Vorkurs Mathematik für Informatiker

Kathrin Gimmi[1]
Dirk Hachenberger[2]
Tobias Mömke[3]

Institut für Informatik und Institut für Mathematik der Universität Augsburg

Wintersemester 2020/21

16. Oktober 2020

Dieser Vorkurs richtet sich an Studierende, die ihr Studium der Informatik in diesem Wintersemester beginnen und deren Nebenfach nicht Mathematik ist. Er findet zwei Wochen vor dem Vorlesungsstart in digitaler Form statt.

Das Ziel dieses Kurses ist die Vermittlung von wichtigen Grundlagen, auf denen die beiden Vorlesungen „Diskrete Strukturen und Logik“ sowie „Mathematik für Informatiker I“ aufbauen. Dazu gehören insbesondere

- die grundlegenden Beweisprinzipien,
- logische Aussagen und deren Verknüpfungen,
- Grundlagen der Mengenlehre,
- Grundlagen über Zahlen,
- das Prinzip der vollständigen Induktion,
- der Umgang mit Summen und Produkten,
- der Abbildungsbegriff,
- einige Grundlagen der Kombinatorik.

Die Teilnahme an diesem Kurs wird dringend empfohlen. Nähere Einzelheiten zum organsatorischen Ablauf werden zeitnah auf der Webseite

https://www.uni-augsburg.de/de/fakultaet/mntf/math/prof/opt/aktuelles/vorkurs/

sowie im Ablaufplan hier im Digicampus verfügbar gemacht.

Sie werden die Teilnahme nicht bereuen, denn Sie werden Vieles über Mathematik erfahren, was Sie noch nie wissen wollten, und an was Sie möglicherweise niemals (nicht einmal im Traum) gedacht hätten. Ihnen werden die Augen aufgehen und Sie werden (danach) die Welt anders, einfach viel tiefsinniger wahrnehmen.

: −)

[1] kathrin.gimmi@math.uni-augsburg.de
[2] hachenberger@math.uni-augsburg.de
[3] tobias.moemke@informatik.uni-augsburg.de

Überblick:

(1) Was ist Mathematik?
(2) Einige Probleme bzw. Knobelaufgaben
(3) Grundbegriffe der Mengenlehre
(4) Die grundlegenden Zahlbereiche
(5) Die drei grundlegenden Beweisprinzipien
(6) Überlegungen zur elementaren Geometrie der Zahlen
(7) Zur Lösung reeller quadratischer Gleichungen
(8) Logische Aussagen und deren Verknüpfungen
(9) Die drei grundlegenden Beweisprinzipien aus dem Blickwinkel der Aussagenlogik
(10) Verknüpfungen von Mengen und deren Gesetzmäßigkeiten
(11) Gesetzmäßigkeiten bei der Verknüpfung von logischen Aussagen
(12) Potenzmengen und kartesische Produkte
(13) Summen und Produkte
(14) Verknüpfungen von mehreren Mengen
(15) Verknüpfungen bei beliebigen Indexmengen und Quantoren
(16) Das Prinzip der vollständigen Induktion
(17) Beispiele zur vollständigen Induktion
(18) Grundlagen über Relationen
(19) Der Abbildungsbegriff
(20) Injektivität, Surjektivität und Bijektivität
(21) Bild und Urbild bei Abbildungen
(22) Verkettung von Abbildungen
(23) Abbildungen zwischen endlichen Mengen
(24) Binomialkoeffizienten
(25) Abzählbar unendliche Mengen
(26) Überabzählbar unendliche Mengen
(27) Ordnungsrelationen
(28) Ganze Zahlen: Division mit Rest
(29) Äquivalenzrelationen
(30) Äquivalenzklassen
(31) Repräsentantensysteme
(32) Die B-adische Darstellung ganzer Zahlen
(33) Größte gemeinsame Teiler
(34) Kleinste gemeinsame Vielfache
(35) Der erweiterte Euklidische Algorithmus
(36) Analyse des (erweiterten) Euklidischen Algorithmus
(37) Die Primfaktorzerlegung
(38) Ein einfaches aber nicht effizientes Faktorisierungsverfahren

1. **Was ist Mathematik?**

a Das ist sehr schwierig in wenigen Worten auf den Punkt zu bringen. Kurz umrissen handelt es sich um eine Wissenschaft, die versucht, Strukturen zu entdecken und deren logische Zusammenhänge auszuloten. Als Grundwerkzeug bedient sie sich dabei gewisser Objekte, vor allem **Axiomen** und **Mengen**, sowie **Zahlen**, deren Gültigkeit bzw. Existenz als gegeben angesehen werden. Ausgehend davon wird versucht, durch logische Schlussfolgerungen zu wahren Aussagen zu kommen, die man dann als *Sätze*, *Theoreme* oder auch *Lemmata* formuliert.

b Eine zentrale Aufgabe der Mathematik ist es, Problemstellungen zu formalisieren bzw. zu modellieren und Lösungsverfahren zu generieren. Wir liefern im kommenden Abschnitt daher eine kleine Sammlung von Problemstellungen zu deren Lösung alle eingeladen sind.

c Es gibt eine Menge einführender Literatur, die sich damit beschäftigen, die wesentlichen Grundzüge der Mathematik einem breiten Publikum nahezubringen. Meiner Meinung nach ist das Büchlein „Mathematics: A very short Introduction“ von Timothy Gowers (Oxford University Press, Oxford, 2002) unübertroffen. Eine deutsche Übersetzung ist bei Reclam verlegt worden.

2. **Einige Probleme bzw. Knobelaufgaben**

a Auf einer Weide stehen Pferde, Kühe und Schafe. Wenn man die Pferde von der Weide führt, verbleiben 26 Tiere auf der Weide. Wenn man die Kühe in den Stall treibt, bleiben 22 Tiere auf der Weide zurück. Ohne Schafe sind es lediglich 12 Tiere. Wieviele Tiere jeder Sorte stehen auf der Weide?

b Welche der beiden Zahlen ist größer,

$$3^{400} \quad \text{oder} \quad 4^{300} \ ?$$

c Ist n eine natürliche Zahl, so ist die Zahl „n Fakultät“ (Notation: $n!$) definiert als das Produkt der Zahlen $1, 2, 3, ...$, bis n. Beispielsweise ist 5! gleich $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ gleich 120.

Wieviele Nullen hat die Zahl 50! am Ende?

d Auf einem Taschenrechner findet man den Ziffernblock der Zahlen 1 bis 9 in folgender Formation vor:

7	8	**9**
4	5	6
1	2	**3**

Wir greifen uns nun irgendein Rechteck heraus (etwa die fett markierten Zahlen) und notieren die Zahlen in der Reihenfolge *oben links*, *unten links*, *unten rechts*, *oben rechts* (also zum Beispiel 7139). Die resultierende Zahl ist dann stets durch 11 teilbar (zum Beispiel $7139 = 11 \cdot 649$). Warum?

e Kann man ein 6×6-Schachbrett mit „Dominosteinen“ vom Typ 1×4 und 4×1 überdecken?

f Zehn Bäume sollen so gepflanzt werden, dass sie in fünf Linien angeordnet sind und auf jeder Linie genau vier Bäume stehen. Wie sieht eine solche Anordnung aus?

g Man versuche, dieses Sudoku zu lösen:

	2	9				4		
			5			1		
	4							
				4	2			
6							7	
5								
7			3					5
	1			9				
							6	

h Bei der Übermittlung der Zahl 15! ist die mittlere Ziffer leider nicht lesbar gewesen:

$$130767?368000.$$

Man möge sie ohne Taschenrechner rekonstruieren.

i Die Zahl 1 ist (trivialerweise) ein Quadrat, eine Kubikzahl, eine vierte Potenz und eine fünfte Potenz (denn $1 = 1^2 = 1^3 = 1^4 = 1^5$). Welches ist (nach der Eins) die kleinste natürliche Zahl, die sowohl ein Quadrat, eine Kubikzahl, eine vierte Potenz und eine fünfte Potenz ist?

j Welches sind die letzten beiden Ziffern der Zahl

$$3^{1776}\ ?$$

k Zwei Spieler sind jeweils mit einer riesigen Menge von 1-Cent-Stücken ausgestattet. Vor ihnen steht ein runder Tisch, dessen Tischplatte einen Durchmesser von einem Meter hat. Der Tisch ist anfangs leer. Nun legen die beiden Spieler abwechselnd jeder ein Centstück auf den Tisch, so dass sich die Geldstücke nicht überlappen. Derjenige Spieler verliert, der keine Münze mehr hinlegen kann. Hat dieses Spiel eine Gewinnstrategie?

l Die Schüler einer Klasse sitzen in fünf Reihen mit je sechs Plätzen. Aus jeder Reihe wird der größte Schüler ausgewählt, und von diesen dann der kleinste, A. Nachdem sich alle wieder gesetzt haben, wird aus jeder Spalte der kleinste Schüler ausgewählt, und von diesen dann der größte, B.

Wer ist größer, A oder B? Können beide gleich groß sein? Können es eventuell sogar die gleichen Personen sein?

3. Grundbegriffe der Mengenlehre

a Ohne Zweifel gehören *Mengen* zu den wichtigsten Bausteinen der Mathematik. Da die formale Regelung darüber, bei welchen „Dingen“ es sich um eine Menge handelt bzw. nicht handelt viel zu abschweifend und schwierig ist, findet man praktisch nirgends eine konkrete Definition darüber, was man (allgemein) unter einer (beliebigen) Menge versteht. Vielmehr belässt man es bei einer anschaulichen Beschreibung, die auf Georg Cantor (1845-1918), den Begründer der Mengenlehre, zurückgeht:

- Eine **Menge** ist eine Zusammenfassung von bestimmten, wohlunterscheidbaren Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

b So bilden beispielsweise die kleinen Buchstaben $a, b, ..., z$ als Objekte unser Alphabet. Durch Verwendung der **Mengenklammern** { und } fassen wir diese Objekte zu einer Menge zusammen, welche wir kurz mit A bezeichnen wollen:

$$A := \{a, b, ..., z\}$$

Das Zeichen := bedeutet dabei einfach, dass A als die (konkrete) Menge $\{a, b, ..., z\}$ definiert ist.

- Bei $\{0, 1\}$ handelt es sich um die Menge der Dualziffern bzw. (besser) Binärziffern;
- bei {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} handelt es sich um die Menge der Dezimalziffern.
- Die folgende Menge besteht aus einigen kleinen griechischen Buchstaben, die wir sehr häufig verwenden werden:

$$\{\alpha, \beta, \gamma, \delta, \varepsilon, \varphi, \phi, \rho, \sigma, \tau, \omega, \xi, \eta, \zeta, \pi, \theta, \iota, \kappa\}$$

c Man nennt die Objekte $a, b, ...$ die **Elemente** der Menge A. Zwischen Elementen und Mengen besteht die **Elementbeziehung** $\in$. Beispielsweise gilt $u \in A$ (lies: „u liegt in A“ oder „u ist Element von A“) und $5 \notin A$ (lies: „5 liegt nicht in A“ oder „5 ist nicht Element von A“).

d Betrachten wir nochmals die obige Definition der Menge A. Sie ist durch **Aufzählung** ihrer Elemente innerhalb der Mengenklammern beschrieben. Man macht sich dabei allerdings nicht die Mühe *alle* ihrer insgesamt 26 Elemente hinzuschreiben, sondern suggeriert durch die Punkte ..., dass klar ist, wie es formal weitergeht.

Alternativ zur Aufzählung werden Mengen sehr häufig durch **charakteristische** oder **definierende Eigenschaften** beschrieben. Dies ist insbesondere dann unerlässlich, wenn die Anzahl der Elemente unendlich groß ist (siehe etwa die Zahlbereiche im kommenden Abschnitt). Generell sind definierende Beschreibungen von folgender Art:

$$M := \{\omega : \ \omega \text{ hat die Eigenschaften ... } \}$$

Man liest „M ist (definiert als) die Menge aller Objekte ω mit den Eigenschaften ...“. Der griechische Buchstabe ω fungiert hier also als eine **Variable** für die Elemente der Menge M. Betrachten wir dazu zwei Beispiele.

- Mit A wie oben sei die Menge S definiert durch $S := \{\omega : \omega \in A \text{ und } \omega \text{ ist Selbstlaut}\}$. Dann ist S gleich $\{a, e, i, o, u\}$ (in aufzählender Schreibweise).
- Definiert man die Menge P durch $P := \{\omega : \omega \text{ ist Dezimalziffer}, \omega \text{ ist Primzahl und } \omega \geq 4\}$, so ist P gleich $\{5, 7\}$ (in aufzählender Schreibweise).

e Wir haben eben anhand von Beispielen verschiedene Darstellungsmöglichkeiten von Mengen gesehen und dabei auch die Gleichheit von Mengen erwähnt. Dies wollen wir nun zusammen mit der Teilmengenbeziehung bei Mengen formal definieren.

Definition: Es seien X und Y zwei Mengen.

(1) Ist jedes Element von X auch Element von Y, so heißt X eine **Teilmenge** von Y; Schreibweise: $X \subseteq Y$.[a]

(2) Gilt $X \subseteq Y$ und $Y \subseteq X$, so heißen die beiden Mengen X und Y **gleich**; Schreibweise: $X = Y$. In diesem Fall ist jedes Element von X ein Element von Y und umgekehrt jedes Element von Y ein Element von X.

(3) Ist X Teilmenge von Y, aber nicht gleich Y (kurz: $X \subseteq Y$ und $X \neq Y$), so sagt man, dass X eine **echte Teilmenge** Teilmenge von Y ist; als Schreibweise verwendet man dazu häufig auch $X \subset Y$.

[a] Bei der Teilmengenbeziehung spricht man auch von einer **Mengeninklusion**.

f Beispielsweise ist die Menge $S = \{a, e, i, o, u\}$ der Selbstlaute eine echte Teilmenge der obigen Menge A. Um die Gleichheit von Mengen zu demonstrieren, betrachten wir die folgenden drei Mengen C, D und E:

$$\begin{array}{lcl} C & := & \{a, c, e, f, g, h\} \\ D & := & \{a, c, a, a, e, f, g, g, g, g, g, h, h\} \\ E & := & \{h, g, f, e, a, c\} \end{array}$$

Bei C und E handelt es sich um Teilmengen der Menge A. Jedes Element von C ist auch Element von E und umgekehrt ist jedes Element von E auch Element von C; nach Definition 3e-(2) sind deshalb C und E gleich, es gilt also $C = E$. Wir lernen daraus, dass bei der Beschreibung von Mengen die Reihenfolge der auftretenden Elemente keine Rolle spielt.

Bei dem Objekt D mag man darüber philosophieren, ob es sich in Cantors Sinne um eine Zusammenfassung „wohlunterscheidbarer“ Objekte, also überhaupt um eine Menge handelt. Wir sind der Meinung, dass man zu je zwei Buchstaben aus D entscheiden kann, ob sie gleich oder verschieden sind und halten sie daher für „wohlunterscheidbar“. Ein weiteres Indiz dafür, dass es sich bei D um eine Menge handeln sollte ist Folgendes: Sicherlich ist jedes Objekt aus D auch in der Menge C enthalten und umgekehrt ist jedes Element aus C auch Objekt von D. Man kann also D getrost als Menge auffassen, und es gilt dann $D = C$. Daraus lernen wir, dass bei der Beschreibung von Mengen die Häufigkeiten der auftretenden Elemente keine Rolle spielt. Insgesamt folgt dann die Gleichheit der drei Mengen C, D und E, also $C = D = E$.

g Da man Mengen mitunter auf recht verschiedene Weisen definieren kann, ist oft überhaupt nicht offensichtlich, ob zwei unterschiedlich beschriebene Mengen gleich sind. Dazu ein **Beispiel:**

Es seien X und Y die beiden durch

$$\begin{array}{lcl} X & := & \{x : x \text{ ist natürliche Zahl und } 7 \leq x^2 < 30\} \text{ und} \\ Y & := & \{y : y \text{ ist natürliche Zahl und } y^3 - 12y^2 + 47y - 60 = 0\} \end{array}$$

definierten Mengen. Wir werden zeigen, dass $X = Y$ gilt. Dazu beginnen wir, X in aufzählender Form aufzuschreiben: Für eine natürliche Zahl x mit $x^2 \geq 7$ gilt $x \geq 3$, und aus $x^2 < 30$ folgt $x < 6$. Andererseits gilt $7 \leq x^2 < 30$, wenn $x = 3$ oder $x = 4$ oder $x = 5$. Also folgt $X = \{3, 4, 5\}$ (in aufzählender Schreibweise).

Setzt man nun die Zahlen 3, 4 und 5 für y in die charakterisierende Eigenschaft der Menge Y ein, so erhält man

$$\begin{array}{lcl} 3^3 - 12 \cdot 3^2 + 47 \cdot 3 - 60 & = & 27 - 108 + 141 - 60 = 0 \\ 4^3 - 12 \cdot 4^2 + 47 \cdot 4 - 60 & = & 64 - 192 + 188 - 60 = 0 \\ 5^3 - 12 \cdot 5^2 + 47 \cdot 5 - 60 & = & 125 - 300 + 235 - 60 = 0, \end{array}$$

woraus insgesamt $X \subseteq Y$ folgt. Zum Nachweis von $X = Y$ bleibt somit $Y \subseteq X$ zu zeigen. Das bedeutet, wir müssen ausschließen, dass es neben den drei bereits angegebenen Lösungen dieser Gleichung keine weiteren mehr gibt. Wie soll das funktionieren? Wir können ja unmöglich die Gleichung an allen natürlichen Zahlen

austesten. Könnte es eventuell nicht doch sein, dass es weitere, möglicherweise astronomisch große Lösungen gibt? Etwa

$$10^{10^{10^{10^{10^{10^{10^{10^{10^{10}}}}}}}}} + 23 \ ?$$

Das ist tatsächlich nicht der Fall! Und hier ist die Begründung:

Für jede natürliche Zahl y gilt $y^3 - 12y^2 + 47y - 60 = (y-3)(y-4)(y-5)$, wie man durch Ausmultiplizieren der rechten Seite schnell verifiziert:

$$(y-3)(y-4)(y-5) = (y^2 - 7y + 12)(y-5) = y^3 - 12y^2 + 47y - 60$$

Weiter gilt folgender wichtige (hoffentlich noch aus der Schule bekannte) Sachverhalt:

> *Ist ein Produkt natürlicher (allgemeiner: ganzer, rationaler oder reeller Zahlen) gleich null, so ist wenigstens einer der Faktoren gleich null.*

Mit $0 = (y-3)(y-4)(y-5)$ muss dann also $y-3 = 0$ oder $y-4 = 0$ oder $y-5 = 0$ gelten, was sofort $y \in \{3, 4, 5\}$ für $y \in Y$ nach sich zieht und daher auch $Y \subseteq X$ liefert. □[4]

h Zur Darstellung von Mengen wäre an dieser Stelle noch Folgendes zu ergänzen. Wenn wir eine Menge H als Teilmenge einer bereits vorher eingeführten Grundmenge G definieren wollen, so schreibt man meist einfach $H := \{\omega \in G : \omega \text{ hat die Eigenschaften ... }\}$ anstatt $H := \{\omega : \omega \in G, \omega \text{ hat die Eigenschaften ... }\}$.

i Ein wichtiges Charakteristikum für eine Menge M ist die Anzahl ihrer Elemente. Diese bezeichnet man mit $|M|$. Man nennt $|M|$ auch die **Mächtigkeit** oder **Kardinalität** von M. Bei den oben eingeführten Mengen gilt beispielsweise $|A| = 26$, sowie $|S| = 5$ und $|C| = |D| = |E| = 6$.

An dieser Stelle müssen wir allerdings einräumen, dass eine strenge formale Definition der Mächtigkeit einer Menge zumindest den **Abbildungsbegriff** voraussetzt, mit dem wir uns später befassen werden. Wir belassen es daher hier mit der intuitiv klaren Vorstellung über die Mächtigkeit von Mengen.

j Intuitiv klar ist auch der Unterschied zwischen einer Menge mit **endlich vielen** und einer Menge mit **unendlich vielen** Elementen: Die Mächtigkeit einer **endlichen Menge** ist eine natürliche Zahl, während die Mächtigkeit einer **unendlichen Menge** durch keine natürliche Zahl angegeben werden kann. Für unendliche Mengen M verwendet man daher die Schreibweise $|M| = \infty$. Wir werden uns natürlich noch intensiver mit unendlichen Mengen befassen und dabei u.a. feststellen, dass die alleinige Verwendung **eines** Symbols ∞ nicht sehr präzise ist, es gibt nämlich verschiedene Hierarchien von unendlichen Mengen.

k Auf eine besondere Menge, nämlich die **leere Menge**, müssen wir abschließend noch zu sprechen kommen. Es handelt sich dabei um diejenige Menge, die **kein** Element enthält; Bezeichnung: $\{\}$ oder $\emptyset$. Es ist $\emptyset \subseteq M$ für jede Menge M. Die Mächtigkeit der leeren Menge ist die Zahl Null:

$$|\emptyset| = |\{\}| = 0$$

[4] Damit haben wir tatsächlich bereits einen ersten Beweis geführt! Das Zeichen □ steht für das Ende einer Definition, eines Beispiels, eines Beweises oder eines sonstigen Ergebnisses. Eine andere geläufige Bezeichnung für ein Beweisende ist „q.e.d.“, was für „quod erat demonstrandum“ steht.

4. **Die grundlegenden Zahlbereiche**

a Nachdem wir im letzten Abschnitt über allgemeine Mengen geredet haben, wollen wir nun einige Mengen betrachten, mit denen man praktisch tagtäglich umgehen muss. Es handelt sich dabei um die zum Großteil aus der Schule bekannten Zahlbereiche.

- $\mathbb{N} := \{0, 1, 2, ...\}$ ist die Menge der **natürlichen Zahlen**.
- $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$ ist die Menge der **ganzen Zahlen**.
- $\mathbb{Q} := \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$ ist die Menge der **rationalen Zahlen**,
  $\mathbb{Q}_0^+ := \{q \in \mathbb{Q} :\ q \geq 0\}$ ist die Menge der **nichtnegativen** rationalen Zahlen,
  $\mathbb{Q}^+ := \{q \in \mathbb{Q} :\ q > 0\}$ ist die Menge der **positiven** rationalen Zahlen.
- $\mathbb{R}$ bezeichnet die Menge der **reellen Zahlen**,
  $\mathbb{R}_0^+ := \{r \in \mathbb{R} :\ r \geq 0\}$ ist die Menge der **nichtnegativen** reellen Zahlen,
  $\mathbb{R}^+ := \{r \in \mathbb{R} :\ r > 0\}$ ist die Menge der **positiven** reellen Zahlen.
- $\mathbb{C}$ bezeichnet die Menge der **komplexen Zahlen**.

b Wir müssen darauf hinweisen, dass die oben eingeführte Notation $\mathbb{N}$ nicht einheitlich verwendet wird. Häufig schreibt man $\mathbb{N}_0$ für $\{0, 1, 2, ...\}$, während $\mathbb{N}$ für die Menge $\{1, 2, ...\}$ reserviert ist. Im Rahmen unserer Vorlesungen wird die Null als natürliche Zahl aufgefasst! Für die Menge $\{1, 2, ...\}$ haben wir häufig die Bezeichnung $\mathbb{N}^*$ verwendet; sinnvoll ist aber auch $\mathbb{Z}^+$, denn bei den Objekten handelt es sich genau um die positiven ganzen Zahlen.

c Es mag aufgefallen sein, dass wir dem reellen Zahlbereich lediglich eine Bezeichnung (nämlich $\mathbb{R}$) gegeben haben, dass wir diese Menge aber nicht durch charakteristische Eigenschaften beschrieben haben. Das liegt daran, dass die Konstruktion bzw. die axiomatische Beschreibung der reellen Zahlen tiefere Kenntnisse der Mathematik erfordert und daher an dieser Stelle unangebracht ist. Dennoch werden wir den Unterschied zwischen den rationalen und den reellen Zahlen im Rahmen der Abschnitte 6 und 7 etwas beleuchten. Die komplexen Zahlen werden wir erst später, im Laufe der Vorlesung einführen.

d Jedenfalls gilt:

$$\begin{array}{ccccccccc}
\mathbb{N}^* & = & \mathbb{Z}^+ & \subset & \mathbb{Q}^+ & \subset & \mathbb{R}^+ & & \\
 & & \cap & & \cap & & \cap & & \\
 & & \mathbb{N} & \subset & \mathbb{Q}_0^+ & \subset & \mathbb{R}_0^+ & & \\
 & & \cap & & \cap & & \cap & & \\
 & & \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R} & \subset & \mathbb{C}
\end{array}$$

5. **Die drei grundlegenden Beweisprinzipien**

In diesem Abschnitt wollen wir anhand von einfachen zahlentheoretischen Aussagen die drei grundlegenden, in der Mathematik immer wieder verwendeten Beweisprinzipien vorstellen.

a Wir beginnen mit dem **direkten Beweis** (siehe auch die Argumentation in Beispiel 3g).

Beispiel: (**Direkter Beweis**)
Die Summe zweier beliebiger ungerader natürlicher Zahlen ist eine gerade natürliche Zahl.

Beweis. Zunächst sollten wir die verwendeten Begriffe klären, nämlich „ungerade“ bzw. „gerade“ natürliche Zahl: Durchläuft man die natürlichen Zahlen in ihrer (natürlichen) Reihenfolge, $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ...$, so erhält man abwechselnd eine gerade Zahl und eine ungerade Zahl, beginnend mit einer geraden Zahl. Es ist also $G = \{0, 2, 4, 6, \dots\}$ die Menge der geraden und $U = \{1, 3, 5, 7, \dots\}$ die Menge der ungeraden natürlichen Zahlen (in aufzählender Form).

In mathematischen Formeln lautet die zu beweisende Aussage nun

$$\underbrace{u, v \in U}_{\text{Voraussetzung}} \quad \underbrace{\Rightarrow}_{\text{impliziert}} \quad \underbrace{u + v \in G.}_{\text{Folgerung}}$$

Um dies nun (überzeugend) nachzuweisen, ist es sinnvoll, die beiden Mengen G und U anders zu beschreiben. So ist eine natürliche Zahl n genau dann gerade, wenn sie durch 2 teilbar ist, das heißt, wenn es eine natürliche Zahl m mit $n = 2m$ gibt:

$$G = \{n \in \mathbb{N} : \text{es gibt ein } m \in \mathbb{N} \text{ mit } n = 2m\} = \{2m : m \in \mathbb{N}\}.$$

Im Gegensatz dazu ist eine natürliche Zahl n genau dann ungerade, wenn bei Division durch 2 der Rest 1 verbleibt, das heißt, wenn es eine natürliche Zahl m mit $n = 2m + 1$ gibt:

$$U = \{n \in \mathbb{N} : \text{es gibt ein } m \in \mathbb{N} \text{ mit } n = 2m + 1\} = \{2m + 1 : m \in \mathbb{N}\}.$$

Der Beweis obiger Aussage kann nun sehr leicht geführt werden: Es seien $u, v \in U$. Dann gibt es ein $k \in \mathbb{N}$ mit $u = 2k + 1$ und ein $\ell \in \mathbb{N}$ mit $v = 2\ell + 1$. Daraus folgt

$$u + v = 2k + 1 + 2\ell + 1 = 2 \cdot (k + \ell + 1).$$

Wegen $k + \ell + 1 \in \mathbb{N}$ ist diese Zahl gerade. □

b Es folgt ein Beispiel für einen **indirekten Beweis**.

Beispiel: (**Indirekter Beweis**)
Ist das Quadrat einer natürlichen Zahl gerade, so ist die Zahl selbst gerade.

Beweis. Es sei $x \in \mathbb{N}$. Zu zeigen ist

$$x^2 \in G \quad \Rightarrow \quad x \in G.$$

Wie wir später im Rahmen der Aussagenlogik genauer begründen werden, ist dies logisch gleichwertig zur **Kontraposition**[5]

$$\neg[x \in G] \quad \Rightarrow \quad \neg[x^2 \in G],$$

was wiederum

$$x \in U \quad \Rightarrow \quad x^2 \in U$$

[5]Dabei bedeutet $\neg A$ die **Negation** der Aussage A.

bedeutet. Diese zur ursprünglichen Aussage äquivalente Form kann nun leicht direkt verifiziert werden: Annahme, $x \in U$. Dann gibt es ein $m \in \mathbb{N}$ mit $x = 2m+1$. Sodann ist

$$x^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2 \cdot (2m^2 + 2m) + 1 \in U,$$

da $2m^2 + 2m \in \mathbb{N}$. □

c Es folgt ein weiteres Beispiel für einen indirekten Beweis.

Beispiel: (**Indirekter Beweis**)
Sind $a, b \in \mathbb{N}$ mit $a + b$ ungerade, so folgt $a^2 \neq 2b^2$.

Beweis. Annahme $a, b \in \mathbb{N}$ mit $a^2 = 2b^2$. Dann folgt $a^2 \in G$, und Beispiel 5b ergibt daher $a \in G$, weshalb ein $m \in \mathbb{N}$ mit $a = 2m$ existiert. Nun folgt die Gleichungskette $2b^2 = a^2 = (2m)^2 = 4m^2$. *Kürzen* mit 2 liefert daher $b^2 = 2m^2$, weshalb $b^2 \in G$. Erneut nach Beispiel 5b ist dann (auch) $b \in G$. Also gibt es ein $n \in \mathbb{N}$ mit $b = 2n$. Insgesamt erhalten wir also $a + b = 2m + 2n = 2 \cdot (m + n) \in G$, da $m + n \in \mathbb{N}$. Also ist $a + b$ eine gerade natürliche Zahl. □

d Unter Verwendung von Beispiel 5c können wir nun bereits ein Aussage beweisen, die den Namen „Satz“ verdient. Beim Beweisprinzip handelt es sich um einen **Widerspruchsbeweis**.

Satz: *Es gibt keine rationale Zahl x mit $x^2 = 2$.*

Beweis. (Durch Widerspruch).

(1) Wir nehmen das Gegenteil der Aussage des Satzes an. Es gebe also eine rationale Zahl x mit $x^2 = 2$.
(2) Dann gilt auch $(-x)^2 = (-1)^2 \cdot x^2 = x^2 = 2$. Also gibt es eine positive rationale Zahl, deren Quadrat gleich 2 ist. Diese Art von Argumentation wird häufig wie folgt zusammengefasst:
O.B.d.A. ist x positiv.[6]
Fazit an dieser Stelle: Es gibt ein Paar (m, n) natürlicher Zahlen mit $x = \frac{m}{n}$.
(3) Aber dann gibt es sogar unendlich viele solcher Paare, denn mit jeder positiven natürlichen Zahl d gilt auch $\frac{dm}{dn} = \frac{m}{n} = x$, weshalb (dm, dn) ein weiteres solches Paar ist. Wir können daher (o.B.d.A.) eine möglichst ökonomische Bruchdarstellung von x betrachten, das heißt: Wir nehmen an, dass x durch ein Paar (m, n) mit *kleinstmöglichem* Zähler m dargestellt wird.
(4) Daraus folgt dann wiederum, dass m und n nicht beides gerade Zahlen sind, denn sonst hätte man $m = 2m'$ und $n = 2n'$ für gewisse $m', n' \in \mathbb{N}^*$ und gelangte sodann zu einer Darstellung $x = \frac{2m'}{2n'} = \frac{m'}{n'}$ mit m' kleiner als m.
(5) Wir betrachten nun die Gleichung $2 = \frac{m^2}{n^2}$. Multiplikation mit n^2 ergibt $2n^2 = m^2$. Das heißt, m^2 ist eine gerade Zahl. Nach Beispiel 5b ist dann auch m eine gerade Zahl. Es sei etwa $m = 2k$ (mit k aus $\mathbb{N}$).
(6) Da m und n nach (4) nicht beides gerade Zahlen sind, muss n eine ungerade Zahl sein. Es sei etwa $n = 2\ell + 1$ (mit ℓ aus $\mathbb{N}$). Dann folgt, dass $m + n = 2 \cdot (k + \ell) + 1$ eine ungerade Zahl ist.
(7) Bestandsaufnahme: Wenn es eine rationale Zahl x mit $x^2 = 2$ gibt, dann gibt es natürliche Zahlen m, n mit $m + n$ ungerade und mit $m^2 = 2n^2$.
(8) Das ist allerdings ein Widerspruch zu der Aussage in Beispiel 5c.

[6] o.B.d.A. steht für „ohne Beschränkung der Allgemeinheit“

(9) Aufgrund dieses Widerspruchs muss die ursprüngliche Annahme, wonach eine rationale Zahl x mit $x^2 = 2$ existiert, fallen gelassen werden. Also ist das Gegenteil davon richtig, womit die Aussage des Satzes bewiesen ist.

□

6. Überlegungen zur elementaren Geometrie der Zahlen

a Nachdem wir nun etwas mit natürlichen, ganzen und rationalen Zahlen gerechnet haben, möchten wir Einiges zu deren geometrischen Bedeutung sagen. Dazu statten wir uns gedanklich mit Bleistift, Zirkel und Lineal aus.

(1) Beginnen wir mit der Zeichnung einer (horizontalen) Geraden g und einem Punkt P oberhalb dieser Geraden.[7] Wir fällen das Lot des Punktes P auf die Gerade und geben dem Lotpunkt die Bezeichnung 0. Die Gerade g bekommt nun die Bedeutung einer „Zahlengerade“ mit **Ursprung** 0 (auch Nullpunkt).

(2) Was wir weiter benötigen, ist eine „Einheitsstrecke“. Tragen wir diese mit dem Zirkel vom Nullpunkt aus (mehrfach) nach rechts ab, so erhalten wir, beginnend mit 1, gefolgt von $1+1=2$, gefolgt von

$$2+1=3, \quad 3+1=4, \quad 4+1=5, \quad \text{usw.}$$

diejenigen Markierungen auf g, die den natürlichen Zahlen entsprechen.

(3) Durch Spiegelung der natürlichen Zahlen am Nullpunkt erhalten wir die Zahlen $-n$ mit $n \in \mathbb{N}$, insgesamt dann also diejenigen Punkte auf g, die den ganzen Zahlen entsprechen.

(4) Um nun auch jeder (gebrochenen) positiven rationalen Zahl (also jeder „Verhältniszahl“) einen Punkt auf g zuweisen zu können, verwenden wir den **Strahlensatz** aus der Elementargeometrie: Es sei $n \in \mathbb{N}^*$.

- Zeichne eine weitere Gerade h (ungleich g) durch den Nullpunkt; trage auf der neuen Gerade, beginnend in 0 die Einheitsstrecken bis n ab.
- Verbinde n auf h mit 1 auf g und erhalte eine Gerade s.
- Konstruiere zu dieser Geraden s jeweils die Parallele durch die Punkte $1, 2, \ldots, n-1$ auf h.
- Nach dem Strahlensatz erhält man als Schnittpunkte dieser Parallelen mit der Gerade g die Teilungsverhältnisse $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$.

Durch entsprechendes Vervielfachen enthält man sodann diejenigen Markierungen auf g (rechts von 0) die den positiven rationalen Zahlen entsprechen: $\mathbb{Q}^+ = \{\frac{m}{n} : m, n \in \mathbb{Z}^+\}$.

