

Kapitel 1

Aussagen und Mengen

Für die Formulierung von Aussagen von mathematischem Gehalt benötigen wir Verabredungen, Sprechweisen, Symbole und eine griffige Notation. Dabei wollen wir aber nicht in die Tiefen der mathematischen Grundlagen (Mengenlehre, Logik) eintauchen, sondern geben uns mit einem „naiven“ Standpunkt zufrieden. Er führt zu keinerlei Konflikten, solange wir uns mit konkret definierten Objekten beschäftigen.

1.1 Aussagen und ihre Verknüpfungen

Argumentationen in der Mathematik beruhen darauf, dass ein Zusammenhang zwischen Aussagen hergestellt wird, dass Aussagen verknüpft werden. Was eine Aussage sein soll, halten wir in einer Definition fest, die umgangssprachlich formuliert ist.

Definition 1.1.1 *Eine Aussage ist eine sprachliche Feststellung, die entweder wahr oder falsch ist. Falsch bzw. wahr charakterisiert man dabei durch einen Wahrheitswert: (w) steht für wahr, (f) steht für falsch.* \square

In der obigen „Definition“ spiegelt sich das aristotelische¹ Prinzip des *tertium non datur* wieder: eine Aussage ist entweder wahr oder falsch, eine dritte Möglichkeit gibt es nicht. Beispiele:

1. 2 ist eine gerade Zahl
2. 1004 ist durch 3 teilbar
3. Brasilien ist ein Entwicklungsland
4. Die Straße X ist nass
5. Das Dreieck ABC ist gleichschenkelig
6. $2^{999999991} - 1$ ist eine Primzahl

Die erste Aussage ist wahr, die zweite Aussage ist falsch, wenn wir eine Definition von Teilbarkeit unterstellen; der Wahrheitsgehalt der dritten Aussage hängt von einer Definition eines Entwicklungslandes ab; die vierte Aussage kann auf ihren Wahrheitsgehalt mit „physikalischen“ Mitteln geprüft werden; ob die fünfte Aussage wahr ist, ist offen, solange keine exakte Definition und Beschreibung des konkreten Dreiecks vorliegt; der Wahrheitsgehalt der letzten Aussage ist offen: $2^{999999991} - 1$ ist eine Primzahl oder sie ist keine, die „Instanz“, die dies (schnell) entscheiden kann, ist wohl noch zu finden.

Als erstes Aussagenkonstrukt betrachten wir die **Verneinung/Negation** einer Aussage. Konkret: Ist P eine Aussage, so bezeichnen wir mit $\neg P$ die Negation der Aussage P ; es ist

¹Aristoteles von Stagira (384-322 v. Chr.)

also P wahr genau dann, wenn $\neg P$ falsch ist. Man bezeichnet die Negation als **einstellige** „Verknüpfung“, benötigen wir doch dabei nur eine Aussage. Logische Verknüpfungen, bei denen zwei Aussagen beteiligt sind, nennen wir **zweistellige** oder **binäre Aussageverknüpfungen**. Die Aussageverknüpfungen werden – in streng mathematischen Sinne – in der boolschen² Algebra zusammengefasst. In der folgenden Tabelle fügen wir logische Operatoren, wie sie in MAPLE nutzbar sind, ein.

Durch logische Verknüpfung zweier Aussagen P, Q entsteht eine dritte Aussage R , eine sogenannte **verbundene Aussage**. Um den Wahrheitsgehalt dieser verbundenen Aussage geht es dann. Bestimmt wird die Aussage R dadurch, welcher Wahrheitswert ihr für die verschiedenen Belegungen mit (w) und (f) der Aussagen P und Q zukommt. Die folgende **Wahrheitstafel** zeigt, wie die oben angeführten Aussageverknüpfungen definiert sind:

Operation	Sprechweise	Symbol	MAPLE
Negation	nicht ...	\neg	<code>&not</code>
Konjunktion	... und ...	\wedge	<code>&and</code>
Alternative	... oder ...	\vee	<code>&or</code>
Implikation	wenn ..., dann ...	\implies	<code>&implies</code>
Äquivalenz	... genau dann, wenn ...	\iff	<code>&iff</code>

P	Q	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$P \iff Q$
(w)	(w)	(w)	(w)	(w)	(w)
(w)	(f)	(f)	(w)	(f)	(f)
(f)	(w)	(f)	(w)	(w)	(f)
(f)	(f)	(f)	(f)	(w)	(w)

P	$\neg P$
(w)	(f)
(f)	(w)

Man beachte insbesondere die Wahrheitstafel zu $P \implies Q$: Ist P falsch, so ist die Implikation $P \implies Q$ wahr, unabhängig vom Wahrheitsgehalt von Q . Die Wahrheitstafel der Negation ist angefügt.

