1 Grundlagen der Analysis

1.1 Mathematische Sprache

Die Mathematische Sprache unterscheidet sich von der Umgangssprache des Alltags (und auch von den in vielen anderen Wissenschaften gebräuchlichen Sprechweisen) durch eine begriffliche Strenge, die oft als spitzfindig erscheinen mag. Diese ist aber unumgänglich, wenn man Aussagen über mathematische Gegenstände übersichtlich darstellen und mathematisch korrekt „beweisbar“ machen will. Am Ende eines solchen Beweises darf eigentlich keine Debatte mehr über die „Richtigkeit“ der Aussage sondern bestenfalls noch über ihre Wichtigkeit oder die Eleganz des Beweises möglich sein.

Mathematische Aussagen zeichnen sich durch folgende Eigenschaften aus:

– eindeutige Erklärung der verwendeten Begriffe;

– vollständige Angabe aller benötigten Voraussetzungen (und möglichst nur dieser);

– präzise Formulierung der Aussage unter Verwendung definierter Begriffe;

– vollständiger Beweis der Aussage unter Verwendung anerkannter logischer Schlussregeln auf der Basis der vereinbarten Voraussetzungen.

Dabei haben sich einige Sprechweisen eingebürgert, die in ihrer Bedeutung oft etwas von ihrer umgangssprachlichen Verwendung abweichen:

– *hinreichend - notwendig:* Folgt aus einem Satz von Voraussetzungen V die Gültigkeit einer Aussage E,

$$V \quad \Rightarrow \quad E,$$

so sagt man *„Wenn V gilt, dann gilt auch E“*, d. h. die Voraussetzungen V sind „hinreichend“ für die Gültigkeit von E. Umgekehrt ist die Gültigkeit von E „notwendig“ für die Gültigkeit von V, oder die Ungültigkeit von E impliziert die Ungültigkeit von V (in seiner Gesamtheit):

$$\neg E \quad \Rightarrow \quad \neg V \qquad (\neg \text{ „Negation“}).$$

Verliert die Aussage E ihre Gültigkeit bei Weglassung irgend eines Teils der Voraussetzungen V, so sagt man *„E gilt genau dann, wenn V gilt“*. Dies darf nicht damit verwechselt werden, dass der vorgeschlagene Beweis bei Weglassung einer Voraussetzung nicht mehr funktioniert, die Aussage aber unter Umständen trotzdem gültig bleibt. Ferner ist es unzulässig, aus der Richtigkeit einer Folgerung auf die Richtigkeit der Annahme zu schließen; z. B.: Aus der falschen Annahme $-1 = 1$ ergibt sich durch Quadrieren die richtige Aussage $(-1)^2 = 1^2 = 1$.

– *ein - genau ein:* Bei Aussagen über die Existenz von Objekten mit gewissen Eigenschaften bedeutet die Aussage *„Es existiert ein a mit der Eigenschaft E“*, dass mindestens eines existiert, unter Umständen aber auch mehrere. Wenn wirklich nur ein einziges solches a existiert, sagt man *„Es existiert genau ein a“*.

– *o.B.d.A. (ohne Beschränkung der Allgemeinheit):* Häufig lassen sich Aussagen mit geringerem Aufwand beweisen, wenn man sie auf einen Spezialfall der durch die gemachten Voraussetzungen beschriebenen Situation einschränkt. Lässt sich der so vereinfachte Beweis dann „direkt“ auch auf die allgemeine Situation übertragen, so wird diese Spezialisierung oft durch die Floskel „o.B.d.A.“ eingeleitet.

– *trivial (Folgerung):* Oft ergeben sich Folgerungen aus den gemachten Voraussetzungen durch einfache (offensichtliche) Argumente. Dies wird dann durch die Floskel *„Die Folgerung ist trivial.“* ausgedrückt. Dabei ist die Klassifikation eines Arguments als „trivial“ natürlich vom Wissensstand des Beweisführers abhängig und sollte daher in einführenden Texten vermieden werden.

Bei der Formulierung von Aussagen mit Hilfe von „Formeln“, d. h. in abgekürzter mathematischer Notation, haben sich einige Konventionen eingebürgert:

– Die Symbole i, j, k, l, m, n werden meist als positive, ganzzahlige Indizes zum Markieren von Elementen von Mengen oder Folgen verwendet; z. B.: $\{a_k, k = 1,\dots,m\}$ oder $(a_n)_{n\in\mathbb{N}}$. Die Symbole ε, δ stehen in der Regel für (beliebig) kleine positive Zahlen. Diese Konventionen sollten eingehalten werden, um die Erfassbarkeit der Inhalte mathematischer Aussagen zu erleichtern. (Der Alptraum des Analytikers sind Bezeichnungen der Art „ $n_\varepsilon \to 0$ für $\varepsilon \to \infty$ “.)

– Gleichheitssymbole „=“ (ist gleich), „≠“ (ist ungleich) und „:=“ (ist definiert durch):

$$2^3 = 8, \quad a+b = b+a, \qquad 2^3 \neq 7, \qquad A_n := \{1,2,\dots,n\}.$$

– Invarianz von Ausdrücken gegenüber Umbenennung von laufenden Indizes; z. B. in Summen (Summensymbol $\sum$) oder in Produkten (Produktsymbol $\prod$):

$$\sum_{k=1}^n a_k := a_1 + \cdots + a_n = \sum_{m=1}^n a_m, \qquad \prod_{k=1}^n a_k := a_1 \cdot \ldots \cdot a_n = \prod_{m=1}^n a_m.$$

– Ordnungssymbole „<“ (kleiner), „≤“ (kleiner oder gleich), „>“ (größer) und „≥“ (größer oder gleich) für Ordnungsbeziehungen:

$$2 < 3, \quad 2 \le 3, \quad 3 > 2, \quad 3 \ge 2.$$

– Implikationssymbole „⇒“ (dann gilt), „⇔“ (dann und nur dann gilt):

$$a < b \;\Rightarrow\; a < b+1; \qquad a < b \;\Leftrightarrow\; a+1 < b+1.$$

Das Symbol „:⇔“ bedeutet, dass der links stehende Ausdruck durch den rechts stehenden definiert ist.

1.2 Grundbegriffe aus Mengenlehre, Logik und Zahlentheorie

1.2.1 Elemente der Mengenlehre

„*Eine Menge ist eine wohldefinierte Zusammenfassung verschiedener Objekte zu einem Ganzen*“ (G. Cantor[1], 1885). Die Elemente einer „Menge“ sind definitionsgemäß alle von einander unterschieden. Ist ein Objekt a Element der Menge A, schreiben wir $a \in A$, andernfalls $a \notin A$. Wir beschreiben Mengen durch explizite Angabe ihrer Elemente oder durch eine charakterisierende Eigenschaft ihrer Elemente:

$$A := \{a, b, c, \dots\}, \qquad A := \{a |\ a \text{ hat die Eigenschaft } E.\}.$$

Für zwei Mengen A, B bedeutet $B \subset A$, dass $a \in B$ auch $a \in A$ impliziert, d. h.: B ist „Teilmenge“ von A oder „in A enthalten“. Die Teilmengeneigenschaft $B \subset A$ schließt die Möglichkeit $B = A$ ein. Die „leere Menge“ oder auch „Nullmenge“ wird mit $\emptyset$ bezeichnet; sie enthält keine Elemente und ist konventionsgemäß in *jeder* Menge als Teilmenge enthalten. Wir sagen, dass $B \subset A$ „strikte“ Teilmenge ist, wenn es ein Element $a \in A$ gibt mit $a \notin B$. Es gilt

$$B \subset A,\ A \subset B \quad \Rightarrow \quad A = B,$$

d. h.: Die beiden Mengen sind „gleich“, in Symbolen $A = B$. Das „Komplement B^c (in A)“ einer Teilmenge $B \subset A$ ist $B^c := \{a \in A |\ a \notin B\}$. Für Mengen sind „Vereinigung“, „Durchschnitt“ und „Differenz“ erklärt durch:

$$\begin{aligned} A \cup B &:= \{a |\ a \in A \ \text{ oder } \ a \in B\}, \\ A \cap B &:= \{a |\ a \in A \ \text{ und } \ a \in B\}, \\ A \setminus B &:= \{a |\ a \in A \ \text{ und } \ a \notin B\}. \end{aligned}$$

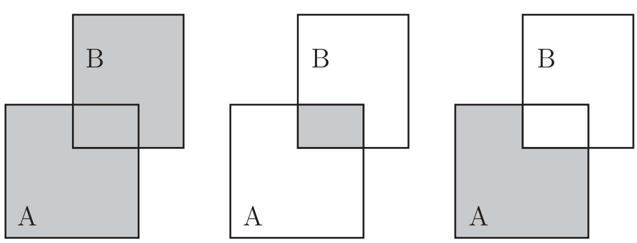

Abbildung 1.1: Vereinigung $A \cup B$, Durchschnitt $A \cap B$ und Differenz $A \setminus B$ von Mengen.