(5) Durch Spiegelung der positiven rationalen Zahlen an 0 erhalten wir Markierungen (links von 0) für die negativen rationalen Zahlen. Insgesamt ist damit jede rationale Zahl q aus $\mathbb{Q}$ durch genau einen Punkt auf g dargestellt.

b Da man nun Strecken beliebig teilen kann (zumindest theoretisch), entsteht rein anschaulich der Eindruck, dass (umgekehrt) auch *jeder* Punkt der Zahlengerade g mit einer rationalen Zahl identifiziert ist. Das würde bedeuten, dass die Verhältniszahlen $\mathbb{Q}$ ausreichen, um jeden Ort in unserer Welt durch rationale Koordinaten zu beschreiben, so dass $\mathbb{Q}$ die Grundlage einer **Analytischen Geometrie** bilden würde. Dem ist aber nicht so, wie durch den folgenden Satz belegt wird.

Satz: *Es gibt wenigstens einen Punkt auf der Zahlengerade, der nicht durch eine rationale Zahl beschrieben werden kann.*

Beweis. Erinnern wir uns an den Punkt P, mit dem wir unseren Gedankengang in (1) begonnen haben. Betrachte nun die Gerade g' durch 0 und P; diese steht senkrecht auf g.

- Wir tragen die Einheitsstrecke vom Nullpunkt aus nach oben auf g' ab und erreichen einen Punkt i.
- Wir konstruieren die Parallele zu g durch i und tragen von i ausgehend nach rechts auf dieser Parallelen nochmals die Einheitsstrecke ab, um einen Punkt

[7] Tatsächlich zeichnen wir nur ein Streckenstück und denken uns dieses Stück nach *links* und *rechts* beliebig weit, also *unendlich* weit ausgedehnt.

$Q = (1|i)$ innerhalb der Ebene zu erreichen (es ist dies der Punkt mit den beiden Koordinaten 1 und i).

- Der Kreis um 0 mit Radiuslänge $\overline{0Q}$ schneidet die Gerade g rechts von 0 in einem Punkt X.

Anschaulich ist X diejenige positive Zahl, die dem *Abstand* von 0 zu X entspricht. Dies ist aber ebenfalls der Abstand von 0 zu Q, da Q und X ja auf einem Kreisrand mit Kreismittelpunkt 0 liegen, also gleichen Abstand zu 0 haben. Nach dem **Satz von Pythagoras** gilt nun

$$X^2 = \overline{01}^2 + \overline{1Q}^2 = 1^2 + 1^2 = 2.$$

Nach Satz 5d wird X *nicht* durch eine rationale Zahl beschrieben! □

c Vom Standpunkt der Zahlentheorie aus gesehen, drängt sich an dieser Stelle die Frage auf, welchem Zahlenbereich die Punkte einer Geraden (in diesem Zusammenhang auch **Kontinuum** genannt) eigentlich entsprechen? Die Antwort ist, dass dies genau die **reellen Zahlen** sind. Diese werden mit

$$\mathbb{R}$$

bezeichnet. $\mathbb{R}$ ist also das Kontinuum. Eine reelle Zahl, die nicht in $\mathbb{Q}$ liegt, heißt eine **irrationale Zahl**. Die oben konstruierte (eindeutige) irrationale Zahl x, die *rechts* von 0 liegt und $x^2 = 2$ erfüllt, wird mit $\sqrt{2}$ bezeichnet, sie heißt die **Quadratwurzel** von 2. Es gehört zu den Grundlagen der **Analysis**, die reellen Zahlen **axiomatisch** zu beschreiben und aus $\mathbb{Q}$ zu *konstruieren*. Dieses Thema werden wir allerdings erst zu Beginn der Vorlesung MfI-2 vertiefen.

d Es ist zu bemerken, dass es neben $\sqrt{2}$ noch viele weitere irrationale Zahlen gibt. Zu den wichtigsten gehören

- die *Kreiszahl* π, also die Maßzahl für den Flächinhalt eines Kreises mit Radius 1;
- die *Eulersche Zahl* e, also die Basis der natürlichen Logarithmusfunktion;
- die *Verhältniszahl des Goldenen Schnitts* $\tau = \frac{1+\sqrt{5}}{2} = 1,618....$

Mit e und π werden wir uns in MfI-2 eingehend beschäftigen.

e In der Tat gibt es *unendlich viele* irrationale Zahlen. Es ist sogar so, dass zwischen je zwei verschiedenen reellen Zahlen (egal wie dicht sie zusammenliegen) sowohl unendlich viele rationale als auch unendlich viele irrationale Zahlen liegen. Darauf werden wir u.a. in den Übungen zurückkommen. Insbesondere bedeutet dies, dass jede irrationale Zahl beliebig genau durch rationale Zahlen **approximiert** werden kann. Ist beispielsweise

$$y = \frac{1414213562}{1000000000} = \frac{707106781}{500000000},$$

so gilt (in Dezimalbruchschreibweise)

$$y^2 = 1,999999998944727844.$$

Von daher ist y eine gute Approximation für die eindeutige positive Lösung der Gleichung $x^2 = 2$, also von $\sqrt{2}$.

f Schließlich bemerken wir, dass es tatsächlich *wesentlich mehr* irrationale Zahlen als rationale Zahlen gibt: Während $\mathbb{Q}$ eine **abzählbare** Menge ist, handelt es sich bei $\mathbb{R}$ und bei $\mathbb{R} \setminus \mathbb{Q}$ um **überabzählbare** Mengen. Dies werden wir später präzisieren.

7. Zur Lösung reeller quadratischer Gleichungen

In diesem Abschnitt wollen wir an die aus der Schule bekannte Lösung von quadratischen Gleichungen erinnern.

a Das Ganze steht und fällt mit den folgenden für reelle Zahlen gültigen Sachverhalten, über die wir uns in MfI-2 Gedanken machen werden.

> *Ist r eine reelle Zahl, so gilt $r^2 \geq 0$; im Falle $r \neq 0$ ist r^2 positiv. Umgekehrt gibt es (im Gegensatz zu den rationalen Zahlen) zu jeder positiven reellen Zahl r eine eindeutige positive reelle Zahl s mit $s^2 = r$; diese Zahl s heißt die **Quadratwurzel** aus r und wird mit $\sqrt{r}$ bezeichnet.*

b Nun also zur Problemstellung: Gegeben seien reelle Zahlen a, b und c (die sog. **Koeffizienten** der quadratischen Gleichung). Gesucht sind alle reellen Zahlen r, welche die Gleichung „$ax^2+bx+c=0$“ erfüllen (x fungiert als **Variable**).

c Der Vollständigkeit halber machen wir zunächst eine ausführliche Fallunterscheidung hinsichtlich der Koeffizienten:

- Falls $a = 0$ und $b = 0$, so reduziert sich die Gleichung zu „$c = 0$“. Diese ist offenbar nicht erfüllbar, wenn $c \neq 0$. Im Gegendsatz dazu ist „$0 = 0$“ durch jede reelle Zahl r erfüllt.
- Falls $a = 0$ und $b \neq 0$, so reduziert sich „$ax^2 + bx + c = 0$“ zur **linearen Gleichung** „$bx + c = 0$“. Man gelangt hier durch Subtraktion von c und Division durch b zur einer eindeutigen Lösung, nämlich $-\frac{c}{b}$.
- Im schwierigsten (und interessantesten) Fall ist der Koeffizient a nicht gleich null, weshalb dann tatsächlich eine quadratische Gleichung vorliegt.

d Es sei also $a \neq 0$. Was nun folgt, bezeichnet man häufig als **Reduktion** (des allgemeinen Ausgangsproblems auf ein Kernproblem).

(1) Division durch a ergibt die äquivalente Gleichung „$x^2 + \beta x + \gamma = 0$“, wobei $\beta = \frac{b}{a}$ und $\gamma = \frac{c}{a}$. Man könnte also sagen „o.B.d.A. ist der Koeffizient a gleich 1“.

(2) Als Nächstes erinneren wie an die erste binomische Formel, „$(u+v)^2 = u^2+2uv+v^2$“, die man vor allen Dingen auch *von rechts nach links gelesen* anwenden muss. Für jede reelle Zahl r gilt

$$r^2 + \beta r + \gamma = (r + \tfrac{\beta}{2})^2 + \gamma - \tfrac{\beta^2}{4},$$

und deshalb ist die Gleichung „$x^2+\beta x+\gamma = 0$“ äquivalent zur Gleichung „$(x+\frac{\beta}{2})^2+\gamma-\frac{\beta^2}{4}=0$“ (man spricht bei diesem Übergang von einer **quadratischen Ergänzung**).

(3) Transformiert man nun x in die Variable y durch $y := x + \frac{\beta}{2}$ und setzt man $\delta := -\gamma + \frac{\beta^2}{4}$, so gelangt man zum Kernproblem, nämlich der Lösung der Gleichung „$y^2 = \delta$“, was insgesamt die Reduktion beendet.

e Aufgrund der eingangs gemachten Bemerkung wissen wir, dass die Gleichung „$y^2 = \delta$“ genau dann eine Lösung hat, wenn δ nicht-negativ ist, wenn also $\delta \geq 0$ gilt. Im Fall $\delta = 0$ ist $y = 0$ (trivialerweise) die einzige Lösung. Betrachten wir also den Fall $\delta > 0$. Es sei $\varepsilon := \sqrt{\delta}$. Nun verwenden wir die dritte binomische Formel, „$(u - v)(u + v) = u^2 - v^2$“, die man ebenfalls vor allem *von rechts nach links* lesen muss: Für jede reelle Zahl r mit $r^2 = \delta$ gilt

$$0 = r^2 - \delta = r^2 - \varepsilon^2 = (r - \varepsilon)(r + \varepsilon).$$

Da ein Produkt reeller Zahlen genau dann gleich null ist, wenn wenigstens ein Faktor gleich null ist (vgl. mit Beispiel 3g), bedeutet dies $r = \varepsilon$ oder $r = -\varepsilon$. Das heißt, wir erhalten in diesem Fall genau zwei (unterschiedliche) Lösungen, die positive Lösung ε und die negative Lösung $-\varepsilon$.

f Wenn man nun die Reduktion bzw. Transformation zurückverfolgt, so gelingt es, die beiden Lösungen in den ursprünglichen Parametern auszudrücken, also in einer Formel in den Koeffizienten a, b und c. Wir überlassen dies als kleine Übungsaufgabe und formlieren abschließend und zusammenfassend das Hauptergebnis:

Satz: *Gegeben seien die reellen Koeffizienten a, b und c, wobei $a \neq 0$. Davon ausgehend nennt man $\Delta := b^2-4ac$ die **Diskriminante** der Gleichung „$ax^2+bx+c=0$“. Hinsichtlich der reellen Lösbarkeit dieser Gleichung gilt Folgendes:*

(1) *Falls $\Delta < 0$, so hat die Gleichung keine Lösung in $\mathbb{R}$;*
(2) *falls $\Delta = 0$, so hat die Gleichung genau eine Lösung in $\mathbb{R}$, nämlich $x = -\frac{b}{2a}$*
(3) *falls $\Delta > 0$, so hat die Gleichung genau zwei verschiedene Lösungen in $\mathbb{R}$, nämlich $\frac{-b+\sqrt{\Delta}}{2a}$ und $\frac{-b-\sqrt{\Delta}}{2a}$.* □

8. **Logische Aussagen und deren Verknüpfungen**

Nachdem wir nun (hoffentlich) bereits ein gewisses Gespür für mathematische Beweise bekommen haben, wollen wir in diesem Abschnitt erläutern auf welchen Grundlagen die logischen Argumente basieren. Konkret geht es hier um die **Aussagenlogik**, die natürlich insbesondere für Informatiker von fundamentaler Bedeutung ist, weil sich nämlich die gesamte Schaltkreistechnik und somit die Computer-Architektur darauf begründet; Logische Aussagen und deren Verknüpfungen sind auch Bestandteil einer jeden Datenbankanfrage oder Internetsuche.

a Unter einer (logischen) Aussage versteht man formal ein Sprachobjekt A, welches einen von zwei möglichen Wahrheitswerten $\omega(A)$ annehmen kann:

- entweder $\omega(A) =$ `wahr` (engl.: *true*)
- oder $\omega(A) =$ `falsch` (engl.: *false*).

Da neben `wahr` und `falsch` keine weiteren Werte geduldet werden, spricht man vom **Prinzip des ausgeschlossenen Dritten** (lat.: tertium non datur). Sind beispielsweise X und Y die beiden Aussagen „7 ist eine gerade natürliche Zahl“ bzw. „6 ist eine gerade natürliche Zahl“, so gilt: $\omega(X) =$ `falsch` und $\omega(Y) =$ `wahr`. Im Folgenden lassen wir das Symbol ω einfach weg und schreiben abkürzend $X =$ `f` und $Y =$ `w`.

b Wie wir bereits in den ersten Abschnitten gesehen haben, treten Aussagen innerhalb der Mathematik unentwegt auf; beim Programmieren stößt man häufig auf bedingte Anweisungen der Form „*if* Bedingung erfüllt *then* ... *else* ... “, die sich je nach Wahrheitswert von „Bedingung erfüllt“ verzweigen. Beispielsweise liefert die nachstehende Anweisungsfolge[8] die Ausgabe $2, 3, 5, 7$:

for i *from* 1 *to* 10 *do*
    if i ist Primzahl
        then Ausgabe von i
    end-if
end-for

c In mathematischen Beweisen werden Aussagen meist zu (komplizierten) Ketten aneinander gereiht, siehe etwa der Irrationalitätsbeweis von $\sqrt{2}$ in Satz 5d. Wir müssen uns daher einen Überblick über die wichtigsten Verknüpfungen[9] von Aussagen verschaffen. Dabei hängen die Wahrheitswerte der zusammengesetzten Aussagen in eindeutiger Weise von den Wahrheitswerten der verknüpften Grundaussagen ab; sie werden hier mit Hilfe einer **Wahrheitstafel** berechnet bzw. definiert.

[8] Die hier verwendeten Beschreibungen für Algorithmen sind an die des Computer-Algebra-Systems *Maple* angelehnt. Wir werden dabei allerdings auch von der Freiheit Gebrauch machen, umgangssprachliche Formulierungen zu verwenden, damit die Sache nicht zu technisch wird. Insbesondere erheben wir keinen Anspruch, lauffähige Programme abzudrucken.

[9] auch **Junktoren** genannt

Definition: Im Folgenden seien A und B Aussagen.

(1) Die **Negation** der Aussage A ist die Aussage $\neg A$ (lies: *nicht* A). Die Aussage $\neg A$ ist `wahr`, wenn A `falsch` ist; sie ist `falsch`, wenn A `wahr` ist.

A	$\neg A$
w	f
f	w

(2) Die **Konjunktion** bzw. das **logische** `und` der Aussagen A und B ist die Aussage $A \wedge B$. Sie ist `wahr`, wenn sowohl A als auch B `wahr` sind; ansonsten ist sie `falsch`. In der Wahrheitstafel findet man entsprechend alle vier Kombinationen der Wahrheitswerte für das Paar (A, B) – siehe die Tabelle nach Punkt (4).

(3) Die **Disjunktion** bzw. das **logische** `oder` der Aussagen A und B ist die Aussage $A \vee B$. Sie ist `wahr`, wenn mindestens eine der beiden Aussagen `wahr` ist; ansonsten ist sie `falsch` – siehe die Tabelle nach Punkt (4).

(4) Die **Antivalenz** bzw. das `exklusive oder` entspricht dem umgangssprachlichen "entweder ... oder". Man verwendet dafür die Notation xor (Herkunft: e**x**clusive **or**).

A	B	$A \wedge B$	$A \vee B$	A xor B
w	w	w	w	f
w	f	f	w	w
f	w	f	w	w
f	f	f	f	f

(5) Die **Implikation** $A \Rightarrow B$ ist durch folgende Wahrheitstafel definiert:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

Sprechweisen sind: „A impliziert B" oder „wenn A gilt, so gilt auch B" oder „aus A folgt B" oder „A ist hinreichend für B" oder „B ist notwendig für A". Man nennt A die **Prämisse** oder die **Hypothese** oder die **Voraussetzung** für B und B die **Konklusion** oder die **Folgerung** aus A.[a]

(6) Man erhält die **Äquivalenz** $A \Leftrightarrow B$ zweier Aussagen A und B, wenn man deren Antivalenz negiert:

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

Man sagt auch, dass A und B **logisch gleichwertig** sind, bzw.: „A ist genau dann `wahr`, wenn B `wahr` ist".

[a] Auf den ersten Blick ist es gewöhnungsbedürftig, dass $A \Rightarrow B$ stets `wahr` ist, wenn A `falsch` ist. Das ist aber durchaus sinnvoll, weil man aus einer falschen Aussage keinerlei Information ziehen und damit alles Mögliche folgern kann.

9. Die drei grundlegenden Beweisprinzipien aus dem Blickwinkel der Aussagenlogik

Die im letzten Abschnitt besprochenen Verknüpfungen (bzw. Operatoren) von Aussagen sind Grundlage für die Bildung komplizierterer Aussagen. Häufig geht es dabei um den Nachweis der logischen Gleichwertigkeit zweier zusammengesetzter Aussagen. Wir wollen anhand von Beispielen u.a. demonstrieren, wie man den Vergleich mit Hilfe einer Wahrheitstafel durchführen kann. Dabei sind komplexe Aussagen sinnvollerweise in geeignete Einzelteile zu zerlegen.

a Wir beginnen mit der Äquivalenz.

Beispiel: Es seien A und B Aussagen. Wir zeigen, dass die beiden zusammengesetzten Aussagen $(A \Rightarrow B) \wedge (B \Rightarrow A)$ sowie $A \Leftrightarrow B$ logisch gleichwertig sind:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$	$A \Leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	w	f	f	f
f	f	w	w	w	w

Dieses Beispiel beinhaltet eine grundlegende Beweismethode! Es besagt nämlich, dass man die Äquivalenz zweier Aussagen durch den Nachweis der Implikation in beiden Richtungen erhält.

b Bei mathematischen Beweisen tritt als Grundbaustein innerhalb einer Argumentationskette die Implikation $\Rightarrow$ auf. Wir wollen im Weiteren anhand von Beispielen erörtern, mit welchen Ansätzen man den Wahrheitswert solcher Aussagen transferieren kann und beginnen dazu mit folgender Definition.

Definition: Ist eine zusammengesetzte Aussage stets `wahr`, unabhängig von der Belegung der Eingabe-Aussagen, so nennt man sie eine **Tautologie** oder eine **allgemeingültige Aussage**. Im Gegensatz dazu heißt eine zusammengesetzte Aussage, die stets den Wert `falsch` annimmt, eine **Kontradiktion** oder ein **Widerspruch**.

c

Beispiel: (Modus Ponens, direkter Beweis) Es sei C die aus den Aussagen A und B zusammengesetzte Aussage $(A \wedge (A \Rightarrow B)) \Rightarrow B$. Dann ist C eine Tautologie.

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$C = (A \wedge (A \Rightarrow B)) \Rightarrow B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

Fazit: Ist A wahr und zeigt man, dass $A \Rightarrow B$ wahr ist, so ist auch B wahr. Dieses Prinzip wird insbesondere beim **direkten Beweis** verwendet, und tritt dort meist in ganzen Ketten auf.

d

Beispiel: (Kontrapositionsgesetz, indirekter Beweis) Es sei C die aus den Aussagen A und B zusammengesetzte Aussage $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. Dann ist C eine Tautologie.

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$C = (A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
w	w	f	f	w	w	w
w	f	f	w	f	f	w
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Fazit: Gelingt einem nicht direkt der Nachweis von $A \Rightarrow B$, so kann man (**indirekt**) vom Gegenteil $\neg B$ ausgehen und versuchen auf $\neg A$ zu folgern (siehe Beispiel 5b).

e

Beispiel: (Widerspruchsbeweis) Es sei C die zusammengesetzte Aussage $(A \wedge (\neg B)) \Rightarrow$ `falsch`. Dann sind die beiden Aussagen $(A \Rightarrow B)$ und C äquivalent.

A	B	$\neg B$	$A \Rightarrow B$	$A \wedge (\neg B)$	$C = (A \wedge (\neg B)) \Rightarrow$ `falsch`
w	w	f	w	f	w
w	f	w	f	w	f
f	w	f	w	f	w
f	f	w	w	f	w

Fazit: Gelingt es einem, ausgehend von A, nicht, direkt $A \Rightarrow B$ zu zeigen, so nehme man $\neg B$ an und führe dies zu einer falschen Aussage (zu einem **Widerspruch**) (siehe etwa den Beweis zu Satz 5d).

10. Verknüpfungen von Mengen und deren Gesetzmäßigkeiten

An dieser Stelle bietet es sich an, unsere mengentheoretischen Grundlagen aus Abschnitt 3 etwas weiter auszubauen, denn bisher können wir (neben der Elementbeziehung) lediglich den Vergleich zweier Mengen anhand der Teilmengenbeziehung (insbesondere der Gleichheit) vorweisen. Es ist aber auch wichtig, aus zwei oder gar mehreren Mengen neue Mengen zu konstruieren, und deshalb besprechen wir in diesem Abschnitt die wichtigsten Verknüpfungen zwischen Mengen (bzw. **Mengenoperatoren**) und deren Gesetzmäßigkeiten.

a Wir wollen uns vorstellen, dass alle Mengen in einer gemeinsamen Grundmenge enthalten sind.

Definition: Es seien X und Y Mengen.

(1) Die **Schnittmenge** (bzw. der **Schnitt**) $X \cap Y$ ist die Menge der Elemente, die in X *und* in Y liegen: $X \cap Y := \{\alpha : \alpha \in X \text{ und } \alpha \in Y\}$

(2) Die **Vereinigungsmenge** (bzw. die **Vereinigung**) $X \cup Y$ von X mit Y ist die Menge der Elemente, die in X *oder* in Y liegen: $X \cup Y := \{\alpha : \alpha \in X \text{ oder } \alpha \in Y\}$

(3) Die **Mengendifferenz** $Y \setminus X := \{\alpha : \alpha \in Y, \alpha \notin X\}$ ist die Menge aller Objekte α, die in Y, aber nicht in X liegen.

(4) Die **symmetrische Differenz** $X \triangle Y$ von X mit Y ist die Menge der Elemente, die in X oder in Y, aber nicht gleichzeitig in X und Y liegen: $X \triangle Y := (X \cup Y) \setminus (X \cap Y)$. [a]

[a] An dieser Stelle sei daran erinnert, dass Terme innerhalb einer Klammer stets **höhere Priorität** haben, was bedeutet, dass die Verknüpfungen in den Klammern zuerst ausgeführt werden müssen.

b Betrachten wir ein konkretes Beispiel. Es seien $A_7 := \{a, b, c, d, e, f, g\}$ und $S := \{a, e, i, o, u\}$. Dann gelten:

$$\begin{array}{lcllcl} A_7 \cap S & = & \{a, e\} & = & & S \cap A_7 \\ A_7 \cup S & = & \{a, b, c, d, e, f, g, i, o, u\} & = & & S \cup A_7 \\ A_7 \triangle S & = & \{b, c, d, f, g, i, o, u\} & = & & S \triangle A_7 \\ A_7 \setminus S & = & \{b, c, d, f, g\}, & \neq & \{i, o, u\} & = \quad S \setminus A_7. \end{array}$$

c Man beachte, dass es sich bei „oder“ in Definition 10a-(2) um eine *mathematische* und *keine umgangssprachliche* Formulierung handelt, weshalb ein **logisches** `oder` gemeint ist. Mit dem **umgangssprachlichen *oder*** meint man häufig **entweder ... oder**. Mathematisch spricht man in diesem Fall vom **exklusiven** bzw. **ausschließenden oder**; die entsprechende Mengenoperation ist die symmetrische Differenz $\triangle$ aus Definition 10a-(3). Eine nützliche alternative Formel für die symmetrische Differenz ist

$$X \triangle Y = (X \setminus Y) \cup (Y \setminus X),$$

wie man sich leicht klar macht. Weiter ist zu erwähnen, dass bei einer Mengendifferenz $Y \setminus X$ die Menge X keine Teilmenge von Y sein muss. Stets gilt aber

$$Y \setminus X = Y \setminus (X \cap Y).$$

d Als ebenso nützliches wie selbstverständliches Hilfsresultat vermerken wir

Lemma: *Sind A und B Mengen, so gelten stets $A \cap B \subseteq A \subseteq A \cup B$ sowie $A \cap B \subseteq B \subseteq A \cup B$. Ist speziell A eine Teilmenge von B, so gelten ferner $A \cap B = A$ und $A \cup B = B$.* $\square$

e Wir wollen auf einen Spezialfall der Mengenvereinigung eingehen. Sind X und Y Mengen mit $X \cap Y = \emptyset$, so nennt man X und Y **disjunkt** bzw. **elementfremd**. Die Vereinigung disjunkter

Mengen X und Y nennt man entsprechend eine disjunkte Vereinigung, was häufig durch die Schreibweise $X \dot\cup Y$ gekennzeichnet wird. Betrachten wir hierzu zwei Beispiele.

(1) Ausgehend von den Mengen A_7 und S in 10b sind die Mengen $A_7 \setminus S$ und $S \setminus A_7$, wie oben gesehen nicht nur ungleich, sondern gewissermaßen total verschieden, nämlich disjunkt. Ferner ist deren disjunkte Vereinigung gleich $A_7 \triangle S$. Dieser Sachverhalt gilt auch noch, wenn A_7 und S durch allgemeine Mengen ersetzt werden, also kann man informativer

$$X \triangle Y = (X \setminus Y) \dot\cup (Y \setminus X)$$

schreiben.

(2) Die beiden Mengen $G := \{0, 2, 4, 6, ...\}$ und $U := \{1, 3, 5, 7, ...\}$ der geraden bzw. der ungeraden natürlichen Zahlen bilden eine disjunkte Zerlegung von $\mathbb{N}$, denn $G \cup U = \mathbb{N}$ und $G \cap U = \emptyset$ (jede natürliche Zahl ist entweder gerade oder ungerade).

f Im Folgenden Satz sind die wichtigsten Gesetzmäßigkeiten für Mengenverknüpfungen zusammengefasst. Neben den (binären) Verknüpfungen $\cap$ und $\cup$ brauchen wir allerdings noch die (unäre) Komplementbildung.

Definition: Wir gehen von einer Grundmenge M aus. Ist $X \subseteq M$, so heißt die Menge $X^c := M \setminus X$ das **(relative) Komplement** von X in M.

Satz: *Es seien X, Y und Z Teilmengen einer Grundmenge M. Dann gelten die folgenden Gesetze.*

(1) *a.* $Y \cap \emptyset = \emptyset$
b. $X \cup M = M$
c. $Y \cup \emptyset = Y$ *(die* **Neutralität** *von $\emptyset$ bzgl. $\cup$)*
d. $X \cap M = X$ *(die* **Neutralität** *von M bzgl. $\cap$)*
(2) **Idempotenz***:* $X \cap X = X$ *und* $X \cup X = X$
(3) **Komplementarität***:* $X \cap X^c = \emptyset$ *und* $X \cup X^c = M$
(4) **Kommutativität***:* $X \cap Y = Y \cap X$ *und* $X \cup Y = Y \cup X$
(5) **Assoziativität***:* $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ *und* $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
(6) **Distributivität***:* $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ *und*
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
(7) **Absorption***:* $X \cap (X \cup Y) = X$ *und* $X \cup (X \cap Y) = X$
(8) **Doppelte Komplementbildung***:* $(X^c)^c = X$
(9) **de Morgan**[a]*:* $(X \cap Y)^c = X^c \cup Y^c$ *und* $(X \cup Y)^c = X^c \cap Y^c$

[a] Augustus de Morgan (1806-1871)

Beweis. Die Aussagen (1), (2), (3), (4) und (8) folgen unmittelbar aus den entsprechenden Definitionen der Komplement-, der Schnitt- sowie der Vereinigungsbildung. Die Aussagen (5), (6), (7) und (9) sind hingegen nicht unbedingt offensichtlich und bedürfen daher einer näheren Erläuterung.

Manch einer wird sich an dieser Stelle vielleicht fragen, warum dann Aussagen wie (1), (2), (3), (4) und (8) überhaupt explizit aufgeführt werden, wenn deren Gültigkeit doch klar ist. Nun, es kommt in der Mathematik auch ganz entscheidend darauf an, immer wiederkehrende Muster und Gesetzmäßigkeiten aufzuspüren und herauszustellen. Das Kommutativgesetz oder das Assoziativgesetz kennt man beispielsweise bei der Addition bzw. bei der Multiplikation von Zahlen — Gleiches tritt also hier bei völlig anderen Verknüpfungen auf. Außerdem müssen wir uns zum gegenwärtigen Stand der Ausbildung auch mit einigen stilistischen Grundprinzipien der mathematischen Beweisführung vertraut machen. So wollen wir

zunächst die Gesetze (1), sowie (2) und (7) durch **Spezialisierung** mit Hilfe von Lemma 10d beweisen:

(1) Spezialisiert man in Lemma 10d zu $A := \emptyset$ und $B := Y$, so folgen (1a) und (1c) unmittelbar wegen $\emptyset \subseteq Y$. Entsprechend folgen (1b) und (1d) wegen $X \subseteq M$, wenn man $A := X$ und $B := M$ setzt.

(2) Wählt man $A := X$ und $B := X$, so erhält man aus Lemma 10d die Idempotenzgesetze.

(7) Spezialisiert man $A := X$ und $B := X \cup Y$ bzw. $A := X \cap Y$ und $B := X$, so erhält man aus Lemma 10d die Absorptionsgesetze.

Es bleibt somit der Nachweis der Aussagen (5) und (6) sowie von (9). Für einen rigorosen Beweis sind wir gezwungen, uns auf die Gleichheit zweier Mengen gemäß Definition 3e zu stützen. Wir werden exemplarisch das zweite Assoziativgesetz, das erste Distributivgesetz und das zweite de Morgan'sche Gesetz behandeln. Die anderen Gesetze ergeben sich durch völlig analoge Argumentationen.

(5) *Zweites Assoziativgesetz:* Zum Nachweis der Gleichheit der beiden Mengen $(X \cup Y) \cup Z$ und $X \cup (Y \cup Z)$ sind gemäß Definition 3e zwei Dinge erforderlich, nämlich

$$(X \cup Y) \cup Z \subseteq X \cup (Y \cup Z) \quad \text{sowie} \quad X \cup (Y \cup Z) \subseteq (X \cup Y) \cup Z.$$

Beginnen wir mit der ersten Mengeninklusion. Wir müssen zeigen, dass jedes Element aus der Menge $(X \cup Y) \cup Z$ auch Element der Menge $X \cup (Y \cup Z)$ ist. An dieser Stelle mag es einem vielleicht hinderlich vorkommen, dass wir eigentlich gar nichts über die Mengen X, Y und Z wissen, also unmöglich Übersicht über deren Elemente haben können. Nun, das ist nicht erforderlich und kann auch nicht erforderlich sein, weil es nämlich um ein allgemeingültiges Mengengesetz geht. Wir denken uns daher ein beliebiges Element aus der Menge $(X \cup Y) \cup Z$; damit wir wissen, worüber wir reden, geben wir diesem Element einen Namen, etwa a. Kurz: „Es sei $a \in (X \cup Y) \cup Z$."
Damit ist der Anfang des Beweises gemacht, und die restliche Argumentationskette kann ins Rollen kommen: Falls $a \in (X \cup Y) \cup Z$, so ist $a \in X \cup Y$ oder $a \in Z$. Machen wir also an dieser Stelle eine Fallunterscheidung.

- Falls $a \in Z$, so ist $a \in X \cup (Y \cup Z)$ wegen $Z \subseteq Y \cup Z \subseteq X \cup (Y \cup Z)$.
- Annahme $a \in X \cup Y$.
  - Falls $a \in X$, so ist $a \in X \cup (Y \cup Z)$ wegen $X \subseteq X \cup (Y \cup Z)$.
  - Ist $a \in Y$, so ist $a \in Y \cup Z$ und damit erst recht Element von $X \cup (Y \cup Z)$.

Innerhalb der Fallunterscheidung haben wir mehrfach auf Lemma 10d zurückgegriffen. Fazit: Egal welchen Weg der Verzweigung man auch nimmt, man gelangt stets zum gleichen Ergebnis, nämlich $a \in (X \cup Y) \cup Z$.
In der Tat ist damit der Beweis der Mengeninklusion $X \cup (Y \cup Z) \subseteq (X \cup Y) \cup Z$ bereits beendet, denn: a ist ein beliebiges Element aus $X \cup (Y \cup Z)$ gewesen und unterliegt daher keinerlei Einschränkung; die Beweiskette ist somit für jedes solche Element a gültig.
Zum Nachweis der umgekehrten Mengeninklusion kann man im Wesentlichen analog vorgehen. Dies wollen wir an dieser Stelle aber nicht tun. Stattdessen führen wir den Nachweis durch „Rückführung auf bereits bekannte Ergebnisse": Aufgrund der Kommutativität (siehe (4)) gilt zunächst $X \cup (Y \cup Z) = (Y \cup Z) \cup X = (Z \cup Y) \cup X$. Nun braucht man nur noch die Rollen von X und Z zu vertauschen, um die umgekehrte Inklusion aus der ersten (eben bereits bewiesenen) Mengeninklusion zu erhalten. Genauer gilt nach dem bereits Bewiesenen, dass $(Z \cup Y) \cup X \subseteq Z \cup (Y \cup X)$ ist. Letzteres ist aufgrund der Kommutativität von $\cup$ aber wieder gleich $(X \cup Y) \cup Z$.

(6) *Erstes Distributivgesetz:* Wir folgen dem selben Schema wie eben bei (5). Der Nachweis von $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ bedeutet $X \cap (Y \cup Z) \subseteq$

$(X \cap Y) \cup (X \cap Z)$ und umgekehrt $(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z)$. Zur ersten Mengeninklusion. Es sei $a \in X \cap (Y \cup Z)$ (beliebig). Dann gilt $a \in X$ und $a \in Y \cup Z$.

- Ist $a \in Y$, so ist $a \in X \cap Y$ und daher $a \in (X \cap Y) \cup (X \cap Z)$.
- Ist $a \in Z$, so ist $a \in X \cap Z$ und daher (erneut) $a \in (X \cap Y) \cup (X \cap Z)$.

Da a beliebig gewählt wurde, haben wir gezeigt, dass $X \cap (Y \cup Z)$ Teilmenge von $(X \cap Y) \cup (X \cap Z)$ ist.
Umgekehrt sei $b \in (X \cap Y) \cup (X \cap Z)$ (beliebig). Ist $b \in X \cap Y$, so liegt b in X und in $Y \cup Z$, also in $X \cap (Y \cup Z)$. Ist $b \in X \cap Z$, so liegt b erneut in X und in $Y \cup Z$, also in $X \cap (Y \cup Z)$. Damit ist $(X \cap Y) \cup (X \cap Z)$ Teilmenge von $X \cap (Y \cup Z)$, woraus insgesamt die Gleichheit der beiden Mengen folgt.