MAPLE - Illustration 1.1

MAPLE kennt den Datentyp *boolsche Variable* und hat die einfachen logischen Operationen `&and`, `&or`, `¬` ständig verfügbar. Eine Aussage ist eine *Tautologie*, wenn sie unabhängig vom Wahrheitswert der zu Grunde liegenden „Literale“ immer wahr wird.

```

> with(logic):
> x:=3: evalb(5*x^3-200>0);
false
> tautology((&and(a,b) &or (&not a) &or
(&not b)));
true
    
```

Mit den nun eingeführten Verknüpfungen stehen uns schon eine große Anzahl von Aussagenkonstrukten zur Verfügung. Halten wir einige logische Gesetze fest:

²George Boole, 1815-1864, Mathematiker

Regel 1.1.2 Seien P, Q Aussagen.

$$(P \implies Q) \iff (\neg Q \implies \neg P) \quad (1.1)$$

$$\neg(P \wedge Q) \iff \neg P \vee \neg Q \quad (1.2)$$

$$\neg(P \vee Q) \iff \neg P \wedge \neg Q \quad (1.3)$$

$$(P \implies Q) \iff (\neg P \vee Q) \quad (1.4)$$

Von der Richtigkeit dieser Aussagen überzeugen wir uns, indem wir die Wahrheitstafeln erstellen. Etwa zu (1.1):

P	Q	$P \implies Q$	$\neg Q$	$\neg P$	$\neg Q \implies \neg P$	$(P \implies Q) \iff (\neg Q \implies \neg P)$
(w)	(w)	(w)	(f)	(f)	(w)	(w)
(w)	(f)	(f)	(w)	(f)	(f)	(w)
(f)	(w)	(w)	(f)	(w)	(w)	(w)
(f)	(f)	(w)	(w)	(w)	(w)	(w)

Die Wahrheitstafel zu $P \implies Q$ ist identisch mit der Wahrheitstafel zu $\neg P \vee Q$, wie man leicht verifiziert. Die Aussage $\neg P \vee Q$ vermeidet also das der Umgangssprache nahestehende "folgt" in $P \implies Q$.

Regel 1.1.3 Seien P, Q, R Aussagen.

$$P \wedge Q \iff Q \wedge P \quad (1.5)$$

$$P \vee Q \iff Q \vee P \quad (1.6)$$

$$(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R) \quad (1.7)$$

$$(P \vee Q) \vee R \iff P \vee (Q \vee R) \quad (1.8)$$

$$P \wedge (P \vee Q) \iff P \quad (1.9)$$

$$P \vee (P \wedge Q) \iff P \quad (1.10)$$

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R) \quad (1.11)$$

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R) \quad (1.12)$$

Die Gültigkeit von (1.5), ..., (1.12) belegt man wieder mit Hilfe von Wahrheitstafeln. Etwa zu (1.11) in nicht vollständiger Aufzählung:

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
(w)	(w)	(f)	(w)	(w)	(w)	(f)	(w)
(w)	(f)	(w)	(w)	(w)	(f)	(w)	(w)
(f)	(w)	(w)	(w)	(f)	(f)	(f)	(f)
(f)	(f)	(f)	(f)	(f)	(f)	(f)	(f)

Sprechweisen:

- (1.5), (1.6) **Kommutativgesetze**
- (1.7), (1.8) **Assoziativgesetze**
- (1.9), (1.10) **Verschmelzungsgesetze**
- (1.11), (1.12) **Distributivgesetze**

In Definitionen weisen wir mathematischen Objekten manchmal Eigenschaften mit einem definierenden Äquivalenzzeichen “ : \iff ,“ zu, etwa:

Objekt O hat Eigenschaft E : \iff Eine Aussage A über das Objekt O , die äquivalent mit dem Eintreten der Eigenschaft E ist, ist wahr (gilt).

Ein **Satz**, **Lemma**, eine **Folgerung**, ... ist die Ausformulierung einer mathematischer Aussage, die wahr ist. Meist stellt sich diese Ausformulierung so dar, dass aus einer **Voraussetzung** V eine **Behauptung** B gefolgert werden soll; V , B sind selbst mathematische Aussagen.

Ein **Beweis eines Satzes** mit **Voraussetzung** V und **Behauptung** B ist also eine Kette von Implikationen, ausgehend von der Aussage V bis zur Aussage B :

$$V \implies \dots \implies B$$

Die Regel (1.1) sagt uns, dass wir den Beweis auch führen können, indem wir die Gültigkeit von $V \implies B$ dadurch zeigen, dass wir $\neg B \implies \neg V$ nachweisen; Beweis durch **Kontraposition**). Der **Widerspruchsbeweis** basiert auf der Regel (1.4) zusammen mit (1.3). Er stellt sich so dar:

$$V \wedge \neg B \implies \dots \implies Q$$

Hierbei ist mit Q dann eine Aussage erreicht, die nicht wahr ist.

Dem Nachweis von Euklid³, dass $\sqrt{2}$ nicht rational ist, liegt die Beweistechnik des Widerspruchsbeweises zugrunde:

V : a ist eine Zahl mit $a^2 = 2$ B : a ist eine Zahl, die nicht rational ist

Aus der Annahme $V \wedge \neg B$, also der Annahme, dass $\sqrt{2}$ eine rationale Zahl ist, leiten wir durch logisches Schließen (gültige Aussageverknüpfungen) eine Aussage ab, die nicht wahr ist. Also kann die Annahme $V \wedge \neg B$ nicht wahr sein; $V \implies B$ ist also wahr. Wir kommen auf diesen Beweis zurück, wenn wir etwas mehr über rationale und irrationale Zahlen Bescheid wissen.