Für diese Verknüpfungen gelten die folgenden offensichtlichen Regeln:

$$\begin{aligned} (A \cup B) \cup C &= A \cup (B \cup C), & (A \cap B) \cap C &= A \cap (B \cap C), \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C), & (A \cap B) \cup C &= (A \cup C) \cap (B \cup C), \\ A \cup \emptyset &= A, & A \cap \emptyset &= \emptyset. \end{aligned}$$

[1] Georg Cantor (1845–1918): Deutscher Mathematiker; Prof. in Halle; Begründer der Mengenlehre und der „Wissenschaft des Unendlichen“.

Für Paare von Mengen A, B kann die sog. „Produktmenge“ $A \times B$ gebildet werden:

$$A \times B := \big\{\{a, b\}|\ a \in A,\ b \in B\big\}.$$

Entsprechend definiert man das Produkt $A_1 \times \ldots \times A_n$ von n Mengen $A_k,\ k = 1, \ldots, n$.

Quantoren: Für Aussagen über die Elemente einer Menge verwendet man häufig den sog. „Allquantor“ $\forall$ und den „Existenzquantor“ $\exists$, z. B.:

Für alle Elemente $a \in A$, in Symbolen „$\forall\, a \in A$“, gilt ... .

Es existiert ein Element $a \in A$, in Symbolen „$\exists\, a \in A$“, mit der Eigenschaft ... .

Äquivalenzrelation: Eine „Äquivalenzrelation“ auf einer Menge A ist eine Beziehung zwischen ihren Elementen, in Symbolen $a \sim b$, mit den Eigenschaften

R_1 : Für je zwei $a, b \in A$ gilt entweder $a \sim b$ oder $a \not\sim b$ (Relation);
R_2 : $a \sim a$ (Reflexivität);
R_3 : $a \sim b \ \Rightarrow\ b \sim a$ (Symmetrie);
R_4 : $a \sim b,\ b \sim c \ \Rightarrow\ a \sim c$ (Transitivität).

Mit Hilfe einer Äquivalenzrelation lassen sich die Elemente einer Menge A in sog. „Äquivalenzklassen“ einteilen:

$$[a] := \{b \in A|\ b \sim a\}.$$

Das (beliebig gewählte) erzeugende Element a wird dann als ein „Repräsentant“ der Äquivalenzklasse $[a]$ bezeichnet.

Beispiel 1.1: Das einfachste Beispiel einer Äquivalenzrelation ist die „Gleichheitsrelation“ $A = B$ für Mengen oder Zahlen. Hier ist das Erfülltsein von Reflexivität, Symmetrie und Transitivität offensichtlich bzw. durch Definition gegeben.

Beispiel 1.2: Sei G die Menge der Geraden der euklidischen Ebene. Die Eigenschaft zweier Geraden, parallel zueinander zu sein, hat offenbar die Eigenschaften Reflexivität, Symmetrie und Transitivität und definiert damit eine Äquivalenzrelation auf G. Die zugehörigen Äquivalenzklassen bestehen dann jeweils aus allen zu einer bestimmten Geraden parallelen Geraden.

Beispiel 1.3: Für die Menge $\mathbb{N} \times \mathbb{N}$ der Paare $\{n, m\}$ natürlicher Zahlen wird durch

$$\{n, m\} \sim \{n', m'\} \quad :\Leftrightarrow \quad n + m' = n' + m \quad (\text{b.z.w. } n - m = n' - m')$$

eine Äquivalenzrelation definiert. Reflexivität und Symmetrie sind offensichtlich. Zum Nachweis der Transitivität beachten wir, dass für $\{n, m\} \sim \{n', m'\}$ und $\{n', m'\} \sim \{n'', m''\}$ gilt $n + m' = n' + m$ und $n' + m'' = n'' + m'$, woraus wir folgern

$$(n + \underline{m'}) + m'' = (n' + m) + m'' = (n' + m'') + m = (n'' + \underline{m'}) + m,$$

bzw. $n + m'' = m + n''$, was $\{n, m\} \sim \{n'', m''\}$ bedeutet. Die zugehörigen Äquivalenzklassen bestehen dann aus allen Paaren natürlicher Zahlen mit gleicher Differenz.

Bemerkung 1.1: In der obigen Definition einer Äquivalenzrelation wird der Begriff „Beziehung zwischen Elementen einer Menge“ verwendet, welcher bisher eigentlich gar nicht definiert ist, für den man aber dennoch ein intuitives Verständnis hat. Um diesen formalen Makel zu beheben, kann man in der Sprache der Mengenlehre wie folgt vorgehen: *Zunächst ist eine „Relation“ auf einer Menge* A *gegeben durch eine ausgezeichnete Teilmenge* $R \subset A \times A$ *ihrer Produktmenge mit der Setzung*

$$a, b \in A: \quad a \sim_R b \quad :\Leftrightarrow \quad \{a, b\} \in R.$$

Damit ist die Bedingung R_1 *erfüllt. Wenn zusätzlich die Bedingungen* R_2*,* R_3 *und* R_4 *erfüllt sind, so liegt eine „Äquivalenzrelation“ vor.* Alternativ kann eine „Relation“ auch als eine Abbildung R (s. folgende Definition) von der Produktmenge $A \times A$ in eine zweielementige Menge $\{1, 0\}$ eingeführt werden, wobei $a \sim b$ durch $R(\{a, b\}) = 1$ und $a \not\sim b$ durch $R(\{a, b\}) = 0$ definiert ist.

Abbildungen zwischen Mengen: Man spricht von einer (eindeutigen) „Abbildung“ zwischen zwei Mengen A, B, wenn durch sie jedem Element („Urbild“) $a \in A$ genau ein Element („Bild“) $b \in B$ zugeordnet ist, d. h. in Symbolen:

$$f : A \to B, \quad a \in A \mapsto f(a) = b \in B.$$

Die Abbildung wird „injektiv“ genannt, wenn gilt:

$$\forall\, a_1, a_2 \in A: \quad f(a_1) = f(a_2) \;\Rightarrow\; a_1 = a_2,$$

und „surjektiv“, wenn gilt:

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

Eine injektive und surjektive Abbildung wird „bijektiv“ genannt. Zu einer bijektiven Abbildung $f : A \to B$ existiert die sog. „Umkehrabbildung“

$$f^{-1} : B \to A, \quad a = f^{-1}(b) \;:\Leftrightarrow\; b = f(a),$$

und ist ebenfalls bijektiv.

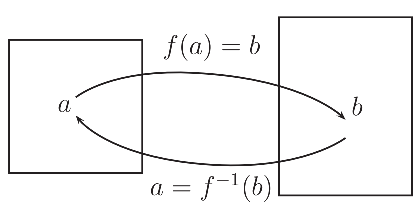

Abbildung 1.2: Abbildungen zwischen Mengen.

In der Analysis kommen auch „mehrdeutige“ Abbildungen vor, welche einem Urbild x eine ganze Menge von Bildern $\{f(x)\}$ zuordnen. Allgemeiner kann man auch Abbildungen von ganzen Teilmengen auf andere Teilmengen betrachten. Im Rahmen dieser Einführung in die Analysis werden aber solche Konstruktionen vermieden.

Existieren auf den Mengen A und B gewisse Operationen $\oplus_A$ bzw. $\oplus_B$, z. B. Addition, Multiplikation oder Ordnungsrelationen, so heißt die Abbildung $f : A \to B$ „homomorph" ("strukturerhaltend"), wenn gilt

$$\forall\, a_1, a_2 \in A : \quad f(a_1 \oplus_A a_2) = f(a_1) \oplus_B f(a_2).$$

Ein bijektiver Homomorphismus wird „Isomorphismus" genannt. Zwei Mengen A und B mit Struktur werden in diesem Sinne als „gleichwertig" (oder „äquivalent" bzw. „ununterscheidbar") angesehen, in Symbolen $A \approx B$, wenn es zwischen ihnen einen Isomorphismus gibt, dessen Umkehrung ebenfalls Isomorphismus ist. Die beiden Mengen heißen dann „isomorph (zu einander)".