(9) *Zweites de Morgan'sches Gesetz:* Wir verfahren nach der mittlerweile eingeübten Methode.
Sei $a \in (X \cup Y)^c$, also $a \notin X \cup Y$. Dann ist $a \notin X$ und $a \notin Y$, also $a \in X^c \cap Y^c$. Es folgt $(X \cup Y)^c \subseteq X^c \cap Y^c$. Ist umgekehrt $b \in X^c \cap Y^c$, so ist $b \notin X$ und $b \notin Y$, so dass $b \notin X \cup Y$ gilt. Folglich ist $b \in (X \cup Y)^c$. Damit ist das zweite de Morgan'sche Gesetz bewiesen.

□

g Es ist zu bemerken, dass den Gesetzen bei Mengenverknüpfungen (abgesehen von (1) und (8)) das **Dualitätsprinzip** zugrunde liegt, d. h.: Vertauscht man in einem Gesetz die Operationen $\cap$ und $\cup$, so gelangt man zu einem weiteren Gesetz.

h Nach Einführung der Mächtigkeit einer Menge einerseits und Mengenverknüpfungen andererseits, sollte man auch über Gesetzmäßigkeiten bei der Verbindung dieser beiden Komponenten nachdenken. Dies wollen wir zum Abschluss dieses Abschnittes tun.

Satz: Es seien X und Y endliche Mengen. Dann gelten
(1) $|X \setminus Y| = |X| - |X \cap Y|$
(2) $|X \cup Y| = |X| + |Y| - |X \cap Y|$
(3) $|X \triangle Y| = |X| + |Y| - 2 \cdot |X \cap Y|$.

Beweis. (1) Die erste Aussage gilt wegen $X \setminus Y = X \setminus (X \cap Y)$ und $X \cap Y \subseteq X$.

(2) Die Aussage ist zunächst im Spezialfall richtig, wenn X und Y disjunkt sind, denn dann ist $|X \cap Y| = |\emptyset| = 0$ und $|X \cup Y| = |X| + |Y|$.

Das allgemeine Gesetz kann aber leicht auf diesen Spezialfall zurückgeführt werden. Sind also X und Y allgemeine endliche Mengen (disjunkt oder auch nicht), so gilt zunächst $X \cup Y = X \cup (Y \setminus X)$. Letzteres, also $X \cup (Y \setminus X)$ ist aber eine disjunkte Vereinigung. Also folgt, unter Verwendung von (1) im letzten Schritt (mit vertauschten Rollen bei X und Y),

$$|X \cup Y| = |X \cup (Y \setminus X)| = |X| + |Y \setminus X| = |X| + |Y| - |X \cap Y|.$$

(3) Es ist $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$. Eine Anwendung von (1) liefert daher $|X \triangle Y| = |X \cup Y| - |X \cap Y|$. Einsetzen von $|X \cup Y|$ aus (2) ergibt dann die Behauptung.

Alternativ kann man auch von der Formel $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$ ausgehen. Die dabei auftretende Vereinigung ist disjunkt. Also folgt

$$|X \triangle Y| = |X \setminus Y| + |Y \setminus X|.$$

Zweifache Anwendung von (1) liefert dann erneut $|X \triangle Y| = |X| - |X \cap Y| + |Y| - |X \cap Y| = |X| + |Y| - 2 \cdot |X \cap Y|$. □

11. Gesetzmäßigkeiten bei der Verknüpfung von logischen Aussagen

a Anhand der letzten beiden Abschnitte ist festzustellen, dass dem Verknüpfen von Aussagen ähnliche strukturelle Eigenschaften zugrunde liegen wie bei den Mengenoperationen. In der Tat kann man (ähnlich wie in den Beispielen 9a bis 9e mit Hilfe von Wahrheitstafeln) Folgendes zeigen.

Satz: *Sind in Satz 10f die Objekte X, Y und Z Aussagen, so erhält man in (1)-(9) stets Tautologien, wenn man folgende Übersetzungen vornimmt:*

Mengenlehre	$\emptyset$	M	$\cap$	$\cup$	^{c}	$=$
Aussagenlehre	$\mathtt{f}$	$\mathtt{w}$	$\wedge$	$\vee$	$\neg$	$\Leftrightarrow$

Im Einzelnen gilt Folgendes:

(1) *a.* $Y \wedge \mathtt{f} \Leftrightarrow \mathtt{f}$
b. $X \vee \mathtt{w} \Leftrightarrow \mathtt{w}$
c. $Y \vee \mathtt{f} \Leftrightarrow Y$ *(***Neutralität** *von* $\mathtt{f}$ *bzgl.* $\vee$*)*
d. $X \wedge \mathtt{w} \Leftrightarrow X$ *(***Neutralität** *von* $\mathtt{w}$ *bzgl.* $\wedge$*)*
(2) **Idempotenz***:* $X \wedge X \Leftrightarrow X$ *und* $X \vee X \Leftrightarrow X$
(3) **Komplementarität***:* $(X \wedge \neg X) \Leftrightarrow \mathtt{f}$ *und* $(X \vee \neg X) \Leftrightarrow \mathtt{w}$
(4) **Kommutativität***:* $X \wedge Y \Leftrightarrow Y \wedge X$ *und* $X \vee Y \Leftrightarrow Y \vee X$
(5) **Assoziativität***:* $(X \wedge Y) \wedge Z \Leftrightarrow X \wedge (Y \wedge Z)$ *und* $(X \vee Y) \vee Z \Leftrightarrow X \vee (Y \vee Z)$
(6) **Distributivität***:* $X \wedge (Y \vee Z) \Leftrightarrow (X \wedge Y) \vee (X \wedge Z)$ *und*
$X \vee (Y \wedge Z) \Leftrightarrow (X \vee Y) \wedge (X \vee Z)$
(7) **Absorption***:* $X \wedge (X \vee Y) \Leftrightarrow X$ *und* $X \vee (X \wedge Y) \Leftrightarrow X$
(8) **Doppelte Negation***:* $\neg(\neg X) \Leftrightarrow X$
(9) **de Morgan***:* $\neg(X \wedge Y) \Leftrightarrow (\neg X) \vee (\neg Y)$ *und* $\neg(X \vee Y) \Leftrightarrow (\neg X) \wedge (\neg Y)$ □

b Es ist an dieser Stelle bemerkenswert, dass die gemeinsame zugrunde liegende Struktur

- einerseits einer **Mengenalgebra** mit binären Operatoren $\cap$ und $\cup$, mit unärem Operator ^{c} und mit Konstanten $\emptyset$ und M und
- andererseits einer **Aussagenalgebra** mit binären Operatoren $\wedge$ und $\vee$, mit unärem Operator $\neg$ und mit Konstanten $\mathtt{f}$ und $\mathtt{w}$

die einer sog. **Boole[10]'schen Algebra** ist. Es ist daher nicht mehr verwunderlich, dass auch in der Aussagenlogik das **Dualitätsprinzip** zugrunde liegt: Vertauscht man in einem Gesetz (mit Ausnahme von (1) und (8)) die Operationen $\vee$ und $\wedge$, so gelangt man zu einem weiteren Gesetz.

c Wir wollen abschließend erwähnen, dass man alle aussagenlogischen Formeln, welche die Operationen $\vee, \wedge, \neg, \Rightarrow$ und $\Leftrightarrow$ beinhalten, stets durch äquivalente Aussagen ersetzen kann, die lediglich die beiden Verknüpfungen $\neg$ und $\vee$ enthalten. Dies kann folgendermaßen begründet werden:

(1) $A \wedge B$ ist gleichwertig zu $\neg(\neg A \vee \neg B)$ (siehe de Morgan).
(2) $A \Rightarrow B$ ist gleichwertig zu $\neg A \vee B$.
(3) Schließlich ist, unter Verwendung von (2), $A \Leftrightarrow B$ logisch gleichwertig zu $(\neg A \vee B) \wedge (\neg B \vee A)$ und wegen (1) somit auch gleichwertig zu $\neg((\neg(\neg A \vee B)) \vee (\neg(\neg B \vee A)))$.

Auf analoge Weise kann man jede aussagenlogische Formel in $\wedge$ und $\neg$ ausdrücken. Dies ist insofern von praktischem Interesse, als man sich bei der Theorie logischer Schaltkreise auf die Realisierung von nur zwei Bausteinen beschränken kann.

d In der Tat kommt man sogar mit der Verwendung eines *einzigen* Operators aus: Die sog. **Sheffer-Operation** $\uparrow$ (auch **Exklusion** genannt) ist durch $A \uparrow B := \neg(A \wedge B)$ definiert. Deshalb ist $A \uparrow A$ logisch gleichwertig zu $\neg A$, und $A \wedge B$ ist gleichwertig zu $(A \uparrow B) \uparrow (A \uparrow B)$, denn

$$(A \uparrow B) \uparrow (A \uparrow B) \Leftrightarrow \neg(A \uparrow B) \Leftrightarrow \neg(\neg(A \wedge B)) \Leftrightarrow A \wedge B.$$

[10] George Boole (1815-1864)

Dies hat eine wichtige Anwendung in der „Hardware“, wo entsprechende Bausteine als `NAND`-Gatter bekannt sind.

12. **Potenzmengen und kartesische Produkte**

In diesem Abschnitt betrachten wir zwei weitere wichtige Konstruktionsformen von Mengen.

a Wir beginnen mit der Potenzmenge einer Menge.

> **Definition:** Ist M eine Menge, so ist die **Potenzmenge** $\mathcal{P}(M)$ von M als die Menge aller Teilmengen von M definiert: $\mathcal{P}(M) := \{U : U \subseteq M\}$

b Beispielsweise ist $\mathcal{P}(\emptyset) = \{\emptyset\}$, weshalb $|\mathcal{P}(\emptyset)| = 1$ gilt. Die Potenzmenge von $\{a, b, c\}$ ist

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Sie besteht insgesamt aus 8 Elementen. Wir werden später den folgenden Satz beweisen:

> **Satz:** Ist M eine endliche Menge, so hat deren Potenzmenge die Mächtigkeit $2^{|M|}$.

c Mengen, deren Elemente selbst wieder Mengen sind, sind nichts Außergewöhnliches in der Mathematik. Allerdings muss vor allzu sorglosen Mengenbildungen gewarnt werden, da diese zu Widersprüchen oder sog. **Antinomien** führen können. Nach dem Logiker Bertrand Russel (1872-1970) führt beispielsweise die „Menge“ *R aller Mengen, die sich nicht selbst als Element enthalten* zu einem Widerspruch. Wäre R wirklich eine Menge, so müsste man anhand der definierenden Eigenschaft von R feststellen können, ob R selbst Element von R ist oder nicht. Es stellt sich aufgrund der Beschreibung von R aber heraus, dass „$R \in R$ genau dann gilt, wenn $R \notin R$ gilt“, ein Widerspruch. Bei R kann es sich demnach unmöglich um eine Menge handeln!

Den entsprechenden Sachverhalt kann man sich leicht am sog. **Barbier von Sevilla** veranschaulichen: Der Barbier von Sevilla rasiert genau diejenigen in Sevilla lebenden Männer, die sich nicht selbst rasieren. Man betrachtet nun die Gesamtheit S aller in Sevilla lebenden Männer, die vom Barbier rasiert werden. Wäre S eine Menge, so folgte, dass der Barbier selbst genau dann zu S gehört, wenn er nicht zu S gehört! Daher kann S keine Menge sein.

Die Disziplin der **axiomatischen Mengenlehre** weist einen Weg aus diesem Dilemma, indem gerade eine allzu willkürliche „Zusammenfassung von bestimmten, wohlunterscheidbaren Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“ verboten wird.

d Ist M eine Menge und ist $\mathcal{S}$ eine Teilmenge von $\mathcal{P}(M)$, so ist also $\mathcal{S}$ eine Menge, deren Elemente Teilmengen von M sind. Man nennt $\mathcal{S}$ daher auch ein Mengensystem über M. Die Partitionen sind spezielle Mengensysteme, die recht häufig, nämlich bei Abbildungen und Äquivalenzrelationen (siehe spätere Abschnitte) auftreten.

> **Definition:** Es sei $\mathcal{S} \subseteq \mathcal{P}(M)$ ein Mengensystem über der Grundmenge M.
>
> (1) Falls je zwei verschiedene Elemente U und V von $\mathcal{S}$ disjunkt sind, so nennt man $\mathcal{S}$ ein **disjunktes Mengensystem**.[a]
>
> (2) Eine **Partition von** M ist ein disjunktes Mengensystem $\mathcal{S}$ über M mit der Eigenschaft, dass jedes Element x aus M in einer (und damit in **genau** einer) Menge von $\mathcal{S}$ enthalten ist. Statt Partition sagt man auch **Zerlegung**.[b]
>
> [a] In diesem Fall sagt man, dass die Elemente von $\mathcal{S}$ **paarweise disjunkt** sind.
>
> [b] Meist ist es sinnvoll zu verlangen, dass die leere Menge nicht Element einer Partition sein soll.

e Betrachten wir beispielsweise die Grundmenge $M = \{1, 2, 3, 4, 5\}$ sowie die drei Mengensysteme $\mathcal{R} := \{\{1\}, \{1, 2, 3\}, \{3, 4\}, \{2, 4, 5\}\}$ und $\mathcal{S} := \{\{2, 4\}, \{3\}, \{5\}\}$ sowie $\mathcal{T} := \{\{1, 3\}, \{4\}, \{2, 5\}\}$.

Dann ist $\mathcal{R}$ keine Partition von M, da $\mathcal{R}$ nicht einmal ein disjunktes Mengensystem ist, wie man an $\{1,2,3\} \cap \{3,4\} = \{3\} \neq \emptyset$ sieht. Das Mengensystem $\mathcal{S}$ ist zwar disjunkt, allerdings keine Partition von M, weil das Element 1 von M in keiner der Mengen aus $\mathcal{S}$ enthalten ist. Das Mengensystem $\mathcal{T}$ ist hingegen eine Partition von M. Jedes Element aus M liegt in genau einer Menge aus $\mathcal{T}$.

f Die Bildung des kartesischen Produktes zweier Mengen ist eine Konstruktion, die zu einer Vielzahl weiterer mathematischer Grundbegriffe führt.

Definition: Es seien M und N zwei Mengen.

(1) Ist $\alpha \in M$ und $\beta \in N$, so nennt man das Objekt (α, β) ein **geordnetes Paar** (kurz: *Paar*) mit **erster Komponente** α und **zweiter Komponente** β.

(2) Das **kartesische Produkt** $M \times N$ ist als die Menge aller geordneten Paare (α, β) mit $\alpha \in M$ und $\beta \in N$ definiert:

$$M \times N := \{(\alpha, \beta) : \alpha \in M,\ \beta \in N\}$$

Im Falle $N = M$ schreibt man auch M^2 für $M \times M$.

(3) Zwei Paare (a_1, a_2) und (b_1, b_2) (mit $a_1, b_1 \in M$ und $a_2, b_2 \in N$) heißen **gleich**, wenn $a_1 = b_1$ und $a_2 = b_2$ gilt. □

g Beispielsweise ist das kartesische Produkt $\{a, b, c\} \times \{0, 1, 2\}$ die Menge mit den neun Elementen $(a,0)$, $(a,1)$, $(a,2)$, $(b,0)$, $(b,1)$, $(b,2)$, $(c,0)$, $(c,1)$, $(c,2)$. Die 32 Karten eines Kartenspiels entsprechen dem kartesischen Produkt `Farbe` × `Wertigkeit`, wobei `Farbe`:= $\{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$ und `Wertigkeit`:= {7, 8, 9, 10, Bube, Dame, König, Ass}.

h Diese einfachen Beispiele weisen bereits auf den folgenden kombinatorischen Sachverhalt hin, den man an **Baumdiagrammen** sehr einfach verdeutlichen kann.

Satz: *Sind M und N endliche Mengen mit $|M| = m$ und $|N| = n$ Elementen, so gilt $|M \times N| = m \cdot n$.*

Beweis. Die Aussage ist richtig, wenn M oder N leer ist, da dann keine Paare gebildet werden können. Sind M und N jeweils nicht leer, so hat man für die Wahl der ersten Komponente α eines Paares (α, β) genau $m = |M|$ Möglichkeiten. Nachdem die Wahl der ersten Komponente getroffen ist, hat man **jeweils** $n = |N|$ Möglichkeiten zur Wahl der zweiten Komponente. Insgesamt ergeben sich daher $m \cdot n$ Möglichkeiten der Paarbildung. □

13. **Summen und Produkte**

Wir haben in den Abschnitten 8 und 10 Verknüpfungen bei Mengen und Aussagen kennengelernt. Dabei werden zunächst einmal **zwei** Objekte miteinander verknüpft. Bei vielen Rechnungen werden aber sukzessive meist **mehrere** Objekte miteinander verknüpft, weshalb man in der Mathematik zur Abkürzung bei mehrfachen Anwendungen ein und derselben Verknüpfung entsprechende Symbole eingeführt hat. Mit den geläufigsten dieser Symbole wollen wir uns im Folgenden beschäftigen.

a Wir beginnen in diesem Abschnitt mit den **arithmetischen Operationen** $+$ (Addition) und $\cdot$ (Multiplikation) bei Zahlen. Gegeben seien n Zahlen x_1, $x_2, ..., x_n$.

- Für die Summe $x_1 + x_2 + ... + x_n$ dieser Zahlen schreibt man $\sum_{i=1}^{n} x_i$,
- für deren Produkt $x_1 \cdot x_2 \cdot ... \cdot x_n$ schreibt man $\prod_{i=1}^{n} x_i$.

Der **Index** i fungiert hierbei als **Laufvariable** (von $i = 1$ bis $i = n$), wie man es von der Programmierung mit *for*-Schleifen her kennt. Betrachten wir einige Beispiele.

- Es seien $n = 8$ und $x_i = i$ für $i = 1, ..., 8$. Dann gilt $\sum_{i=1}^{8} x_i = 1+2+3+4+5+6+7+8 = 36$ und $\prod_{i=1}^{8} x_i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40320$.
- Nun seien $n = 7$ und $x_j = 2j - 1$ für $j = 1, ..., 7$. Dann gilt $\sum_{j=1}^{7} x_j = 1 + 3 + 5 + 7 + 9 + 11 + 13 = 49$, sowie $\prod_{j=1}^{7} x_j = 1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13 = 135135$.

b Der Bereich, welcher von der Laufvariablen durchlaufen wird, heißt die zugrunde liegende **Indexmenge**. Sie ist in den obigen beiden Beispielen von der Form $\{1, 2, ..., n\}$. Man sollte sich aber gleich daran gewöhnen, dass Indexmengen häufig anders und komplizierter aussehen. Dazu ein weiteres Beispiel.

- Für $i \in \mathbb{N}$ sei $x_i := 2i + 1$ (die i-te ungerade Zahl). Mit $I := \{0, 2, 9, 21, 300\}$ ist dann $\sum_{i \in I} x_i = x_0 + x_2 + x_9 + x_{21} + x_{300} = 1 + 5 + 19 + 43 + 601 = 669$.

c Mitunter ist nicht von vornherein klar, in welcher Reihenfolge die Elemente einer Indexmenge durchlaufen werden. Bei endlichen Mengen ist die Reihenfolge glücklicherweise irrelevant, da in Zahlbereichen wie $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder auch $\mathbb{R}$ bzgl. $+$ und $\cdot$ das Kommutativgesetz gilt. Gleiches gilt für die Mengenoperatoren $\cup$ und $\cap$, wie wir aus Abschnitt 10 wissen.

- Als konkretes Beispiel betrachten wir die folgende Tabelle:

	1	2	3
1	14	12	0
2	1	3	9
3	2	2	17

  Für $i, j \in \{1, 2, 3\}$ sei $X_{i,j}$ der Eintrag der Tabelle, der in Zeile i und Spalte j steht. Ist T die Menge aller Indizes (i, j), mit der man auf einen Tabelleneintrag zugreifen kann, also $T = \{1, 2, 3\}^2$, so beschreibt $\sum_{(i,j) \in T} X_{i,j}$ die Summe über alle Einträge der Tabelle (unabhängig davon, ob etwa zeilenweise oder spaltenweise summiert wird) – das Ergebnis ist gleich 60.

  Will man ein kartesisches Produkt, wie die Menge T, als Indexmenge vermeiden, so könnte man beispielsweise $Y_i := \sum_{j=1}^{3} X_{i,j}$ setzen (für $i = 1, 2, 3$) und erhält dann zunächst die drei Zeilensummen Y_1, Y_2 und Y_3. Sodann ist

$$\sum_{(i,j) \in T} X_{i,j} = \sum_{i=1}^{3} Y_i = 26 + 13 + 21 = 60.$$

  Das entspricht aber letztendlich dem Auswerten einer sog. Doppelsumme, nämlich

$$\sum_{i=1}^{3} \left(\sum_{j=1}^{3} X_{i,j} \right).$$

d Wir diskutieren nun die wichtigsten Grundregeln für das Rechnen mit Summen und Produkten.

(1) Ist $c \in \mathbb{R}$ und ist $x_i = c \in \mathbb{R}$ konstant für jedes $i = 1, ..., n$, so gilt

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} c = c^n, \text{ entsprechend ist } \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} c = nc.$$

Ist allgemeiner I eine beliebige nicht-leere und endliche Indexmenge und ist $x_i = c \in \mathbb{R}$ konstant für jedes $i \in I$, so gilt

$$\prod_{i \in I} x_i = c^{|I|}, \text{ entsprechend ist } \sum_{i \in I} x_i = |I| \cdot c.$$

(2) Es sei I eine nicht-leere Indexmenge. Ferner seien x_i sowie y_i für jedes $i \in I$ reelle Zahlen. Ebenso seien c und d reelle Zahlen. Dann gilt

$$\sum_{i \in I} (cx_i + dy_i) = c \cdot \sum_{i \in I} x_i + d \cdot \sum_{i \in I} y_i.$$

Entsprechend gilt bei der Produktbildung (für sinnvolle Basen x_i bzw. y_i sowie Exponenten c und d)

$$\prod_{i \in I} (x_i^c y_i^d) = \left(\prod_{i \in I} x_i \right)^c \cdot \left(\prod_{i \in I} y_i \right)^d.$$

(3) Ist die Indexmenge I eine disjunkte Vereinigung zweier endlicher Mengen I_1 und I_2, so gilt

$$\sum_{i \in I} x_i = \sum_{a \in I_1} x_a + \sum_{b \in I_2} x_b, \text{ entsprechend ist } \prod_{i \in I} x_i = \prod_{a \in I_1} x_a \cdot \prod_{b \in I_2} x_b.$$

Insbesondere spricht man in der Situation, wo $I_2 = \{s\}$ einelementig ist von der **Isolation eines Summanden bzw. eines Faktors**:

$$\sum_{i \in I} x_i = \sum_{j \in I_1} x_j \ + \ x_s \quad \text{bzw.} \quad \prod_{i \in I} x_i = \prod_{j \in I_1} x_j \ \cdot \ x_s$$

(4) Ist die Indexmenge I gleich dem kartesischen Produkt $I_1 \times I_2$ zweier endlicher Mengen I_1 und I_2, so gilt wie in Beispiel 13d (Stichwort **Doppelsumme**):

$$\sum_{(i,j) \in I} x_{i,j} = \sum_{i \in I_1} \left(\sum_{j \in I_2} x_{i,j} \right) = \sum_{j \in I_2} \left(\sum_{i \in I_1} x_{i,j} \right)$$

Analoges gilt bei der Produktbildung.

e Abschließend ein

Beispiel: Wir wollen zeigen, dass für jede positive natürliche Zahl n Folgendes gilt:

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

Beweis. Dazu geben wir einen direkten Beweis, der auf Carl Friedrich Gauß (1777-1855) zurückgeht. Es sei n zunächst eine gerade Zahl, etwa $n = 2m$. Die $2m$ Summanden aus der Summe

$$\sum_{i=1}^{2m} i = 1 + 2 + 3 + ... + m + (m+1) + ... + (2m-1) + 2m$$

fügt man nun paarweise wie folgt zusammen: erster und letzter Term zu $[1 + 2m]$; zweiter und vorletzter Term zu $[2 + (2m - 1)]$; ...; m-ter und m-letzter Term zu $[m + (m + 1)]$. Allgemein wird (für $i = 1, ..., m$) der i-te Summand mit dem $(2m-i+1)$-sten Summanden zu $i+2m-i+1$ zusammengefügt, was gleich $2m+1$,

also unabhängig von i ist! Das entspricht insgesamt gesehen einer Umsortierung der Summanden, so dass wir mit $2m = n$ daraus

$$\sum_{i=1}^{n} i = \sum_{i=1}^{m}(i + 2m - i + 1) = \sum_{i=1}^{m}(2m + 1) = \sum_{i=1}^{m}(n + 1)$$

erhalten. Innerhalb der letzten Summe handelt es sich bei $n + 1$ aber um einen konstanten Summanden, so dass obige erste Regel in diesem Fall

$$\sum_{i=1}^{m}(n + 1) = m(n + 1) = \frac{n}{2}(n + 1)$$

ergibt, was der Behauptung für ein gerades n entspricht. Falls n ungerade ist, so gibt es ein $k \in \mathbb{N}$ mit $n = 2k + 1$. Sodann erhält man durch Isolierung des letzten Summanden $n = 2k + 1$ die Formel

$$\sum_{i=1}^{n} i = \sum_{i=1}^{2k+1} i = \sum_{i=1}^{2k} i \quad + \quad (2k + 1).$$

Diese Isolierung des letzten Summanden entspricht der Zerlegung der gesamten Indexmenge in $\{1, 2, ..., 2k\}$ und $\{2k + 1\}$ (siehe dazu die obige dritte Regel in 13d). Nach dem bereits für gerade natürliche Zahlen Gezeigten ist aber

$$\sum_{i=1}^{2k} i = \frac{2k}{2}(2k + 1) = k(2k + 1) = kn$$

und somit $\sum_{i=1}^{n} i = kn + n = (k + 1)n$. Aus $n = 2k + 1$ folgt aber $k + 1 = \frac{n-1}{2} + 1 = \frac{n+1}{2}$ und somit erhält man im ungeraden Fall insgesamt ebenfalls $\sum_{i=1}^{n} i = \frac{n+1}{2} \cdot n$. □

14. **Verknüpfungen von mehreren Mengen**

a Analog zum Summen- $\sum$ und zum Produktzeichen $\prod$ verwendet man für den Durchschnitt bzw. die Vereinigung von mehreren (endlich vielen) Mengen M_1, ..., M_n die Schreibweisen

$$\bigcap_{i=1}^{n} M_i \quad \text{bzw.} \quad \bigcup_{i=1}^{n} M_i.$$

b Der folgende Sachverhalt wird in der Kombinatorik die **Summenregel** genannt. Der Beweis erfordert das Prinzip der vollständigen Induktion und wird später erbracht.

Satz: *Es seien $M_1, M_2, ..., M_n$ paarweise disjunkte, endliche Menge Dann ist die Mächtigkeit von deren Vereinigung gleich der Summe der Mächtigkeiten der einzelnen Mengen:*

$$\left| \bigcup_{i=1}^{n} M_i \right| = \sum_{i=1}^{n} |M_i|$$

c Wir betrachten nun die Bildung kartesischer Produkte aus mehreren (aber endlich vielen) Mengen.

Definition: Es sei $n \in \mathbb{N}$ mit $n \geq 2$, und $M_1, ..., M_n$ seien n Mengen.

(1) Jedes Objekt der Form $(a_1, ..., a_n)$ mit $a_1 \in M_1$, ..., $a_n \in M_n$ heißt ein **(geordnetes) n-Tupel**. Für jedes $i \in \{1, 2, ..., n\}$ nennt man dabei a_i die **i-te Komponente**. Der Einfachheit halber schreibt man für das n-Tupel $(a_1, ..., a_n)$ häufig einfach a; auf seine k-te Komponente greift man mit a_k zu.
(2) Das **kartesische Produkt** $M_1 \times ... \times M_n$ ist die Menge aller solcher n-Tupeln.
(3) Zwei n-Tupel a und b heißen **gleich**, wenn $a_i = b_i$ für alle Komponenten i gilt.

Entsprechend der bereits eingeführten abkürzenden Notationen bei Summen, Produkten, Vereinigungen und Schnitten ist

$$\times_{i=1}^{n} M_i$$

eine Kurzschreibweise für das kartesische Produkt der Mengen $M_1, ..., M_n$. Gilt speziell $M_i = M$ für jedes i, so schreibt man einfach M^n für $\times_{i=1}^{n} M$ es handelt sich dabei um **das n-fache kartesische Produkt von M mit sich selbst**.

c

Beispiel: Eine Münze habe die beiden Seiten „Kopf“ und „Zahl“; in einem Eimer mögen zwei rote, drei gelbe, vier grüne und ein schwarzer Ball liegen; weiterhin sei ein Würfel gegeben. Ein Zufallsexperiment bestehe nun aus der Hintereinanderausführung von „einem Münzwurf, einem Ziehen eines Balles aus dem Eimer und einmaliges Würfeln“. Das Ergebnis des Experimentes ist dann ein Element aus dem kartesischen Produkt {Kopf, Zahl} $\times$ {rot, gelb, grün, schwarz} $\times$ $\{1, 2, 3, 4, 5, 6\}$. Die gesamte Anzahl aller möglichen Versuchsausgänge ist hierbei gleich $2 \cdot 4 \cdot 6 = 48$. □

d Der folgende Sachverhalt wird in der Kombinatorik als **Produktregel** bezeichnet. Der Beweis erfordert (zumindest) das Prinzip der vollständigen Induktion und wird später erbracht.

Satz: *Sind $M_1, ..., M_n$ endliche Mengen, so ist die Mächtigkeit von deren kartesischem Produkt gleich dem Produkt der Mächtigkeiten der einzelnen Mengen:*

$$|\times_{i=1}^{n} M_i| = \prod_{i=1}^{n} |M_i|$$

15. **Verknüpfungen bei beliebigen Indexmengen und Quantoren**

Im vergangenen Abschnitt haben wir bei der Bildung mehrfacher Verknüpfungen stets **endliche** Indexmengen betrachtet. Wir wollen diese Voraussetzung hier fallen lassen und mitunter (völlig) **beliebige** Indexmengen zulassen.

a Bei Grenzprozessen, welche später im Rahmen der Analysis behandelt werden, hat man es oft mit der Summation von **unendlich** vielen Zahlen zu tun. Beispielsweise versteht man unter

$$\sum_{n\in\mathbb{N}} \left(\tfrac{1}{3}\right)^n \quad \text{bzw.} \quad \sum_{n=0}^{\infty} \left(\tfrac{1}{3}\right)^n \quad \text{bzw.} \quad 1+\tfrac{1}{3}+\tfrac{1}{9}+\tfrac{1}{27}+\tfrac{1}{81}+\ldots$$

die Summation über alle Potenzen des Bruches $\frac{1}{3}$. In der Analysis erlernt man Methoden zur Berechnung der Werte solcher Summen; in diesem Zusammenhang spricht man allerdings von Reihen. So hat beispielsweise obige Reihe, es handelt sich um eine sog. **geometrische Reihe**, den Wert $\frac{3}{2}$. Es ist allerdings auch möglich, dass eine Summation über unendlich viele Zahlen keinen endlichen Wert liefert; so ist etwa die **harmonische Reihe**

$$\sum_{n=1}^{\infty} \tfrac{1}{n} = 1+\tfrac{1}{2}+\tfrac{1}{3}+\tfrac{1}{4}+\tfrac{1}{5}+\ldots$$

unbeschränkt, d. h., dass man für jede Zahl x ein $m\in\mathbb{N}$ findet mit $\sum_{n=1}^{m}\frac{1}{n} > x$. Dies fasst man so zusammen: $\sum_{n=1}^{\infty}\frac{1}{n}=\infty$.

b Bei mengentheoretischen und aussagenlogischen Verknüpfungen ist es durchaus sinnvoll, beliebige Indexmengen zuzulassen. Dies wollen wir im weiteren Verlauf dieses Abschnittes näher erklären. Bei Mengen stellen wir uns wieder vor, dass sich alles innerhalb einer gemeinsamen Grundmenge abspielt.

Definition: Es sei I eine nicht-leere Indexmenge. Für jedes $i\in I$ sei M_i eine Menge. Dann sind die beiden Mengen $\bigcap_{i\in I} M_i$ und $\bigcup_{i\in I} M_i$ definiert durch

(1) $\bigcap_{i\in I} M_i := \{x:\ x \text{ liegt in } \textbf{jeder} \text{ Menge } M_i\}$,
(2) $\bigcup_{i\in I} M_i := \{x:\ x \text{ liegt in } \textbf{mindestens einer} \text{ Menge } M_i\}$.

c In Definition 15d werden wir gleich die Analogien der beliebigen Vereinigungs- bzw. Durchschnittsbildung innerhalb der Aussagenlogik betrachten. Zunächst wollen wir aber erörtern, was bei der Komplementbildung von beliebigen Schnitten bzw. beliebigen Vereinigungen passiert. Die de Morgan'schen Gesetze aus Satz 10f-(9) lassen sich nämlich allgemeiner wie folgt formulieren.

Satz: *Es sei I eine nicht-leere Indexmenge. Für jedes $i\in I$ sei M_i eine Menge. Dann gelten*

$$\left(\bigcap_{i\in I} M_i\right)^c = \bigcup_{i\in I} M_i^c \qquad \textit{und} \qquad \left(\bigcup_{i\in I} M_i\right)^c = \bigcap_{i\in I} M_i^c.$$

Beweis. Wir wollen nur das erste Gesetz beweisen. Der Nachweis des zweiten sei als Übung gestellt. Ist $x\in\left(\bigcap_{i\in I} M_i\right)^c$, so gilt $x\notin\bigcap_{i\in I} M_i$. Daher gibt es (mindestens) einen Index j mit $x\notin M_j$, also mit $x\in M_j^c$. Folglich ist x in $\bigcup_{i\in I} M_i^c$ enthalten, womit, aufgrund der beliebigen Wahl von x, die Mengeninklusion $\left(\bigcap_{i\in I} M_i\right)^c\subseteq\bigcup_{i\in I} M_i^c$ bewiesen ist. Zur Umkehrung: Ist $x\in\bigcup_{i\in I} M_i^c$, so gibt es einen Index k mit $x\in M_k^c$, also $x\notin M_k$. Daher liegt x nicht in $\bigcap_{i\in I} M_i$. Folglich ist x Element von $\left(\bigcap_{i\in I} M_i\right)^c$. Da x wieder beliebig aus $\bigcup_{i\in I} M_i^c$ gewählt

wurde, ist auch die umgekehrte Mengeninklusion, und damit die Gleichheit der beiden Mengen gezeigt. □

d Bei der Beweismethode der vollständigen Induktion (Abschntt 16) treten sog. **Prädikate** über den natürlichen Zahlen auf. Ein solches Prädikat P liefert für jedes $n \in \mathbb{N}$ eine Aussage $P(n)$, beispielsweise

$$P(n) \quad = \quad „ \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} “.$$

Die vollständige Induktion ist eine elegante Methode, um die Wahrheit von **allen** (oder zumindest von **fast allen**) Aussagen der Form $Q(n)$ für ein Prädikat Q zu zeigen. Um nun die Sprachgebilde „für alle“ (bzw. „für jedes“) und „es gibt ein“ (bzw. „es existiert ein“) zu modellieren führt man in der Logik die so genannten **Quantoren** $\forall$ (für alle) und $\exists$ (es gibt) ein. Anstelle von $\mathbb{N}$ darf natürlich auch eine beliebige Indexmenge verwendet werden.