1.2 Mengen

Den Begriff der Menge wollen und können wir hier ebenso wie die obige „Aussagenlogik“ nicht im strengen Sinne der mathematischen Grundlagen einführen. Er dient uns nur als Hilfsmittel für eine möglichst kurze Notation von konkreten Mengen. Von G. Cantor,⁴ dem Begründer der Mengenlehre, haben wir folgende Definition:

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

Diese Begriffsbildung hat die Mathematik tief beeinflusst.

Eine Menge besteht also aus Elementen, kennt man alle Elemente der Menge, so kennt man die Menge. Beispiele, die wir noch genauer studieren werden, sind:

\mathbb{N} := Menge der natürlichen Zahlen \mathbb{Z} := Menge der ganzen Zahlen
 \mathbb{Q} := Menge der rationalen Zahlen \mathbb{R} := Menge der reellen Zahlen .

³Euklid, 365(?) – 300(?), „Mathematiker“

⁴Georg Cantor, 1845-1918, Mathematiker

Mit den natürlichen Zahlen $1, 2, 3, \dots$ sind wir schon (aus der Schule) wohlvertraut. Später gehen wir etwas struktureller darauf ein.

Man kann eine Menge dadurch bezeichnen, dass man ihre Elemente zwischen zwei geschweifte Klammern (Mengenklammern) schreibt. Die Zuordnung eines Elements zu einer Menge erfolgt mit dem Zeichen " \in ". Gehört ein Objekt x nicht zu einer Menge M , so schreiben wir $x \notin M$. Es hat sich als zweckmäßig erwiesen, den Mengenbegriff so aufzufassen, dass eine Menge aus gar keinem Element bestehen kann. Dies ist dann die **leere Menge**, das Zeichen dafür ist \emptyset . Beispielsweise ist die Menge der rationalen Zahlen, deren Quadrat gleich 2 ist, leer. Dies wissen wir aus der Anmerkung über die Irrationalität von $\sqrt{2}$.

Das Hinschreiben der Elemente einer Menge kann auf zweierlei Weisen geschehen. Hat die Menge nur ganz wenige Elemente, so kann man sie einfach alle hinschreiben, durch Kommata getrennt, auf die Reihenfolge kommt es dabei nicht an und eine Mehrfachnennung ist nicht von Bedeutung, etwa:

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

Abgekürzt verfährt man oft auch so: Elemente, die man nicht nennt aber gut kennt, werden durch Punkte angedeutet, etwa:

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

Man nennt diese Art, Mengen hinzuschreiben, zu definieren, die **Umfangsdefinition**. Die zweite Möglichkeit besteht darin, Objekte einer Menge als Elemente dadurch zuzuordnen, dass man ihnen eine charakterisierende Eigenschaft zuweist. Ist E eine Eigenschaft, die jedes Objekt x einer Menge M hat oder nicht hat, so bezeichne

$$\{x \in M \mid x \text{ hat die Eigenschaft } E\}$$

die Menge aller Elemente von M , die die Eigenschaft E haben; etwa

$$\begin{aligned} \text{KO} &:= \{x \in \text{Obst} \mid x \text{ Kernobst}\} \\ \text{UNO} &:= \{x \in \text{Länder} \mid x \text{ Mitglied der UNO}\} \end{aligned}$$

Man nennt diese Art, Mengen hinzuschreiben, zu definieren, die **Inhaltsdefinition**.

Wichtig beim Hinschreiben von Mengen ist, dass stets nachgeprüft werden kann, ob ein spezielles Objekt einer in Frage stehenden Menge angehört oder nicht; in der Definition von Cantor ist dies festgehalten. Dies korrespondiert mit dem ausgeschlossenen Dritten bei Aussagen.

Bei J.A. Poulos⁵ lesen wir:

... Ähnlich ist es mit der Notation der Mengenlehre. Sie ist so einfach, dass sie schon an der Grundschule gelehrt werden kann. Was manchmal seitenlang in einem Vorwort zu einem Lehrbuch steht, passt schon in ganz wenige Sätze: Mit $p \in F$ wird ausgedrückt, dass p ein Element der Menge F ist, und mit $F \subset G$, dass jedes Element von F ebenso ein Element von G ist. Haben wir zwei Mengen A und B , dann ist $A \cap B$ die Menge, die jene Elemente enthält, die sowohl zu A als auch zur Menge B gehören; mit $A \cup B$ ist die Menge gemeint, die jene Elemente enthält, die zur Menge A, B oder zu beiden gehören; und A' ist die Menge jener Elemente, die nicht zu A gehören. Eine Menge, die keine Elemente enthält, ist eine leere Menge und wird mit \emptyset , manchmal auch mit $\{\}$ angegeben, geschweifte Klammern ohne Inhalt. Ende des Mini-Kurses.

