobei $f : R \to R/P$ der in Satz 8.39 beschriebene Ringepimorphismus ist. Wegen $Kern(f) = P$ folgt insbesondere $1 \in P$. Wie bereits festgestellt, ist ein Ideal, das die 1 enthält immer schon der ganze Ring. Dieses steht aber im Widerspruch zu $P \subset R$. □

In Strukturen wie den rationalen oder reellen Zahlen existieren auch multiplikativ inverse Elemente. Dem wird durch einer weiteren Verfeinerung des Begriffes desb Integritätsbereiches Rechnung getragen.

Definition 8.48 (Körper) *Ein Integritätsbereich $\langle R, \oplus, \odot \rangle$ heißt* Körper *genau dann, wenn $\langle R \backslash \{0\}, \odot \rangle$ eine kommutative Gruppe ist.*

Liegt mit $\langle R \backslash \{0\}, \odot \rangle$ nur eine (nicht notwendendig kommutative) Gruppe vor, spricht man von einem *Schiefkörper*. Gemäß Definition ist jeder Körper auch ein Integritätsbereich. Der Umkehrschluss gilt jedoch nicht wie man am Beispiel von $\langle \mathbb{Z}, +, \cdot \rangle$ erkennen kann (3 besitzt z.B. kein multiplikativ Inverses).

Beispiel 8.49 (Körper)

- $\langle \mathbb{Z}, +, \cdot \rangle$ *ist kein Körper, denn die multiplikativ Inversen fehlen.*
- $\langle \mathbb{Z}_p, +_p, \cdot_p \rangle$ *(p Primzahl) ist Körper.*[a]
- $\langle \mathbb{Q}, +, \cdot \rangle$ *ist ein Körper.*
- $\langle \mathbb{R}, +, \cdot \rangle$ *ist ein Körper.*

[a] Die Existenz der Inversen folgt aus dem erweiterten Eukldischen Algorithmus.