Definition: Es sei I eine nicht-leere Indexmenge und $Q(i)$ sei für jedes $i \in I$ eine Aussage.

(1) Dann bezeichnet $B := \forall_{i \in I} Q(i)$ die Aussage „**für alle** $i \in I$ gilt $Q(i)$“. Das bedeutet, dass B genau dann wahr ist, wenn **(ausnahmslos) alle** $Q(i)$ wahr sind.

(2) Es bezeichnet $C := \exists_{i \in I} Q(i)$ die Aussage „**es gibt** ein $j \in I$, so dass $Q(j)$ wahr ist“. Das bedeutet, dass C genau dann wahr ist, wenn **mindestens ein** $Q(j)$ wahr ist.

Man nennt $\forall$ den **Allquantor** und $\exists$ den **Existenzquantor**.

e Betrachten wir uns diese Quantoren einmal im Zusammenhang mit den verallgemeinerten de Morgan'schen Gesetzen in Satz 15c. Dazu seien B und C wie in Definition 15d.

- Die Negation der Aussage C ist gleichwertig zu $\forall_{\ell \in I} \neg Q(\ell)$, denn dann ist $Q(\ell)$ für kein ℓ erfüllt.
- Will man zeigen, dass $\neg B$ gilt, so genügt es **ein Gegenbeispiel** anzugeben, d. h. ein j zu bestimmen, für das $\neg Q(j)$ gilt, denn die Negation von B ist logisch gleichwertig zu $\exists_{k \in I} \neg Q(k)$.

f Betrachten wir zum letzten Punkt ein konkretes **Beispiel:**

Für jedes $k \in \mathbb{N}$ sei $Q(k)$ die Aussage „$2^{2^k} + 1$ ist eine Primzahl“. Die Tatsache

k	$2^{2^k} + 1$	Primzahl?
0	3	ja
1	5	ja
2	17	ja
3	257	ja
4	65537	ja

empfand Pierre de Fermat (1601-1665) als ausreichende Evidenz für seine Vermutung, dass $B = \forall_{k \in \mathbb{N}} Q(k)$ wahr ist, welche er im Jahre 1637 aufstellte. Nun fand Leonhard Euler im Jahre 1732 aber heraus, dass $2^{2^5} + 1$ wegen

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

keine Primzahl und damit $Q(5)$ falsch ist. Daher ist auch B, also Fermats Vermutung, falsch! — Ein Gegenbeispiel genügt eben zum Kippen einer „für alle-Aussage“.

16. **Das Prinzip der vollständigen Induktion**

a Wir beginnen mit der sog. **natürlichen Ordnung** $\leq$ („kleiner gleich“) auf der Menge $\mathbb{N}$ der natürlichen Zahlen, die wie folgt definiert ist:

$$a \leq b :\Leftrightarrow \exists_{n\in\mathbb{N}}\ (a+n=b)$$

In Worten: die natürliche Zahl a ist definitionsgemäß kleiner oder gleich der natürlichen Zahl b, falls eine natürliche Zahl n mit $a+n=b$ existiert.[11]

b Ist M eine nicht-leere Teilmenge von $\mathbb{N}$, so heißt $c \in M$ ein **kleinstes Element** bzw. ein **Minimum** von M, falls $c \leq x$ für jedes $x \in M$ gilt. Die sog. **Wohlordnungseigenschaft**, auf der das Prinzip der vollständigen Induktion beruht, besagt Folgendes:

> *Jede nicht-leere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.*

Man sagt dazu auch, dass $\mathbb{N}$ bzgl. $\leq$ **wohlgeordnet** ist bzw. dass $\leq$ eine **Wohlordnung** auf $\mathbb{N}$ ist.

c Da wir von Kindesbeinen an mit dem Umgang der natürlichen Zahlen vertraut sind, erscheint die Wohlordnungseigenschaft als eine Selbstverständlichkeit. „Eine nicht-leere Teilmenge der natürlichen Zahlen muss schließlich einen *Anfang* haben“. Wir wollen daher anhand eines konkreten Beispiels die Stärke dieses Prinzips erläutern. Zuvor ist noch zu bemerken, dass das kleinste Element von $M \subseteq \mathbb{N}$ eindeutig bestimmt ist und im Folgenden mit $\min(M)$ bezeichnet wird.

Beispiel: Wir werden mit diesem Beispiel demonstrieren, wie man durch die Kombination der **Wohlordnungseigenschaft** mit einem **Widerspruchsbeweis** zeigen kann, dass für jedes $n \in \mathbb{N}$ die Gleichung

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

gültig ist.

Beweis. Es sei dazu N die Menge der natürlichen Zahlen n, für die diese Gleichung zutrifft:

$$N := \left\{ n \in \mathbb{N} : \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \right\}$$

Wir werden zeigen, dass $N = \mathbb{N}$ gilt. Es bezeichne $M := \mathbb{N}\backslash N$ das Komplement von N in $\mathbb{N}$. Annahme, $N \neq \mathbb{N}$. Dann ist M eine nicht-leere Menge. Somit impliziert die Wohlordnungseigenschaft, dass M ein kleinstes Element hat; dieses nennen wir t. Da $n=0$ die obige Gleichung erfüllt, denn $\sum_{k=0}^{0} k^2 = 0^2 = 0$ und $\frac{0\cdot(0+1)\cdot(2\cdot 0+1)}{6} = 0$, gilt $0 \in N$ und damit $0 \notin M$, weshalb $t = \min(M)$ größer als 0, also positiv ist. Folglich ist $t-1 \in \mathbb{N}$. Da t nun aber das kleinste Element von M ist, folgt $t-1 \in N = \mathbb{N} \setminus M$, weshalb die Gleichung $\sum_{k=0}^{t-1} k^2 = \frac{[t-1]([t-1]+1)(2[t-1]+1)}{6}$ gemäß Definition von N erfüllt ist. Für die Summation der natürlichen Zahlen bis einschließlich der Zahl t ergibt sich dann aber

$$\sum_{k=0}^{t} k^2 = \sum_{k=0}^{t-1} k^2 + t^2 = \frac{[t-1]([t-1]+1)(2[t-1]+1)}{6} + t^2.$$

(Im ersten Schritt wurde der letzte Summand t isoliert, um im zweiten Schritt die Summe wegen $t-1 \in N$ vereinfachen zu können.) Den Term der rechten Seite

[11] Der Doppelpunkt vor $\Leftrightarrow$ bedeutet, dass die linke Aussage per Definition logisch gleichwertig zur rechten Aussage ist.

vereinfacht man nun leicht zu

$$\frac{(t-1)t(2t-1)}{6}+t^2=\frac{2t^3-3t^2+t+6t^2}{6}=\frac{2t^3+3t^2+t}{6}=\frac{t(t+1)(2t+1)}{6},$$

so dass insgesamt $\sum_{k=0}^{t} k^2=\frac{t(t+1)(2t+1)}{6}$, also $t\in N$ folgt. Das widerspricht aber der Eigenschaft $t\in M=\mathbb{N}\setminus N$. Wir müssen daher die Annahme, dass $N\neq\mathbb{N}$ ist, fallen lassen und erhalten $N=\mathbb{N}$. □

d Die vollständige Induktion liefert eine Methode, mit der man Formeln wie aus dem letzten Beispiel oder auch kompliziertere Formeln wie

$$\sum_{k=0}^{n} k^3=\frac{n^2(n+1)^2}{4}$$

direkt nachzuweisen kann. Sie beruht auf dem folgenden Satz, dem wir eine Definition voranstellen.

Definition: Ist $n\in\mathbb{N}$, so heißt $\mathrm{succ}(n):=n+1$ der **Nachfolger**[a] von n.

[a] engl.: *successor*

Satz: *Ist M eine Teilmenge von $\mathbb{N}$ mit den folgenden beiden Eigenschaften*

(1) $0\in M$,
(2) *aus $n\in M$ folgt* $\mathrm{succ}(n)\in M$,

so gilt $M=\mathbb{N}$.

Beweis. Ist dies nicht der Fall, so ist die Komplementmenge $M^c:=\mathbb{N}\setminus M$ nicht leer. Es sei m das kleinste Element von M^c. Dann ist $m\neq 0$, da ja $0\in M$. Insofern ist $m-1$ eine natürliche Zahl. Diese liegt nicht in M^c, da $m-1<m$ und m das kleinste Element von M^c ist. Aus $m-1\in M$ folgt dann aber $m=(m-1)+1=\mathrm{succ}(m-1)\in M$. Das ist ein Widerspruch. □

e Wir formulieren die Aussage des letzten Satzes nun etwas um.

Satz: (Induktionsprinzip) *Für jedes n aus $\mathbb{N}$ sei $P(n)$ eine Aussage. Angenommen, es gelten:*

(1) **Induktionsanfang (IA)***: $P(0)=$* `wahr`.
(2) **Induktionsschritt (IS)***: Aus* $\boxed{P(m)=\texttt{wahr}}$ *folgt $P(m+1)=$* `wahr`.

Dann gilt $P(n)=$ `wahr` *für jedes $n\in\mathbb{N}$.* □

Anstelle von Induktionsanfang sagt man häufig auch **Induktionsverankerung**. Die eingekastelte Bedingung nennt man die **Induktionsvoraussetzung (IV)**.

f Bisweilen ist es so, dass eine Aussage bzw. ein Prädikat nicht für jede natürliche Zahl erfüllt ist, sondern lediglich für **fast alle** natürlichen Zahlen. Das bedeutet „für alle natürlichen Zahlen bis auf höchstens endliche viele Ausnahmen“ (siehe etwa Beispiel 17e im kommenden Abschnitt). Dies erfordert eine etwas flexiblere Handhabung des Induktionsprinzips.

Satz: (Induktionsprinzip) *Für jedes n aus $\mathbb{N}$ sei $P(n)$ eine Aussage. Angenommen, es gibt eine konkrete Zahl $n_0 \in \mathbb{N}$, für die man die beiden folgenden Eigenschaften nachweisen kann.*

(1) **Induktionsanfang (IA)***: Es ist $P(n_0) =$* `wahr`*.*

(2) **Induktionsschritt (IS)***: Ist $\boxed{m \geq n_0 \text{ beliebig mit } P(m) = \texttt{wahr}}$, so folgt, dass auch $P(m+1) =$* `wahr` *ist.*

Dann ist $P(n) =$ `wahr` *für jedes $n \geq n_0$.*

g Eine weitere Flexibilisierung ergibt sich, wenn man die Gültigkeit von $P(m+1)$ nicht aus dem direkten Vorgänger $P(m)$ sondern durch ein $P(n)$ mit $n \leq m$ folgert. Dann liest sich dieses Prinzip wie folgt:

Satz: (Induktionsprinzip) *Für jedes n aus $\mathbb{N}$ sei $Q(n)$ eine Aussage. Angenommen, es gibt eine konkrete Zahl $n_0 \in \mathbb{N}$, für die man die beiden folgenden Eigenschaften nachweisen kann.*

(1) **Induktionsanfang (IA)***: Es ist $Q(n_0) =$* `wahr`*.*

(2) **Induktionsschritt (IS)***: Ist*
$\boxed{m \geq n_0 \text{ beliebig und gilt } Q(k) = \texttt{wahr} \text{ für alle } k \text{ mit } n_0 \leq k \leq m}$,
so folgt, dass auch $Q(m+1) =$ `wahr` *ist.*

Dann ist $Q(n) =$ `wahr` *für jedes $n \geq n_0$.*

Beweis. Zum Beweis führt man die Aussage dieses Satzes auf die von Satz 16f zurück. Für $n \in \mathbb{N}$ mit $n \geq n_0$ sei dazu $P(n)$ die Aussage $\forall_{n_0 \leq k \leq n} Q(k)$.

Dann gilt $P(n_0) = Q(n_0)$. Bei Gültigkeit der Induktionsverankerung ist daher $P(n_0) =$ `wahr` wenn $Q(n_0) =$ `wahr` ist.

Es sei nun $m \geq n_0$ beliebig und es folge $Q(m+1) =$ `wahr`, falls $Q(k) =$ `wahr` **für alle** k mit $n_0 \leq k \leq m$, d.h., es folgt $Q(m+1) =$ `wahr`, falls $P(m) =$ `wahr`. Dann gilt $Q(k) =$ `wahr` **für alle** k mit $n_0 \leq k \leq m+1$, also $P(m+1) =$ `wahr`. Insgesamt entspricht dies genau dem Nachweis des Induktionsschrittes von m nach $m+1$ gemäß Satz 16f für das Prädikat P. Folglich gilt auch die Konklusion von Satz 16f, wonach $P(n)$ für alle $n \geq n_0$ wahr ist. Aufgrund der Definition von P ist dann aber auch $Q(n)$ für alle $n \geq n_0$ wahr, was zu zeigen war. □

17. **Beispiele zur vollständigen Induktion**

Das Verfahren der vollständigen Induktion verinnerlicht man sich am besten durch Betrachten von Beispielen und eigenes Üben. Wir wollen daher eine Fülle von Beispielen studieren, die das Phänomen der vollständigen Induktion in seiner Vielseitigkeit deutlich machen.

a

Beispiel: Wir werden mit vollständiger Induktion nachweisen, dass **die Summe der ersten** n **ungeraden Zahlen** gleich n^2 ist. Zur Formalisierung setzen wir für n aus $\mathbb{N}^*$ zunächst $u(n) := 2n-1$ sowie

$$S_u(n) := \sum_{k=1}^{n} u(k) = \sum_{k=1}^{n} (2k-1).$$

Dann ist beispielsweise $u(1) = 1$ und $u(2) = 3$ und $u(3) = 5$, woran man sieht, dass $u(n)$ die n-te ungerade Zahl ist. Ferner ist $S_u(n)$ dann die Summe der ersten n ungeraden Zahlen, und wir wollen beweisen, dass $S_u(n) = n^2$ für alle $n \in \mathbb{N}^*$ gilt.

Beweis. In der Tat ist $S_u(1) = 1 = 1^2$ und $S_u(2) = 1+3 = 4 = 2^2$ und $S_u(3) = 1+3+5 = 9 = 3^2$, was unser Vertrauen in diese Aussage stärkt.

(1) Induktionsverankerung: Es ist $S_u(n_0) = n_0^2$ für $n_0 = 1$.

(2) Induktionsschritt: Annahme, es gilt $S_u(m) = m^2$ für ein beliebiges $m \geq n_0 = 1$. Zum Vollzug des Induktionsschrittes müssen wir beweisen, dass dann auch $S_u(\mathrm{succ}(m)) = \mathrm{succ}(m)^2$ gilt, bzw. $S_u(m+1) = (m+1)^2$. Durch Isolierung des letzten Summanden erhält man zunächst einmal

$$S_u(m+1) = \sum_{k=1}^{m+1} u(k) = \sum_{k=1}^{m} u(k) + u(m+1) = S_u(m) + u(m+1).$$

Nun verwendet man die Induktionsannahme $S_u(m) = m^2$ und erhält durch Einsetzen: $S_u(m+1) = m^2 + u(m+1)$. Weiter ist $u(m+1) = 2(m+1)-1 = 2m+1$. Insgesamt ergibt sich also dann mit der aus der Schule bekannten ersten binomischen Formel:

$$S_u(m+1) = m^2 + 2m + 1 = (m+1)^2$$

Nach dem Prinzip der vollständigen Induktion ist damit $S_u(n) = n^2$ für alle $n \geq n_0 = 1$ bewiesen. □

b Um das Rechnen mit Summen weiter zu festigen, wollen wir an dieser Stelle kurz demonstrieren, wie man die Gleichung $\sum_{k=1}^{n}(2k-1) = n^2$ unter Verwendung der Formel $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ auch direkt nachweisen kann. Zunächst gilt

$$\sum_{k=1}^{n}(2k-1) = 2 \cdot \sum_{k=1}^{n} k - \sum_{k=1}^{n} 1,$$

und dies ist nach Beispiel 13e gleich

$$2 \cdot \tfrac{n(n+1)}{2} - n = n(n+1) - n = n^2.$$

c

Beispiel: Für $n \in \mathbb{N}^*$ bezeichne $v(n)$ den größten ungeraden Teiler von n. Beispielsweise ist $v(1) = 1$ und $v(8) = 1$ und $v(12) = 3$. Ist n ungerade, so ist $v(n) = n$; ist n gerade, etwa $n = 2m$, so ist der größte ungerade Teiler von n gleich dem größten ungeraden Teiler von m, also $v(n) = v(m)$. Damit ist klar, wie man die Zahl $v(n)$ für ein konkretes n bestimmt: Man dividiert n solange durch 2, bis man eine ungerade Zahl k erhält; dieses k ist dann gleich $v(n)$. Beispielsweise ist $v(10000) = 625$, denn

$$v(10000) = v(5000) = v(2500) = v(1250) = v(625) = 625.$$

Nun aber zum eigentlichen Problem. Für $n \in \mathbb{N}^*$ definieren wir die Größe $\sigma_v(n)$ durch

$$\sigma_v(n) := \sum_{k=1}^{2^n} v(k).$$

Man beachte unbedingt, dass die Summation bis 2^n geht! Es geht also um die Summation der größten ungeraden Teiler der ersten 2^n Zahlen aus $\mathbb{N}^*$. Beispielsweise ist $\sigma_v(1) = v(1) + v(2) = 2$ und $\sigma_v(2) = v(1) + v(2) + v(3) + v(4) = 6$ und $\sigma_v(3) = v(1) + ... + v(8) = 22$. Wir behaupten nun, dass Folgendes gilt:

$$\sigma_v(n) = \frac{4^n + 2}{3} \text{ für jedes } n \in \mathbb{N}^*$$

Wie man auf diese Formel kommt ist eine andere Geschichte; wir beschäftigen uns hier lediglich mit dem Nachweis der Formel.

Beweis. Den Beweis führt man mit vollständiger Induktion, wobei hier $n_0 = 1$ zu wählen ist.

(1) Induktionsanfang: Es gilt $\frac{4^1+2}{3} = \frac{6}{3} = 2 = \sigma_v(1)$.

2a. Induktionsvoraussetzung: Für ein beliebiges $m \geq 1$ gelte $\sigma_v(m) = \frac{4^m+2}{3}$.

2b. Induktionsschluss: Wir betrachten $\sigma_v(\text{succ}(m)) = \sigma_v(m+1)$ und müssen nachweisen, dass dies gleich $\frac{4^{\text{succ}(m)}+2}{3} = \frac{4^{m+1}+2}{3}$ ist. Die Grundidee dazu ist, ähnlich zum Vorgehen in Beispiel 17a, die Gesamtsumme in zwei Teile zu zerlegen, um die Induktionssannahme ins Spiel zu bringen. So gilt

$$\sigma_v(m+1) = \sum_{k=1}^{2^{m+1}} v(k) = \sum_{k=1}^{2^m} v(k) + \sum_{k=2^m+1}^{2^{m+1}} v(k) = \sigma_v(m) + \sum_{k=2^m+1}^{2^{m+1}} v(k).$$

Das Einsetzen der Induktionsannahme liefert dann $\sigma_v(m+1) = \frac{4^m+2}{3} + \sum_{k=2^m+1}^{2^{m+1}} v(k)$. Beim Weiterrechnen wird man aber feststellen, dass die Behandlung des resultierenden Summenterms zu unübersichtlich wird, weshalb man sich eingestehen muss, dass obige Zurückführung auf die Induktionsannahme nichts bringt ...

Betrachten wir daher nochmals die Indexmengen, über die summiert wird. Zur Formalisierung sei für jedes $\ell \in \mathbb{N}$ die Menge I_ℓ definiert durch $I_\ell := \{1, 2, ..., 2^\ell\}$. Dann ist also

$$\sigma_v(m+1) = \sum_{k \in I_{m+1}} v(k).$$

Wir zerlegen jetzt I_{m+1} in die disjunkten Teilmengen $G := \{2, 4, 6, ..., 2^{m+1}\}$ der geraden und $U := \{1, 3, 5, ..., 2^{m+1}-1\}$ der ungerade Zahlen. Dann zerlegt sich die gesamte Summe entsprechend wie folgt:

$$\sigma_v(m+1) = \sum_{k \in G} v(k) + \sum_{k \in U} v(k)$$

Beim ersten (gescheiterten) Ansatz wurde die Partition $\{I_m, \{2^m+1, 2^m+2, ..., 2^{m+1}\}\}$ von I_{m+1} betrachtet, nun verwenden wir stattdessen die Partition $\{G, U\}$ von I_{m+1}. Weiter sieht man unmittelbar, dass $\{2\ell : \ell \in I_m\} = G$ und $\{2\ell - 1 : \ell \in I_m\} = U$ alternative Beschreibungen für die Mengen G und U sind. Daher können wir die letzte Formel auch als

$$\sigma_v(m+1) = \sum_{\ell \in I_m} v(2\ell) + \sum_{\ell \in I_m} v(2\ell - 1)$$

schreiben. Aufgrund der eingangs gemachten Bemerkungen über v, nämlich $v(2\ell) = v(\ell)$ und $v(2\ell - 1) = 2\ell - 1$ (da $2\ell - 1$ ungerade), lässt sich das zu

$$\sigma_v(m+1) = \sum_{\ell \in I_m} v(\ell) + \sum_{\ell \in I_m} (2\ell - 1)$$

vereinfachen. Die erste Summe, also $\sum_{\ell \in I_m} v(\ell)$, ist nun aber gerade gleich $\sigma_v(m)$, was nach Induktionsannahme gleich $\frac{4^m+2}{3}$ ist. Bei der zweiten Summe werden die ersten 2^m ungeraden Zahlen aufsummiert – dies ist ein Problem, welches wir bereits gelöst haben! Nach Beispiel 17a ist die zweite Summe nämlich gleich $S_u(2^m) = (2^m)^2 = 2^{2m} = 4^m$. Wir erhalten daher insgesamt

$$\sigma_v(m+1) = \frac{4^m+2}{3} + 4^m = \frac{4^m+2+3\cdot 4^m}{3} = \frac{4^{m+1}+2}{3},$$

womit der Induktionsschluss vollzogen ist.

□

d Wir fahren mit zwei weiteren Beispielen zur vollständigen Induktion fort. Beim ersten Beispiel handelt es sich um eine induktive Definition; beim zweiten Beispiel demonstrieren wir, wie schwierig ein Induktionsanfang sei kann.

Beispiel: Wir definieren die **Fakultätsfunktion** ! auf $\mathbb{N}$. Dazu sei $0! := 1$ und, wenn $n!$ bereits bekannt ist, so sei $\mathrm{succ}(n)! := \mathrm{succ}(n) \cdot n!$, also $(n+1)! := (n+1) \cdot n!$. Gemäß vollständiger Induktion ist dann $m!$ (lies: m**-Fakultät**) in der Tat für alle $m \in \mathbb{N}$ definiert. Diese Form der Definition nennt man eine **rekursive Definition**. Es ist klar, dass $n! = \prod_{k=1}^{n} k$ ist (für $n \geq 1$).

e

Beispiel: Es sei $b \in \mathbb{N}^*$; zunächst sei b beliebig, später werden wir exemplarisch den Fall $b = 7$ betrachten. Wir wollen die Ungleichung $n! \geq b^n$ untersuchen. Das Ziel ist es zu zeigen, dass die Menge $M_b := \{n \in \mathbb{N}^* : n! \geq b^n\}$ **fast alle** natürlichen Zahlen enthält, was definitionsgemäß bedeutet, dass $\mathbb{N} \setminus M_b$ eine **endliche** Menge ist. Dazu bietet sich wieder die vollständige Induktion an.

(1) Induktionsverankerung: Hierzu benötigen wir eine konkreten Startwert n_0. Wir werden gleich sehen, dass es alles andere als einfach ist, einen solchen Startwert zu finden, und arbeiten zunächst einmal unter der Annahme, dass es ein $n_0 \in M_b$ mit $n_0 \geq b$ gibt.
(2) Induktionsschritt: Aus $m \geq n_0$ mit $m \in M_b$ (also $m! \geq b^m$) folgt dann wegen $m+1 > m \geq n_0 \geq b$ (also $m+1 > b$) sofort

$$(m+1)! = (m+1) \cdot m! > b \cdot m! \geq b \cdot b^m = b^{m+1},$$

so dass dann auch $m+1$ in M_b enthalten ist.

Zusammenfassend können wir sagen:

- Wenn es uns gelingt, ein $n_0 \geq b$ anzugeben, welches in M_b liegt, so ist das Endstück $\{x \in \mathbb{N} : x \geq n_0\}$ ganz in M_b enthalten und daher $\mathbb{N} \setminus M_b \subseteq \mathbb{N} \setminus \{x \in \mathbb{N} : x \geq n_0\} \subseteq \{0, 1, ..., n_0 - 1\}$ eine endliche Menge.
- Wenn es uns hingegen nicht gelingt, ein $n_0 \geq b$ in M_b zu finden, so könnte als andere Alternative auch $M_b \subseteq \{0, 1, ..., b-1\}$ gelten, so dass M_b eine endliche Menge wäre.

Die Handhabung des Induktionsanfangs entscheidet hier also über die beiden äußerst extremen Alternativen „$n! \geq b^n$ für fast alle n“ und „$n! \geq b^n$ für nur endlich viele n“. Dieses Beispiel demonstriert damit einerseits, dass der Induktionsschluss relativ einfach, ja fast schon trivial zu bewältigen ist und dass ein Großteil der Arbeit in den Induktionsanfang investiert werden muss. Keinesfalls darf auf den Induktionsanfang verzichtet werden!

Wie steht es nun mit dem Induktionsanfang? Wir machen uns für den Spezialfall $b = 7$ auf die Suche und werten die Ungleichung einfach an einigen Zahlen aus, wobei wir allerdings schnell an

die Grenzen eines 8-stelligen Taschenrechners herankommen.

m	$m!$	7^m
1	1	7
2	2	49
3	6	343
4	24	2401
5	120	16807
6	720	117649
7	5040	823543
8	40320	5764801
9	362880	40353607
10	3628800	282475249

Ist die Aussage $n! \geq 7^n$ möglicherweise für kein $n \geq 1$ gültig, also $M_7 = \emptyset$? Irgendwie widerspricht das jeglicher Intuition, da mit wachsendem n im Term $n!$ die sukzessive hinzukommenden Faktoren (linear) wachsen, während sie im Term 7^n konstant bleiben. Es sollte also nur eine Frage der Zeit sein, wann die Ungleichung kippt. In der Tat gilt

$$18! = 6402373705728000 > 1628413597910449 = 7^{18}.$$

Mit dem oben Bewiesenen folgt damit $\{18, 19, ...\} \subseteq M_7$. Wir beenden den Fall $b = 7$ mit zwei Bemerkungen.

(1) Zunächst wollen wir demonstrieren, wie die Wahrheit von „$18! > 7^{18}$“ mit einem 8-stelligen Taschenrechner nachgewiesen werden kann. Wir betrachten dazu die folgenden Faktorisierungen von 18!, die man einfach aus der Primfaktorzerlegung (siehe ein späterer Abschnitt) der Zahlen von 2 bis 18 gewinnen kann. Es gilt:

$$\begin{aligned} 18! &= 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= (2 \cdot 3^2) \cdot 17 \cdot (2^4) \cdot (3 \cdot 5) \cdot (2 \cdot 7) \cdot 13 \cdot (2^2 \cdot 3) \cdot 11 \cdot \\ &\quad \cdot (2 \cdot 5) \cdot (3^2) \cdot 2^3 \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2^2) \cdot 3 \cdot 2 \\ &= 2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \\ &= (2^{15}) \cdot (9^4 \cdot 5) \cdot (2 \cdot 5^2) \cdot (7^2) \cdot (11 \cdot 13 \cdot 17) \\ &= (8^5) \cdot 32805 \cdot 50 \cdot (7^2) \cdot 2431 \end{aligned}$$

Nun ist $8 > 7$ und daher auch $8^5 > 7^5$; weiter ist $32805 > 16807$ und $50 > 49$, sowie $2431 > 2401$. Daraus folgt dann

$$18! > (7^5) \cdot 16807 \cdot 49 \cdot (7^2) \cdot 2401.$$

Wegen $16807 = 7^5$ und $2401 = 7^4$ sowie $49 = 7^2$ ergibt dies weiter

$$18! > (7^5) \cdot (7^5) \cdot (7^2) \cdot (7^2) \cdot (7^4) = 7^{18}$$

und damit $18 \in M_7$.

(2) In der Tat gilt bereits $17! \geq 7^{17}$, allerdings darf man beim Abschätzen nicht so grob arbeiten wie oben bei der Abschätzung von 18!. Für $k = 1, 2, ..., 16$ gilt $7^k > k!$.

Wie sieht es bei einer allgemeinen Basis b aus? Diese Frage kann mit Methoden der Analysis geklärt werden: Der Term $\frac{b^n}{n!}$ **konvergiert** bei wachsendem n gegen 0 und wird damit ab einem von b abhängigen n_0 kleiner als 1. Das bedeutet letztendlich, dass M_b für jedes $b \in \mathbb{N}^*$ fast alle natürlichen Zahlen enthält. □

e In Zusammenhang des letzten Beispiels ist noch zu erwähnen, dass für große Zahlen n die Zahl $n!$ durch die **Stirling[12]'sche Formel** angenähert werden kann. Diese lautet

$$n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n,$$

[12] James Stirling (1692-1770)

wobei π die Kreiszahl und e die Euler'sche Zahl sind. Daran erkennt man aufgrund der mit n wachsenden Basis $\frac{n}{e}$ einmal mehr das schnellere Wachstum von $n!$ gegenüber dem exponentiellen Wachstum b^n bei einer konstanten Basis.

f Als weitere Anwendung der vollständigen Induktion beweisen wir die **Formel für geometrische Summen**.

Es sei a eine reelle Zahl. Für $n \in \mathbb{N}$ definieren wir $G_a(n) := \sum_{j=0}^{n} a^j$. Dabei ist definitionsgemäß $a^0 := 1$.[13] Wir behaupten, dass folgendes gilt:

$$G_a(n) = \sum_{j=0}^{n} a^j = \frac{a^{n+1}-1}{a-1} \quad \text{für alle } a \in \mathbb{R} \text{ mit } a \neq 1 \text{ und alle } n \in \mathbb{N}$$

Beweis. Der Beweis erfolgt wieder durch vollständige Induktion. Ist $n = 0$, so ist $G_a(n) = a^0 = 1$. Ebenso ist $\frac{a^{0+1}-1}{a-1} = \frac{a-1}{a-1} = 1$, weshalb $n = 0$ als Induktionsanfang dient. Zum Induktionsschritt: Nach Isolierung des letzten Summanden und Einbringen der Induktionsvoraussetzung erhält man

$$G_a(n+1) = \sum_{j=0}^{n+1} a^j = \sum_{j=0}^{n} a^j \quad + \quad a^{n+1} = G_a(n) + a^{n+1} = \frac{a^{n+1}-1}{a-1} + a^{n+1}.$$

Der Rest ist eine Routinerechnung: Es ist

$$\frac{a^{n+1}-1}{a-1} + a^{n+1} = \frac{a^{n+1}-1+a^{n+1}(a-1)}{a-1} = \frac{a^{n+1}-1+a^{n+2}-a^{n+1}}{a-1} = \frac{a^{n+2}-1}{a-1},$$

was insgesamt zu beweisen war. □

g Für eine reelle Zahl a mit $-1 < a < 1$ zeigt man in der Analysis, dass sich die Zahlenfolge a^0, a^1, a^2, ..., a^n, ... immer mehr der 0 annähert, weshalb sich die Folge

$$G_a(0), \quad G_a(1), \quad G_a(2), \quad ..., \quad G_a(n) = \tfrac{a^{n+1}-1}{a-1}, \quad ...$$

bei großem n immer mehr an die Zahl $\frac{0-1}{a-1} = \frac{1}{1-a}$ annähert. In diesem Zusammenhang nennt man $\frac{1}{1-a}$ den **Grenzwert der Reihe der** a^j und schreibt dafür $\frac{1}{1-a} = \sum_{j=0}^{\infty} a^j$. Beispielsweise ist $\sum_{j=0}^{\infty} (\frac{1}{3})^j = \frac{3}{2}$, wie zu Beginn von Abschnitt 15 bemerkt wurde.

h Zum Ende dieses Abschnitts möchten wir die **Summenregel** aus Satz 14b beweisen.

Beweis. Wir nehmen also an, dass die Mengen $M_1, ..., M_n$ ein **disjunktes** Mengensystem (über einer bestimmten Grundmenge) bilden, und dass jede dieser Mengen eine endliche Mächtigkeit hat.

Der Fall $n = 1$ ist trivial und der Fall $n = 2$ ist mit Satz 10h abgedeckt. Dies dient als Induktionsverankerung. Wir nehmen nun induktiv an, dass die Aussage für m paarweise disjunkte Mengen richtig ist (für ein beliebiges $m \geq 1$) und vollziehen den Induktionsschritt von m auf $m+1$. Für das dazu gegebene, aus $m+1$ Mengen $M_1, ..., M_{m+1}$ bestehende disjunkte Mengensystem setzen wir nun $X := \cup_{i=1}^{m} M_i$ und $Y := M_{m+1}$. Dann ist insgesamt $\cup_{i=1}^{m+1} M_i = X \cup Y$ und daher, unter Verwendung der Formel aus Satz 10h-(2):

$$\left| \bigcup_{i=1}^{m+1} M_i \right| = |X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Die Anwendung der Induktionsannahme auf X liefert zusammen mit $Y = M_{m+1}$ dann

$$|X| + |Y| = \left| \dot{\bigcup_{i=1}^{m}} M_i \right| + |M_{m+1}| = \sum_{i=1}^{m} |M_i| \quad + \quad |M_{m+1}| = \sum_{i=1}^{m+1} |M_i|,$$

[13] Das gilt insbesondere auch für $a = 0$; es ist also $0^0 := 1$.

so dass letztendlich zu zeigen bleibt, dass $X \cap Y$ die leere Menge ist. Wäre $u \in X \cap Y$, so gäbe es wegen $X = \cup_{i=1}^{m} M_i$ ein $i \in \{1, 2, ..., m\}$ mit $u \in M_i$ und mit $u \in Y = M_{m+1}$, also mit $u \in M_i \cap M_{m+1}$. Das widerspräche aber der Voraussetzung, wonach M_i und M_{m+1} disjunkt sind. Also folgt in der Tat $X \cap Y = \emptyset$, womit die Behauptung insgesamt bewiesen ist. (Bei diesem durchgeführten Induktionsschritt ist zu beachten, dass wir auch den Fall $n = 2$ benötigt haben.) $\square$

18. **Grundlagen über Relationen**

a

Definition: Es seien M und N zwei Mengen. Eine **binäre Relation zwischen M und N** ist eine Teilmenge des kartesischen Produktes $M \times N$. Im Falle $M = N$ spricht man von einer **binären Relation auf M**.