⁵Poulos, J.A.: Von Algebra bis Zufall, Campus, Frankfurt, 1992

Was uns von den Begriffen aus dem obigen Minikurs noch nicht begegnet ist, bringen wir noch in eine „anständige“ Form:

Definition 1.2.1 Seien A, B Mengen und sei z irgendein Objekt.

$$(a) A \subset B : \iff (x \in A \implies x \in B)$$

Damit ist die **Teilmengeneigenschaft/Inklusion** \subset definiert.

$$(b) A = B : \iff (A \subset B \text{ und } B \subset A)$$

$$(c) z \in A \cap B : \iff (z \in A \text{ und } z \in B).$$

Damit ist der **Durchschnitt** $A \cap B$ definiert: $A \cap B := \{x | x \in A \text{ und } x \in B\}$

$$(d) z \in A \cup B : \iff (z \in A \text{ oder } z \in B).$$

Damit ist die **Vereinigung** $A \cup B$ definiert: $A \cup B := \{x | x \in A \text{ oder } x \in B\}$

□

Das Symbol “ $:=$ “ haben wir als definierendes Gleichsetzen von Mengen eingeführt. Es korrespondiert mit dem Symbol “ \iff “.

Definition 1.2.2 Sei A eine Menge. Die **Potenzmenge** von A ist die Menge der Teilmengen von A einschließlich der leeren Menge:

$$POT(A) := \{B | B \subset A\}.$$

□

Beispiel 1.2.3 Sei $A := \{p, q, r\}$. Wie sieht die Potenzmenge $POT(A)$ aus? Wir haben

$$POT(A) = \{\emptyset, \{p\}, \{q\}, \{r\}, \{p, q\}, \{q, r\}, \{p, r\}, \{p, q, r\}\}$$

Wir stellen fest, dass die Menge A drei und die Menge $POT(A)$ $8 = 2^3$ Elemente enthält. Dies hat dazugeführt, dass man $POT(A)$ auch als 2^A schreibt, und die Bezeichnung „Potenzmenge“ leitet sich daraus ab. □

MAPLE - Illustration 1.2

MAPLE kennt den Datentyp <i>Menge</i> . Eine Menge ist eine in geschweifte Klammern eingeschlossene Folge von Ausdrücken, Objekten; Mehrfachnennungen werden unterdrückt. Die gängigen Operationen mit endlichen Mengen sind durchführbar. Aufzählende Definition, Element von, Durchschnitt und Vereinigung von Mengen sind handhabbar.	<pre> > M:= {2,3,rot,Hahn,rot}; A:={Hut,Hahn,†}; M:= {2,3,rot,Hahn} A:={Hut,Hahn,†} > member(rot,M); true > M intersect A; {Hahn} </pre>
--	--

Mitunter wollen wir eine Bezeichnung für diejenigen Elemente haben, die eine gewisse Eigenschaft nicht haben. Dies ist Inhalt von

Definition 1.2.4 Seien A, B Teilmengen von U .

(a) $A \setminus B := \{x \in A \mid x \notin B\}$ heißt das **relative Komplement** von B in A .

(b) $\complement A := U \setminus A$ heißt das **Komplement** von A (in U).

(In der Definition (b) steht U für die (universelle) Grundmenge, auf die wir uns bei der Komplementbildung beziehen.) \square

Ein bequemes Hilfsmittel beim Nachdenken über Mengen sind die **Venn-Diagramme**, bei denen in der Zeichenblattebene Gebiete zur Darstellung von Mengen benutzt werden: Durch Kurven umschlossene Gebiete stellen Mengen A, B, \dots dar. Solche Darstellungen sind gut geeignet, formale Argumente für einen zu beweisenden Sachverhalt zu finden.

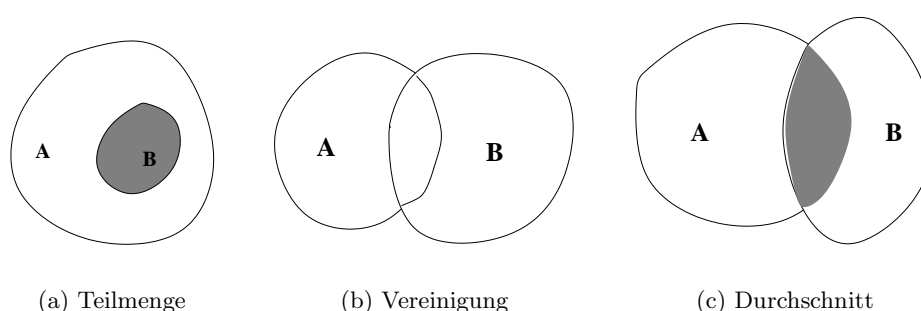


Abbildung 1.1: Venn-Diagramme

Die Nützlichkeit der leeren Menge \emptyset wird deutlich bei der Definition des Durchschnitts. Hier ist ja der Fall, dass $A \cap B$ kein Element enthält, sicherlich nicht auszuschließen, wie uns ein geeignetes Venn-Diagramm sofort lehrt. Zwei Mengen, deren Durchschnitt leer ist, heißen **disjunkt**.

Regel 1.2.5 Seien A, B, C Mengen.

$$A \subset B, B \subset C \implies A \subset C \quad (1.13)$$

$$A \cup (B \cup C) = (A \cup B) \cup C \quad (1.14)$$

$$A \cap (B \cap C) = (A \cap B) \cap C \quad (1.15)$$

$$A \cup B = B \cup A \quad (1.16)$$

$$A \cap B = B \cap A \quad (1.17)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad (1.18)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad (1.19)$$

Beweis von (1.18):

Wir haben zu zeigen: $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$, $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.