Die „Mächtigkeit" einer Menge ist die Anzahl ihrer Elemente; z. B. hat die Menge

$$A = \{a_1, a_2, a_3, a_4, a_5\}$$

die Mächtigkeit $\#A = 5$. Eine Menge ist „unendlich", wenn sie bijektiv auf eine ihrer echten Teilmengen abgebildet werden kann; in diesem Fall ist $\#A = \infty$. Die Menge der natürlichen Zahlen, $\mathbb{N} = \{1, 2, 3, \dots, n, \dots\}$, ist das prototypische Beispiel einer unendlichen Menge. Eine Teilmenge von $\mathbb{N}$ bilden die *geraden* natürlichen Zahlen; eine natürliche Zahl n heißt „gerade", wenn mit einer weiteren natürlichen Zahl m gilt: $n = 2m$. Die Menge $\mathbb{N}$ wird offenbar durch die Zuordnung $n \mapsto 2n$ bijektiv auf die Teilmenge der geraden natürlichen Zahlen abgebildet. Eine (unendliche) Menge, deren Elemente mit Hilfe der natürlichen Zahlen durchnummeriert werden kann, heißt „abzählbar (unendlich)" sonst „überabzählbar". Offenbar ist die Menge $\mathbb{N}$ und jede ihrer Teilmengen abzählbar. Wir werden später Mengen kennenlernen, die nicht abzählbar sind. Insbesondere ist für jede unendliche Menge A ihre „Potenzmenge" $\mathcal{P}(A) = \{B |\ B \subset A\}$, d. h. die Menge ihrer Teilmengen, überabzählbar.

Bemerkung 1.2: Der Umgang mit unendlichen Mengen bringt Aussagen mit sich, welche der Intuition zu widersprechen scheinen. Ein Beispiel ist das sog. *„Hilbertsche[2] Hotel"*: *In einem Hotel mit (abzählbar) unendlich vielen Zimmern, welches voll belegt ist, muss ein weiterer wichtiger Gast untergebracht werden. Das Problem ist leicht lösbar. Man quartiere einfach den Gast in Zimmer* 1 *in Zimmer* 2 *um, den in Zimmer* 2 *in Zimmer* 3 *und so weiter. Allgemein wird der Gast in Zimmer* n *in Zimmer* $n+1$ *verlegt. Damit sind alle bisherigen Gäste untergebracht, und der neue Gast kann in das nun freie Zimmer* 1 *einziehen. Mit Hilfe einer ähnlichen Strategie könnten auch (abzählbar) unendlich viele neue Gäste in dem ursprünglich voll belegten Hotel untergebracht werden.*

Bemerkung 1.3: Bei der Definition von Mengen muss Vorsicht walten, um nicht mathematisch unsinnige, d. h. in sich widersprüchliche, Konstruktionen zu erhalten. Während

[2] David Hilbert (1862–1943): Bedeutender deutscher Mathematiker; wirkte in Königsberg und Göttingen; begründete u.a. den axiomatischen Aufbau der Mathematik; zum Wesen der Axiomatik (in der Geometrie) sagte er „Man muß jederzeit anstelle von Punkten, Geraden, Ebenen - Tische, Stühle, Bierseidel sagen können".

die Potenzmenge einer Menge noch ein sinnvoller Begriff ist, wird es bei Konstrukten der Art der *„Menge aller Mengen mit gewissen Eigenschaften“* gefährlich, wenn die erlaubten charakterisierenden Eigenschaften nicht gewissen Einschränkungen unterworfen werden. Die *„Menge aller Mengen, die sich nicht selbst als Element enthalten“* ist eine solche widersprüchliche Konstruktion: Denn enthält diese Menge sich selbst nicht als Element, so muss sie sich nach Definition gerade doch als Element enthalten: ein Widerspruch. Dieses Problem wird in der modernen Mengenlehre durch Restriktionen bei der Definition „erlaubter“ Mengen behoben ($\rightarrow$ *Mengenlehre*). Diese Beobachtung macht folgende pointierte Charakterisierung der Situation der Mathematik durch B. Russel[3] verständlich: *„Mathematik ist die Wissenschaft, bei der man weder weiß, wovon man spricht, noch ob das, was man sagt, wahr ist.“*.

1.2.2 Die natürlichen Zahlen

Die natürlichen Zahlen

$$\mathbb{N} = \{1, 2, 3, \dots, n, \dots\}, \qquad \mathbb{N}_0 := \mathbb{N} \cup \{0\},$$

werden, wie der Name schon ausdrückt, als „natürlich“ gegeben angesehen und bedürfen keiner weiteren Erläuterung. (Manche Autoren verwenden die Bezeichnung $\mathbb{N}$ auch für $\mathbb{N}_0$.) Der Mathematiker Kronecker[4] hat einmal gesagt, dass *„die natürlichen Zahlen der liebe Gott gemacht habe, der Rest sei Menschenwerk“*. Tatsächlich kann man alle anderen Zahlensysteme mengentheoretisch, ausgehend von den natürlichen Zahlen, konstruieren und ihre Eigenschaften aus denen der natürliche Zahlen ableiten. Dies wird im Folgenden in gewissem Umfang durchgeführt werden.

Man unterscheidet zwischen dem abstrakten Begriff einer „natürlichen Zahl“ und ihrer jeweiligen Darstellung; z. B. hat die Zahl „Acht“ in unserem dezimalen System die Darstellung 8, während sie im primitiven Strichsystem durch $||||||||$ und im römischen System durch VIII dargestellt wird. Neben der dezimalen Form mit der „Basis“ $b = 10$,

$$\begin{aligned} n &= n_k n_{k-1} \dots n_1 n_0, \qquad n_0, \dots, n_k \in \{0, 1, \dots, 9\}, \\ &:= n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \dots n_1 \cdot 10 + n_0, \end{aligned}$$

kommen noch analog gebildete Darstellungen zu den Basen $b = 60$ (Sumerer, 3. Jtsd. v. Chr.), $b = 20$ (Kelten und Mayas, 500 v. Chr. - 500 n. Chr.) und $b = 2$ sowie $b = 16$ (Binär- bzw. Hexadezimaldarstellung der modernen Informationsverarbeitung) vor.

[3] Bertrand A.W. Russel (1872–1970): Englischer Mathematiker und Philosoph; lieferte fundamentale Beiträge zu den logischen Grundlagen der Mathematik; Hauptwerk „Principia Mathematica“ (zus. mit A. N. Whitehead); erhielt 1950 den Nobel-Preis für Literatur; starkes Engagement in der Friedensbewegung.

[4] Leopold Kronecker (1823–1891): Deutscher Mathematiker; wirkte in Berlin als „Privatgelehrter“; betrieb die Arithmetisierung der Mathematik; wichtiger Vertreter des „Konstruktivismus“, welcher die generelle Verwendung des Widerspruchsbeweises und des „aktual Unendlichen“ in Form z. B. der allgemeinen reellen Zahlen ablehnt.

Auf $\mathbb{N}$ sind die arithmetischen Operationen „+“ (Addition) und „·“ (Multiplikation) erklärt. Für diese gelten u. a. die Regeln:

$$n+m=m+n, \quad n\cdot m=m\cdot n \qquad \text{(Kommutativität)}$$
$$(n+m)+k=n+(m+k), \quad (n\cdot m)\cdot k=n\cdot(m\cdot k) \qquad \text{(Assoziativität)}$$
$$(n+m)\cdot k=n\cdot k+m\cdot k \qquad \text{(Distributivität)}$$

Im Folgenden werden wir zur Kennzeichnung der Multiplikation zweier Ausdrücke a und b in der Regel den Punkt weglassen, d. h.: $a\cdot b=ab$. Die allgemeine Gültigkeit der arithmetischen Grundregeln erscheint uns aus Gewohnheit gegeben. In der Mathematik ist die Verwendung von Gewohnheitsregeln natürlich nicht akzeptabel. Die übliche Vorgehensweise ist es, einen Satz von möglichst wenigen Grundannahmen zu formulieren, aus denen alle weiteren Aussagen mit Hilfe der vorher vereinbarten logischen Schlussweisen erhalten werden können. Diese Grundannahmen (sog. „Axiome“) sollen so einfach und offensichtlich sein, dass sie keiner weiteren Begründung bedürfen. Außerdem sollen die Axiome untereinander „widerspruchsfrei“ sein, d.h.: Aus ihnen dürfen sich keine offensichtlich falschen Aussagen der Art $1=2$ ableiten lassen. Für die natürlichen Zahlen wurde solch ein Axiomensystem von Peano[5] formuliert:

Peanosches Axiomensystem der natürlichen Zahlen:

1. Die Zahl 1 ist eine natürliche Zahl, d. h. $1\in\mathbb{N}$.
2. Zu jeder natürlichen Zahl n gibt es eine natürliche Zahl n' $(=: n+1)$ als „Nachfolger“ von n.
3. Die Zahl 1 ist nicht Nachfolger einer natürlichen Zahl.
4. $n'=m' \;\Rightarrow\; n=m.$
5. Enthält eine Teilmenge $M\subset\mathbb{N}$ die Zahl 1 und mit jedem $n\in\mathbb{N}$ auch den Nachfolger n', so ist $M=\mathbb{N}$.