Wir lassen das Adjektiv „binär“ im Folgenden weg und sprechen einfach von einer **Relation**.

b Eine Relation ist also etwas sehr allgemeines. Die wichtigsten Typen von Relationen sind

- Abbildungen,
- Äquivalenzrelationen,
- partielle Ordnungen.

Diese sind von ihren spezifischen Gesetzmäßigkeiten her sehr unterschiedlich. Dementsprechend sind die Bezeichnungen für Relationen je nach ihren spezifischen Eigenschaften recht unterschiedlich:

- Abbildungen werden oft mit f, g, h bezeichnet;
- für Äquivalenzrelationen verwendet man vorwiegend symmetrische Symbole wie $\approx$, $\equiv$, $\cong$, $\doteq$, $\parallel$;
- im Gegensatz dazu werden partielle Ordnungen häufig mit einseitigen Symbolen wie $\preceq$, $\leq$, $\sqsubseteq$, $\to$, $\rightsquigarrow$, $\vdash$, $\models$ bezeichnet.

c Ist $R \subseteq M \times N$ eine Relation, so schreibt man (je nach Art von R) für $(\alpha, \beta) \in R$ auch einfach $\alpha R \beta$. Beispielsweise ist die Formel $\alpha \sim \beta$ angenehmer zu lesen als $(\alpha, \beta) \in \sim$, und $a \leq b$ ist vertrauter als $(a, b) \in \leq$.

d Bevor wir in den folgenden Abschnitten die wichtigsten Eigenschaften von Relationen studieren, die sich in der Mathematik herauskristallisiert haben, führen wir zwei Begriffe für allgemeine Relationen ein.

Definition: Ist $R \subseteq M \times N$ eine Relation, so nennt man die durch die Vertauschung der Komponenten entstehende Relation

$$R^\kappa := \{(y, x) : (x, y) \in R\} \subseteq N \times M$$

die zu R gehörende **konverse Relation** oder auch die **Umkehrrelation** von R.

Offensichtlich ist $(R^\kappa)^\kappa = R$. Beispielsweise ist die zur natürlichen Ordnung „kleiner gleich“ $\leq$ gehörende konverse Relation die Relation „größer gleich“ $\geq$. Die zur Teilbarkeitsrelation „teilt“ $|$ (siehe kommender Abschnitt) gehörende konverse Relation ist die Relation „wird geteilt von“. Die Gleichheitsrelation „gleich“ $=$ ist selbstverständlich zu sich selbst konvers.

e Mit der sog. Hintereinanderausführung bzw. Verkettung kann man zwei Relationen zu einer dritten Relation verknüpfen.

Definition: Es seien M, N und K Mengen. Ferner seien $R \subseteq M \times N$ eine Relation zwischen M und N und $S \subseteq N \times K$ eine Relation zwischen N und K. Davon ausgehend definiert man eine Relation $R \star S$ zwischen M und K durch

$$R \star S := \{(x, z) \in M \times K : \exists y \in N \text{ mit } ((x, y) \in R) \wedge ((y, z) \in S)\}.$$

Man nennt $R \star S$ die **Verkettung** (bzw. **Hintereinanderausführung** oder auch **Komposition**) der Relationen R und S.[a]

[a] Es kann sein, dass die Bezeichnung $\star$ eher unüblich ist; eine Standardnotation ist mir nicht bekannt.

f Betrachten wir dazu als Beispiel die drei Mengen $M := \{x, y, z\}$, $N := \{a, b, c, d\}$ und $K := \{U, V, W\}$. Ferner seien R und S die beiden Relationen $R := \{(x, a), (y, a), (y, b), (z, b), (z, c), (z, d)\}$ und $S := \{(a, U), (a, V), (b, U), (c, W), (d, V), (d, W)\}$. Dann ist $R \star S = \{(x, U), (x, V), (y, U), (y, V), (z, U), (z, V), (z, W)\}$.

g Es sei noch erwähnt, dass bei der Komposition von Abbildungen (siehe Abschnitt 22) das Symbol $\circ$ anstelle von $\star$ verwendet wird und dass in der Notation die Reihenfolge der zu verknüpfenden Abbildungen umgekehrt wird. Daher definieren wir schon jetzt

$$S \circ R := R \star S.$$

h Ist V eine endliche Menge und R eine Relation auf V, so ist natürlich auch R endlich, so dass das Objekt (V, R) häufig graphisch dargestellt werden kann, indem man die Elemente von V als Punkte in der Ebene repräsentiert und zwei Punkte x, y aus V durch einen gerichteten Pfeil oder Bogen von x nach y verbindet, wenn genau xRy gilt. Die Elemente von V nennt man in diesem Zusammenhang auch **Punkte** oder **Ecken** oder **Knoten**, während man die Elemente aus R **gerichtete Kanten** nennt. Das Paar (V, R) nennt man einen gerichteten Graphen oder auch einen **Digraphen**.

i Allgemeiner versteht man unter einer **n-ären Relation** zwischen den Mengen M_1, M_2, ..., M_n eine Teilmenge des kartesischen Produktes $\times_{i=1}^{n} M_i$, während eine *n-äre Relation auf M* eine Teilmenge von M^n ist.

19. **Der Abbildungsbegriff**

Abbildungen (auch **eindeutige Zuordnungen** oder **Funktionen** genannt) sind spezielle Relationen, die in der gesamten Mathematik eine zentrale Rolle spielen. Daher wird es höchste Zeit, den Abbildungsbegriff zu formalisieren.

a Wir beginnen mit einigen spezifischen Eigenschaften von Relationen.

Definition: Eine binäre Relation $R \subseteq M \times N$ heißt

(1) **linkstotal**, wenn zu jedem $x \in M$ ein $y \in N$ existiert mit $(x, y) \in R$;
kurz: $\forall_{x\in M}\exists_{y\in N} : (x, y) \in R$

(2) **rechtseindeutig**, falls aus $(x, y_1), (x, y_2) \in R$ folgt $y_1 = y_2$;
kurz: $((x, y_1) \in R) \wedge ((x, y_2) \in R) \Rightarrow y_1 = y_2$

(3) **rechtstotal**, wenn zu jedem $y \in N$ ein $x \in M$ existiert mit $(x, y) \in R$;
kurz: $\forall_{y\in N}\exists_{x\in M} : (x, y) \in R$

(4) **linkseindeutig**, falls aus $(x_1, y), (x_2, y) \in R$ folgt $x_1 = x_2$;
kurz: $((x_1, y) \in R) \wedge ((x_2, y) \in R) \Rightarrow x_1 = x_2$.

b Nun also zu Definition dessen, was eine Abbildung ist.

Definition: Eine Relation f zwischen M und N heißt eine **Abbildung von** M **nach** N, falls sie **linkstotal** und **rechtseindeutig** ist. Dies kann man alternativ wie folgt ausdrücken (und sollte man sich so auch merken):

- *Für jedes* $x \in M$ **gibt es genau ein** $y \in N$ *mit* $(x, y) \in f$.

In logischen Symbolen verwendet man für den Ausdruck „es gibt genau ein“ häufig das Symbol $\exists_1$. Demnach ist die Abbildungseigenschaft einer Relation f durch die logische Formel

$$\forall_{(x\in M)}\exists_{1(y\in N)} : (x, y) \in f$$

beschrieben.

c Wie bereits erwähnt, werden Abbildungen häufig mit dem Symbol f bezeichnet. Zur Spezifikation der Bereiche M und N schreibt man

$$f : M \to N.$$

Die Menge M heißt der **Definitionsbereich** von f, während N der **Bildbereich** bzw. **Wertebereich** von f ist. Das zu jedem $x \in M$ gehörende eindeutige $y \in N$ mit $(x, y) \in f$ wird meist mit $f(x)$ bezeichnet[14]. Man nennt $f(x)$ das **Bild von** x **unter** f. Häufig ergibt sich das Bild $f(x)$ aus x durch eine ganz konkrete Rechen- oder Funktionsvorschrift. Solche Arten von Abbildungen sind aus der Schule bestens bekannt, wo man sie als Funktionen kennen gelernt hat (was die Bezeichnung f rechtfertigt). Bei konkreten Funktionsvorschriften verwendet man zur Berücksichtigung von Definitions- und Bildbereich auch die Notation

$$f : M \to N,\ x \mapsto f(x).$$

Man liest: „f ist die Abbildung von M nach N, die x nach $f(x)$ abbildet“.

d Betrachten wir dazu ein konkretes **Beispiel**: Die Relation $f = \{(x, y) \in \mathbb{R}^2 : y = x^2 - 4x + 1\}$ ist eine Abbildung bzw. eine Funktion und wird durch

$$f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2 - 4x + 1$$

beschrieben (bzw. einfach kurz durch $f(x) = x^2 - 4x + 1$). Das Bild von $x = \sqrt{2}$ unter f ist gleich $f(\sqrt{2}) = \sqrt{2}^2 - 4 \cdot \sqrt{2} + 1 = 3 - 4 \cdot \sqrt{2}$.

[14] hin und wieder findet man auch die Bezeichnungen f_x oder x^f

e Die Variable x kann natürlich ebenso wie die (überstrapazierte) Bezeichnung f durch ein beliebiges Symbol ersetzt werden. So ist etwa

$$\Gamma : \mathbb{Q}^+ \setminus \{3,4,5\} \to \mathbb{R},\ \omega \mapsto \frac{\sqrt{\omega} + \omega^{3.1415}}{\omega^3 - 12\omega^2 + 47\omega - 60}$$

ebenfalls eine Abbildung.

g Abbildungen der Form $g : M \to N$ mit $M, N \subseteq \mathbb{R}$ entsprechen als Relation der Teilmenge $\{(x, g(x)) : x \in M\}$ der euklidischen Ebene $\mathbb{R}^2$; deren Visualisierung wird auch als **Funktionsgraph** bezeichnet. Solche Objekte (wie Parabeln, Hyperbeln, Sinuskurven, etc.) sollten aus der Schule wohlbekannt sien.

h Schließlich ist zu bemerken, dass zwei Abbildungen $g : M \to N$ und $h : M \to N$ **gleich** heißen, wenn $g(x) = h(x)$ für alle x aus M gilt. Beispielsweise sind die beiden Abbildungen $g : \{-1, 0, 1\} \to \mathbb{R}$, $x \mapsto x^3 + 2x^2 - x - 5$ und $h : \{-1, 0, 1\} \to \mathbb{R}$, $x \mapsto 2x^2 - 5$ gleich, denn $g(x) - h(x) = x^3 - x = (x + 1)x(x - 1) = 0$ für jedes x aus dem Definitionsbereich dieser beiden Abbildungen.

i Ist $f : M \to N$ eine Abbildung und ist U eine (nichtleere) Teilmenge von M, so ist auch $U \to N$, $u \mapsto f(u)$ eine Abbildung. Man nennt sie die **Einschränkung** von f auf U. Als Bezeichnung verwendet man häufig das Symbol $f_{|_U}$.

20. **Injektivität, Surjektivität und Bijektivität**

Bisher sind lediglich zwei der vier Eigenschaften aus Definition 19a in den Abbildungsbegriff eingeflossen. Die anderen beiden Eigenschaften werden dazu verwendet, um besondere Abbildungen hervorzuheben.

a

Definition: Eine Abbildung $f : M \to N$ heißt:
(1) **injektiv**, falls sie linkseindeutig ist;
(2) **surjektiv**, falls sie rechtstotal ist;
(3) **bijektiv**, falls sie injektiv und surjektiv ist.

b Für das konkrete Überprüfen der Injektivität, der Surjektivität oder der Bijektivität einer Abbildung f sollte man Folgendes berücksichtigen.

(1) Zum Nachweis der Injektivität ist zu zeigen: Sind $a, b \in M$ mit $f(a) = f(b)$, so folgt $a = b$.
(2) Zum Nachweis der Surjektivität muss man zeigen: Für jedes $y \in N$ gibt es ein $x \in M$ mit $f(x) = y$.
(3) Eine Abbildung ist dementsprechend bijektiv, wenn gilt: Zu jedem $y \in N$ gibt es **genau** ein $x \in M$ mit $f(x) = y$.

c Eine Bijektion (also eine bijektive Abbildung) nennt man daher auch eine **ein-eindeutige Zuordnung**. Ein anderes Synonym für „bijektive Abbildung auf einer Menge M“ ist (insbesondere wenn M endlich ist) der Begriff **Permutation**.

d

Beispiel: Die Abbildung $h : \mathbb{N} \to \mathbb{Z}$ sei definiert durch

$$h(x) := \begin{cases} \frac{x+1}{2}, & \text{falls } x \text{ ungerade} \\ -\frac{x}{2}, & \text{falls } x \text{ gerade.} \end{cases}$$

Wir behaupten, dass h bijektiv ist. Dazu sind die Injektivität und die Surjektivität nachzuweisen.

Beweis. Zunächst zur Injektivität: Es seien $a, b \in \mathbb{N}$ mit $h(a) = h(b)$. Wir führen eine Fallunterscheidung durch. Falls a ungerade und b gerade ist, so folgt $-\frac{b}{2} = \frac{a+1}{2}$, also $-b = a + 1$, was wegen $-b \leq 0 < 1 \leq a + 1$ nicht sein kann. Ganz analog ergibt sich ein Widerspruch, wenn b ungerade und a gerade ist. Sind a und b beide gerade, so folgt $-\frac{a}{2} = -\frac{b}{2}$, was $a = b$ impliziert. Sind schließlich a und b beide ungerade, so erhält man $\frac{a+1}{2} = \frac{b+1}{2}$; erneut zeigt eine einfache Termumformung, dass dann $a = b$ gilt. Insgesamt liefert dies die Injektivität von h.

Nun zur Surjektivität: Es sei $y \in \mathbb{Z}$ beliebig. Wir müssen ein $x \in \mathbb{N}$ präsentieren mit $h(x) = y$. Auch hier ist eine Fallunterscheidung notwendig. Ist $y < 0$, so betrachten wir die Zahl $x := 2 \cdot |y|$. Dann ist $x \in \mathbb{N}$ gerade und daher (wegen der Definition von h und wegen $y < 0$)

$$h(x) = -\frac{x}{2} = -\frac{2|y|}{2} = -|y| = -(-y) = y.$$

Falls $y \geq 0$, so betrachten wir $x := 2y - 1$. Dann ist $x \in \mathbb{N}$ ungerade und daher (erneut wegen der Definition von h und wegen $y \geq 0$)

$$h(x) = \frac{x+1}{2} = \frac{2y-1+1}{2} = y.$$

Insgesamt folgt, dass jedes y aus $\mathbb{Z}$ als Bild unter h angenommen wird, was bedeutet, dass h auch surjektiv ist. Also ist h eine bijektive Abbildung. □

e

Beispiel: Es sei $\mathcal{P}(M)$ die Potenzmenge einer Menge M. Die **Komplementbildung** $X \mapsto X^c = M \setminus X$ ist eine Abbildung auf $\mathcal{P}(M)$. Sie ist offensichtlich injektiv, denn $A^c = B^c$ bedeutet $M \setminus A = M \setminus B$ und daher $A = B$. Sie ist auch surjektiv. Ist nämlich $Y \subseteq M$ beliebig gegeben, so betrachte $X := M \setminus Y = Y^c$; dann ist $X^c = (Y^c)^c = Y$, so dass Y als Bild von X angenommen wird. Das bedeutet insgesamt, dass die Komplementbildung eine Bijektion ist.

f

Beispiel: Die **Nachfolgerfunktion** $\mathrm{succ} : \mathbb{N} \to \mathbb{N}$, definiert durch $\mathrm{succ}(n) := n + 1$, ist eine injektive Abbildung, denn $n+1 = m+1$ impliziert $n = m$. Sie ist aber keine surjektive Abbildung, weil $0 \in \mathbb{N}$ nicht als Bild von succ angenommen wird; es gibt kein $x \in \mathbb{N}$ mit $\mathrm{succ}(x) = x + 1 = 0$. Die Abbildung succ^* hingegen, definiert durch $\mathrm{succ}^* : \mathbb{N} \to \mathbb{N}^*$, $n \to \mathrm{succ}(n)$ (Einschränkung des Bildbereiches auf $\mathbb{N}^*$), ist injektiv und surjektiv, also bijektiv.

g Der Prototyp einer bijektiven Abbildung von einer Menge M in sich selbst ist die **identische Abbildung auf** M, Bezeichnung: id_M. Diese ist einfach durch $\mathrm{id}_M : M \to M$, $x \mapsto x$ definiert.

21. **Bild und Urbild bei Abbildungen**

a Unter dem **Bild einer Abbildung** $f : M \to N$ versteht man die folgende Teilmenge von N:

$$\text{Bild}(f) := \{v \in N : \text{ es gibt ein } u \in M \text{ mit } f(u) = v\}$$

b Eine weitere wichtige Bezeichnung im Kontext zu Abbildungen ist das Urbild.

Definition: Sind $f : M \to N$ eine Abbildung und $y \in N$, so versteht man unter dem **Urbild von y unter f** (Bezeichnung: $f^{-1}(y)$) die Menge aller x aus M, die unter f auf y abgebildet werden:

$$f^{-1}(y) := \{x \in M : f(x) = y\} \subseteq M.$$

c Ist $f : M \to N$ eine Abbildung und sind y und z verschiedene Elemente aus N, so gilt $f^{-1}(y) \cap f^{-1}(z) = \emptyset$, denn: Wegen $y \neq z$ und der Rechtseindeutigkeit von f kann kein $x \in f^{-1}(y) \cap f^{-1}(z)$ existieren, denn dann wären ja (x, y) und (x, z) beides Elemente der Relation f und das würde aufgrund der Abbildungseigenschaft von f bedeuten $f(x) = y \neq z = f(x)$, ein Widerspruch. Ferner gibt es zu jedem $x \in M$ ein $y \in N$ mit $x \in f^{-1}(y)$, denn $x \in f^{-1}(f(x))$. Damit haben wir Folgendes nachgewiesen.

Satz: *Die Menge aller Urbilder einer Abbildung $f : M \to N$ bildet eine Partition bzw. eine Zerlegung des Definitionsbereiches M.* □

Man nennt daher $\{f^{-1}(y) : y \in N\} \subseteq \mathcal{P}(M)$ die **Urbildpartition** von M unter f.[15]

d

Beispiel: Betrachten wir als Beispiel nochmals die Funktion $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 - 4x + 1$ aus 19d. Durch eine quadratische Ergänzung erhalten wir

$$f(x) = x^2 - 4x + 1 = x^2 - 4x + 4 - 4 + 1 = (x - 2)^2 - 3.$$

Wegen $(x - 2)^2 \geq 0$ für alle $x \in \mathbb{R}$ folgt $f(x) \geq -3$ für jedes x, weshalb die Zahlen y mit $y < -3$ nicht als Bild von f auftreten, i.e., $f^{-1}(y) = \emptyset$ für $y < -3$.

Ferner ist $f(x) = -3$ genau dann, wenn $(x-2)^2 = 0$, also wenn $x = 2$ ist. Somit gilt $f^{-1}(-3) = \{2\}$; in der Tat ist ja $(2, -3)$ der Scheitelpunkt von f.

Um die Urbildmenge $f^{-1}(y)$ für $y > -3$ zu berechnen betrachten wir ausgehend von $f(x) = y$ die quadratische Gleichung $0 = f(x) - y = x^2 - 4x + 1 - y$ mit Koeffizienten $a = 1$ und $b = -4$ und $c = 1 - y$. Die Diskriminante $\Delta = b^2 - 4ac$ ist somit gleich $16 - 4 + 4y = 12 + 4y = 4(3 + y)$, was wegen $y > -3$ echt größer als null ist. Nach Satz 7f hat jedes $y > -3$ daher die beiden Urbilder $\frac{-b+\sqrt{\Delta}}{2a}$ und $\frac{-b-\sqrt{\Delta}}{2a}$ unter f. Wegen $\Delta = 2 \cdot \sqrt{3 + y}$ ergibt sich somit leicht die zweielementige Urbildmenge

$$f^{-1}(y) = \{2 - \sqrt{3 + y}, 2 + \sqrt{3 + y}\}$$

für jedes $y > -3$.

e Wir bemerken, dass man anschaulich gesehen die Urbildmengen für allgemeine Funktionen $g : \mathbb{R} \to \mathbb{R}$ wir folgt bekommt. Für $y \in \mathbb{R}$ zieht man die Parallele zur x-Achse durch den Punkt $(0, y)$. Die Schnittpunkte dieser Parallelen mit dem Funktionsgraph zu g ergeben dann genau die Punkte (x, y) mit $g(x) = y$.

f Anhand von Urbildmengen erhält man unmittelbar die folgenden nützlichen Charakterisierungen für injektive bzw. surjektive bzw. bijektive Abbildungen.

[15] Ist f nicht surjektiv, so tritt der Schönheitsfehler auf, dass die leere Menge in der Urbildpartition vertreten ist.

Satz: *Es sei $f : M \to N$ eine Abbildung. Dann gelten:*

(1) *f ist genau dann surjektiv, wenn $f^{-1}(y) \neq \emptyset$ für jedes $y \in N$ gilt, also wenn $|f^{-1}(y)| \geq 1$ für alle y erfüllt ist;*
(2) *f ist genau dann injektiv, wenn $|f^{-1}(y)| \leq 1$ für alle $y \in N$ erfüllt ist;*
(3) *f genau dann bijektiv, wenn $f^{-1}(y)$ für jedes $y \in N$ eine einelementige Menge ist.* □

g Wir müssen auf eine weitere Besonderheit bei der Notation für Abbildungen hinweisen, wobei wir uns an die Grundlagen aus Abschnitt 18 erinnern.

Wie wir wissen, ist eine Abbildung g eine spezielle Relation, nämlich eine linkstotal und rechtseindeutige. Die durch g^{-1} gekennzeichnete Urbildpartition beschreibt im Wesentlichen die zu g gehörende konverse Relation g^κ. Die Relation g^κ ist im Allgemeinen aber keine Abbildung! Konkret gilt: g^κ ist genau dann linkstotal, wenn g rechtstotal ist, und genau dann rechtseindeutig, wenn g linkseindeutig ist. Somit ist g^κ genau dann selbst eine Abbildung, wenn g eine Bijektion ist!

Ist $g : M \to N$ nun eine bijektive Abbildung, so ist $g^{-1}(y)$ nach Satz 21e-(3) für jedes $y \in N$ eine einelementige Menge. Ist beispielsweise $g^{-1}(y) = \{t\}$, so schreibt man daher einfach $g^{-1}(y) = t$. In diesem Sinne ist dann aber g^{-1} die g^κ entsprechende Abbildung von N nach M; man nennt sie daher die **Umkehrabbildung** von g. Es ist g^{-1} (alias g^κ) dann sogar selbst eine Bijektion, deren Umkehrabbildung $(g^{-1})^{-1}$ (alias $(g^\kappa)^\kappa$) wiederum gleich g ist.

h Beispielsweise ist $\mathbb{R} \to \mathbb{R}$, $y \mapsto \frac{1}{4}y - \frac{1}{4}$ die Umkehrabbildung von $\mathbb{R} \to \mathbb{R}$, $x \mapsto 4x + 1$, wie man durch Auflösen der Gleichung $y = 4x + 1$ nach x leicht sieht.

22. **Verkettung von Abbildungen**

a Wir wollen nun u.a. zeigen, dass die Verkettung $\circ$ (bzw. Hintereinanderausführung bzw. Komposition, siehe 18e und 18g) zweier Abbildungen wieder eine Abbildung liefert. Das Wichtigste ist in folgendem Satz zusammengefasst.

Satz: *Es seien $f : M \to N$ und $g : N \to K$ zwei Abbildungen. Dann gilt für die verkettete Relation $g \circ f \subseteq M \times K$ Folgendes:*

(1) *$g \circ f$ ist eine Abbildung von M nach K, ferner gilt $g \circ f(x) = g(f(x))$ für jedes $x \in M$;*
(2) *sind f und g beide injektiv, so ist auch $g \circ f$ injektiv;*
(3) *sind f und g beide surjektiv, so ist auch $g \circ f$ surjektiv;*
(4) *sind f und g beide bijektiv, so ist auch $g \circ f$ bijektiv; in diesem Fall erfüllen die Umkehrabbildungen die Gleichung $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Beweis. (1) Da die Abbildungseigenschaft erst gezeigt werden soll, müssen wir notgedrungen auf die allgemeine Relationenschreibweise zurückgreifen. Ist $x \in M$, so gibt es ein eindeutiges $y \in N$ mit $f(x) = y$. Da g eine Abbildung ist, gibt es ein eindeutiges $z \in K$ mit $g(y) = z$. Wegen $(x, y) \in f$ und $(y, z) \in g$ ist $(x, z) \in f \star g = g \circ f$. Damit ist gezeigt, dass $g \circ f$ linkstotal ist. Ist neben (x, z) auch $(x, z') \in f \star g$, so gibt es (neben y) ein $y' \in N$ mit $(x, y') \in f$ und $(y', z') \in g$. Wegen der Rechtseindeutigkeit von f und $(x, y) \in f$ ist $y' = y$; wegen der Rechtseindeutigkeit von g und $(y, z) \in g$ ist $z' = z$. Also ist $g \circ f$ rechtseindeutig, insgesamt also eine Abbildung. Wegen $y = f(x)$ haben wir gleichzeitig nachgewiesen, dass $g \circ f(x) = g(f(x))$ ist.

(2) Wir nehmen nun an, dass f und g injektiv sind. Falls $g \circ f(x_1) = g \circ f(x_2)$, so gilt $g(f(x_1)) = g(f(x_2))$. Aufgrund der Injektivität von g folgt $f(x_1) = f(x_2)$. Da auch f injektiv ist, folgt $x_1 = x_2$. Das beweist die Injektivität von $g \circ f$.

(3) Es seien f und g surjektiv. Ist $z \in K$, so gibt es wegen der Surjektivität von g ein $y \in N$ mit $g(y) = z$. Da auch f surjektiv ist, gibt es ein $x \in M$ mit $f(x) = y$. Also ist $z = g(f(x)) = g \circ f(x)$, so dass auch $g \circ f$ surjektiv ist.

(4) Aus (2) und (3) folgt die Bijektivität von $f \circ g$, wenn f und g beide bijektiv sind. Für $x \in M$ sei wieder $y = f(x) \in N$ und $z = g(y) = g \circ f(x) \in K$. Dann ist

$$(g \circ f)^{-1}(z) = x = f^{-1}(y) = f^{-1}(g^{-1}(z)) = f^{-1} \circ g^{-1}(z).$$

Da dies für alle $z \in K$ gilt, folgt $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

b Es ist zu bemerken, dass bei bijektiven Abbildungen $f : M \to N$ insbesondere $f^{-1} \circ f(x) = f^{-1}(f(x)) = x$ für alle $x \in M$ und entsprechend $f \circ f^{-1}(y) = f(f^{-1}(y)) = y$ für alle $y \in N$ gilt. Das bedeutet aber nichts anderes, als dass $f \circ f^{-1} = \mathrm{id}_M$ und $f^{-1} \circ f = \mathrm{id}_N$ gilt.

c In Bezug auf Satz 22a sei weiter bemerkt, dass man die konkrete Funktionsvorschrift einer verketteten Abbildung durch Einsetzen der jeweiligen Funktionsvorschriften erhält. So ist etwa bei den reellwertigen Funktionen $f(x) := x^2 + 4$ und $g(x) := -x - 2$ und $h(x) := \frac{1}{3x+8}$ die Verkettung $h \circ g \circ f(x)$ gleich[16]

$$(h \circ g) \circ f(x) = h \circ g(f(x)) = h(g(f(x))) = h(g(x^2 + 4)) = h(-(x^2 + 4) - 2),$$

was sich zu $h \circ g \circ f(x) = \frac{1}{3 \cdot [-(x^2+4)-2]+8} = \frac{1}{-3x^2-10}$ auswerten lässt.

[16] Aufgrund des geltenden Assoziativgesetzes für die Verkettung von Abbildungen, ist es egal, ob man $h \circ g \circ f$ als $(h \circ g) \circ f$ oder als $h \circ (g \circ f)$ auswertet. Der Nachweis sei als Übung gestellt.

23. **Abbildungen zwischen endlichen Mengen**

a Zu jeder natürlichen Zahl $n \in \mathbb{N}^*$ bezeichne (der Einfachheit halber)

$$[n] \quad \text{die Menge} \quad \{x \in \mathbb{N}^* : 1 \leq x \leq n\}.$$

Die ureigenste Funktion der Zahl n ist offenbar, dass $[n]$ genau n (paarweise verschiedene) Elemente enthält, nämlich die Zahlen

$$1, 2, 3, ..., n-1, n.$$

Ausgehend davon kann man präzise definieren, was man unter einer endlichen Menge versteht:

Eine Menge L heißt eine **endliche** Menge, falls sie leer ist, oder falls ein $n \in \mathbb{N}^*$ und eine bijektive Abbildung $\sigma : [n] \to L$ existieren.

Die Existenz einer solchen Bijektion $\sigma : [n] \to L$ bedeutet nichts anderes, als dass man die Elemente von L der Reihe nach *aufzählen* kann:

$$\sigma(1),\ \sigma(2),\ \sigma(3),\ \ \ldots,\ \ \sigma(n-1),\ \sigma(n).$$

Diese Zahl n ist (in Abhängigkeit von L) selbstverständlich eindeutig festgelegt; und man nennt sie die **Mächtigkeit** von L.

b Wir betrachten nun zwei endliche, nicht-leere Mengen, M und N, mit Mächtigkeiten $m = |M|$ bzw. mit $n = |N|$. Es sei weiter $\psi : M \to N$ eine Abbildung. Aufgrund der Summenregel (Satz 14b) in Verbindung mit Satz 21c gilt dann

$$|M| = \sum_{y \in \mathrm{Bild}(\psi)} |\psi^{-1}(y)|.$$

Das **Taubenschlagprinzip**[a] (auch **Schubfachprinzip**) besagt, dass ψ im Falle $m > n$ *nicht* injektiv sein kann:

Ist $m > n$, so gibt es ein $j \in N$ und $a, b \in M$ mit $a \neq b$ und mit $\psi(a) = j = \psi(b)$.

[a] Probieren Sie es Zuhause einmal aus: Bringen Sie fünf Tauben (irgendwie) in drei Taubenhäuschen unter; danach befinden sich in wenigstens einem Taubenhäuschen mindestens zwei Tauben. Wer keine Tauben hat, werfe (irendwie) fünf Tennisbälle in drei Behälter.

Beweis. Wäre ψ injektiv, so folgte $|\psi^{-1}(y)| \leq 1$ für jedes $y \in N$ (siehe Satz 21f), und daraus erhielte man $|M| = \sum_{y \in N} |\psi^{-1}(y)| \leq \sum_{y \in N} 1 = |N|$. □

Verwandt mit dem Taubenschlagprinzip ist der Sachverhalt, wonach ψ im Falle $m < n$ *nicht* surjektiv sein kann:

Ist $m < n$, so gibt es ein $j \in N$, für das $\psi^{-1}(j)$ leer ist.

Beweis. Wäre ψ surjektiv, so folgte $|\psi^{-1}(y)| \geq 1$ für jedes $y \in N$ (siehe Satz 21f), und daraus erhielte man $|M| = \sum_{y \in N} |\psi^{-1}(y)| \geq \sum_{y \in N} 1 = |N|$. □

c Sind M und N zwei endliche Mengen mit gleicher Mächtigkeit n, und sind $\sigma : [n] \to M$ und $\tau : [n] \to N$ jeweils Bijektionen, so ist $\tau \circ \sigma^{-1}$ eine Bijektion von M nach N. Zusammen mit dem, was in 23b gesagt wurde erhält man daher das folgende wichtige Grundprinzip der Kombinatorik.

Satz: (Gleichmächtigkeitsregel) *Genau dann sind zwei endliche Mengen M und N bijektiv aufeinander abbildbar, wenn M und N die gleiche Mächtigkeit haben.* □

d Der folgende Sachverhalt ist ebenso sehr wichtig.

Satz: *Es seien M und N zwei nicht-leere endliche Mengen mit gleicher Mächtigkeit. Weiter sei $\psi : M \to N$ eine Abbildung. Dann gilt:*

$$\psi \text{ ist injektiv} \Leftrightarrow \psi \text{ ist bijektiv} \Leftrightarrow \psi \text{ ist surjektiv.}$$

Beweis. Es gelte also $|M| = |N|$. Ist $\psi : M \to N$ injektiv, so ergibt sich

$$|M| = \sum_{y \in N} |\psi^{-1}(y)| \leq \sum_{y \in N} 1 \leq |N| = |M|.$$

Bei der vermeintlichen Abschätzung „$\leq$“ in dieser Kette muss daher Gleichheit gelten. Das bedeutet $|\psi^{-1}(y)| = 1$ für jedes $y \in N$, was der Bijektivität von ψ entspricht. Ganz analog argumentiert man, wenn ψ surjektiv ist. □

e Als eine erste Anwendung der Gleichmächtigkeitsregel wollen wir die Produktregel aus Satz 14d beweisen, also:

Satz: *Sind $M_1, ..., M_n$ endliche Mengen, so ist die Mächtigkeit von deren kartesischem Produkt gleich dem Produkt der Mächtigkeiten der einzelnen Mengen:*

$$|\times_{i=1}^{n} M_i| = \prod_{i=1}^{n} |M_i|$$

Beweis. Es seien also $M_1, ..., M_n$ jeweils endliche Mengen. Es sei $n \geq 2$. Weiter seien $X := \times_{k=1}^{n-1} M_k$ und $Y := M_n$. Bei der Abbildung

$$\times_{k=1}^{n} M_k \to X \times Y,\ (a_1, a_2, ..., a_{n-1}, a_n) \mapsto ((a_1, a_2, ..., a_{n-1}), a_n)$$

handelt es sich offensichtlich um um eine Bijektion. Daher gilt

$$|\times_{k=1}^{n} M_k| = |X \times Y|.$$

Mit Satz 12h folgt weiter $|X \times Y| = |X| \cdot |Y|$. Mit Induktion gilt weiter $|X| = \prod_{k=1}^{n-1} |M_k|$. □

f Als Nächstes beweisen wir Satz 12b, also:

Satz: Ist M eine endliche Menge, so hat deren Potenzmenge die Mächtigkeit $2^{|M|}$.

Beweis. Es sei also M eine endliche Menge, welche nicht leer sei. Es gelte $|M| = m$. Aufgrund der Produktregel wissen wir, dass der binäre m-Tupelraum $\{0,1\}^m$ genau $|\{0,1\}|^m = 2^m$ Elemente enthält. Wir denken uns die Elemente von M nun durchnummeriert (bzw. abgezählt): $x_1, ..., x_m$. Ist nun U eine Teilmenge von M, so ordnen wir U das folgende binäre m-Tupel χ_U zu: Es ist $\chi_U(i) = 1$ falls $x_i \in U$ und $\chi_U(i) = 0$, andernfalls. Das liefert eine Bijektion

$$\chi : \mathcal{P}(M) \to \{0,1\}^m,\ U \mapsto \chi_U.$$

Aufgrund der Gleichmächtigkeitsregel folgt $|\mathcal{P}(M)| = |\{0,1\}^m| = |\{0,1\}|^m = 2^m$. □

24. **Binomialkoeffizienten**

a Wir bleiben in diesem Abschnitt bei der Berachtung der Potenzmenge $\mathcal{P}(N)$ einer endlichen Menge N. Es gelte $n = |N|$ und im Falle $n \geq 1$ sei ohne Einschränkung N gleich der **Standard-n-Menge** $[n]$ (siehe 23a).