Sei $x \in A \cap (B \cup C)$. Dann gilt: $x \in A, x \in B \cup C$. Daraus folgt: $x \in A \cap B$ oder $x \in A \cap C$, je nachdem, ob $x \in B$ und/oder $x \in C$. Daraus schließen wir: $x \in (A \cap B) \cup (A \cap C)$. Für den Beweis der anderen Inklusion lese man die eben vorgeführten Beweisschritte rückwärts. \blacksquare

Sprechweisen:

- (1.13) **Transitivität**
 (1.14), (1.15) **Assoziativgesetze**
 (1.16), (1.17) **Kommutativgesetze**
 (1.18), (1.19) **Distributivgesetze.**

Definition 1.2.6 Seien A, B Mengen.

- (a) Sind $a \in A, b \in B$, so heißt (a, b) das damit gebildete **geordnete Paar** (bezogen auf die Reihenfolge „zuerst A , dann B “).
- (b) Zwei Paare $(a, b), (a', b')$ mit $a, a' \in A, b, b' \in B$, heißen **gleich genau** dann, wenn $a = a', b = b'$ gilt.
- (c) Die Menge $A \times B := \{(a, b) | a \in A, b \in B\}$ heißt das **kartesische Produkt** der Faktoren A, B .

□

Mit geordneten Paaren notieren wir etwa die kartesischen Koordinaten (Vielfache der Einheitsstrecke) eines Punktes in der Ebene: wir kommen darauf zurück.⁶

Regel 1.2.7 Seien A, B, C Mengen:

$$A \times (B \cup C) = (A \times B) \cup (A \times C). \quad (1.20)$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C). \quad (1.21)$$

Diese Regeln bestätigt man ganz leicht. Nehmen wir uns die Regel (1.20) vor und beweisen eine der Inklusionen, die es zu beweisen gilt: $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$.

Sei $x \in A \times (B \cup C)$. Dann gibt es $a \in A, d \in B \cup C$ mit $x = (a, d)$. Nach Definition von $B \cup C$ bedeutet dies

$$x = (a, d) \text{ mit } a \in A, d \in B, \text{ oder } x = (a, d) \text{ mit } a \in A, d \in C.$$

Also $x \in A \times B$ oder $x \in A \times C$.

Es ist klar, dass wir das kartesische Produkt auf mehr als zwei „Faktoren“ ausdehnen können. Etwa korrespondiert ein (gültiger) Lottoschein mit den Elementen der Menge

$$\{x = (x_1, x_2, x_3, x_4, x_5, x_6) \in Z \times \cdots \times Z | x_1, \dots, x_6 \text{ sind paarweise verschieden}\};$$

dabei ist $Z = \{1, 2, 3, \dots, 49\}$. Ein Element (x_1, \dots, x_6) der Menge nennt man ein **6-Tupel**.

Das **mehrfache kartesische Produkt** einer Menge A erhält eine Kurzschreibweise, nämlich

$$A^n := \underbrace{A \times \cdots \times A}_{n\text{-mal}} := \{x = (x_1, \dots, x_n) | \text{alle } x_i \in A\}.$$

Ein Element $x = (x_1, \dots, x_n)$ der Menge A^n nennt man ein **n-Tupel**.

Eine Menge kann endlich viele Elemente haben oder unendlich viele. Hier begnügen wir uns mit einer Definition der „Endlichkeit“, die aus unserer Erfahrung heraus sehr wohl geeignet ist; später, wenn wir uns mit Abbildungen beschäftigt haben, bessern wir nach:

Eine Menge heißt **endlich**, wenn jedem Element der Menge der Reihe nach die Zahlen $1, 2, \dots, N$ zugeordnet werden kann, wobei mit N dann allen Elementen eine Zahl zugeordnet ist. Eine Menge heißt **unendlich**, wenn sie nicht endlich ist.

Eine endliche Menge $\{x_1, \dots, x_n\}$ hat somit n Elemente, wenn alle x_i paarweise verschieden sind.

⁶Da René Descartes, 1596-1650, sehr erfolgreich die Koordinatisierung algebraischer Probleme betrieben hat, ist die Bezeichnung „kartesisch“ wohl angebracht.

1.3 Alphabete

Alphabete sind ein zentraler Begriff der theoretischen Informatik im Zusammenhang mit Grammatiken und Verschlüsselungsverfahren.

Definition 1.3.1 Sei A eine nichtleere Menge. A^* bezeichne die Menge der endlichen Tupel von Elementen von A , also $x \in A^*$ genau dann, wenn $x = ()$ oder $x \in A^n$ für ein $n \in \mathbb{N}$.

Die Elemente von A^* werden **A-Wörter** – in der Informatik **A-Strings** – genannt, das Symbol $()$ bezeichnet das so genannte **leere Wort** (leeres Tupel). (Wörter sind Bausteine von Sprachen.) Die Menge A wird in diesem Zusammenhang ein **Alphabet** genannt; die Elemente von A sind der **Zeichenvorrat** für die Wörter.

Einem Element $w \in A^*$ mit $w \in A^n$ wird die **Länge** n zugesprochen; wir nennen es ein n -Wort; das leere Wort $()$ hat die Länge 0.