Ausgehend von diesen Axiomen lassen sich die arithmetischen Grundoperation „+“ und „·“ auf $\mathbb{N}$ wie folgt rekursiv erklären:

$$n+1:=n', \quad n+m':=(n+m)'.$$
$$n\cdot 1:=n, \quad n\cdot m':=n\cdot m+n.$$

Aus diesen Definitionen lassen sich alle Rechengesetze für die Addition und die Multiplikation ableiten. Man kann zeigen, dass jede Menge, welche die Peanoschen Axiome erfüllt, „isomorph“ bzgl. Addition und Multiplikation (d. h. nicht unterscheidbar) zur Menge der natürlichen Zahlen $\mathbb{N}$ ist. Ferner ist das System der Peanoschen Axiome „widerspruchsfrei“.

[5]Guiseppe Peano (1858–1932): Italienischer Mathematiker; Prof. in Turin; Beiträge zur Analysis, gewöhnlichen Differentialgleichungen, einer der Väter der Mathematischen Logik

Vollständige Induktion

Zum Beweis von Aussagen, die sich auf unendliche Mengen beziehen, verwendet man häufig das sog. Prinzip der „vollständigen Induktion“ („Induktionsschluss“). Seien E_n durch die natürlichen Zahlen $n \in \mathbb{N}$ „indizierte“ Aussagen. Der Induktionsschluß erlaubt es, die gleichzeitige Gültigkeit aller dieser Aussagen zu garantieren:

Satz 1.1 (Induktionsprinzip): *Es seien die folgenden Schritte vollzogen:*

1. Induktionsverankerung: Die Aussage E_1 ist gültig.

2. Induktionsschluß: Ist für ein $n \in \mathbb{N}$ die Aussage E_n gültig, so folgt auch die Gültigkeit von E_{n+1}.

Dann sind alle Aussagen E_n $(n \in \mathbb{N})$ gültig.

Beweis: Das Induktionsprinzip ist eine direkte Folgerung aus dem 5. Peanoschen Axiom. Dazu definieren wir die folgende Teilmenge $M \subset \mathbb{N}$:

$$M := \{n \in \mathbb{N} | \ E_n \ \text{ist gültig}\}.$$

Die Induktionsverankerung besagt dann, dass $1 \in M$, und die Induktionsannahme, dass aus $n \in M$ auch $n+1 \in M$ folgt. Folglich ist nach dem 5. Peanoschen Axiom $M = \mathbb{N}$.
Q.E.D.

Bemerkung 1.4: Der Induktionsschluss kann auch für jede Teilmenge $\mathbb{N}' = \{n \in \mathbb{N} | \ n \geq n_0\}$ mit „Anfangselement“ n_0 durchgeführt werden. Ferner ist die Bestätigung der Induktionsverankung wesentlich. Aus der Annahme z. B., dass $n > 100$ folgt auch $n+1 > 100$, was aber für allgemeine $n \in \mathbb{N}$ nicht richtig ist; es fehlt die Induktionsverankerung für $n = 1$.

Wir wollen die Arbeitsweise des „Induktionsbeweises“ anhand zweier einfacher Beispiele illustrieren. Da wir „rationale Zahlen“, d. h. „Brüche“, noch nicht formal eingeführt haben, wollen wir im Folgenden Ausdrücke der Form $r = n/m$ für $n, m \in \mathbb{N}$ als $mr = n$ verstehen.

Beispiel 1.4: Für die Summe der ersten n natürlichen Zahlen gilt die Formel

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}. \tag{1.2.1}$$

Dies erschließt man mit Hilfe der vollständigen Induktion wie folgt: Die Aussage E_n ist gerade die Gültigkeit der Summationsformel für das jeweilige $n \in \mathbb{N}$. Die Induktionsverankerung ist wegen

$$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$$

gegeben. Als Induktionsannahme sei die Formel nun gültig für ein $n \in \mathbb{N}$. Dann ist

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

Die Formel ergibt sich nun nach dem Induktionsprinzip als richtig für alle n. Die Summationsformel läßt sich auch durch direkte Berechnung (scheinbar ohne Verwendung des Induktionsprinzips) erschließen. Dazu schreibt man (wie es angeblich schon der damals gerademal 6-jährige Gauß[6] in der Schule tat)

$$\sum_{k=1}^{n} k = \frac{1}{2}\Big\{ \sum_{k=1}^{n} k + \sum_{k=1}^{n} (n+1-k) \Big\} = \frac{1}{2} \sum_{k=1}^{n} (k+n+1-k) = \frac{n(n+1)}{2} \,.$$

Das Prinzip, dass bei arithmetischen Aufgaben oft Nachdenken und Anwenden eines „Tricks" viel stupide Rechnerei ersparen kann, gilt auch in mancher Übungsaufgabe zu diesem Text.

Beispiel 1.5: Für jede natürliche Zahl $x \neq 1$ gilt die sog. „geometrische Summenformel"

$$1 + x + x^2 + \cdots + x^n = \sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}. \tag{1.2.2}$$

Dies wird wieder mit vollständiger Induktion erschlossen. Für $n = 1$ ist die Aussage wegen $1 - x^2 = (1+x)(1-x)$ offensichtlich richtig. Ist sie nun für ein $n \in \mathbb{N}$ richtig, so folgt

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

d. h.: Sie ist auch für $n+1$ richtig, womit das Induktionsprinzip anwendbar ist. Die geometrische Summenformel gilt auch für die noch einzuführenden rationalen, rellen und komplexen Zahlen.

Die exakte Formulierung der vollständigen Induktion als logisches Beweisprinzip geht wohl auf Pascal[7] zurück, obwohl es schon seit Euklid verschiedendlich in speziellen Situationen verwendet wurde. Das Induktionsprinzip ist nicht nur wichtig als Beweisargument sondern auch als Mittel zur rekursiven Definition von Eigenschaften oder Beziehungen zwischen den Elemente unendlicher Mengen. Die einfachen Potenzen einer Zahl x lassen sich so z. B. rekursiv definieren durch

$$x^0 := 1, \quad \forall\, n \in \mathbb{N} : x^n := x^{n-1}x.$$

Dieses Prinzip steckt auch hinter der obigen, rekursiven Definition der Addition und Multiplikation ausgehend von den Peanoschen Axiomen.

[6]Carl Friedrich Gauß (1777–1855): Bedeutender deutscher Mathematiker, Astronom und Physiker; wirkte in Göttingen.

[7]Blaise Pascal (1623–1662): Französischer Mathematiker und Philosoph; Prof. in Paris; arbeitete u. a. über Kegelschnitte, Kombinatorik und Wahrscheinlichkeitsrechnung; baute 1642 die erste Rechenmaschine.

1.2.3 Das Prinzip des Widerspruchsbeweises

Sei E eine Aussage über Elemente einer Menge A. Ist die Aussage „wahr“, so ist ihre Negation „falsch“. Die Negation ihrer Negation ist wieder die ursprüngliche Aussage. Dabei wird es als selbstverständlich angesehen, dass eine „vernünftige“ Aussage dieser Art entweder *wahr* oder *falsch* ist; ein Drittes gibt es nicht (lateinisch: „Tertium non datur“). Diese fundamentale Annahme und ihre verschiedenen, durch das Prädikat „vernünftig“ charakterisierten Interpretationen sind Gegenstand tiefgehender Forschung zu den Grundlagen der Mathematik ($\rightarrow$ *Mathematische Logik*).

Beispiel 1.6: Für die Menge $A = \mathbb{N}$ ist die Aussage *„Das Produkt von je zwei ungeraden natürlichen Zahlen ist ungerade“* wahr. Ihre Negation *„Es gibt zwei ungerade natürliche Zahlen, deren Produkt gerade ist“* ist also falsch.