Zu jeder weiteren natürlichen Zahl k sei

$$\mathcal{P}_k(n) := \{U \subseteq [n] : |U| = k\}$$

das Mengensystem aller k-elementigen Teilmengen von $[n]$.

Definition: In der eben beschriebenen Situation steht

$$\binom{n}{k} := |\mathcal{P}_k(n)|$$

für die Anzahl der k-elementigen Teilmengen einer (beliebigen) n-Menge. Die Zahl $\binom{n}{k}$ nennt man einen **Binomialkoeffizienten**.

b Im Folgenden geht es um die Berechnung der Binomialkoeffizienten. Offenbar ist $\binom{n}{k} = 0$ für $k \geq n+1$. Weiter gilt $\binom{n}{0} = 1 = \binom{n}{n}$. Es bleibt daher die Bestimmung von $\binom{n}{k}$ in den Fällen wo $1 \leq k < n$.

Satz: *Sind $k, n \in \mathbb{N}$ mit $1 \leq k < n$, so gilt*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Beweis. Man zerlegt die Menge $\mathcal{P}_k(n)$ in die beiden Teilmengen

- $\mathcal{P}_k^-(n) := \{U \subseteq [n] : |U| = k, n \notin U\}$, und
- $\mathcal{P}_k^+(n) := \{U \subseteq [n] : |U| = k, n \in U\}$.

Dann ist $\mathcal{P}_k^-(n) = \mathcal{P}_k(n-1)$. Weiter entspricht $\mathcal{P}_k^+(n)$ ein-eindeutig (also bijektiv) der Menge $\mathcal{P}_{k-1}(n-1)$. Konkret ist folgende Abbildung eine Bijektion zwischen diesen beiden Mengen:

$$\mathcal{P}_k^+(n) \to \mathcal{P}_{k-1}(n-1),\ U \mapsto U \setminus \{n\}.$$

Insgesamt liefern die Summen- und die Gleichmächtigkeitsregel dann

$$\begin{aligned}\binom{n}{k} &= |\mathcal{P}_k(n)| \\ &= |\mathcal{P}_k^-(n)| + |\mathcal{P}_k^+(n)| \\ &= |\mathcal{P}_k(n-1)| + |\mathcal{P}_{k-1}(n-1)| \\ &= \binom{n-1}{k} + \binom{n-1}{k-1},\end{aligned}$$

die Behauptung. □

c Die Rekursionsformel aus Satz 24b führt zum sog. **Pascalschen Dreieck**[17], bei dem die Binomialkoeffizienten so übereinander angeordnet sind, dass jede Zahl gleich der Summe der beiden direkt oberhalb liegenden Nachbarzahlen ist:

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \end{array}$$

[17] Blaise Pascal (1623-1662)

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$
$$\cdots\cdots\cdots\cdots$$

Wegen $\binom{n}{0} = 1 = \binom{n}{n}$ für jedes $n \in \mathbb{N}$ ist damit genügend Information vorhanden, um die Binomialkoeffizienten rekursiv zu berechnen.

d

Satz: *Für jedes $n \in \mathbb{N}$ und jedes $k \in \mathbb{N}$ mit $0 \leq k \leq n$ gilt*

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Beweis. Ist $k = 0$, so ist $\binom{n}{k} = \binom{n}{0} = 1$ (für jedes n); ebenso gilt

$$\frac{n!}{0! \cdot (n-0)!} = \frac{n!}{n!} = 1.$$

Ist $k = n$, so ist $\binom{n}{n} = 1$; ebenso gilt

$$\frac{n!}{n! \cdot (n-n)!} = \frac{n!}{n!} = 1.$$

Ist speziell $n = 0$ oder $n = 1$, so ist nichts weiter zu zeigen. Dies dient als Induktionsanfang. Wir nehmen daher $n \geq 2$ an. Außerdem betrachten wir ein k mit $1 \leq k \leq n-1$. Nach Satz 24b gilt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Das Einsetzen der Induktionsannahme für die beiden Terme $\binom{n-1}{k-1}$ und $\binom{n-1}{k}$ liefert

$$\binom{n}{k} = \frac{(n-1)!}{(k-1)! \cdot ((n-1)-(k-1))!} + \frac{(n-1)!}{k! \cdot ((n-1)-k)!},$$

und dies ist gleich

$$\frac{(n-1)!}{(k-1)! \cdot (n-k)!} + \frac{(n-1)!}{k! \cdot ((n-1)-k)!},$$

Erweitert man den ersten Bruch mit k und den zweiten Bruch mit $n-k$, so erhält man gleichnamige Nenner, nämlich $k! \cdot (n-k)!$, und damit

$$\binom{n}{k} = \frac{(n-1)! \cdot k + (n-1)! \cdot (n-k)}{k! \cdot (n-k)!} = \frac{(n-1)! \cdot (k + (n-k))}{k! \cdot (n-k)!} = \frac{(n-1)! \cdot n}{k! \cdot (n-k)!},$$

was gleich $\frac{n!}{k! \cdot (n-k)!}$ ist. □

e

Satz: *Sind $k, n \in \mathbb{N}$ mit $0 \leq k \leq n$, so gilt*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Beweis. Das folgt unmittelbar aufgrund der Symmetrie von „k“ und „$n-k$“ im Term $\frac{n!}{k! \cdot (n-k)!}$, denn $n-(n-k) = k$. Alternativ kann man die Gleichmächtigkeitsregel anwenden, weil die Abbildung auf $\mathcal{P}(n)$, die jedem $U \subseteq [n]$ ihr Komplement $[n] \setminus U$ zuordnet, eine Bijektion von $\mathcal{P}_k(n)$ nach $\mathcal{P}_{n-k}(n)$ liefert (für jedes k), denn $|[n] \setminus U| = n - |U|$. □

f

Binomialsatz: *Es seien x und y zwei beliebige reelle Zahlen.*[a] *Ist $n \in \mathbb{N}$, so gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

[a] Allgemeiner können x und y zwei Elemente aus der algebraischen Struktur eines Rings sein, für die $xy = yx$ gilt.

Beweis. Wegen $r^0 = 1$ und $r^1 = r$ für alle $r \in \mathbb{R}$ stimmt die Behauptung auf jeden Fall für $n = 0$ und $n = 1$, wie man durch Einsetzen in die Formel leicht verifiziert. Den Induktionsschritt vollziehen wir von n nach $n+1$. Zunächst gilt

$$(x+y)^{n+1} = (x+y)^n \cdot (x+y).$$

Einsetzen der Induktionsannahme liefert

$$(x+y)^{n+1} = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right) \cdot (x+y).$$

Wir wenden nun das in $\mathbb{R}$ gültige *Distributivgesetz* an, um die beiden Klammern auszumultiplizieren:

$$(x+y)^{n+1} \quad = \quad \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1}.$$

In der ersten Summe wird zunächst eine sog. *Indextransformation* vorgenommen. Anstatt von $k = 0$ bis n summieren wir über $\ell = 1$ bis $n+1$, wobei dann der Summand $\binom{n}{k} x^{k+1} y^{n-k}$ entsprechend durch $\binom{n}{\ell-1} x^{(\ell-1)+1} y^{n-(\ell-1)} = \binom{n}{\ell-1} x^\ell y^{n-\ell+1}$ zu ersetzen ist. Also folgt

$$(x+y)^{n+1} = \sum_{\ell=1}^{n+1} \binom{n}{\ell-1} x^\ell y^{n-\ell+1} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1}.$$

Auf der rechten Seite dieser Gleichung ziehen wir nun aus der ersten Summe den letzten Summanden (das ist x^{n+1}) und aus der zweite Summe den ersten Summanden (das ist y^{n+1}) heraus, um

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{\ell=1}^{n} \binom{n}{\ell-1} x^\ell y^{n-\ell+1} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n-k+1}$$

zu erhalten. Der Vorteil dieser Darstellung ist, dass die beiden Summen nun über die gleiche Indexmenge gebildet werden. Ersetzt man daher die Laufvariable ℓ der ersten Summe wieder durch k, so kann man die beiden großen Summen auf der rechten Seite zu einer einzigen (großen) Summe zusammenfassen, nämlich zu

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) x^k y^{n+1-k}.$$

Eine Anwendung von Satz 24d liefert als Nächstes:

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k}$$

Schließlich verarbeiten wir die Summanden x^{n+1} und y^{n+1} wieder innerhalb der großen Summe als $\binom{n+1}{n+1} x^{n+1} y^0$ und $\binom{n+1}{0} x^0 y^{n+1}$, um insgesamt das gewünschte Ergebnis

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}$$

zu erhalten.

Der zweite Teil der Formel ist wegen $x + y = y + x$ richtig. □

g Wir wollen nun nochmals nachweisen, dass die Anzahl aller Teilmengen einer n-elementigen Menge gleich 2^n ist: Betrachte o.B.d.A. wieder die Menge $[n]$. Es ist

$$\{\mathcal{P}_k(n) : 0 \leq k \leq n\}$$

eine Zerlegung von $\mathcal{P}(n)$. Aufgrund der Summenregel ist daher

$$|\mathcal{P}(n)| = \sum_{k=0}^{n} |\mathcal{P}_k(n)| = \sum_{k=0}^{n} \binom{n}{k}.$$

Nach dem Binomialsatz ist dies gleich

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n = 2^n.$$

25. **Abzählbar unendliche Mengen**

a In diesem und dem kommenden Abschnitt möchten wir über unendliche Mengen nachdenken. Formal können solche Menge wie folgt definiert werden.

> Eine Menge L heißt eine **unendliche** Menge, falls es eine injektive Abbildung von $\mathbb{N}^*$ nach L gibt.

b Aufgrund dieser Definition handelt es sich bei $\mathbb{N}$, bei $\mathbb{Z}$, bei $\mathbb{Q}$ und bei $\mathbb{R}$ offensichtlich allesamt um unendliche Mengen, denn $\mathbb{N}^*$ ist ja eine (echte) Teilmenge all dieser Mengen. Umgekehrt gibt es aber auch echte Teilmengen von $\mathbb{N}^*$, die unendlich sind. Beispielsweise ist die Menge

$$P_2 := \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...\}$$

aller Zweierpotenzen unendlich, denn es ist ja

$$\mathbb{N}^* \to P_2,\ n \mapsto 2^{n-1}$$

eine bijektive (insbesondere injektive) Abbildung.

c Ist M eine unendliche Menge, so drückt man dies meist durch die Schreibeweise „$|M| = \infty$“, also durch das „Unendlichkeitssymbol“ aus. Dies ist allerdings sehr grob, da es im Bereich der unendlichen Mengen viele *Mächtigkeits-Hierarchien* gibt, wie wir noch näher erläutern werden. Für eine erste Abgrenzung benötigen wir folgende Definition.

> **Definition:** Eine unendliche M heißt **abzählbar unendlich**, falls eine Bijektion $\sigma : \mathbb{N}^* \to M$ existiert.

Die abzählbare Unendlichkeit einer Menge L bedeutet wortwörtlich, dass man sämtliche Elemente der Menge L einzeln abzählen kann:

$$\sigma(1),\ \sigma(2),\ ...,\ \sigma(k),\ ...\ .$$

Beispielsweise ist die (obige) Menge P_2 aller Zweierpotenzen aus $\mathbb{N}^*$ abzählbar unendlich. Das zeigt (ganz im Gegensatz zu endlichen Mengen), dass es unendliche Mengen gibt, die bijektiv auf eine ihrer *echten* Teilmengen abbildbar sind.[18]

d

> **Satz:** *Es gelten:*
> (1) *Die Menge $\mathbb{N}$ der natürlichen Zahlen (inklusive der Null) ist abzählbar unendlich.*
> (2) *Die Menge $\mathbb{Z}$ aller ganzen Zahlen ist abzählbar unendlich.*
> (3) *Die Menge $\mathbb{Q}$ aller rationalen Zahlen ist ebenfalls abzählbar unendlich.*

Beweis. (1) Die Nachfolgerabbildung $\text{succ} : \mathbb{N} \to \mathbb{N}^*,\ x \mapsto x+1$ ist eine Bijektion. Deren Umkehrabbildung, nämlich die Vorgängerabbildung $\text{pred} : \mathbb{N}^* \to \mathbb{N}$, $y \mapsto y - 1$, zählt deshalb die Menge $\mathbb{N}$ ab.

(2) Ist h die Bijektion von $\mathbb{N}$ nach $\mathbb{Z}$ aus Beispiel 20d, so ist $h \circ \text{succ}^{-1}$ eine Bijektion von $\mathbb{N}^*$ nach $\mathbb{Z}$.

(3) Kommen wir zu den rationalen Zahlen. Der wesentliche Schritt des Beweises stammt von Georg Cantor (1845-1918), dem Begründer der Mengenlehre. Nach Cantors **Diagonalverfahren** zählt man die positiven rationalen Zahlen zunächst wie in der Graphik auf Seite 97 im Lehrbuch (bzw. wie in der Vorlesung erklärt) ab.

[18] In der Tat ist eine Menge M genau dann unendlich, wenn sie bijektiv auf eine ihrer echten Teilmengen abbildbar ist.

Die zugrunde liegende Abbildung für dieses Schema sei δ. Das heißt, $\delta : \mathbb{N}^* \to \mathbb{Q}^+$ ist eine (wenn auch nicht explizit durch eine konkrete Formel gegebene) Bijektion. Nun verwendet man die Idee aus Beispiel 20d, um eine Bijektion von $\mathbb{N}$ nach $\mathbb{Q}$ zu erhalten:

$$\psi : \mathbb{N} \to \mathbb{Q},\ n \mapsto \begin{cases} 0, & \text{falls } n = 0 \\ \delta(\frac{n+1}{2}), & \text{falls } n \text{ ungerade} \\ -\delta(\frac{n}{2}), & \text{falls } n \text{ gerade, } n \neq 0. \end{cases}$$

Der Rest ist eine reine Formalität: Schalte succ^{-1} vor ψ und erhalte eine Bijektion $\psi \circ \mathrm{succ}^{-1}$ von $\mathbb{N}^*$ nach $\mathbb{Q}$.

□

26. Überabzählbar unendliche Mengen

a

Definition: Eine Menge, die weder endlich noch abzählbar unendlich ist, nennt man eine **überabzählbar unendliche** Menge.

b Aufgrund Satz 25d ist die Existenz einer überabzählbaren Menge keinesfalls offensichtlich. Um dies nachzuweisen zu können, betrachten wir nochmals die Potenzmenge $\mathcal{P}(M)$ einer Menge M.

Satz: *Zu jeder nicht-leeren Menge M gibt es zwar eine injektive Abbildung von M nach $\mathcal{P}(M)$, jedoch keine surjektive Abbildung von M nach $\mathcal{P}(M)$.*

Beweis. Die erste Behauptung ist trivialerweise richtig, da

$$M \to \mathcal{P}(M),\ x \mapsto \{x\}$$

injektiv ist.

Die zweite Behauptung ist nicht offensichtlich, man kann sie sich aber mit einem sehr schönen Argument klarmachen (vgl. mit 12c): Es sei dazu $\omega : M \to \mathcal{P}(M)$ irgendeine Abbildung. Davon ausgehend sei die Teilmenge X von M wie folgt definiert.

$$X := \{x \in M : x \in \omega(x)\}$$

Schließlich sei $Y := M \setminus X$ das Komplement von X in M. Wir behaupten, dass Y *nicht* im Bild von ω liegt, so dass ω nicht surjektiv sein kann. Wäre nämlich Y im Bild von ω enthalten, so gäbe es ein $a \in M$ mit $Y = \omega(a)$. Nun gibt es zwei Möglichkeiten. Entweder $a \in Y$ oder $a \notin Y$.

(1) Falls $a \in Y$, so ist $a \in \omega(a)$, da ja $Y = \omega(a)$. Nach Definition von X ist dann aber $a \in X$. Wegen $X = M \setminus Y$ folgt $a \notin Y$, ein Widerspruch.
(2) Falls $a \notin Y$, so ist $a \notin \omega(a)$, da ja $Y = \omega(a)$. Nach Definition von X ist dann aber $a \notin X$. Wegen $X = M \setminus Y$ folgt $a \in Y$, erneut ein Widerspruch.

Also ist Y tatsächlich nicht im Bild von ω enthalten. □

c Als Folgerung aus Satz 26b erhalten wir

Satz: *Die Menge $\mathcal{P}(\mathbb{N}^*)$, also die Menge aller Teilmengen von $\mathbb{N}^*$ ist überabzählbar unendlich.*

Beweis. Wende Satz 26b auf die Menge $M = \mathbb{N}^*$ an. Es gibt eine injektive Abbildung von $\mathbb{N}^*$ nach $\mathcal{P}(\mathbb{N}^*)$ und deshalb ist $\mathcal{P}(\mathbb{N}^*)$ eine unendliche Menge. Da es allerdings keine surjektive Abbildung von $\mathbb{N}^*$ nach $\mathcal{P}(\mathbb{N}^*)$ geben kann, kann es auch keine bijektive Abbildung von $\mathbb{N}^*$ nach $\mathcal{P}(\mathbb{N}^*)$ geben, und deshalb ist $\mathcal{P}(\mathbb{N}^*)$ nicht abzählbar unendlich. Folglich ist $\mathcal{P}(\mathbb{N}^*)$ eine überabzählbar unendliche Menge. □

d Kommen wir zu einer weiteren überabzählbaren Menge.

Satz: *Die Menge* $\mathrm{Abb}(\mathbb{N}^*, \{0,1\})$ *aller Abbildungen von $\mathbb{N}^*$ nach $\{0,1\}$, man spricht auch von der Menge aller* ***binären Folgen****, ist überabzählbar unendlich.*

Beweis. Wir verwenden ein ähnliche Idee wie im Beweis zu Satz 12b (siehe 23f). Zu jeder Teilmenge U von $\mathbb{N}^*$ sei

$$\chi_U : \mathbb{N}^* \to \{0,1\},\ n \mapsto \begin{cases} 1, \text{ falls } n \in U \\ 0, \text{ falls } n \notin U \end{cases}$$

die zu U gehörende **charakteristische binäre Folge**. Bei der Abbildung

$$\chi : \mathcal{P}(\mathbb{N}^*) \to \mathrm{Abb}(\mathbb{N}^*, \{0,1\}),\ U \mapsto \chi_U$$

handelt es sich um eine Bijektion. Deren Umkehrabbildung ist

$$\chi^{-1} : \mathrm{Abb}(\mathbb{N}^*, \{0,1\}) \to \mathcal{P}(\mathbb{N}^*),\ (x_n)_{n\in\mathbb{N}^*} \mapsto \{j \in \mathbb{N}^* : x_j = 1\}.$$

Da $\mathcal{P}(\mathbb{N}^*)$ unendlich ist, gibt es eine injektive Abbildung $\gamma : \mathbb{N}^* \to \mathcal{P}(\mathbb{N}^*)$. Nach Satz 22a-(1) ist dann auch $\chi \circ \gamma$ injektiv, und das zeigt, dass $\mathrm{Abb}(\mathbb{N}^*, \{0,1\})$ eine unendliche Menge ist. Wäre nun $\mathrm{Abb}(\mathbb{N}^*, \{0,1\})$ eine abzählbar unendliche Menge, so gäbe es eine Bijektion $\sigma : \mathbb{N}^* \to \mathrm{Abb}(\mathbb{N}^*, \{0,1\})$. Dann wäre nach Satz 22a-(3) aber auch $\chi^{-1} \circ \sigma$ eine Bijektion von $\mathbb{N}^*$ nach $\mathcal{P}(\mathbb{N}^*)$, und demnach $\mathcal{P}(\mathbb{N}^*)$ abzählbar unendlich. Das widerspricht Satz 26c. □

e Wir beenden diesen Abschnitt mit einer wichtigen Erkenntnis über die reellen Zahlen.

Satz: *Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar unendlich.*

Beweis. Der Beweis verwendet Grundlegendes aus der Analysis, so dass wir hier auf Schulkenntnisse bauen müssen.

(1) Es sei $J := \{x \in \mathbb{R} : 0 < x < 1\}$ die Menge aller reellen Zahlen zwischen 0 und 1 (das offene Intervall von 0 bis 1). Mit Methoden der Analysis zeigt man, dass die Abbildung

$$\phi : J \to \mathbb{R},\ x \mapsto \frac{x - \frac{1}{2}}{x(x-1)}$$

bijektiv ist:
- Die erste Ableitung von ϕ erfüllt $\phi'(x) < 0$ für jedes $x \in J$, und deshalb ist ϕ streng monoton fallend, insbesondere injektiv.
- Bei $x \to 0^+$ geht $\phi(x)$ gegen $+\infty$. Bei $x \to 1^-$ geht $\phi(x)$ gegen $-\infty$.
- Da ϕ eine stetige Funktion ist, und deshalb keine Sprungstelle hat, muss ϕ auch jeden Wert $y \in \mathbb{R}$ als Funktionswert annehmen. Das heißt: ϕ ist surjektiv.

(2) Wie im Beweis von Satz 26d folgert man die Unendlichkeit von J aus der Unendlichkeit von $\mathbb{R}$. Ferner ist entsprechend die Überabzählbarkeit von $\mathbb{R}$ gleichbedeutend mit der Überabzählbarkeit von J. Es reicht daher die Überabzählbarkeit von J nachzuweisen, was wir in (3) tun werden.

(3) Man nimmt an, dass J abzählbar unendlich ist und führt dies zum Widerspruch. Dazu bedient man sich eines weiteren *Diagonalargumentes* von Cantor, das auch in Variationen innerhalb der *Theoretischen Informatik* zum Tragen kommt.
Wir nehmen also an, es gibt eine Bijektion von $\mathbb{N}^*$ nach J, nennen wir sie σ. Wir denken uns die reellen Zahlen $\sigma(1)$, $\sigma(2)$, $\sigma(3)$, ... allesamt in Dezimalschreibweise dargestellt.[19] Für jedes $n \in \mathbb{N}^*$ seien α_n und β_n wie folgt definiert:
- α_n sei die n-te Nachkommastelle der Zahl $\sigma(n)$ in ihrer Dezimaldarstellung.

[19] Aus der Analysis weiß man, dass es zu jeder Zahl $r \in J$ genau eine entsprechende Dezimalfolge gibt, die r darstellt, und die nicht ab einem bestimmten Zeitpunkt konstant gleich 9 ist.

- Es sei
$$\beta_n := \begin{cases} 0, \text{ falls } \alpha_n = 1 \\ 1, \text{ falls } \alpha_n \neq 1. \end{cases}$$
Ausgehend von β ist dann
$$s := 0.\beta_1\beta_2\beta_3\beta_4\beta_5...\beta_i...$$
eine konkrete Zahl aus J, nämlich diejenige Zahl, deren Dezimalbruchentwicklung gerade durch β beschrieben wird. Aufgrund der Bijektivität von σ gibt es eine natürliche Zahl $m \in \mathbb{N}^*$ mit $\sigma(m) = s$. Es sei b die m-te Nachkommastelle von s. Dann gilt einerseits $b = \alpha_m$ und andererseits $b = \beta_m$, also folgt $\alpha_m = \beta_m$. Das ist aber offensichtlich ein Widerspruch zur Definition von β. Insgesamt muss man daher die Annahme, dass es eine Bijektion von $\mathbb{N}^*$ nach J gibt, verwerfen.

□

f Ergänzend ist Folgendes zu erwähnen.

Zwei Mengen K und L heißen **gleichmächtig**, falls eine Bijektion von K nach L (und durch die Umkehrabbildung dann auch eine Bijektion von L nach K) existiert.

- Beispielsweise sind die Mengen $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, sowie $\mathbb{Q}$ als abzählbar unendliche Mengen untereinander jeweils gleichmächtig.
- Ebenso sind J (aus dem Beweis von Satz 26e) und $\mathbb{R}$ gleichmächtig.
- Allerdings sind $\mathbb{N}$ und $\mathbb{R}$ nicht gleichmächtig, da $\mathbb{R}$ ja überabzählbar ist.
- Nach dem Beweis von Satz 26d sind die beiden Mengen $\text{Abb}(\mathbb{N}^*, \{0,1\})$ und $\mathcal{P}(\mathbb{N}^*)$ gleichmächtig und überabzählbar unendlich. Man kann zeigen, dass $\mathbb{R}$ und $\text{Abb}(\mathbb{N}^*, \{0,1\})$ gleichmächtig sind, und deshalb sind auch $\mathbb{R}$ und $\mathcal{P}(\mathbb{N}^*)$ gleichmächtig.
- Es gilt $\mathcal{P}(\mathbb{N}^*) \subseteq \mathcal{P}(\mathbb{R})$. Außerdem gibt es nach Satz 26b keine surjektive Abbildung von $\mathbb{R}$ nach $\mathcal{P}(\mathbb{R})$. Das belegt, dass $\mathcal{P}(\mathbb{R})$ überabzählbar unendlich ist und gleichzeitig nicht gleichmächtig zu $\mathbb{R}$ ist.

  Um die Mächtigkeit von $\mathcal{P}(\mathbb{R})$ zu erfassen, müsste man also einen weiteren Begriff einführen, etwa *über-über-abzählbar*. Die Menge $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ wäre dann *über-über-über-abzählbar*, etc. Das deutet insgesamt an, was mit einer *Mächtigkeits-Hierarchie* bei unendlichen Menge gemeint ist. Mehr zu diesem Thema findet man in der Literatur unter dem Stichwort „Kardinalzahlen“.

27. **Ordnungsrelationen**

a

Definition: Eine Relation $\sim$ auf einer Menge M heißt
(1) **reflexiv**, falls $a \sim a$ für alle $a \in M$ gilt,
(2) **transitiv**, falls für $a, b, c \in M$ mit $a \sim b$ und $b \sim c$ stets $a \sim c$ folgt.
Eine Relation, die reflexiv und transitiv ist, nennt man auch eine **Quasi-Ordnung**.

b Die einfachsten Quasi-Ordnungen auf M sind id_M (also die Gleichheit auf M) und $M \times M$.

c Betrachten wir daher ein nicht-triviales Beispiel, die **Teilbarkeit** bei ganzen Zahlen.

Sind $a, d \in \mathbb{Z}$, so heißt d ein **Teiler** von a (in Zeichen: $d \mid a$), falls ein $z \in \mathbb{Z}$ mit $dz = a$ existiert.

Wegen $(-d)\cdot(-z) = a$ ist dann auch $-d$ ein Teiler von a. Andererseits gilt dann auch $d\cdot(-z) = -a$, weshalb d bzw. $-d$ auch Teiler von $-a$ sind.

Jedenfalls handelt es sich bei $\mid$ um eine Quasi-Ordnung auf $\mathbb{Z}$, denn:

- Wegen $1 \cdot z = z$ gilt $z \mid z$ für jede ganze Zahl z.
- Sind a, b, c ganze Zahlen mit $a \mid b$ und mit $b \mid c$, so gibt es ganze Zahlen x, y mit $xa = b$ und mit $yb = c$. Daraus folgt $(xy)a = c$. Wegen $xy \in \mathbb{Z}$ bedeutet dies $a \mid c$.

d Es folgt eine dritte Eigenschaft, die uns noch fehlt um zur Klasse der partiellen Ordnungen, dem Hauptthema dieses Abschnittes zu gelangen. Hierbei verwenden wir wie üblich ein einseitiges Relationssymbol.

Definition: Eine Relation $\preceq$ auf einer Menge M heißt **antisymmetrisch**, falls für $a, b \in M$ gilt: Aus $a \preceq b$ und $b \preceq a$ folgt $a = b$.
Die Relation $\preceq$ heißt eine **partielle Ordnung**, falls $\preceq$ reflexiv, transitiv und antisymmetrisch ist.

e Betrachten wir nochmals die Teilbarkeit auf $\mathbb{Z}$. Sind $a, b \in \mathbb{Z}$ mit $a \mid b$ und mit $b \mid a$, so gibt es ganze Zahlen x, y mit $xa = b$ und mit $yb = a$. Sodann folgt $(xy)a = a$. Ist nun $a \neq 0$, so muss $xy = 1$ gelten und das bedeutet $x = y = 1$ oder $x = y = -1$. Daher müssen a und b nicht gleich sein.

f Wenn wir die Teilbarkeitsrelation allerdings auf die natürlichen Zahlen einschränken, also $(\mathbb{N}, \mid)$ betrachten, so erhalten wir eine partiell geordnete Menge.

g Ein weiteres (grundlegendes) Beispiel für eine partielle Ordnung liefert (selbstverständlich) die natürliche Ordnung $\leq$ auf $\mathbb{N}$, also

$$x \leq y :\Leftrightarrow \quad \text{es gibt ein } n \in \mathbb{N} \text{ mit } x + n = y.$$

- Diese Relation ist reflexiv, denn es ist $0 \in \mathbb{N}$ und $x + 0 = x$ für jedes $x \in \mathbb{N}$.
- Sie ist auch transitiv: Falls nämlich $x \leq y$ und $y \leq z$, so gibt es natürliche Zahlen n und m mit $x + n = y$ und $y + m = z$. Sodann folgt $z = y + m = (x + n) + m = x + (n + m)$, also $x \leq z$ (wegen $n + m \in \mathbb{N}$).
- Sie ist ebenso antisymmetrisch: Falls nämlich $x \leq y$ und $y \leq x$ gilt, so gibt es natürliche Zahlen n und n' mit $x+n = y$ und mit $y+n' = x$. Daraus folgt $x = y+n' = (x+n)+n' = x + (n + n')$, also $n + n' = 0$, was wiederum $n = n' = 0$ und damit $x = y$ nach sich zieht.

h Betrachten wir ein weiteres **Beispiel:**

Es sei N eine Menge. Auf deren Potenzmenge $\mathcal{P}(N)$ ist die Mengeninklusion bzw. **Teilmengenordnung** $\subseteq$ erklärt.

- Diese ist reflexiv, denn $X \subseteq X$ für jede Menge X.
- Sie ist auch transitiv, denn aus $X \subseteq Y$ und $Y \subseteq Z$ folgt $X \subseteq Z$.
- Sie ist auch antisymmetrisch, denn $X \subseteq Y$ und $Y \subseteq X$ ist ja nach Definition 3e nichts anderes als die Gleichheit von X und Y.

Also handelt es sich auch bei $\subseteq$ um eine partielle Ordnung.

i Noch ein **Beispiel**:
Wir betrachten die Menge $\mathbb{R}^n$ aller reellen n-Tupel. Für zwei n-Tupel x und y aus $\mathbb{R}^n$ definieren wir $x \sqsubseteq y$, falls gilt $x_i \leq y_i$ für alle i. Das liefert, wie man als Übung nachrechnen möge, eine partielle Ordnung durch komponentenweisen Vergleich.[20]

j Und noch ein **Beispiel:**
Die lexikographische Ordnung $\preceq_{\text{lex}}$ auf $\mathbb{R}^n$ ist für jedes n ebenfalls eine partielle Ordnung. Dabei gilt per Definition: $x \preceq_{\text{lex}} y$, falls $x = y$ (d. h. $x_i = y_i$ für alle i), oder falls $x_k < y_k$ für den kleinsten Index k mit $x_k \neq y_k$. Beispielsweise ist $(1, 2, -1) \preceq_{\text{lex}} (1, 3, -2)$ (mit $n = 3$).

k Einige, aber nicht alle der eben betrachteten Ordnungen haben eine weitere interessante Eigenschaft, nämlich die Totalität im Sinne der folgenden Definition.

Definition: Es sei $\preceq$ eine partielle Ordnung auf einer Menge M. Dann heißt $\preceq$ eine **totale Ordnung**, wenn für alle $(a, b) \in M \times M$ gilt: $a \preceq b$ oder $b \preceq a$. Das bedeutet, dass je zwei Elemente hinsichtlich $\preceq$ vergleichbar sind.

l Wir gehen die obigen Beispiele nochmals durch und untersuchen die dort angegebenen partiellen Ordnungen hinsichtlich der Totalität.

- Die natürliche Ordnung $\leq$ ist eine totale Ordnung.
- Die Teilbarkeitsordnung $\mid$ ist hingegen nicht total, weil beispielsweise weder $2 \mid |5$ noch $5 \mid 2$ gilt.
- Die Teilmengenrelation $\subseteq$ auf $\mathcal{P}(N)$ ist nicht total, wenn $|N| \geq 2$ ist. Sind nämlich $x, y \in N$ verschieden, so stehen die beiden Mengen $\{x\}$ und $\{y\}$ nicht in Relation.
- Der komponentenweise Vergleich zweier n-Tupel aus $\mathbb{R}^n$ ist bei $n \geq 2$ keine totale Ordnung, denn beispielsweise sind $(4, -13)$ und $(5, -15)$ unvergleichbar (hier ist $n = 2$).
- Hingegen ist die lexikographische Ordnung auf $\mathbb{R}^n$ für jedes $n \in \mathbb{N}^*$ total.

[20] Hier bedeutet $\leq$ selbstverständlich die aus der Schule bekannte „kleiner gleich“-Relation reeller Zahlen.

28. **Ganze Zahlen: Division mit Rest**

a Nachdem wir im letzten Abschnitt auf die Teilbarkeit bei ganzen Zahlen eingegangen sind, bietet es sich hier an, über die Division mit Rest zu reden (was man natürlich auch schon viel früher hätte machen können).

Dazu bemerken wir zunächst, dass auf der Menge $\mathbb{R}$ der reellen Zahlen der **Absolutbetrag** (kurz: **Betrag**) durch

$$|x| := \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{falls } x < 0 \end{cases}$$

definiert ist. Anschaulich (vgl. mit Abschnitt 6) ist $|x|$ der Abstand zwischen dem Ursprung und dem der Zahl x entsprechenden Punkt auf der Zahlengerade bzw. dem Kontinuum.[21]

b Im Hinblick auf die Division bei ganzen Zahlen ist nun Folgendes sehr wichtig.

Satz: *Es seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es eindeutige ganze Zahlen q und r mit $a = qb + r$ und mit $0 \leq r < |b|$.*

Beweis. (1) Wir beweisen zunächst die *Existenz* für den Spezialfall, wo $a \in \mathbb{N}$ und $b \in \mathbb{N}^*$. Betrachte dazu die Menge $M := \{m \in \mathbb{N} : mb \leq a\}$. Es ist $0 \in M$. Falls $n \in \mathbb{N}$ mit $n > a$, so ist $nb \geq n > a$, also $n \notin M$. Daraus folgt $M \subseteq \{0, 1, \ldots, a\}$. Es sei nun q das größte Element von M. Das bedeutet $qb \leq a$, aber $(q+1)b > a$. Setze $r := a - qb$. Dann ist $r \geq 0$ (da $a \geq qb$) und $r < b$ (da $a - (q+1)b < 0$, also $a - qb < b$). Insgesamt erhält man also $a = qb + r$ und $0 \leq r < b = |b|$.