Im Spezialfall $A = \{0, 1\}$ spricht man bei A^* von **binären Worten**. □

In der Definition haben wir Wörter als Tupel definiert. Im Kontext von Alphabeten und deren Wörtern läßt man in der Tupel-Schreibweise begrenzende runde Klammern und trennende Kommata weg: $x = x_1x_2 \dots x_n$ ist ein Wort der Länge n . Damit ist die Bezeichnung „String“ in der Informatik auch erklärt.

Beispiel 1.3.2

BAUM	:	Deutsches Alphabet $\{A, B, C, \dots, X, Y, Z, \ddot{A}, \ddot{U}, \ddot{O}\}$
1234	:	Dezimalziffern-Alphabet $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
01001	:	Binäres Alphabet $\{0, 1\}$
– – • –	:	Morsealphabet $\{-, \bullet, \sqcup\}$ (– – • – steht für “q”)

□

Bemerkung 1.3.3 Sei $X = \{x_1, \dots, x_n\}$ eine Menge mit n Elementen. Jeder Teilmenge A von X , d.h. jedem Element der Potenzmenge von X , entspricht eindeutig ein n -Wort aus dem Alphabet $\{0, 1\}$:

$$A \longleftrightarrow b_1b_2 \dots b_n, \text{ wobei } b_i = \begin{cases} 1 & , \text{ falls } x_i \in A \\ 0 & , \text{ falls } x_i \notin A \end{cases}$$

Also ist die Anzahl der Elemente von $POT(X)$ gleich der Anzahl der möglichen binären n -Worte. Diese können wir so abzählen:

Es gibt w_n n -Wörter und w_{n+1} $(n+1)$ -Wörter. Wir „sortieren“ die $(n+1)$ -Wörter nach dem 1. Buchstaben: genau w_n Wörter beginnen mit 0, genau w_n Wörter beginnen mit 1. Daher gilt: $w_{n+1} = 2 \cdot w_n$, $w_1 = 2$. Daraus folgt die Formel $w_n = 2^n$, $n \in \mathbb{N}$.

(Wir haben hier eine Art „Induktionsbeweis“ aufgeschrieben; dazu später.) □

Bemerkung 1.3.4 Es gilt heute als gesicherte Tatsache, dass die Erbanlagen von Pflanzen und Tieren durch die DNS (Desoxyribonukleinsäure) in den Chromosomen übertragen werden. Man konnte zeigen, dass die DNS aus einer langen Kette besteht, die aus 4 Bausteinen, die durch die Buchstaben A, T, G, C dargestellt werden, aufgebaut ist. Hier ist ein Ausschnitt:

ATGGCAAAGTTACA...

Vererbung besteht daher aus langen Nachrichten, die in Worten (Strängen) aus einem Vierbuchstabenalphabet geschrieben werden können; das Ergebnis einer Genom-Analyse ist also so hinschreibbar. □

Die Übertragung von Nachrichten geschieht mittels durch Hardware realisierter mechanischer oder elektronischer Impulse. Telefon, Morseapparat, Telegraph, Funkgerät sind Instrumente der Nachrichtenübermittlung. Die Strecke (physikalische Verbindung), auf der die Übermittlung vor sich geht, bezeichnet man als **Kanal**. Zur Übertragung werden die Nachrichten in besonderer Weise vorbereitet. Eine erste Vorbereitung ist die sogenannte **Quellencodierung**, bei der eine Nachricht (einer natürlichen Sprache), die ein Sender an einen Empfänger übermitteln will, in einem vorgegebenen System, **Code** genannt, dargestellt wird. Quellencodierung bedeutet in der Regel, einer Nachricht x einer Gesamtheit X von Nachrichten ein Wort w , geschrieben in einem Alphabet A zuzuordnen.

Ein eventuell so codiertes Wort des Senders geht nun über den Kanal an den Empfänger. Hier ergeben sich zwei wesentliche Probleme. Zum einen kann der Kanal Störungen ausgesetzt sein (atmosphärische Störungen bei Satelliten, ...), zum anderen können beabsichtigte Eingriffe (Lauschen, Stören, gezieltes Abändern, ...) von Unbefugten vorgenommen werden. Der erste Aspekt erfordert eine Technik, die Fehler erkennt und korrigiert, der zweite Aspekt eine Technik, die die Nachrichten für Unbefugte unlesbar macht. Die Methode für Abhilfe ist bei beiden Aspekten die gleiche: die Nachricht im Quellencode wird vor der Sendung über den Kanal einer Sicherheitsmaßnahme unterzogen; sie wird nochmals codiert. Diesen zweiten Schritt fasst man unter dem Stichwort **Kanalcodierung** zusammen. Auf der Empfängerseite hat man dann entsprechend zwei Decodierungsmaßnahmen zu treffen, die **Kanaldecodierung** und die **Quellendecodierung**.