Bei Aussagen, die mit Hilfe des All- und des Existenz-Quantors formuliert sind, folgt die Aufstellung der Negation festen Regeln. Die Beherrschung derselben ist für die korrekte Durchführung von Beweisen wichtig.

Beispiel 1.7: Die wahre Aussage *„Für jedes $k \in \mathbb{N}$ gibt es ein $n_k \in \mathbb{N}$, so dass gilt $n_k > k^2$*, oder in Symbolen:

$$\forall\, k \in \mathbb{N} \;\; \exists\, n_k \in \mathbb{N}: \;\; n_k > k^2,$$

hat die Negation *„Es gibt ein $k \in \mathbb{N}$, so dass für alle $n \in \mathbb{N}$ gilt $n \leq k^2$* “, bzw. in Symbolen:

$$\exists\, k \in \mathbb{N} \;\; \forall\, n \in \mathbb{N}: \quad n \leq k^2.$$

Der Beweis, dass eine Aussage *richtig* ist, lässt sich häufig leichter dadurch führen, dass ihre Negation als *falsch* bewiesen wird. Dies ist insbesondere bei Aussagen für Elemente *unendlicher* Mengen der Fall. Einen solchen Beweis nennt man „Widerspruchsbeweis“.

Beispiel 1.8: Eine natürliche Zahl $p\ (p \neq 1)$ wird „prim“ genannt, wenn sie nur durch sich selbst und die Eins teilbar ist (z. B.: $p = 2, 3, 5, 7, 11, 13, 17, 19, \dots$). Jede natürliche Zahl lässt sich als Produkt von Primzahlen darstellen (Beweis Übungsaufgabe). Die Behauptung ist nun, dass es unendlich viele solcher „Primzahlen“ gibt. Der *Widerspruchsbeweis* beginnt mit der (zu widerlegenden) Annahme, dass es nur endlich viele Primzahlen gibt. Diese seien ihrer Größe nach nummeriert: $p_1, p_2, \dots, p_N$. Jenseits der größten Primzahl p_N soll es also nach Annahme keine weitere Primzahl geben. Wir betrachten nun die Zahl

$$p := \prod_{n=1}^{N} p_n + 1 = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1. \tag{1.2.3}$$

Wegen $p_k \geq 2$ $(k = 1, \ldots, N-1)$, ist sicherlich $p > p_N$. Ferner kann p wegen

$$p - \prod_{n=1}^{N} p_n = 1$$

nicht durch irgend eine der N Primzahlen p_n teilbar sein. Da sich nun p als Produkt von Primzahlen darstellen lässt, muss es selbst prim sein. Dies ist aber ein Widerspruch zur Annahme, dass p_N die größte Primzahl ist. Woraus die Falschheit der Widerspruchsannahme bzw. die Richtigkeit der ursprünglichen Behauptung folgt. Wir betonen, dass ohne die spezielle Widerspruchsannahme durch (1.2.3) nicht notwendig eine Primzahl gegeben ist; z. B.: $2{\cdot}3{\cdot}5{\cdot}7{\cdot}11{\cdot}13 + 1 = 30031 = 59{\cdot}509$. Die Unendlichkeit der Menge der Primzahlen wurde bereits von dem griechischen Mathematiker Euklid[8] erkannt.

Bemerkung 1.5: Die Primzahlen haben Mathematiker schon seit jeher fasziniert. Ein wichtiges Hilfsmittel ist die Tatsache, dass sich jede natürliche Zahl auf eindeutige Weise (bis auf die Reihenfolge) als Produkt von Primzahlpotenzen darstellen läßt:

$$n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m},$$

mit paarweise verschiedenen p_i und $k_j \in \mathbb{N}$, Es ist erstaunlich, dass es zu den so übersichtlichen natürlichen Zahlen eine Reihe von sehr einfach zu formulierenden, aber auch heute noch ungeklärten Fragen gibt:

1. Man spricht von einem „Primzahlpärchen“ $\{p, p+2\}$, wenn beide, p und $p+2$, prim sind. Beispiele von Primzahlpärchen sind $\{11, 13\}, \{17, 19\}, \{29, 31\}$ und $\{87, 89\}$. Es ist unbekannt, ob es nur endlich viele oder unendlich viele solcher Primzahlpärchen gibt. Es ist sogar noch nicht einmal klar, ob man dies mit den Mitteln der „elementaren“ Zahlentheorie entscheiden kann. Dies lässt das gerade formulierte Prinzip des „Tertium non datur“ etwas fragwürdig erscheinen. Mit diesen kritischen Fragen zu den Grundlagen der Mathematik beschäftigt sich die sog. „Metamathematik“.

2. Die Beispiele $6 = 3+3$, $10 = 5+5$, $12 = 5+7$ oder $100 = 29+71$ legen die Vermutung nahe, dass sich jede gerade natürliche Zahl $n > 2$ als Summe zweier Primzahlen darstellen lässt. Diese sog. „Goldbachsche [9] Vermutung“ ist bis heute ungeklärt.

1.2.4 Grundlegendes über Zahlenmengen

Auf der Menge $\mathbb{N}$ der natürlichen Zahlen sind die elementaren arithmetischen Operationen Addition „$a + b$“ und Multiplikation „$a \cdot b$“ sowie unter gewissen Voraussetzungen auch die Subtraktion „$a - b$“ und Division „a/b“ erklärt. Subtraktion und Division sind nicht für alle Paare natürlicher Zahlen erklärt, d. h.: Die natürlichen Zahlen sind bzgl.

[8]Euklid (ca. 355–290 v. Chr.): Griechischer Philosoph und Mathematiker; wirkte in Alexandria; sein mehrbändigen Lehrbuch „Die Elemente“ faßte die Grundlagen der klassischen Geometrie zusammen; von ihm stammt das klassische mathematische Ausdrucksschema „Voraussetzung - Behauptung - Beweis“.

[9]Christian Goldbach (1698–1764): Deutscher Mathematiker und Historiker; wirkte in St. Petersburg und Moskau; lieferte u.a. Beiträge zur Zahlentheorie.

dieser Operationen „unvollständig“. Dies kann man auch so ausdrücken, dass für gegebene $n, m \in \mathbb{N}$ z. B. die Gleichung

$$n + x = m \tag{1.2.4}$$

nicht immer durch $x \in \mathbb{N}$ lösbar sind. Um diese Beschränkung zu beseitigen, werden die natürlichen Zahlen zunächst zu den „ganzen“ Zahlen (inkl. der Null) erweitert:

$$\mathbb{Z} := \{0, \pm n,\ n \in \mathbb{N}\}.$$

Diese Zahlmengenerweiterung ist, wenn man sie mathematisch präzise formulieren will, ein recht komplizierter Prozess. Zunächst gilt es, überhaupt zu definieren, was eine „negative“ natürliche Zahl $-n$ ist. Wir verstehen darunter genau genommen die Zahl, mit der die Gleichung $n + (-n) = 0$ gelöst wird. Diese Erklärung ist aber formal nicht eindeutig, da $-n$ auch die Gleichung $(2n) + 2(-n) = 0$ löst. Zur Beseitigung dieser Mehrdeutigkeit verwendet man das Hilfsmittel der Äquivalenzrelation. Wie schon oben in Beispiel 1.3 gezeigt wurde, wird auf $\mathbb{N} \times \mathbb{N}$ eine Äquivalenzrelation definiert durch

$$\{n, m\} \sim \{n', m'\} \quad :\Leftrightarrow \quad n + m' = n' + m.$$

Die zugehörigen Äquivalenzklassen $[\{n, m\}]$ bilden dann eine Menge, in welche die Menge der natürlichen Zahlen $\mathbb{N}$ durch die Setzung

$$n \in \mathbb{N} \mapsto \{2n, n\} \in [\{2n, n\}]$$

„eingebettet“ werden kann. Die Äquivalenzklasse $[\{n, m\}]$ korrespondiert im Fall $n > m$ zur natürlichen Zahl $n - m \in \mathbb{N}$, im Fall $n = m$ zur „neutralen“ Zahl 0 und im Fall $n < m$ zu einer „neuen“ Zahl $n - m = -(m - n)$, welche als „negative“ natürliche Zahl bezeichnet wird. In diesem Sinne kann man die Menge $\mathbb{Z}$ der Äquivalenzklassen $[\{n, m\}]$ von Paaren natürlicher Zahlen als Menge der ganzen Zahlen definieren. Für diese werden weiter die vertrauten Bezeichnungen $a = \pm n$ oder $a = 0$ verwendet. Man muss sich dabei aber im Klaren darüber sein, dass die „negative Zahl“ $-n \in \mathbb{Z}$ ihre eigentliche Erklärung erst als Lösung der Gleichung $n + (-n) = 0$ erhält.