(2) Als Nächstes zeigen wir die *Eindeutigkeit* im allgemeinen Fall ($a, b \in \mathbb{Z}$ und $b \neq 0$). Es gelte $a = q_1 b + r_1 = q_2 b + r_2$ mit $0 \leq r_1 < |b|$ und mit $0 \leq r_2 < |b|$. Annahme, $r_1 \neq r_2$; o.B.d.A. gelte dann $r_1 < r_2$. Dann folgt

$$0 < r_2 - r_1 = |r_2 - r_1| = |(q_1 - q_2)b|.$$

Also folgt $q_1 \neq q_2$, und damit $|q_1 - q_2| \geq 1$. Das wiederum impliziert

$$|b| \leq |q_1 - q_2| \cdot |b| = |r_2 - r_1| = r_2 - r_1 \leq r_2 < |b|,$$

also den Widerspruch $|b| < |b|$. Das bedeutet, dass die Annahme $r_1 \neq r_2$ verworfen werden muss. Es gilt also $r_1 = r_2$. Daraus folgt aber $0 = r_2 - r_1 = |q_1 - q_2| \cdot |b|$. Wegen $b \neq 0$ erhalten wir $|q_1 - q_2| = 0$, also auch $q_1 = q_2$.

(3) Kommen wir schließlich zur *Existenz* im allgemeinen Fall. Hierbei erweist sich die **Vorzeichenfunktion** sgn als überaus nützlich; sie ist wie folgt definiert:

$$\operatorname{sgn}(x) := \begin{cases} 1 & \text{falls } x > 0 \\ 0 & \text{falls } x = 0 \\ -1 & \text{falls } x < 0. \end{cases}$$

Es gilt also $|x| = \operatorname{sgn}(x) \cdot x$ für alle x aus $\mathbb{R}$; ferner ist $\operatorname{sgn}(x)^2 = 1$ für jedes $x \neq 0$. Nach Teil (1) des Beweises gibt es nun (eindeutige) ganze Zahlen Q und R mit $|a| = Q \cdot |b| + R$ und mit $0 \leq R < |b|$. Also folgt

$$\operatorname{sgn}(a) \cdot a = Q \cdot \operatorname{sgn}(b) \cdot b + R.$$

Multiplikation beider Seiten mit $\operatorname{sgn}(a)$ liefert

$$a = Q \cdot \operatorname{sgn}(a) \cdot \operatorname{sgn}(b) \cdot b + \operatorname{sgn}(a) \cdot R.$$

Ist $R = 0$, so setzt man $r := 0$ und $q := Q \cdot \operatorname{sgn}(a) \cdot \operatorname{sgn}(b)$ und erhält dann $a = qb + r$ und $0 \leq r < |b|$. Ab jetzt sei daher $R \neq 0$. Insbesondere ist dann $a \neq 0$.

[21] Die Betragsfunktion hat wichtige Eigenschaften, auf die wir in den Übungen bzw. später im Rahmen der Analysis weiter eingehen werden.

(a) Ist $a > 0$, so reduziert sich obige Gleichung zu $a = Q \cdot \operatorname{sgn}(b) \cdot b + R$. Mit $r := R$ und $q := Q \cdot \operatorname{sgn}(b)$ ist dann $a = qb + r$ und $0 \leq r < |b|$.

(b) Es bleibt die Betrachtung des Falls $a < 0$. Dann ist $\operatorname{sgn}(a) = -1$ und daher

$$a = -Q \cdot \operatorname{sgn}(b) \cdot b - R = -Q \cdot \operatorname{sgn}(b) \cdot b - |b| + |b| - R.$$

Wegen $|b| = \operatorname{sgn}(b) \cdot b$ ist das gleichbedeutend mit

$$a = -(Q+1) \cdot \operatorname{sgn}(b) \cdot b + |b| - R.$$

Setze nun $r := |b| - R$ und $q := -(Q+1) \cdot \operatorname{sgn}(b)$. Dann ist $a = qb + r$ und $0 \leq r < |b|$, da $0 < R < |b|$.

□

c Die Berechnung von (q, r) aus (a, b) nennt man eine **Division mit Rest**. Diese gehört zu den Grundrechenarten, wobei man üblicherweise die Darstellung ganzer Zahlen im Dezimalsystem verwendet. Die Zahl q heißt **Quotient**, während r der **Rest** genannt wird. Schreibweisen: $q = a \,\texttt{div}\, b$ und $r = a \,\texttt{mod}\, b$.

29. Äquivalenzrelationen

a Neben Abbildungen und partiellen Ordnungen bilden die Äquivalenzrelationen die wichtigsten Relationen. Wie bei partiellen Ordnungen handelt es sich bei Äquivalenzrelationen um spezielle Quasi-Ordnungen. Der Unterschied zwischen einer partiellen Ordnung und einer Äquivalenzrelation besteht darin, dass die Eigenschaft der „Antisymmetrie“ durch die der „Symmetrie“ ersetzt wird. Wir verwenden daher wieder ein symmetrisches Relationssymbol.

Definition: Eine Relation $\sim$ auf einer Menge M heißt **symmetrisch**, falls für $a, b \in M$ gilt: aus $a \sim b$ folgt $b \sim a$.

Definition: Eine Relation $\sim$ auf einer Menge M heißt eine **Äquivalenzrelation**, falls sie reflexiv, symmetrisch und transitiv ist.

b Eine der wichtigsten Äquivalenzrelationen ist die Kongruenz modulo n. Sie ist Grundlage für das modulare Rechnen, auf das wir irgendwann später zurückkommen werden.

Definition: Für jedes $n \in \mathbb{N}^*$ ist auf der Menge $\mathbb{Z}$ der ganzen Zahlen eine Relation $\equiv_n$ durch

$$a \equiv_n b :\Leftrightarrow n \mid (a - b)$$

definiert. Man nennt $\equiv_n$ die Kongruenz modulo n. Man liest „a ist kongruent zu b modulo n“ und schreibt dazu auch $a \equiv b \bmod n$.

Satz: *Bei $\equiv_n$ handelt es sich um eine Äquivalenzrelation auf $\mathbb{Z}$.*

Beweis. Diese Relation ist reflexiv, denn $n \mid 0$ und $a-a = 0$ für alle a aus $\mathbb{Z}$. Sie ist transitiv: Falls nämlich $n \mid (a-b)$ und $n \mid (b-c)$, so gibt es ganze Zahlen s und t mit $ns = a-b$ und mit $nt = b-c$. Sodann ist $a-c = (a-b)+(b-c) = ns+nt = n(s+t)$, weshalb n auch Teiler von $a - c$ ist und damit $a \equiv_n c$ gilt. Sie ist symmetrisch: Falls $a \equiv_n b$, so gilt $n \mid (a - b)$; dann ist aber auch n ein Teiler von $b - a$, so dass $b \equiv_n a$ folgt. □

c Betrachten wir als weiteres Beispiel die **Parallelität von Geraden**.

Ausgangspunkt ist die Euklidische Ebene $\mathbb{R}^2$. Für ein Paar $(\alpha, \beta) \in \mathbb{R}^2$ mit $\alpha \neq 0$ definieren wir eine Teilmenge $G_{\alpha,\beta}$ des $\mathbb{R}^2$ durch

$$G_{\alpha,\beta} := \{(x, y) \in \mathbb{R}^2 : \alpha x + \beta = y\}.$$

Hierbei handelt es sich um den Funktionsgraphen der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto \alpha x + \beta$. Jeder solche Menge ist eine **Gerade** (mit endlicher Steigung α und y-Achsenabschnitt β). Wir definieren weiter eine Relation $||$ (lies: **parallel**) auf der Menge all dieser Geraden durch

$$G_{\alpha,\beta} || G_{\gamma,\delta} :\Leftrightarrow \ G_{\alpha,\beta} \cap G_{\gamma,\delta} = \emptyset \text{ oder } G_{\alpha,\beta} = G_{\gamma,\delta}.$$

Bei der Parallelität handelt es sich um eine Äquivalenzrelation. Zum Nachweis werden wir allerdings nicht die drei Axiome gemäß Definition 29a durchgehen; vielmehr berechnen wir den Schnitt zweier beliebiger Geraden und leiten daraus alles Weitere ab.

Annahme, der Punkt (x, y) liegt auf den beiden Geraden $G_{\alpha,\beta}$ und $G_{\gamma,\delta}$. Dann gilt $\alpha x + \beta = y = \gamma x + \delta$. Ist $\alpha = \gamma$, so folgt daraus sofort $\beta = \delta$, und damit natürlich $G_{\alpha,\beta} = G_{\gamma,\delta}$. Ist $\alpha \neq \gamma$, so kann man die Gleichung nach x auflösen; man erhält $x = \frac{\delta-\beta}{\alpha-\gamma}$, woraus dann wiederum $y = \frac{\alpha\delta-\beta\gamma}{\alpha-\gamma}$ folgt.

Insgesamt können wir daher Folgendes festhalten: Für $(\alpha, \beta) \neq (\gamma, \delta)$ ist $G_{\alpha,\beta} \cap G_{\gamma,\delta}$ entweder leer oder einelementig; letzteres liegt genau bei $\alpha \neq \gamma$ vor. Somit gilt, dass $G_{\alpha,\beta}$ und $G_{\gamma,\delta}$ genau dann parallel sind, wenn $\alpha = \gamma$ ist. Aufgrund dieser Charakterisierung, und da die Gleichheit (trivialerweise) eine Äquivalenzrelation ist, ist auch die Parallelität eine Äquivalenzrelation.

30. Äquivalenzklassen

a Das wichtigste Phänomen einer Äquivalenzrelation ist, dass man die zugrunde liegende Menge in Äquivalenzklassen zerlegen (bzw. partitionieren) kann.

Definition: Es sei $\sim$ eine Äquivalenzrelation auf einer Menge M. Ist $a \in M$, so heißt die Menge

$$[a]_\sim := \{x \in M : x \sim a\}$$

die zu a gehörende **Äquivalenzklasse**. In diesem Zusammenhang nennt man a einen **Repräsentanten** seiner Klasse.[a] Die Menge aller Äquivalenzklassen von $\sim$ wird im Allgemeinen mit $M/\sim$ bezeichnet.[b]

[a] Aufgrund der Reflexivität von $\sim$ ist nämlich stets $a \in [a]_\sim$.
[b] auch wenn dieses Symbol auf den ersten Blick etwas merkwürdig aussieht

b Ist $\sim$ eine Äquivalenzrelation auf einer Menge M und sind $a, b \in M$, so gilt

- entweder $[a]_\sim \cap [b]_\sim = \emptyset$
- oder $[a]_\sim = [b]_\sim$.

Denn: Annahme, die Äquivalenzklassen $[a]_\sim$ und $[b]_\sim$ haben ein gemeinsames Element x. Dann ist zu zeigen, dass $[a]_\sim = [b]_\sim$ folgt. Dazu sei $y \in [a]_\sim$ beliebig. Nach Definition von $[a]_\sim$ gilt dann $y \sim a$. Ferner ist auch $a \sim x$, so dass aufgrund der Transitivität auch $y \sim x$ ist. Wegen $x \sim b$ folgt erneut wegen der Transitivität, dass $y \sim b$ ist, was $y \in [b]_\sim$ bedeutet. Das beweist insgesamt $[a]_\sim \subseteq [b]_\sim$. Mit der gleichen Argumentation erhält man $[b]_\sim \subseteq [a]_\sim$ und damit die Gleichheit der beiden Mengen. Damit ist folgender Satz bewiesen.

Satz: *Ist $\sim$ eine Äquivalenzrelation auf einer Menge M, so bildet das Mengensystem $M/\sim$ der Äquivalenzklassen eine Partition, also eine Zerlegung von M.* □

c Wir wollen gleich die zur „Kongruenz modulo n“ gehörende Partition von $\mathbb{Z}$ bestimmen und führen dazu folgende vereinfachenden Bezeichnungen ein.

Definition: Für $a \in \mathbb{Z}$ sei $[a]_n := [a]_{\equiv_n}$ die Äquivalenzklasse von a modulo n. Die Äquivalenzklassen nennt man auch **Restklassen modulo** n. Ferner bezeichne $\mathbb{Z}_n$ (statt $\mathbb{Z}/\equiv_n$) die Menge aller Restklassen modulo n.

d Der eben eingeführte Begriff der Restklasse modulo n liegt in folgendem Resultat begründet. Wir erinnern dazu an die Division mit Rest, wonach es zu gegebenen $z \in \mathbb{Z}$ und $n \in \mathbb{N}^*$ genau ein Paar $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ mit $z = qn + r$ und mit $0 \leq r < n$ gibt. Man nennt r den Rest und schreibt $r = z \,\mathtt{mod}\, n$, und q den Quotienten und schreibt $z \,\mathtt{div}\, n$.

Satz: *Es sei $n \in \mathbb{N}^*$. Dann gelten:*

(1) $a \equiv_n b \Leftrightarrow a \,\mathtt{mod}\, n = b \,\mathtt{mod}\, n$
(2) *ist* $r := a \,\mathtt{mod}\, n$, *so gilt* $[a]_n = \{r + nt : t \in \mathbb{Z}\} = [a \,\mathtt{mod}\, n]_n$
(3) *die Anzahl* $|\mathbb{Z}_n|$ *der Restklassen modulo n ist gleich n.*

Beweis. (1) Es seien $a = q_1 n + r_1$ und $b = q_2 n + r_2$ mit $q_1, q_2 \in \mathbb{Z}$ und mit $0 \leq r_1 < n$ und $0 \leq r_2 < n$. Dann ist $b - a = n(q_2 - q_1) + (r_2 - r_1)$. Zur Implikation $\Rightarrow$: Falls $r_1 = r_2$, so folgt $b - a = n(q_2 - q_1)$, so dass n Teiler von $b - a$

ist und daher $a \equiv_n b$ gilt. Zur Implikation $\Leftarrow$: Falls $a \equiv_n b$, etwa $sn = b - a$ für ein $s \in \mathbb{Z}$, so ist

$$r_2 - r_1 = b - a - n(q_2 - q_1) = ns - n(q_2 - q_1) = n(s - q_2 + q_1)$$

durch n teilbar. Wegen $r_1, r_2 \in \{0, 1, ..., n-1\}$ kann dies aber nur für $r_1 = r_2$ sein. Damit ist die Äquivalenz in (1) bewiesen.

(2) Mit $q := a \,\mathtt{div}\, n$ ist also $a = qn + r$, so dass die Differenz $a - r = qn$ durch n teilbar ist, was wiederum $a \equiv_n r$ bedeutet. Nach Satz 30b ist daher $[a]_n = [r]_n = [a \,\mathtt{mod}\, n]_n$. An dieser Stelle kann bereits $|\mathbb{Z}_n| \leq n$ gefolgert werden, da es ja nach Satz 28b nur n verschiedene Reste gibt, nämlich $0, 1, ..., n-1$. Zum Nachweis von $[r]_n = \{r + nt : t \in \mathbb{Z}\}$ setzen wir der Einfachheit halber $B_r := \{r + nt : t \in \mathbb{Z}\}$. Sicher gilt dann $r \equiv_n r + nt$ (i.e., $n|(r + nt - r)$) für alle $t \in \mathbb{Z}$, weshalb B_r Teilmenge von $[r]_n$ ist. Ist umgekehrt $b \in [r]_n$, also $b \equiv_n r$, so ist n Teiler von $b - r$, etwa $ns = b - r$. Damit ist $b = r + ns$ Element der Menge B_r. Es folgt also auch $[r]_n \subseteq B_r$ und damit insgesamt $B_r = [r]_n$.

(3) Es bleibt der Nachweis, dass $\mathbb{Z}_n$ mindestens n Elemente enthält. Es seien dazu $r, s \in \{0, 1, 2, ..., n-1\}$ mit $r \neq s$. Ohne Einschränkung gelte $r < s$. Dann sind r und s nicht kongruent modulo n (vgl. mit dem Beweis von (1)), da sonst n Teiler von $s - r$ wäre, was wegen $0 < s - r \leq n - 1$ nicht geht. Also sind $[r]_\sim$ und $[s]_\sim$ verschieden für $s \neq r$ aus $\{0, 1, ..., n-1\}$. □

e Beispielsweise sind die Restklassen modulo $n = 3$ gleich $[0]_3 = \{3t : t \in \mathbb{Z}\}$ und $[1]_3 = \{1 + 3t : t \in \mathbb{Z}\}$ sowie $[2]_3 = \{2 + 3t : t \in \mathbb{Z}\}$.

f Wir wollen auch die Äquivalenzklassen bei der Parallelität von Geraden im $\mathbb{R}^2$ aus 29c angeben. Hier ist die zur Geraden $G_{\alpha,\beta}$ gehörende Klasse $[G_{\alpha,\beta}]_{||}$ gleich $\{G_{\alpha,b} : b \in \mathbb{R}\}$; sie umfasst also genau diejenigen Geraden, deren Steigung gleich α ist.

31. **Repräsentantensysteme**

a Ist $\sim$ eine Äquivalenzrelation auf einer Menge M und ist $b \in M$ in der Klasse von $a \in M$ enthalten, so gilt $[a]_\sim = [b]_\sim$ nach Satz 30b, weshalb auch b Repräsentant der Klasse $[a]_\sim$ ist; generell ist also jedes Element einer Klasse gemäß Definition auch ein Repräsentant.

Definition: Unter einem **Repräsentantensystem** oder **Vertretersystem** einer Äquivalenzrelation $\sim$ auf einer Menge M versteht man eine Teilmenge $\mathcal{R}$ von M mit der Eigenschaft, dass **jede** Klasse durch **genau einen** Repräsentanten in $\mathcal{R}$ vertreten ist. Mit anderen Worten ist die Abbildung $\mathcal{R} \to M/\sim,\ r \mapsto [r]_\sim$ eine Bijektion.

b Beispielsweise ist $\mathcal{R} := \{-19, 47, 10004, -5122, 78955\}$ ein Repräsentantensystem aller Restklassen modulo 5.

c Häufig sticht ein Element einer Klasse besonders hervor, meist weil es besonders einfach aussieht, etwa der Rest 1 in der Klasse $[-19]_5$. Fasst man die jeweils besonderen Klassenelemente zu einem Repräsentantensystem zusammen, so spricht man von einem **kanonischen Repräsentantensystem**. Modulo 5 ist das sicherlich $\{0, 1, 2, 3, 4\}$; allerdings ist aufgrund der Symmetrie sicher auch $\{-2, -1, 0, 1, 2\}$ ein heißer Kandidat für das Prädikat kanonisch.

d Bei der Parallelität ist ein kanonischer Repräsentant der Klasse $[G_{\alpha,\beta}]_{||}$ die Gerade $G_{\alpha,0}$, denn sie ist die einzige innerhalb der Klasse, welche durch den Ursprung $(0, 0)$ des Koordinatensystems $\mathbb{R}^2$ verläuft.

32. Die B-adische Darstellung ganzer Zahlen

Im weiteren Verlauf dieses Kurses wollen wir auf die Grundlagen der elementaren Zahlentheorie eingehen. Wir beginnen mit der B-adischen Darstellung ganzer Zahlen.

a Ist $B \in \mathbb{N}$ mit $B \geq 2$, so nennt man die Menge

$$\{B^k : k \in \mathbb{N}\} = \{1, B, B^2, B^3, ...\}$$

das **Stellwertsystem zur Basis** B.

Definition: Annahme, $N \in \mathbb{N}$ mit $N \neq 0$. Ist dann $\ell \in \mathbb{N}$ und sind α_0, α_1, ..., α_ℓ aus $\{0, 1, 2, \dots B-1\}$ mit $\alpha_\ell \neq 0$ und mit

$$N = \sum_{k=0}^{\ell} \alpha_k B^k,$$

so nennt man $(\alpha_\ell, \alpha_{\ell-1}, \dots, \alpha_0)_B$ die B**-adische Darstellung** von N.

b Der folgende Algorithmus zeigt, dass jede natürliche Zahl N aus $\mathbb{N}^*$ eine solche Darstellung hat, und zwar durch explizite Berechnung. Diese Darstellung ist eindeutig bestimmt, weshalb man sie die B-adische Darstellung von N nennt.

Zuvor noch eine kurze Bemerkung zur Terminologie bei Algorithmen: Die in Klammern (* ... *) angegebenen Aussagen sind *Kommentare*. Ein Pfeil $\leftarrow$ bedeutet eine *Wertzuweisung*.

Algorithmus: (B-adische Darstellung) Nach Eingabe von $N \in \mathbb{N}^*$ wird die B-adische Darstellung von N berechnet und in einer Liste L ausgegeben.

$k \leftarrow 0$,
$x \leftarrow N$ `div` B, $\alpha_0 \leftarrow N$ `mod` B,
(* $N = xB^{k+1} + \sum_{i=0}^{k} \alpha_i B^i$ und $\alpha_i \in \{0, 1, ..., B-1\}$ für alle i aus $\{0, 1, ..., k\}$ *)
$L \leftarrow [\alpha_0]$,
`while` $x \neq 0$ `do`
    $k \leftarrow k + 1$,
    $y \leftarrow x$ `div` B, $\alpha_k := x$ `mod` B,
    $x \leftarrow y$,
    (* $N = xB^{k+1} + \sum_{i=0}^{k} \alpha_i B^i$ und $\alpha_i \in \{0, 1, ..., B-1\}$ für alle $i \in \{0, 1, ..., k\}$ *)
    füge α_k an den Anfang der Liste L hinzu
    (* $L = [\alpha_k, ..., \alpha_0]$ *)
`end (while)`
(* $N = \sum_{i=0}^{k} \alpha_i B^i$ und $\alpha_i \in \{0, 1, ..., B-1\}$ für alle i aus $\{0, 1, ..., k\}$. *)
Ausgabe von L.

Beweis. [22] **(Korrektheit und Terminierung)** Bei den Objekten k, x und y handelt es sich um Variablen bzw. Speicherplätze, die ihren Inhalt ändern können.

(1) Nach der Initialisierung ist $k = 0$ und $N = xB + \alpha_0$ mit $0 \leq \alpha_0 < B$. Der anschließende Kommentar ist korrekt, weil $xB^{k+1} = xB$ und $\sum_{i=0}^{k} \alpha_i B^i = \alpha_0 B^0 = \alpha_0$ gilt.

(2) Wir nehmen an, dass $N = xB^{k+1} + \sum_{i=0}^{k} \alpha_i B^i$ mit $\alpha_i \in \{0, 1, ..., B-1\}$ für alle $i = 0, ..., k$ bei irgendeinem Eintritt in die while-Schleife gilt. Es sei

[22] „Nein! Um Gottes Willen! Muss das sein, ein Beweis zu einem Algorithmus?“ — werden Sie womöglich denken. Klar muss das sein, schließlich soll er ja korrekt funktionieren und irgendwann auch einmal aufhören zu Rechnen. Davon hat man sich zu überzeugen.

$\ell := k+1$, weshalb die while-Schleife dann zum ℓ-ten Mal durchlaufen wird. Division von x durch B mit Rest ergibt $x = yB + \alpha_\ell$, wobei $y := x \,\texttt{div}\, B$ und $\alpha_\ell := x \,\texttt{mod}\, B$. Sodann folgt

$$\begin{aligned} N &= xB^{k+1} + \sum_{i=0}^{k} \alpha_i B^i \\ &= (yB + \alpha_\ell)B^{k+1} + \sum_{i=0}^{k} \alpha_i B^i \\ &= yB^{k+2} + \alpha_\ell B^{k+1} + \sum_{i=0}^{k} \alpha_i B^i. \end{aligned}$$

Wegen $\ell = k+1$ ist dies gleich

$$yB^{\ell+1} + \alpha_\ell B^\ell + \sum_{i=0}^{\ell-1} \alpha_i B^i = yB^{\ell+1} + \sum_{i=0}^{\ell} \alpha_i B^i.$$

Tätigt man nun die Wertzuweisungen $x \leftarrow y$ und $k \leftarrow k+1$ (also $k \leftarrow \ell$), so ergibt sich die Gültigkeit des Kommentares auch nach dem Durchlaufen der while-Schleife (beachte, dass $\alpha_\ell \in \{0, 1, ..., B-1\}$). Bei der Beziehung

$$\text{„}N = xB^{k+1} + \textstyle\sum_{i=0}^{k} \alpha_i B^i \text{ und } \alpha_i \in \{0, 1, ..., B-1\} \text{ für alle } i\text{“}$$

handelt es sich deshalb um eine sog. **Schleifeninvariante**.

(3) Bei jedem Schleifendurchlauf verringert sich der Inhalt der Variablen x (echt). Während des gesamten Algorithmus ist der Inhalt von x eine natürliche Zahl. Also ist nach endlich vielen Durchläufen x irgendwann mit 0 belegt, wodurch die Schleife dann nicht mehr durchlaufen wird. Der Algorithmus **terminiert**.

(4) Ist ℓ die letzte Belegung des Schleifenzählers k, so ergibt sich am Ende $N = xB^{\ell+1} + \sum_{i=0}^{\ell} \alpha_i B^i$ und $\alpha_i \in \{0, 1, ..., B-1\}$ für alle i aus $\{0, 1, ..., k\}$. Außerdem ist $x = 0$ und deshalb folgt wie gewünscht $N = \sum_{i=0}^{\ell} \alpha_i B^i$. Der Algorithmus arbeitet **korrekt**. □

□

c Ein **Beispiel**:

Es sei $B = 3$. Gesucht ist die 3-adische Darstellung von $N = 220$.

	k	N	x	y	α_k	L
Initialisierung	0	220	73		1	[1]
Schleifendurchläufe	1		24	24	1	[1, 1]
	2		8	8	0	[0, 1, 1]
	3		2	2	2	[2, 0, 1, 1]
	4		0	0	2	[2, 2, 0, 1, 1]

Es folgt $N = (2, 2, 0, 1, 1)_3$. In der Tat ist $2 \cdot 3^4 + 2 \cdot 3^3 + 3 + 1 = 162 + 54 + 3 + 1 = 220$.

d Die B-adische Darstellung einer negativen Zahl z besteht aus dem Vorzeichen "$-$" und der B-adischen Darstellung von $|z|$. Schließlich kann man $(0)_B$ als B-adische Darstellung der 0 auffassen. Jede ganze Zahl besitzt somit genau eine B-adische Darstellung.

e Bei der Analyse eines Algorithmus sollte man sich noch Gedanken um dessen **Komplexität** machen, das heißt, darüber nachzudenken, wieviele Resourcen an Zeit und Speicherplatz er in Abhängigkeit von der Eingabegröße benötigen wird.

Zu Algorithmus 32b ist in dieser Hinsicht Folgendes zu vermerken: Ist $N \in \mathbb{N}^*$ und m diejenige natürliche Zahl mit $B^m \leq N < B^{m+1}$, so ist m die Anzahl der Schleifendurchläufe bei Eingabe von N. Logarithmieren zur Basis B liefert also $m \leq \log_B(N) < m+1$, so dass $\log_B(N)$ ein Maß für den Rechen- bzw. Zeitaufwand ist, um das Ergebnis zu produzieren. In der Tat benötigt man

entsprechend viel Speicherplatz (nämlich Größenordnung $\log_2(B) \cdot \log_B(N)$ Bits) für die berechnete Liste L. Hinsichtlich der Maßstäbe der Komplexitätstheorie gilt dies als **effizient**.

33. **Größte gemeinsame Teiler**

In diesem Abschnitt werden wir nochmals die Teilbarkeitsrelation bei ganzen Zahlen aufgreifen. Allerdings werden wir uns auf natürliche Zahlen beschränken.

a Für jede natürliche Zahl a bezeichne

$$T(a) := \{d \in \mathbb{N} : d \text{ teilt } a\}$$

die Menge aller (natürlichen) Teiler von a. Sind $a, b \in \mathbb{N}$, so ist $T(a) \cap T(b)$ also die Menge aller **gemeinsamen Teiler** von a und b.

b

Lemma: Es seien $a, b \in \mathbb{N}$. Sind weiter $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $a = qb + r$, so gilt

$$T(a) \cap T(b) = T(b) \cap T(r).$$

Beweis. Ist t ein gemeinsamer Teiler von a und b, etwa $ta' = a$ und $tb' = b$ (mit a', b' aus $\mathbb{N}$), so ist t auch Teiler von r, denn $r = a - bq = ta' - tb'q = t(a' - b'q)$. Also ist t ein gemeinsamer Teiler von b und r. Damit ist $T(a) \cap T(b) \subseteq T(b) \cap T(r)$ gezeigt.

Ist umgekehrt s ein gemeinsamer Teiler von b und r, etwa $b = sb''$ und $r = sr'$ (mit b'', r' aus $\mathbb{N}$), so ist wegen $a = bq + r = sb''q + sr' = s(b''q + r')$ die Zahl s auch ein Teiler von a und daher ein gemeinsamer Teiler von a und b. Das bedeutet umgekehrt $T(b) \cap T(r) \subseteq T(a) \cap T(b)$. □

c

Satz: Es seien $a, b \in \mathbb{N}$. Dann gibt es eine eindeutige natürliche Zahl d mit

$$T(a) \cap T(b) = T(d).$$

Diese Zahl d heißt der **größte gemeinsame Teiler** von a und b, kurz: $d = \mathrm{ggT}(a, b)$.

Beweis. Die Eindeutigkeit folgt aus der Antisymmetrie der Teilbarkeitsrelation auf $\mathbb{N}$.

Betrachten wir also die Existenz: Falls $b = 0$, so ist $T(a) \cap T(b) = T(a) \cap \mathbb{N} = T(a)$ (denn $n \mid 0$ für jedes $n \in \mathbb{N}$), und damit folgt $a = \mathrm{ggT}(a, b)$ (was auch für $a = 0$ gültig ist). Die Idee zum Nachweis der Existenz für beleibige a, b führt uns bereits zum sog. **Euklidischen Algorithmus**. Ist $b \neq 0$, so führt man eine Division mit Rest durch: $a = qb + r$ mit $0 \leq r < b$. Sodann gilt $T(a) \cap T(b) = T(b) \cap T(r)$ nach Lemma 33b. Ist $r = 0$, so ist man fertig, denn dann gilt $T(a) \cap T(b) = T(b)$ und b ist die gesuchte Zahl. Ist hingegen $r \neq 0$, so wendet man Lemma 33b erneut an, diesmal auf b und r. Division mit Rest ergibt $b = q'r + r'$ mit $0 \leq r' < r$ und es gilt $T(b) \cap T(r) = T(r) \cap T(r')$. Wir erkennen, dass sich bei diesem Prozess das zweite Argument stets betragsmäßig verkleinert: $b > r > r'$. Durch Iteration gelangt man irgendwann zu einem Rest 0, d.h., man findet irgendwann die zuerst erörterte Situation vor. □

d Es folgt die algorithmische Ausformulierung des eben geführten Beweises.

Algorithmus: (Euklidischer Algorithmus)

Eingabe: $a, b \in \mathbb{N}$.
Ausgabe: $d = \mathrm{ggT}(a, b)$
$s \leftarrow a$, $t \leftarrow b$, $(*\ \mathrm{ggT}(a, b) = \mathrm{ggT}(s, t)\ *)$
`while` $t \neq 0$ `do`
    $r \leftarrow s \,\mathtt{mod}\, t$,
    $s \leftarrow t$, $t \leftarrow r$
    $(*\ \mathrm{ggT}(a, b) = \mathrm{ggT}(s, t)\ *)$
`end (while)`,
$(*\ \mathrm{ggT}(a, b) = \mathrm{ggT}(s, t),\ t = 0\ *)$
$d \leftarrow s$,
$(*\ d = \mathrm{ggT}(a, b)\ *)$
Ausgabe von d.

e Ein **Beispiel**: Bei Eingabe der Zahlen $a = 2413$ und $b = 473$ ergeben sich im Laufe des Algorithmus folgende Belegungen der Variablen.

s	t	$r = s \,\mathtt{mod}\, t$	$q = s \,\mathtt{div}\, t$
2413	473		
473	48	48	5
48	41	41	9
41	7	7	1
7	6	6	5
6	1	1	1
1	0	0	6

Demnach gilt $\mathrm{ggT}(2413, 473) = 1$.

f Wir werden später eine Komplexitätsanalyse zum Euklidischen Algorithmus durchführen. Wir beenden diesen Abschnitt mit einer wichtigen Definition.

Definition: Sind $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$, so nennt man a und b **teilerfremd** bzw. **relativ prim**.

34. **Kleinste gemeinsame Vielfache**

a Zu jeder natürlichen Zahl a bezeichne $V(a) = \{na : n \in \mathbb{N}\}$ die Menge aller **Vielfachen** von a. Ist b eine weitere natürliche zahl, so ist $V(a) \cap V(b)$ die Menge aller **gemeinsamen Vielfachen** von a und b.

Klar: Ist $a = 0$ oder $b = 0$, so ist $V(a) \cap V(b) = \{0\}$.

b

Satz: Es seien $a, b \in \mathbb{N}$. Dann gibt es eine eindeutige natürliche Zahl v mit

$$V(a) \cap V(b) = V(v).$$

Diese Zahl v heißt das **kleinste gemeinsame Vielfache** von a und b, Notation: $v = \mathrm{kgV}(a, b)$.

Beweis. Seien a und b beide verschieden von 0. Es ist dann offensichtlich $a \cdot b$ ein Element der Menge $V(a) \cap V(b)$, welches von 0 verschieden ist. Es sei v das Minimum der Menge $\mathbb{N}^* \cap V(a) \cap V(b)$. Wir behaupten, dass gilt:

$$V(a) \cap V(b) = V(v).$$

Zum Nachweis starten wie wie folgt: Da v gemeinsames Vielfaches von a und b ist, gibt es natürliche Zahlen x und y mit $v = xa = yb$.

- Ist $w \in V(v)$, so gibt es ein $u \in \mathbb{N}$ mit $w = uv$. Sodann ist $w = (ux)a = (uy)b$ gemeinsames Vielfaches von a und b, also $w \in V(a) \cap V(b)$. Damit ist $V(v) \subseteq V(a) \cap V(b)$ gezeigt.
- Sei umgekehrt $z \in V(a) \cap V(b)$ beliebig. Dann gibt es $s, t \in \mathbb{N}$ mit $z = sa = tb$. Wir dividieren nun z durch v mit Rest und erhalten $z = qv + r$ mit $0 \leq r < v$. Wegen

  $$r = z - qv = (s - qx) \cdot a \quad \text{und } r = z - qv = (t - qy) \cdot b$$

  ist r ein gemeinsames Vielfaches von a und von b, also $r \in N \cap V(a) \cap V(b)$. Da außerdem $r < v$ und v das kleinste Element in $\mathbb{N}^* \cap V(a) \cap V(b)$ ist, folgt $r = 0$. Aber das bedeutet $z = qv$, also $z \in V(v)$. Das liefert umgekehrt $V(a) \cap V(b) \subseteq V(v)$, insgesamt also $V(a) \cap V(b) = V(v)$ und damit die *Existenz* einer Zahl v wie in der Aussage des Satzes.

Die *Eindeutigkeit* folgt wie im Beweis von Satz 33c: Aus $V(v) = V(w)$ folgt $v \mid w$ und $w \mid v$. Da beides natürliche Zahlen sind, ergibt sich $v = w$. □

c Es stellt sich die Frage, wie man das kleinste gemeinsame Vielfache zweier natürlicher Zahlen berechnet. Die Antwort darauf gibt der folgende Satz, dessen Nachweis wir am Ende des kommenden Abschnitts führen.