ASCII-Zeichen	Codewort
␣ (Zwischenraum)	00100000
0	00110000
1	00110001
2	00110010
!	00100001
A	01000001
B	01000010
C	01000011

Abbildung 1.2: Ascii-Code

Beispiel 1.3.5 *Beispiele für in der Praxis verwendete Codes sind:*

- **ASCII-Code** (*American Standard Code for Information Interchange*)

Damit wird ein Alphabet, das aus Buchstaben, Ziffern und Sonderzeichen besteht, über dem Alphabet $\{0,1\}$ mit Wortlänge 8 codiert. Ein Ausschnitt ist in Abbildung 1.2 zu sehen.

- **Lochstreifencode**

Damit wird ein Alphabet aus Buchstaben und Sonderzeichen über dem Alphabet $\{0,1\}$ mit Wortlänge 5 dargestellt, physikalisch realisiert als Fünferkombination von gestanzten Löchern und ungestanzten Leerstellen im Lochstreifen.

- **Zeichensatzcode** etwa bei LATE_X .

Damit wird ein Alphabet aus Buchstaben, Ziffern und Sonderzeichen über dem Alphabet der Ziffern $\{0,1,\dots,7\}$ (oktal) mit Wortlänge 3 dargestellt. Ein Beispiel: 046 steht für & im Zeichensatz $\text{cmr}10$. Dabei ist $\text{cmr}10$ selbst wieder ein Codewort, dessen Bauart sich so erklärt: "cm" steht für "Computer Modern", "r" steht für die Schriftart "Roman", "10" steht für die Entwurfsgröße.

- **ISBN (International Standard Book Number)**

Beispiel: 3 – 127 – 01901 – 7

(Die Zahl 3 steht für den deutschsprachigen Raum, 127 steht für den Verlag, 01901 steht für die Nummer des Buches in der internen Zählung des Verlages, 7 ist eine Prüfziffer, die so zustande kommt:

$$1 \cdot 3 + 2 \cdot 1 + 3 \cdot 2 + 4 \cdot 7 + 5 \cdot 0 + 6 \cdot 1 + 7 \cdot 9 + 8 \cdot 0 + 9 \cdot 1 \text{ hat Rest } 7 \text{ bei Teilung durch } 11$$

Eine Prüfziffer 10 wird als X (römische 10) geschrieben.)

- **E A N (European Article Number/Strichcode)**

Beispiel: | || | || |

□

1.4 Relationen

Das Gleichheitszeichen “=“ verwenden wir in einer Menge unter der stillschweigenden Annahme der folgenden Regeln:

$$x = x; (x = y \implies y = x); (x = y, y = z \implies x = z).$$

Dies nehmen wir zum Anlass für

Definition 1.4.1 Sei X eine Menge. Eine Teilmenge $R \subset X \times X$ heißt **Äquivalenzrelation** auf X , falls

$$(i) (x, x) \in R \text{ für alle } x \in X \quad (\text{Reflexivität})$$

$$(ii) (x, y) \in R \implies (y, x) \in R \quad (\text{Symmetrie})$$

$$(iii) (x, y), (y, z) \in R \implies (x, z) \in R \quad (\text{Transitivität})$$

gilt.

□

Liegt mit R auf X eine Äquivalenzrelation vor, so schreiben wir für $(x, y) \in R$ $x \overset{R}{\sim} y$ oder kurz $x \sim y$, wenn R uns aus dem Zusammenhang klar ist.

Die Bedeutung einer Äquivalenzrelation R auf X liegt darin, dass man damit die Menge X in Teilmengen (Klassen, Bündel) einteilen kann, eine Einteilung, die eventuell gröber ist, als die Aufteilung in einelementige Mengen, und die bezüglich eines „Merkmals“ doch noch aussagekräftig ist. Die Einteilung geschieht durch

$$[x] := \{y \in X \mid y \overset{R}{\sim} x\}, x \in X, \text{ und } X/R := \{[x] \mid x \in X\}.$$

Die Objekte $[x]$ heißen **Äquivalenzklassen**, x heißt **Repräsentant** der Klasse $[x]$. Man beachte, dass jedes $y \in X$ mit $y \overset{R}{\sim} x$ als Repräsentant für $[x]$ Verwendung finden kann.

Beispiel 1.4.2 Blutgruppen werden grob eingeteilt in $A, AB, B, 0$. Sei K eine Gruppe von Kindern. Wir erklären darauf eine Relation durch

$$x \sim y : \iff x, y \text{ haben dieselbe Blutgruppe}$$

In der Tat liegt eine Äquivalenzrelation vor. Dadurch wird die Gruppe der Kinder in 4 Klassen eingeteilt. □

Beispiel 1.4.3 Man überlege sich, in welcher Weise, die Geraden in der Ebene durch eine Äquivalenzrelation in Klassen eingeteilt werden können. □

Das folgende Lemma zeigt, dass X durch “ $\overset{R}{\sim}$ “ in disjunkte Klassen zerlegt wird.

Lemma 1.4.4 Sei X eine Menge und sei R eine Äquivalenzrelation auf X . Dann gilt:

$$(a) \text{ Für jedes } x \in X \text{ gibt es } [y] \in X/R \text{ mit } x \in [y].$$

- (b) Es ist $x \overset{R}{\sim} y$ genau dann, wenn $[x] = [y]$ gilt.
- (c) Zwei Äquivalenzklassen besitzen genau dann nichtleeren Durchschnitt, wenn sie gleich sind.