In $\mathbb{Z}$ hat die Gleichung (1.2.4) die (eindeutige) Lösung $x = m - n$. Die Menge $\mathbb{Z}$ ist offenbar vollständig bzgl. der Subtraktion. Sie ist aber noch unvollständig bzgl. der Division. Dies wiederum besagt, dass für beliebige $b, y \in \mathbb{Z},\ b \neq 0,$ die „lineare“ Gleichung

$$b \cdot x = y \tag{1.2.5}$$

nicht immer durch ein $x \in \mathbb{Z}$ lösbar ist. Diese letzte Beschränkung wird durch die Einführung der „rationalen“ Zahlen

$$\mathbb{Q} = \{r/s,\ r \in \mathbb{Z},\ s \in \mathbb{N}\}$$

behoben. Bei genauerem Hinsehen, zeigt sich, dass die Erzeugung der rationalen Zahlen aus den ganzen Zahlen dabei wieder mit Hilfe einer Äquivalenzrelation erfolgt. Für Paare von Zahlen $\{r, s\},\ \{r', s'\} \in \mathbb{Z} \times \mathbb{N}$ wird durch

$$\{r, s\} \sim \{r', s'\} \quad :\Leftrightarrow \quad rs' = r's.$$

wieder eine Äquivalenzrelation definiert (Übungsaufgabe). Die zugehörigen Äquivalenzklassen $[\{r,s\}]$ bzw. ihre Repräsentanten $\{r,s\}$ werden dann als „rationale" Zahlen definiert, welche man in der üblichen Form als Quotient schreibt:

$$\{r,s\} \mapsto \frac{r}{s} \in \mathbb{Q}.$$

Man sollte aber in Erinnerung behalten, dass es sich dabei wirklich nur um eine Konvention der Schreibweise handelt; die mathematische Bedeutung liegt in der obigen Definition als Äquivalenzklasse von Paaren ganzer Zahlen.

Die ganzen Zahlen lassen sich durch die Setzung

$$r \in \mathbb{Z} \to \{r,1\} \in [\{r,1\}]$$

in diese Menge $\mathbb{Q}$ einbetten. Im Folgenden werden wir für rationale Zahlen stets die übliche Bezeichnung $a = r/s$ als Quotient ganzer Zahlen verwenden, wobei die Konvention verwendet wird, dass $r \in \mathbb{Z}$ und $s \in \mathbb{N}$; d. h.: Der Zähler r beinhaltet das Vorzeichen $\pm$. Ferner werden Zähler r und Nenner s als „teilerfremd" angenommen; andernfalls kann dies durch „Kürzen" hergestellt werden.

In $\mathbb{Q}$ hat die lineare Gleichung (1.2.5) die (eindeutige) Lösung $x = y/b$. Die Menge $\mathbb{Q}$ ist nun vollständig bzgl. der vier elementaren arithmetischen Operationen (bis auf die unzulässige Division durch Null):

$$a = \frac{r}{s},\ b = \frac{u}{v} \in \mathbb{Q} \quad \Rightarrow \quad \left\{ \begin{array}{l} a+b = \frac{r}{s} + \frac{u}{v} := \frac{rv+su}{sv} \\ a-b = \frac{r}{s} - \frac{u}{v} := \frac{rv-su}{sv} \\ a\cdot b = \frac{r}{s}\cdot\frac{u}{v} := \frac{ru}{sv} \\ a/b = \frac{r}{s}/\frac{u}{v} := \frac{rv}{su}\ (u \neq 0) \end{array} \right\}.$$

Man sagt, dass $\mathbb{Q}$ mit den Operationen „+" und „·" einen „Körper" bildet (nach Dedekind[10]). Ein solcher Körper ist charakterisiert durch die Existenz sog. „neutraler Elemente" 0 und 1 für die Addition ($a+0=a$) und die Multiplikation ($a\cdot 1 = a$) sowie die Gültigkeit der folgenden Axiome:

(I) Regeln der Addition und Multiplikation:

1. $a+b=b+a, \quad a\cdot b = b\cdot a$ (Kommutativität)
2. $(a+b)+c = a+(b+c), \quad (a\cdot b)\cdot c = a\cdot(b\cdot c)$ (Assoziativität)
3. $(a+b)\cdot c = a\cdot c + b\cdot c$ (Distributivität)

sowie durch die Lösbarkeit der Gleichungen (1.2.4) und (1.2.5). Aus diesen Grundtatsachen ergeben sich die bekannten Regeln der Arithmetik; z. B. die binomischen Formeln

$$(a\pm b)^2 = a^2 \pm 2ab + b^2, \quad a^2 - b^2 = (a+b)(a-b).$$

[10] Richard Dedekind (1831–1916): Deutscher Mathematiker; Prof. in Braunschweig; wichtige Beiträge zur Zahlentheorie.

Als Körper ist $\mathbb{Q}$ „nullteiler-frei“, d. h.: Für beliebige $a, b \in \mathbb{Q}$ folgt aus $a \cdot b = 0$ notwendig, dass $a = 0$ oder $b = 0$ ist (Folgerung aus der Lösbarkeit der Gleichung $ax = b,\ a \neq 0$). Eine eingehendere Diskussion der Eigenschaften von solchen „Körpern“ ist nicht Gegenstand dieses Kurses ($\rightarrow$ *Algebra*).

(II) Regeln der Ordnungsrelationen:
In $\mathbb{Q}$ ist der Begriff der „Positivität“ erklärt durch Auszeichnung einer Teilmenge

$$\mathbb{Q}_+ := \{a \in \mathbb{Q} |\, a = r/s,\ r, s \in \mathbb{N}\}.$$

Dies erlaubt die Definition einer „Ordnungsrelation“ für Paare $\{a, b\} \in \mathbb{Q}$ durch

$$a < b \quad (a \text{ „kleiner“ } b) \quad :\Leftrightarrow \quad b - a \in \mathbb{Q}_+.$$

Entsprechend wird definiert $\{b > a\} \ :\Leftrightarrow\ \{a < b\}$, $\{a \leq b\} \ :\Leftrightarrow\ \{a < b \text{ oder } a = b\}$ und $\{b \geq a\} \ :\Leftrightarrow\ \{a \leq b\}$. Für je zwei $a, b \in \mathbb{Q}$ gilt genau eine der Relationen $a < b,\ a = b,\ a > b$. Für diese Ordnungsrelationen gelten die vertrauten Regeln:

1. $a < b,\ b < c \quad \Rightarrow \quad a < c$ (Transitivität).

2. $a < b \quad \Rightarrow \quad a + c < b + c,\ c \in \mathbb{Q}, \quad a \cdot c < b \cdot c,\ c \in \mathbb{Q}_+$.

Hieraus folgt insbesondere für zwei Zahlen $a, b \in \mathbb{Q}$, für die man $a \geq b$ und $b \geq a$ gezeigt hat, dass notwendig $a = b$ ist. Ferner ergibt sich für beliebige Zahlen $a, b \in \mathbb{Q}$ mit $a, b > 0$ die bekannte Beziehung

$$a < b \quad \Leftrightarrow \quad \frac{1}{a} > \frac{1}{b},$$

auf deren formale Ableitung aus den Axiomen wir verzichten wollen.

Für natürliche Zahlen $n > m$ gibt es einen „größten gemeinsamen Teiler“ $\mathrm{ggt}(n, m)$, den man mit dem „euklidischen Algorithmus“ bestimmt. Dieser basiert auf der eindeutigen Darstellbarkeit $n = pm + r$ mit einem $p \in \mathbb{N}_0$ und einem „Rest“ $r \in \mathbb{N}_0$ mit $0 \leq r < m$.

Euklidischer Algorithmus

1. Bestimme r_1 und p_0, so dass $r_0 := m,\ n = p_0 r_0 + r_1,\ r_1 < r_0$,

2. Für $k \in \mathbb{N}$ bestimme r_{k+1} und p_k, so dass $r_{k-1} = p_k r_k + r_{k+1},\ r_{k+1} < r_k$.

Da nach Konstruktion $r_{k+1} < r_k$ ist, muss der Prozess nach spätestens $l \leq m$ Schritten mit Rest $r_l = 0$ abbrechen. Dann ist $r_{l-1} = \mathrm{ggt}(n, m)$, da aus $r_{l-2} = p_l r_{l-1}$ folgt, dass r_l alle vorausgehenden r_k und damit sowohl m als auch n teilt. Gäbe es einen größeren gemeinsamen Teiler von n und m, so hätte der euklidische Algorithmus schon früher abbrechen müssen.