Satz: Es seien a, b zwei positive natürliche Zahlen. Dann gilt

$$\mathrm{kgV}(a, b) = \frac{a \cdot b}{\mathrm{ggT}(a, b)}.$$

35. **Der erweiterte Euklidische Algorithmus**

a Bei vielen Anwendungen benötigt man nicht nur den ggT zweier ganzer Zahlen, sondern auch eine sog. **Vielfachsummendarstellung** desselben:

$$\mathrm{ggT}(a,b) = xa + yb \quad \text{mit} \quad x, y \in \mathbb{Z}.$$

b Die Berechnung (insbesondere die Existenz) einer solchen Darstellung erfolgt durch den sog. erweiterten Euklidischen Algorithmus.

Algorithmus: (Erweiterter Euklidischer Algorithmus)

Eingabe: $a, b \in \mathbb{N}$.
Ausgabe: $d = \mathrm{ggT}(a,b)$ und $x, y \in \mathbb{Z}$ mit $xa + yb = d$.

$s \leftarrow a$, $t \leftarrow b$,
$x \leftarrow 1$, $y \leftarrow 0$, $u \leftarrow 0$, $v \leftarrow 1$,
$(* \; x \cdot a + y \cdot b = s,\ u \cdot a + v \cdot b = t \; *)$
`while` $t \neq 0$ `do`
    $q \leftarrow s$ `div` t, $r \leftarrow s$ `mod` t
    $s \leftarrow t$, $t \leftarrow r$,
    $\zeta \leftarrow x - qu$, $(* \; \zeta$ ist eine Hilfsvariable $*)$
    $x \leftarrow u$, $u \leftarrow \zeta$,
    $\eta \leftarrow y - qv$, $(* \; \eta$ ist eine Hilfsvariable $*)$
    $y \leftarrow v$, $v \leftarrow \eta$
    $(* \; x \cdot a + y \cdot b = s,\ u \cdot a + v \cdot b = t \; *)$
`end (while)`,
$(* \; s = x \cdot a + y \cdot b,\ u \cdot a + v \cdot b = t,\ t = 0,\ s = \mathrm{ggT}(a,b) \; *)$
$d \leftarrow s$,
Ausgabe von x, y, d.

Beweis. Die Terminierung erfolgt analog zu Algorithmus 33d, weil t in jedem Schleifendurchlauf echt verkleinert wird, aber nichtnegativ bleibt.

Zur Korrektheit: Anfangs gilt $x = 1 = v$ und $y = 0 = u$, so dass $xa + yb = s$ und $ua + vb = t$ gültig sind. Die entsprechende Aussage gilt daher bei erstmaligem Eintritt in die while-Schleife. Wir nehmen nun (induktiv) an, dass diese Beziehung bei irgendeinem Schleifeneintritt erfüllt ist. Nach der Division mit Rest innerhalb des Schleifenkörpers erfolgt $s = qt + r$ mit $q = s$ `div` t und $r = s$ `mod` t. Ersetzt man daher s durch t, sowie x durch u und y durch v, so gilt (durch entsprechende Indizes zeitlich hervorgehoben)

$$s_{neu} = t_{alt} = u_{alt} \cdot a + v_{alt} \cdot b = x_{neu} \cdot a + y_{neu} \cdot b.$$

Weiter werden die beiden Hilfsvariablen ζ bzw. η durch $x - qu$ bzw. $y - qv$ belegt. Daher gilt danach die Beziehung

$$\begin{aligned} r &= s - qt \\ &= (x \cdot a + y \cdot b) - q \cdot (u \cdot a + v \cdot b) \\ &= (x - qu) \cdot a + (y - qv) \cdot b \\ &= \zeta \cdot a + \eta \cdot b. \end{aligned}$$

Ersetzt man nun t durch r sowie u durch ζ und v durch η, so gilt in Folge dessen

$$t_{neu} = r = \zeta \cdot a + \eta \cdot b = u_{neu} \cdot a + v_{neu} \cdot b.$$

Die angegebene Bedingung bleibt also bei jedem Schleifendurchlauf erhalten. Am Ende der Schleife gilt überdies $t = 0$ und $s = \mathrm{ggT}(a,b)$. Letzteres aufgrund der Korrektheit von Algorithmus 33d. Damit arbeitet Algorithmus 35b ebenfalls korrekt. □

b Betrachten wir ein **Beispiel**:

Wir verfolgen den Lauf von Algorithmus 35b bei Eingabe von $a = 2413$ und $b = 473$ und verwenden dabei nach der Initialisierung (wie beim eben geführten Beweis) die folgenden **Update-Formeln**:

$$\begin{array}{lcllcl} q_{neu} & := & s_{alt} \,\mathtt{div}\, t_{alt} & r_{neu} & := & s_{alt} \,\mathtt{mod}\, t_{alt} \\ u_{neu} & := & x_{alt} - q_{neu} u_{alt} & v_{neu} & := & y_{alt} - q_{neu} v_{alt} \\ x_{neu} & := & u_{alt}, & y_{neu} & := & v_{alt} \\ s_{neu} & := & t_{alt} & t_{neu} & := & r_{neu} \end{array}$$

Dann ergibt sich:

s	t	$q = s \,\mathtt{div}\, t$	$r = s \,\mathtt{mod}\, t$	x	y	u	v
2413	473			1	0	0	1
473	48	5	48	0	1	1	−5
48	41	9	41	1	−5	−9	46
41	7	1	7	−9	46	10	−51
7	6	5	6	10	−51	−59	301
6	1	1	1	−59	301	69	−352
1	0	6	0	69	−352	−473	2413

Demnach folgt am Ende $s = 1 = \mathrm{ggT}(a, b) = 69 \cdot a + (-352) \cdot b$.

c Als erste Anwendung der Existenz einer Vielfachsummendarstellung werden wir den Nachweis von Satz 34c bringen. Etwas anders formuliert zeigen wir Folgendes:

$$\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) = a \cdot b.$$

Dabei seien a und b positive natürliche Zahlen.

Beweis. Seien $v := \mathrm{kgV}(a, b)$ und $d = \mathrm{ggT}(a, b)$. Zu zeigen ist $a \cdot b = vd$. Dazu weisen wir nach:

(1) vd teilt ab,

(2) ab teilt vd.

Wegen $vd, ab \in \mathbb{N}$ folgt sodann die Behauptung, nämlich $vd = ab$.

Also:

(1) Wir schreiben $kd = a$ und $\ell d = b$ und das liefert

$$ab = kdb = a\ell d.$$

Kürzen mit d ergibt $kb = a\ell$. Setzt man $w := kb$, so bedeutet das, dass w gemeinsames Vielfaches von a und b ist, also $w \in V(a) \cap V(b)$. Nach Satz 34b ist aber $V(a) \cap V(b) = V(v)$. Deshalb ist w ein Vielfaches von v (bzw. v teilt w). Dementsprechend ist dann dv ein Teiler von $dw = dkb = ab$, also ist dv auch Teiler von ab.

(2) Andererseits gibt es $e, f \in \mathbb{N}$ mit $ea = v = fb$. Nun benötigen wir die Existenz einer Vielfachsummendarstellung des ggT: Der erweiterte Euklidische Algorithmus liefert ganze Zahlen x, y mit $xa + yb = d$. Sodann folgt

$$vd = v(xa + yb) = xav + ybv = xafb + ybea = (xf + xe)ab.$$

Daran sieht man, dass ab Teiler von vd ist.

□

36. **Analyse des (erweiterten) Euklidischen Algorithmus**

a Die Analyse des Euklidischen bzw. des Erweiterten Euklidischen Algorithmus gestaltet sich etwas schwieriger (dafür interessanter) als die Analyse von Algorithmus 32b zur Gewinnung der B-adischen Darstellung einer ganzen Zahl. Ein Satz von Lamé aus dem Jahre 1844 besagt Folgendes:

Satz: Bei Eingabe von $a, b \in \mathbb{N}^*$ mit $a > b$ ist die Anzahl der Schleifendurchläufe des (Erweiterten) Euklidischen Algorithmus kleiner als

$$1 + 5 \cdot \log_{10}(b).$$

b Da $\log_{10}(b)$ im Wesentlichen der Anzahl der Dezimalstellen von b entspricht, ist die Anzahl der Schleifendurchläufe demnach *linear* in dieser Größe. Dies ist *effizient* im Sinne der *Komplexitätstheorie*.

c Wir kommen zum Beweis von Satz 36a. Dieser vollzieht sich in mehreren Schritten, wobei die Folge $(F_n)_{n\in\mathbb{N}}$ der **Fibonacci-Zahlen** herangezogen wird. Diese ist durch folgende Vorschriften rekursiv definiert:

$$F_0 := 0,\ F_1 := 1,\ F_n := F_{n-1} + F_{n-2} \text{ für } n \geq 2.$$

Die ersten Fibonacci-Zahlen sind demnach

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ \ldots\ .$$

Weiter sei

$$\tau := \tfrac{1+\sqrt{5}}{2}.$$

Dabei handelt es sich um die positive Lösung der quadratischen Gleichung $x^2 = x + 1$. Man nennt τ die **Verhältniszahl des goldenen Schnitts**.

Schließlich bezeichne ℓ die Anzahl von Schleifendurchläufen, die der (erweiterte) Euklidische Algorithmus bei Eingabe von $a > b \geq 1$ benötigt.

Beweis. (1) Als Erstes zeigen wir (mit Induktion über ℓ), dass $b \geq F_{\ell+1}$ und $a \geq F_{\ell+2}$ gilt:

- Generell ist $b \geq 1 = F_2$ und $a > b$, also $a \geq 2 = F_3$, so dass die Aussage trivialerweise für $\ell = 1$ erfüllt ist.
- Annahme, $\ell \geq 2$. Führe eine Division mit Rest von a durch b durch, also $a = qb + r$ mit $0 \leq r < b$. Dabei ist $q \geq 1$ wegen $a > b$. Außerdem ist $r \neq 0$, denn sonst wäre b ein Teiler von a und der Algorithmus würde bereits nach einem Schleifendurchlauf enden. Es seien $a' := b$ und $b' := r$. Dann benötigt der (erweiterte) Euklidische Algorithmus bei Eingabe von a' und b' nur noch $\ell - 1$ Schritte. Wegen der Induktionsannahme erhält man $b' \geq F_\ell$ und $a' \geq F_{\ell+1}$. Daraus folgt $b = a' \geq F_{\ell+1}$ und

  $$a = qb + r = qb + b' \geq b + b' = a' + b' \geq F_{\ell+1} + F_\ell = F_{\ell+2}.$$

(2) Als Nächstes weisen wir (mit Induktion über n) nach, dass Folgendes gilt:

$$F_{n+1} < \tau^n < F_{n+2} \quad \text{für alle } n \in \mathbb{N}^*.$$

(Für den Beweis von Satz 36a benötigen wir allerdings lediglich die obere Schranke von τ^n.)

- Ist $n = 1$, so ist

  $$F_2 = 1 < \tfrac{3}{2} = \tfrac{1+\sqrt{4}}{2} < \tau < \tfrac{1+\sqrt{9}}{2} = 2 = F_3.$$

  Damit ergibt sich für $n = 2$ die Abschätzung

  $$F_3 = 2 < \tau + 1 = \tau^2 < 3 = F_4.$$

- Es sei nun $n \geq 2$ gegeben. Wir nehmen induktiv an, dass die Abschätzung für alle $m \in \mathbb{N}$ mit $1 \leq m \leq n$ gültig ist. Betrachte also die entsprechende Ungleichung für $n+1$. Unter Verwendung der Gültigkeit für die Indizes $n-1$ und n erhält man

  $$F_{n+2} = F_{n+1} + F_n < \tau^n + \tau^{n-1} < F_{n+2} + F_{n+1} = F_{n+3}.$$

  Wegen

  $$\tau^n + \tau^{n-1} = \tau^{n-1} \cdot (\tau + 1) = \tau^{n-1} \cdot \tau^2 = \tau^{n+1}$$

  ist die Behauptung bewiesen.

(3) Zusammenfassend erhalten wir aus (1) und (2) nun Folgendes:

$$b \geq F_{\ell+1} > \tau^{\ell-1}.$$

Anwenden der (streng monoton wachsenden) Logarithmus-Funktion zur Basis 10 auf die Ungleichung $b > \tau^{\ell-1}$ und die Verwendung der grundlegenden Logarithmengesetze implizieren die Ungleichung $\log_{10}(b) > (\ell - 1) \cdot \log_{10}(\tau)$, also

$$\ell < 1 + \frac{\log_{10}(b)}{\log_{10}(\tau)}.$$

Weiter gilt (etwa unter Verwendung des Binomialsatzes)[23]

$$\tau^5 = \left(\tfrac{1+\sqrt{5}}{2}\right)^5 = \tfrac{1}{32} \cdot (176 + 80 \cdot \sqrt{5}) = \tfrac{11}{2} + \tfrac{5}{2} \cdot \sqrt{5}.$$

Wegen $\sqrt{5} > 2$ liefert dies $\tau^5 > \frac{11}{2} + 5 > 10$. Daher ist

$$5 \cdot \log_{10}(\tau) = \log_{10}(\tau^5) > \log_{10}(10) = 1,$$

also $\log_{10}(\tau) > \frac{1}{5}$. Daraus folgt schließlich

$$\ell < 1 + \frac{\log_{10}(b)}{\log_{10}(\tau)} < 1 + 5 \cdot \log_{10}(b),$$

die Behauptung.

□

[23] Alternativ: $\tau^2 = \tau + 1$ ergibt $\tau^4 = \tau^2 + 2\tau + 1 = \tau + 1 + 2\tau + 1 = 3\tau + 2$, und daher ist $\tau^5 = (3\tau + 2) \cdot \tau = 3\tau^2 + 2\tau = 3(\tau + 1) + 2\tau = 5\tau + 3$.

37. **Die Primfaktorzerlegung**

a In diesem Abschnitt geht es zunächst darum, den Begriff einer Primzahl zu formalisieren. Zu jeder positiven natürlichen Zahl n bezeichne dazu $T(n)$ wieder die Menge aller natürlichen (bzw. positiven) Teiler von n.

Definition: Ist p eine natürliche Zahl mit $p \geq 2$, so heißt p eine **Primzahl**, falls $T(p) = \{1, p\}$.

b Für den Umgang mit Primzahlen erweist sich folgende Charakterisierung als sehr nützlich.

Ist p eine Primzahl, und sind a, b natürliche Zahlen mit $p = ab$, so folgt $a = 1$ oder $b = 1$. Eine Primzahl p lässt sich also nur *auf triviale Weise faktorisieren*, oder besser: p ist multiplikativ unzerlegbar (bzw. **irreduzibel**).

c Beispielsweise sind

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

alles Primzahlen, genauer gesagt sind dies alle Primzahlen, die kleiner als 100 sind.

d Das Ziel dieses Abschnitts ist der Nachweis, dass sich jede von 1 verschiedene positive natürliche Zahl im Wesentlichen eindeutig als Produkt von Primzahlen schreiben lässt (siehe die Formulierung von Satz 37h). Ein erster Schritt in diese Richtung ist folgendes

Lemma: *Ist n eine natürliche Zahl mit $n \geq 2$, so gibt es ein $\ell \in \mathbb{N}^*$ und Primzahlen $p_1, ..., p_\ell$, die nicht unbedingt verschieden sein müssen, mit $n = \prod_{i=1}^{\ell} p_i$. Insbesondere wird n von mindestens einer Primzahl geteilt.*

Beweis. Die Aussage ist sicher richtig, wenn $n = p$ selbst eine Primzahl ist: Man wählt einfach $\ell = 1$ und $p_1 = p$, sodann ist $p = \prod_{i=1}^{\ell} p_i$. Wir verwenden nun $n = 2$ als Induktionsanfang. Zum Induktionsschritt sei $n \in \mathbb{N}^*$ mit $n > 2$. Außerdem können wir annehmen, dass n keine Primzahl ist. Wir nehmen per Induktion an, dass jedes $n' < n$ eine Zerlegung gemäß Aussage des Lemmas hat.[24] Da n nicht prim ist, gibt es nach 37b zwei natürliche Zahlen a, b mit $1 < a < n$ und $1 < b < n$ und mit $n = ab$ (das heißt: n hat eine nicht-triviale Faktorisierung). Wende nun die Induktionsvoraussetzung auf a und b an: Es gibt ein $s \in \mathbb{N}^*$ und Primzahlen $p_1, ..., p_s$ mit $a = \prod_{i=1}^{s} p_i$. Außerdem gibt es ein $t \in \mathbb{N}^*$ und Primzahlen $q_1, ..., q_t$ mit $b = \prod_{i=1}^{t} q_i$. Sodann ist n gleich $\prod_{i=1}^{s} p_i \cdot \prod_{i=1}^{t} q_i$ ein Produkt von $\ell = s + t$ Primzahlen. Damit ist alles gezeigt. □

e

Satz: (von Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis. Wir führen einen Widerspruchsbeweis. Annahme, es gibt nur endlich viele Primzahlen, etwa k Stück, $p_1, ..., p_k$. Man betrachtet die Zahl

$$n := 1 + \prod_{i=1}^{k} p_i = 1 + p_1 \cdot p_2 \cdot ... \cdot p_k.$$

[24] Wir verwenden also das Prinzip der vollständigen Induktion in der Version von Satz 16g.

Wegen $n \geq 2$ wird n nach Lemma 37d von einer Primzahl geteilt, sagen wir p_ℓ (mit $\ell \in \{1, 2, \ldots, k\}$). Somit lässt sich n auch schreiben als $n = a \cdot p_\ell$ für ein $a \in \mathbb{N}^*$. Nun ist p_ℓ aber auch ein Teiler der Zahl $n - 1$, denn

$$n - 1 = \prod_{i=1}^{k} p_i = p_\ell \cdot b \quad \text{mit} \quad b = \prod_{i=1, i\neq\ell}^{k} p_i.$$

Weiter folgt dann $1 = n - (n-1) = p_\ell \cdot a - p_\ell \cdot b = p_\ell \cdot (a - b)$. Also ist p_ℓ ein Teiler von 1. Das widerspricht aber $p_\ell \geq 2$. □

f Zum Zeitpunkt des WS 2011/12 war die größte (explizit) bekannte Primzahl gleich

$$2^{43\,112\,609} - 1.$$

Sie wurde am 29.9.2008 im Rahmen der GIMPS („great internet Mersenne prime search“) gefunden. Die Anzahl ihrer Stellen in der Dezimaldarstellung ist gleich 12 978 189.

Im Laufe der Zeit wurde diese Rekorde immer weiter verbesssert. Aktuell (Stand Dezember 2018) ist die von Patrick Laroche gefundene Zahl

$$2^{82\,589\,933} - 1$$

die größte bekannte Primzahl; sie hat 24 862 048 Dezimalstellen (siehe https://www.rieselprime.de/ziki/M51).

Primzahlen der Form $2^m - 1$ nennt man übrigens **Mersenne[25]-Primzahlen**. Damit $2^m - 1$ prim ist, muss notwendigerweise m selbst prim sein (der Nachweis ist eine schöne Übungsaufgabe); allerdings ist das nicht hinreichend (das Aufsuchen eines Gegenbeispiels sei ebenfalls eine schöne Übungsaufgabe).

g Nun folgt ein ganz wichtiges Resultat. Der interessanteste Schritt im Beweis ist der Induktionsanfang (siehe den Fall „$k = 2$“ unten).

Lemma: *Es seien b_1, b_2, ..., b_k ganze Zahlen, wobei $k \geq 1$. Weiter sei p eine Primzahl, die das Produkt $\prod_{i=1}^{k} b_i$ teilt. Dann gibt es wenigstens einen Faktor b_i, der von p geteilt wird.*

Beweis. Der Bewesi erfolgt induktiv über die Größe k.

(1) Ist $k = 1$, so ist nichts zu zeigen. Für den Induktionsschritt benötigen wir aber auch den Fall $k = 2$. Daher gelte $p \mid bc$ für zwei Zahlen b, c aus $\mathbb{N}$. Es sei etwa $pa = bc$ mit $a \in \mathbb{N}$.
   - Falls p *kein* Teiler von b ist, so muss $\mathrm{ggT}(p, b) = 1$ sein, da $T(p) = \{1, p\}$ und $\mathrm{ggT}(b, p) = p$ bedeutet, dass p Teiler von b ist. Das bedeutet, dass p und b teilerfremd sind.
   - Aufgrund des erweiterten Euklidischen Algorithmus existieren dann ganze Zahlen x und y mit $1 = xb + yp$.

   Daher folgt

$$c = 1 \cdot c = (xb + yp) \cdot c = x(bc) + ypc = x(pa) + ypc = p \cdot (xa + yc),$$

   weshalb c Vielfaches von p ist.

(2) Induktionsschritt von $k - 1$ nach k, wobei $k \geq 3$. Annahme, p teilt das Produkt $\prod_{i=1}^{k} b_i$. Mit $b := \prod_{i=1}^{k-1} b_i$ und $c := b_k$ bedeutet das: p teilt bc. Aufgrund des bereits behandelten Falls $k = 2$ gilt $p \mid b$ oder $p \mid c$. Falls $p \mid c$, ist der Induktionsschritt wegen $c = b_k$ vollzogen. Falls $p \mid b$, so greift die Induktionsvoraussetzung, also $p \mid b_i$ für ein i aus $\{1, \ldots, k-1\}$.

□

[25] Marin Mersenne (1588-1648)

h Nun also zum angekündigten Hauptergebnis, welches man als **Fundamentalsatz der elementaren Zahlentheorie** bezeichnet.

Satz: *Es sei n eine natürliche Zahl mit $n \geq 2$. Dann gibt es*

- *eine eindeutige Zahl $t \in \mathbb{N}^*$,*
- *eindeutige Primzahlen q_1, ..., q_t mit $q_1 < q_2 < ... < q_t$,*
- *eindeutige natürliche Zahlen $a_1 \geq 1, ..., a_t \geq 1$*

mit

$$n = \prod_{i=1}^{t} q_i^{a_i} = q_1^{a_1} \cdot q_2^{a_2} \cdot ... \cdot q_t^{a_t}.$$

i Man nennt dies die **eindeutige** bzw. **kanonische Primfaktorzerlegung** von n. Jedes a_i heißt die **Vielfachheit** der Primzahl q_i in n. Beispielsweise ist

$$720 = 2^4 \cdot 3^2 \cdot 5.$$

Hier ist demnach $t = 3$, sowie $q_1 = 2$ und $q_2 = 3$ und $q_3 = 5$, sowie $a_1 = 4$ und $a_2 = 2$ und $a_3 = 1$.

j Zum Beweis des Fundamentalsatzes:

Beweis. Nachzuweisen sind die Existenz und die Eindeutigkeit einer Primfaktorzerlegung. Beides wird induktiv gemacht.

Nach Lemma 37d wissen wir bereits, dass es ein $\ell \in \mathbb{N}^*$ und Primzahlen $p_1, \ldots, p_\ell$ gibt, mit $n = \prod_{i=1}^{\ell} p_i$. Wir dürfen ohne Einschränkung davon ausgehen, dass die p_i aufsteigend geordnet sind: $p_1 \leq p_2 \leq ... \leq p_\ell$. Annahme, es sind auch $k \in \mathbb{N}^*$ und $r_1, ..., r_k$ Primzahlen mit $n = \prod_{j=1}^{k} r_j$. Dann ist also p_ℓ ein Teiler von $\prod_{j=1}^{k} r_j$, so dass mit Lemma 37g gilt: $p_\ell \mid r_i$ für wenigstens ein i. Nach eventueller Abänderung der Reihenfolge der r_i dürfen wir weiter $p_\ell \mid r_k$ annehmen. Da aber p_ℓ und r_k beides Primzahlen sind, muss $p_\ell = r_k$ gelten. Nun kürzen wir p_ℓ (links) und r_k (rechts) aus der Gleichung $\prod_{i=1}^{\ell} p_i = \prod_{j=1}^{k} r_j$ und erhalten für die Zahl n' mit $n' \cdot p_\ell = n$, dass n' die beiden Zerlegungen

$$n' = \prod_{i=1}^{\ell-1} p_i \quad \text{und} \quad n' = \prod_{j=1}^{k-1} r_j$$

hat. Es ist $n' < n$. Damit wurde die Situation auf eine echt kleinere Zahl als n übertragen. Das ist die Stelle, wo man einmal mehr mit vollständiger Induktion (in der Version von Satz 16g) arbeiten kann. So dürfen wir annehmen, dass für n' die Aussage über die eindeutige Primfaktorzerlegung erfüllt ist. Das liefert dann $\ell - 1 = k - 1$ (also auch $\ell = k$) und $p_i = r_i$ für $i = 1, ..., k-1$ (vorausgesetzt, dass auch die $r_1, ..., r_{k-1}$ aufsteigend sortiert sind, was man natürlich o.B.d.A. annehmen kann).

Als Induktionsverankerung dient, dass sich jede Primzahl (speziell die Zahl 2) nur trivial faktorisieren lässt. Im Falle $n' = 1$ erweist sich n als Primzahl, so dass auch dieser Fall abgedeckt ist.

Die Aussage des Satzes folgt schließlich durch Zusammenfassen gleicher Primfaktoren zu Primzahlpotenzen, in denen die jeweiligen Vielfachheiten festgehalten sind. □

38. **Ein einfaches aber nicht effizientes Faktorisierungsverfahren**

Wir beenden diesen Vorkurs mit der Angabe eines Verfahrens, mit dem man eine natürliche Zahl in ihre Primfaktoren zerlegen kann. Dies beinhaltet insbesondere einen Test, ob eine gegebene natürliche Zahl eine Primzahl ist, oder nicht.

a Zu $n \in \mathbb{N}$ mit $n \geq 2$ bezeichne $s(n) := \lfloor \sqrt{n} \rfloor$ den ganzzahligen Antreil von $\sqrt{n}$. Das bedeutet, dass es sich bei $s(n)$ um die größte natürliche Zahl m handelt, die $m^2 \leq n$ erfüllt.

Satz: *Mit der eben eingeführten Bezeichnung gelten:*
(1) *Ist n keine Primzahl, so gibt es einen Primteiler p von n mit $p \leq s(n)$.*
(2) *Ist $n \,\mathtt{mod}\, p \neq 0$ für jede Primzahl p mit $p \leq s(n)$, so ist n eine Primzahl.*

Beweis. (1) Ist $n \geq 2$ keine Primzahl, so gibt es $a, b \in \mathbb{N}$ mit $1 < a < n$ und $1 < b < n$ und mit $n = ab$ (siehe Bemerkung 37b). Ferner gibt es nach Lemma 37d Primteiler p_1 von a und p_2 von b. Aufgrund der Transitivität der Teilbarkeitsrelation sind p_1 und p_2 Primteiler von n.
Sind nun p_1 und p_2 jeweils größer als $s(n)$, so gilt $p_1 \geq s(n) + 1$ und $p_2 \geq s(n) + 1$, und außerdem ist (gemäß Definition) $s(n) + 1 > \sqrt{n}$. Daraus ergibt sich dann

$$n < (s(n) + 1)^2 \leq p_1 \cdot p_2 \leq a \cdot b = n,$$

also der Widerspruch $n < n$. Also ist $p_1 \leq s(n)$ oder $p_2 \leq s(n)$.
(2) Das folgt unmittelbar aus (1).

□

b Die Anwendung des Sachverhalts aus Satz 38a bezeichnet man als **naives Faktorisierungsverfahren**. Hierzu ein Beispiel:
Wir wollen die Zahl

$$n = 3\,138\,428\,376\,720$$

in ihre Primteiler zerlegen. Dazu verwenden wir die in 37c angegebene Liste

$$P_{100} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$$

aller Primzahlen $p \leq 100$ und testen, welche der Zahlen aus P_{100} die Zahl n mit welcher Vielfachheit teilen: Wir finden damit durch sukzessives Dividieren die Primteiler $2, 3, 5, 7, 13, 19, 37$, sowie 61 von n samt Vielfachheiten und leiten daraus die folgende (möglicherweise partielle) Faktorisierung ab:

$$n = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 61 \cdot 1117$$

Aufgrund dieser Prozedur ist die Zahl 1117 durch keine der Primzahlen aus P_{100} teilbar. Wäre 1117 keine Primzahl, so hätte diese Zahl nach Satz 38a einen Primteiler p mit $p \leq \lceil \sqrt{1117} \rceil = 35$, was mit dem Durchlaufen der Menge P_{100} aber bereits überprüft wurde. Daher ist 1117 eine Primzahl und die oben angegebene Faktorisierung in der Tat die (vollständige) Primfaktorisierung von $n = 3\,138\,428\,376\,720$.

c Kommen wir an dieser Stelle auf das Beispiel 15f zurück.
Im Jahre 1637 vermutete Pierre de Fermat, dass

$$2^{2^n} + 1$$

für jede natürliche Zahl n eine Primzahl ist. Dies ist in der Tat für n aus $\{0,1,2,3,4\}$ korrekt, wie man zu Zeiten von Fermat bereits wusste:

n	$2^{2^n}+1$	Primzahl?
0	3	ja
1	5	ja
2	17	ja
3	257	ja
4	65 537	ja

(1) Um nachzuweisen, dass 257 eine Primzahl ist, erstellen wir uns die Liste aller Primzahlen bis $s(257)$, also bis 16:

$$2,3,5,7,11,13$$

Division durch Rest zeigt, dass keine dieser Zahlen ein Teiler von 257 ist. Also ist 257 nach Satz 38a eine Primzahl.

(2) Die Anwendung dieses Verfahrens auf 65537 ist schon aufwändiger. Es ist nämlich $s(65537)$ gleich 256. Die Liste aller Primzahlen bis 257 kann beispielsweise mit dem **Siebverfahren von Eratosthenes** erstellt werden und liefert:

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251						

Keine dieser Zahlen teilt 65 537 und deshalb ist 65 537 nach Satz 38a eine Primzahl.

(3) Der kleinste offene Fall zu Fermats Zeit war

$$2^{2^5}+1 = 4\,294\,967\,297.$$

Um mit Satz 38a nachzuweisen, ob es sich dabei um eine Primzahl handelt, müsste man jede Primzahl p mit $p \leq s(4\,294\,967\,297) = 65\,536$ dahin testen, ob sie $4\,294\,967\,297$ teilt. Das erscheint uferlos[26], zumindest wenn man davon überzeugt ist, dass die Vermutung von Fermat stimmt. Das tut sie aber nicht(!), wie Euler im Jahre 1732 durch Angabe eines **Gegenbeispiels** herausfand. Aufgrund des Resultates hätte es die Mühe schon gelohnt, es mit dem naiven Faktorisierungsverfahren zu versuchen, denn:

$$2^{2^5}+1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

Man wäre also (etwa an einem verregneten Wochenende[27]) relativ schnell auf den Primteiler 641 gekommen, der gemessen am Bereich bis 65 536 ja noch relativ weit am Anfang liegt.

Die naive Faktorisierungsmethode zum Einsatz der vollständigen Faktorisierung ist letztendlich nur bei Zahlen erfolgreich, die sich aus kleinen Primfaktoren zusammensetzen. Der Nachweis, dass 6 700 417 Primzahl ist benötigt wieder Testen bis $s(6\,700\,417) = 2\,588$.[28]

d Wir präsentieren nun einen theoretischen Nachweis der Tatsache, dass 641 Teiler von $2^{2^5}+1$ ist, und folgen dabei einem Buch des Geometers Coxeter; eine elegante Argumentation, die möglicherweise auch von Euler im Jahre 1732 verwendet wurde.

Beweis. Es sei $a = 641$.

(1) Dann ist einerseits

$$a = 640 + 1 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1,$$

[26] Die Anzahl der Primzahlen $\leq 65\,537$ ist gleich 6 543.

[27] Die Anzahl der Primzahlen ≤ 641 ist gleich 116.

[28] Die Anzahl der Primzahlen $\leq 2\,588$ ist gleich 376.

und daran erkennt man, dass a Teiler von $x := 5^4 \cdot 2^{28} - 1$ ist, denn (unter zweifacher Verwendung der dritten binomischen Formel) ist

$$\begin{aligned} a \cdot (5 \cdot 2^7 - 1) \cdot (5^2 \cdot 2^{14} + 1) &= (5 \cdot 2^7 + 1) \cdot (5 \cdot 2^7 - 1) \cdot (5^2 \cdot 2^{14} + 1) \\ &= (5^2 \cdot 2^{14} - 1) \cdot (5^2 \cdot 2^{14} + 1) \\ &= 5^4 \cdot 2^{28} - 1 \\ &= x. \end{aligned}$$

(2) Andererseits gilt aber auch $a = 625 + 16 = 5^4 + 2^4$ und deshalb ist a ein Teiler von $y := 5^4 \cdot 2^{28} + 2^{32}$, denn

$$a \cdot 2^{28} = (5^4 + 2^4) \cdot 2^{28} = 5^4 \cdot 2^{28} + 2^{32} = y.$$

Wegen $a \mid y$ und $a \mid x$ ist a dann aber auch Teiler von $y - x$ (denn aus $au = x$ und $av = y$ folgt $y - x = a \cdot (v - u)$). Schließlich gilt

$$y - x = 5^4 \cdot 2^{28} + 2^{32} - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1 = 2^{2^5} + 1.$$

□

e Noch eine abschließende Bemerkung zur Komplexität der naiven Faktorisierungsmethode im Vergleich zu der des Erweiterten Euklidischen Algorithmus.

(1) Bei Eingabe von Zahlen $a, b \in \mathbb{N}^*$ mit $a > b$ benötigt der Erweiterte Euklidische Algorithmus nach Satz 36a höchstens $1 + 5 \cdot \log_{10}(b)$ Schleifendurchläufe. Es sei $m := \lceil \log_2(b) \rceil$ die kleinste natürliche Zahl, die größer oder gleich $\log_2(b)$ ist. Dann ist m genau die Anzahl der Binärstellen von b, also die Anzahl von Bits, um das Eingabedatum b abzuspeichern. Wegen

$$\log_{10}(b) = \log_{10}(2) \cdot \log_2(b) \leq \log_{10}(2) \cdot m$$

und wegen $\log_{10}(2) = 0,3010299...$ endet der Erweiterte Euklidische Algorithmus (unabhängig von der Größe der Eingabezahl a) nach höchstens

$$1 + 1,51 \cdot m < 2m$$

Schleifendurchläufen. Diese Zahl ist *linear* in der Bitlänge der Eingabegröße b. Dieses Verfahren ist daher definitiv effizient.

(2) Will man b mit Hilfe des naiven Faktorisierungsverfahrens in seine Primfaktoren zerlegen, so muss man potentiell jede Zahl $c \leq \lfloor \sqrt{b} \rfloor$ darauf hin testen, ob sie prim ist und ob sie b teilt. Es sei m wie in (1). Wegen $\sqrt{2} > \frac{141}{100}$ (siehe Bemerkung 6e) ist

$$\sqrt{b} = \sqrt{2^{\log_2(b)}} > \sqrt{2}^{m-1} > \left(\tfrac{141}{100}\right)^{m-1}.$$

Das zeigt, dass der Aufwand dieses Verfahrens *exponentiell* in der Bitlänge der Eingabegröße b ist. Dieses Verfahren ist daher definitiv nicht effizient.