Beweis:

Zu (a). Klar: $x \in [x]$ für alle $x \in X$ wegen der Reflexivität von “ \sim “.
 Zu (b). Sei $x \sim y$. Sei $u \in [x]$. Dann ist $u \sim x$ und aus der Symmetrie und der Transitivität folgt $u \sim y$, d.h. $u \in [y]$. Also ist $[x] \subset [y]$ gezeigt. Die Aussage $[y] \subset [x]$ folgt völlig analog.
 Ist $[x] = [y]$ dann ist $x \sim y$, da wir $x \in [y] = [x]$ haben.
 Zu (c). Unter Beachtung der Transitivität, der Symmetrie von “ \sim “ und (b) folgt

$$z \in [x] \cap [y] \implies z \sim x, z \sim y \implies x \sim y \implies [x] = [y]$$

was zu beweisen war. ■

1.5 Übungen

- 1.) Verneine folgende Aussagen:
 - (a) Wenn es regnet, ist die Straße nass.
 - (b) Es gibt kein Tier, das genau ein Ohr und genau zwei Augen hat.
 - (c) Alle Quadrate von ganzen Zahlen sind gerade.

Was läßt sich über den Wahrheitsgehalt der Aussagen in (a), (b), (c) sagen?

- 2.) A, B, C, D sind vier Tatverdächtige. Genau einer unter ihnen ist der Täter. Beim Verhör machen sie folgende Aussagen:

A: B ist der Täter B: D ist der Täter C,D: Ich bin nicht der Täter
 Wer ist der Täter, wenn

- (a) genau einer lügt,
- (b) genau einer die Wahrheit sagt ?

- 3.) Seien P, Q Aussagen. Stelle die Wahrheitstafel zu

- (a) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$
- (b) $P \wedge (P \vee Q) \iff P$

auf.

- 4.) (a) Fülle die folgende Wahrheitstabelle aus:

P	Q	$\neg P$	$\neg Q$	$(\neg P \vee Q)$	$\neg(\neg P \vee Q)$	$P \wedge \neg Q$
(w)	(w)					
(w)	(f)					
(f)	(w)					
(f)	(f)					

Was schließt man aus den beiden letzten Spalten?

- (b) Fülle die folgende Wahrheitstabelle aus:

P	Q	$P \implies Q$	$(P \implies Q) \vee P$
(w)	(w)		
(w)	(f)		
(f)	(w)		
(f)	(f)		

Was schließt man aus der letzten Spalte?

- 5.) Seien A, B Mengen. Zeige:
- Zeige: $POT(A \cap B) = POT(A) \cap POT(B)$
 - Zeige: $POT(A) \cup POT(B) \subset POT(A \cup B)$
 - Ist sogar $POT(A \cup B) = POT(A) \cup POT(B)$ richtig?
- 6.) Seien A, B Mengen. Welche Beziehung besteht zwischen A und B , falls $A \cap B = A$ oder $A \cup B = B$ gilt?
- 7.) Seien G, M Mengen und sei $I \subset G \times M$. Zu $A \subset G$ setze

$$A := \{m \in M \mid (a, m) \in I \text{ für alle } a \in A\}.$$

Zeige:

- $B^{\wedge} \subset A^{\wedge}$ falls $A \subset B$.
- $A \subset A^{\sim}$, $A^{\wedge} = A^{\sim\sim}$.

(In der Literatur heisst ein solches Tripel (G, M, I) auch Kontext mit Gegenstandsmenge G , Merkmalen M und Inzidenz I .)

- 8.) Beweise für Mengen A, B, C : $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- 9.) Die symmetrische Differenz von Mengen A und B ist definiert durch

$$A \Delta B := \{x \in A \mid x \notin B\} \cup \{x \in B \mid x \notin A\}$$

Beweise für Mengen A, B, C : $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.

- 10.) Seien A, B Mengen und definiere

$$((a, b)) := \{\{a\}, \{a, b\}\}, \quad a \in A, b \in B.$$

Zeige für $a, p \in A, b, q \in B$: $((a, b)) = ((p, q)) \iff a = p, b = q$.
(Damit haben wir geordnete Paare neu definiert.)

- 11.) Zeige für Mengen A, B die Äquivalenz der folgenden beiden Aussagen:
- $A = B$.
 - $A \cup B = A \cap B$.

- 12.) MAPLE: Was schliesst man aus der folgenden Sequenz?

```
> with(logic):
> bequal((p &nand q) &nand r, p &nand (q &nand r));
```

false

- 13.) MAPLE: Gegeben seien die Mengen $A := \{a, b, c\}$ und $B := \{c, d\}$. Berechne die Potenzmenge von A und teste, ob B eine Teilmenge von A ist. Hinweis: Berechne die Potenzmenge in einer Schleife.
- 14.) MAPLE: Zeige:
- $p \text{ &or } q$ genau dann, wenn $\text{\&nand}(\text{\&nand}(p, p), \text{\&nand}(q, q))$.
 - $\text{\¬ } p$ genau dann, wenn $\text{\&nand}(p, p)$.
- 15.) MAPLE: Ermittle die Arbeitsfunktion des booleschen Operators \&xor durch Erstellen einer Wahrheitstafel.