Satz 1.2 (Dezimalbruchdarstellung): *Jede rationale Zahl a besitzt eine endliche oder periodische Dezimalbruchdarstellung der Form*

$$a = \pm(a_0 + 0{,}d_1 \dots d_s) \quad :\Leftrightarrow \quad a = \pm\Big(a_0 + \sum_{k=1}^{s} d_k \cdot 10^{-k}\Big), \quad \textit{bzw.}$$

$$a = \pm(a_0 + 0, d_1 \dots d_s \overline{d_{s+1} \dots d_{s+t}}) := \pm(a_0 + 0, d_1 \dots d_s \underbrace{d_{s+1} \dots d_{s+t}}\underbrace{d_{s+1} \dots d_{s+t}} \dots)\,,$$

mit einem ganzzahligen Anteil $a_0 \in \mathbb{N}_0$ *und „Ziffern“* $d_1, \dots, d_s \in \{0, 1, \dots, 9\}$. *Umgekehrt stellt jede Dezimalbruchzerlegung dieser Art eine rationale Zahl dar. Dabei ist bei periodischen Dezimalbrüchen die Periode* $\overline{9}$ *nicht zugelassen, d. h.: Es wird identifiziert:*

$$a_0 + 0, d_1 \dots d_{k-1} d_k \overline{9} \;:=\; a_0 + 0, d_1 \dots d_{k-1}(d_k + 1), \quad d_k < 9.$$

Beweis: i) Eine rationale Zahl $a = r/s$ mit teilerfremden $r \in \mathbb{Z}$ und $s \in \mathbb{N}$ kann nach der üblichen Divisonsregel in einen Dezimalbruch umgewandelt werden. Dabei treten „Reste“ auf, die aber höchstens $s-1$ verschiedene Werte annehmen können. Bei Auftreten des Restes Null bricht der Prozess ab, und wir erhalten einen endlichen Dezimalbruch. Andernfalls müssen sich die Reste einmal wiederholen, und wir erhalten einen periodischen Dezimalbruch.

ii) Ein endlicher Dezimalbruch stellt offenbar eine rationale Zahl dar. Ein periodischer Dezimalbruch lässt sich in der Form

$$a = \pm(a_0 + 0, d_1 \dots d_s + 0, \overline{d_{s+1} \dots d_{s+t}} \cdot 10^{-s})$$

schreiben. Es genügt also, zu zeigen, dass periodische Dezimalbrüche der Art $0, \overline{d_1 \dots d_s}$ rationale Zahlen darstellen. Nach den üblichen Regeln der Division ist nun aber

$$0, \overline{d_1 \dots d_s} = \frac{d_1 \dots d_s}{\underbrace{9 \dots 9}_{s\text{-mal}}},$$

so dass auch der periodische Dezimalbruch eine rationale Zahl darstellt. Q.E.D.

Auf $\mathbb{Q}$ ist der „Absolutbetrag“ definiert:

$$|a| := \left\{ \begin{array}{ll} a & \text{für } a > 0 \\ 0 & \text{für } a = 0 \\ -a & \text{für } a < 0 \end{array} \right\}.$$

Dieser kann als eine Abbildung $|\cdot| : \mathbb{Q} \to \mathbb{Q}$ angesehen werden, welche die folgenden charakteristischen Eigenschaften besitzt:

1. $|a| = 0 \;\Leftrightarrow\; a = 0$ (Definitheit).
2. $|a \cdot b| = |a|\,|b|$ (Multiplikativität).
3. $|a + b| \le |a| + |b|$ (Subadditivität oder sog. „Dreiecksungleichung“).

Die Definitheit und die Multiplikativität ergeben sich unmittelbar aus der Definition. Die Dreiecksungleichung folgt bei Beachtung von $\pm a \le |a|$ aus

$$a + b \le |a| + |b|, \quad -(a + b) \le |a| + |b|.$$

Eine Abbildung mit diesen Eigenschaften wird auf einem Vektorraum „Norm“ und auf einem Körper „Bewertung“ genannt. Sie dient z. B. zur Messung des „Abstandes“ $|a-b|$ zweier Zahlen $a, b \in \mathbb{Q}$; offenbar impliziert $|a-b| = 0$ notwendig $a = b$. Aus der Definition ergeben sich unmittelbar die weiteren Rechenregeln

$$|-a| = |a|, \qquad \left|\frac{a}{b}\right| = \frac{|a|}{|b|} \quad \text{für } b \neq 0.$$

Eine wichtige Eigenschaft des Absolutbetrags ist die Ungleichung

$$\big||a| - |b|\big| \leq |a-b|, \tag{1.2.6}$$

welche man aus folgenden Beziehungen erhält:

$$|a| = |a-b+b| \leq |a-b| + |b|, \qquad |b| = |b-a+a| \leq |b-a| + |a|.$$

1.3 Elemente der Kombinatorik

Für die natürlichen Zahlen $n \in \mathbb{N}$ ist die „Fakultät“ $n!$ rekursiv definiert durch

$$1! := 1, \quad \forall\, n \in \mathbb{N}: \ (n+1)! := (n+1)\, n!,$$

bzw. etwas weniger formal $n! := 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. Die Fakultät $n!$ wächst mit n enorm schnell an; z. B. ist $10! = 3.628.800$ und $1000! > 4{\cdot}10^{2.568}$. Es ist häufig praktisch, auch mit der Fakultät von 0 arbeiten zu können. Dazu setzt man $0! := 1$, was verträglich mit der Rekursionsformel $(n+1)! = (n+1)\, n!$ ist.

Satz 1.3 (Permutationen): *Die Anzahl der möglichen Anordnungen (oder „Permutationen“) der Elemente einer Menge A mit Mächtigkeit $\#A = n$ ist $n!$.*

Beweis: Wir bezeichnen die Elemente der Menge mit $1, 2, 3, \ldots, n$. Für $n = 1$ gibt es die eine Anordnung $\{1\}$ und für $n = 2$ die zwei Anordnungen $\{1, 2\}, \{2, 1\}$. Die Behauptung ist damit für $n = 1$ und $n = 2$ bewiesen (Induktionsverankerung). Zum Schluss von n nach $n+1$ beachten wir, dass die Klasse (bzw. „Menge“) derjenigen Anordnungen der Elemente $\{1, \ldots, n{+}1\}$, die das Element k auf Platz eins haben bei beliebiger Anordnung der anderen Elemente, nach Induktionsannahme $n!$ Anordnungen enthält. Es gibt nun $n+1$ solcher Klassen. Die Anzahl aller Anordnungen der Elemente $\{1, \ldots, n, n+1\}$ ist also $(n+1)n! = (n+1)!$, was zu zeigen war. Q.E.D.

Lemma 1.1 (Binominalkoeffizienten): *Die Anzahl der k-elementigen Teilmengen einer nicht leeren Menge A mit Mächtigkeit $\#A = n$ ist im Fall $1 \leq k \leq n$:*

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

und im Fall $k = 0$:

$$\binom{n}{0} := 1.$$

Beweis: Statt des üblichen formalen Induktionsbeweises verwendet wir ein „direktes“ Argument, das aber versteckt doch Elemente der Induktion beinhaltet.

i) Es sei zunächst $k \neq 0$. Zur Bildung k-elementiger Teilmengen stehen für ein erstes Element einer Teilmenge alle n Elemente der Menge zur Auswahl; für ein zweites Element bleiben dann noch $n-1$ Elemente zur Auswahl, u.s.w. Insgesamt hat man $n(n-1)\cdots(n-k+1)$ Möglichkeiten, k-elementige Teilmengen herzustellen. Dabei ergeben solche Möglichkeiten dieselbe k-elementige Teilmenge, die sich nur in der Reihenfolge der ausgewählten k Elemente unterscheidet. Nach dem Permutationssatz ist also die gerade errechnete Anzahl durch $k!$ zu dividieren. Für die gesuchte Anzahl erhalten wir damit den behaupteten Ausdruck.

ii) Für $k = 0$ ist die leere Menge $\emptyset$ die einzige 0-elementige Teilmenge. Die gesuchte Zahl ist also 1. Q.E.D.

Beispiel 1.9: Zur Bestimmung der Gewinnchancen beim Lottospiel „6 aus 49“ ist der Binomialkoeffizient für $n = 49$ und $k = 6$ auszuwerten. Dies ergibt

$$\binom{49}{6} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13.983.816,$$

was nicht gerade zum Lottospielen motiviert.

Satz 1.4 (Binomische Formel): *Die „binomische Formel“ besagt, dass für beliebige Zahlen $a, b \in \mathbb{Q}$ und $n \in \mathbb{N}$ gilt:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k, \tag{1.3.7}$$

bzw. ausgeschrieben:

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

Beweis: i) Wir stellen zunächst ein paar Eigenschaften der Binomialkoeffizienten bereit. Nach Definition gilt die Beziehung

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\,\dots\,(n-k+1)}{k!} \\ &= \frac{n(n-1)\,\dots\,(n-k+1)(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}.\end{aligned}$$

Weiter besteht die Rekursionsformel

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}. \tag{1.3.8}$$

Für $k = 0$ ist dies offensichtlich richtig,

$$\binom{n+1}{1} = 1 + n = \binom{n}{0} + \binom{n}{1},$$

und für $k \geq 1$ ergibt es sich wie folgt:

$$\begin{aligned}\binom{n}{k} + \binom{n}{k+1} &= \frac{n(n-1)\cdots(n-k+1)}{k!} + \frac{n(n-1)\cdots(n-k+1)(n-k)}{k!(k+1)} \\ &= \frac{n(n-1)\cdots(n-k+1)(k+1+n-k)}{(k+1)!} \\ &= \frac{(n+1)n\cdots(n+1-k)}{(k+1)!} = \binom{n+1}{k+1}.\end{aligned}$$

ii) Der Beweis der binomischen Formel erfolgt durch Induktion nach n. Für $n = 1$ ist sie offenbar richtig. Sei sie richtig für ein $n \geq 1$. Dann gilt

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)\left\{\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n\right\} \\ &= \binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{n-1}a^2b^{n-1} + \binom{n}{n}ab^n \\ &\quad + \binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n-1}ab^n + \binom{n}{n}b^{n+1} \\ &= \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.\end{aligned}$$

Durch Induktion ergibt sich dann die Behauptung. Q.E.D.

Mit Hilfe der Rekursionsformel (1.3.8) können ausgehend von

$$\binom{n}{0} = \binom{n}{n} = 1$$

die Binomialkoeffizienten explizit berechnet werden. Diese Rechnung führt auf das sog. „Pascalsche Dreieck“[11], in welchem sich jeder Eintrag als Summe der beiden darüber

[11] Das nach Blaise Pascal (1623–1662) benannte „Dreick“ taucht bereits in einem Lehrbuch der Arithmetik von 1527 auf, und war den Arabern bereits im 13. Jahrhundert bekannt.)

stehenden Einträge ergibt:

$$\begin{array}{lccccccccccccc}
n=0: & & & & & & & 1 & & & & & & \\
n=1: & & & & & & 1 & & 1 & & & & & \\
n=2: & & & & & 1 & & 2 & & 1 & & & & \\
n=3: & & & & 1 & & 3 & & 3 & & 1 & & & \\
n=4: & & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
n=5: & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
n=6: & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
\ldots & & & & & & & \ldots & & & & & &
\end{array}$$

Bemerkung 1.6: Der allgemeine binomische Lehrsatz ist hier zunächst nur für Zahlen $a,\, b \in \mathbb{Q}$ formuliert worden. Er ist aber auch auf der im nächsten Kapitel zu konstruierenden größeren Menge der „reellen“ Zahlen gültig.

1.4 Übungen

Übung 1.1 (Aufgabe zur Mengenlehre):
Man gebe Schnitt $A \cap B$, Vereinigung $A \cup B$ und Differenz $A \setminus B$ der folgenden Paare von Mengen an:

$$\begin{array}{ll}
a) & A = \{1,2,3,5,6,7,8,10\}, \quad B = \{3,4,9,10\}, \\
b) & A = \{n \in \mathbb{N} |\, n \le 100\}, \quad B = \{n \in \mathbb{N} |\, n > 5\}, \\
c) & A = \{n \in \mathbb{N} |\, n \ \text{ Primzahl}\}, \quad B = \{n \in \mathbb{N} |\, n \ \text{ ungerade}\}.
\end{array}$$

Übung 1.2 (Aufgabe zum Widerspruchsbeweis):
Zum formalen Nachweis der Aussage

$$\forall\, a \in \mathbb{Q} \;\; \exists\, n_a \in \mathbb{N} \;\; \forall\, n \ge n_a : \; n > a.$$

mit einem Widerspruchsargument ist ihre Negation zu bilden. Wie sieht diese aus?

Übung 1.3 (Aufgabe zum Widerspruchsbeweis):
Man zeige durch einen Widerspruchsbeweis, dass eine natürliche Zahl n, für welche n^2 gerade ist, selbst gerade sein muss.

Übung 1.4 (Aufgabe zur Mächtigkeit von Mengen):
Man zeige mit Hilfe vollständiger Induktion, dass für eine Menge A mit der Mächtigkeit $\#A = n$ die zugehörige Potenzmenge $\mathcal{P}(A) := \{B |\, B \subset A\}$ die Mächtigkeit $\#\mathcal{P}(A) = 2^n$ hat.

Übung 1.5 (Aufgabe zu Abbildungen):
Man untersuche, ob die folgenden Abbildungen injektiv, surjektiv oder bijektiv sind:

1. $f : \mathbb{N} \to \mathbb{N}, \quad f(n) := n^2\,;$

2. $f : \mathbb{Q} \to \mathbb{Z}, \quad f(r/s) := r\,;$

3. $f : \mathbb{N}_0 \to \mathbb{N}, \quad f(n) := n + 1\,.$

Übung 1.6 (Aufgabe zur vollständigen Induktion):
a) Man rekapituliere den Induktionsbeweis für die Gültigkeit der Gleichung

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

b) Man zeige durch Induktion die Gleichung

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

c) Man versuche, eine Formel für die folgende Summe abzuleiten (z. B. durch einen Blick ins Vorlesungsskriptum):

$$\sum_{k=1}^{n} k^3 = ?$$

Man beweise die Formel durch vollständige Induktion.

Übung 1.7 (Aufgabe zu Äquivalenzrelationen):
a) Man rekapituliere die Definition einer Äquivalenzrelation für die Elemente a einer Menge A.

b) Man verifiziere, dass für Paare $\{r, s\}, \{r', s'\} \in \mathbb{Z} \times \mathbb{N}$ durch

$$\{r, s\} \sim \{r', s'\} \quad :\Leftrightarrow \quad rs' = r's$$

eine Äquivalenzrelation definiert ist. Welche Menge erhält man mit den zugehörigen Äquivalenzklassen? Man gebe für jede dieser Äquivalenzklassen einen „Repräsentanten“ an.

Übung 1.8 (Aufgabe zum Widerspruchsbeweis):
a) Man rekapituliere den „klassischen“ Widerspruchsbeweis, dass die Menge der Primzahlen unendlich ist. Dazu gebe man insbesondere einen detaillierten Beweis für die Aussage, dass sich jede natürliche Zahl als Produkt von Primzahlen schreiben lässt.

b) Man zeige, dass für jede Primzahl p die Gleichung $x^2 = p$ keine rationale Lösung besitzt, d. h. die Quadratwurzel $\sqrt{p}$ ist irrational.

Übung 1.9 (Aufgabe zu Abbildungen zwischen Mengen):
Man konstruiere eine bijektive Abbildung zwischen den Mengen $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$. (Hinweis: Man betrachte die Paare $\{n, m\} \in \mathbb{N} \times \mathbb{N}$ als Koordinaten von Punkten eines Gitters mit Maschenweite 1 in der Tafelebene und nummeriere diese auf geeignete Weise durch.)

Übung 1.10 (Aufgabe zur Kombinatorik):
Wie groß ist die Chance, beim Lotto 6-aus-49 den Gewinn „5 Richtige mit Zusatzzahl“ zu ziehen?

Übung 1.11 (Aufgabe zur Kombinatorik):
Man beweise durch vollständige Induktion die allgemeine *polynomische* Formel:

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{\nu_1,\ldots,\nu_m \in \mathbb{N}_0 \\ \nu_1+\ldots+\nu_m=n}} \frac{n!}{\nu_1! \cdot \ldots \cdot \nu_m!}\, a_1^{\nu_1} \cdot \ldots \cdot a_m^{\nu_m}\,.$$

(Hinweis: Die Gültigkeit der allgemeinen *binomischen* Formel kann vorausgesetzt werden.)