1 Grundlagen

1.1 Was ist eigentlich Mathematik?

Jeder von uns hat eine naive Vorstellung davon, was der Gegenstand der Mathematik ist: sie befasst sich mit Zahlen, geometrischen Figuren, und Beziehungen zwischen solchen Objekten. Oft wird die Mathematik zusammen mit den Naturwissenschaften genannt, auch an der JKU gehören die mathematischen Institute zur Technisch-Naturwissenschaftlichen Fakultät. Ist also die Mathematik eine Naturwissenschaft? Wo in der Natur gibt es "37" oder "$y = x + 1$" (die Gerade durch $(-1, 0)$ und $(0, 1)$) ? Wo in der Natur gibt es wirklich einen Kreis? Hat nicht jedes scheinbar kreisförmige Gebilde, wenn wir es nur genau genug betrachten, Unregelmässigkeiten, ist also nicht wirklich kreisförmig? Und auch wenn es ein wirklich kreisförmiges Gebilde gäbe, wäre das dann "der Kreis"? Oder wäre es nicht doch nur ein spezielles Beispiel für das "Prinzip des Kreises", den "Kreis an sich"?

Wenn wir diesen Fragen zur Philosophie der Mathematik nachgehen, merken wir sehr bald, dass die Mathematik eben keine Naturwissenschaft ist, die Gegenstände ihrer Betrachtung kommen in der Natur nicht vor. Sie sind einzig und allein Schöpfungen unseres Geistes. Als solche haben wir sie im Prinzip völlig unter Kontrolle. Wir können sie exakt definieren und die Regeln festlegen, wie wir mit ihnen operieren wollen. Und dennoch entziehen sich die mathematischen Objekte unserem völligen Zugriff. In seinem berühmten Unvollständigkeitssatz hat Kurt Gödel im Jahr 1931 bewiesen, dass es in jedem formalen System, welches umfassend genug ist um die natürlichen Zahlen darin auszudrücken, Aussagen gibt, die im System weder bewiesen noch widerlegt werden können. Mit anderen Worten: nicht alles, was "gilt", ist auch "beweisbar".

Mathematik ist also sicherlich keine Naturwissenschaft, mathematische Theorien werden nicht experimentell überprüft. Nicht das Experiment ist der letzte Massstab, sondern der Beweis. Mathematik ist aber natürlich auch keine Geisteswissenschaft im klassischen Sinn. Sie stellt eine eigene Kategorie im Gebäude der Wissenschaften dar.

Umso verblüffter stellen wir immer wieder fest, dass zahlreiche Zweige der Mathematik ganz überraschende Anwendungen etwa in den Naturwissenschaften haben. In seinem Artikel "*The Unreasonable Effectiveness of Mathematics in the Natural Sciences*" [1] erzählt der Physiknobelpreisträger Eugene P. Wigner (Princeton University) folgende Geschichte: *There is a story about two friends, who were classmates in high school, talking about their jobs. One of them became a statistician and was working on population trends. He showed a reprint to his former classmate. The reprint started, as usual, with the Gaussian distribution and the statistician explained to his former classmate the meaning of the symbols for the actual population, for the average populatioin, and so on. His classmate was a bit incredulous and was not quite sure whether the statistician was pulling his leg. "How can you know this?" was his query. "And what is this symbol here?" "Oh," said the statistician, "this is π." "What is that?" "The ratio of the circumferance of the circle to its diameter." "Well, now you are pushing your joke too far," said the classmate, "surely the population has nothing to do with the circumference of the circle."* In seinem Artikel gibt Wigner zahlreiche Beispiele unerwarteter Anwendbarkeit von Mathematik

[1] Communications on Pure and Applied Mathematics, Vol.XIII, 1–14 (1960)

in den Naturwissenschaften, und er schliesst mit der Erkenntnis: *The miracle of the appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve. We should be grateful for it and hope that it will remain valid in future research and that it will extend, for better or for worse, to our pleasure even though perhaps also to our bafflement, to wide branches of learning.*

Mathematik ist die Wissenschaft von Zusammenhängen abstrakter Objekte. Beispiele solcher Objekte können Zahlen sein, oder Abbildungen, oder geometrische Figuren; aber auch Graphen, Formelausdrücke, oder mathematische Theorien selbst. Die Mathematik zieht logisch stichhaltige Schlüsse über das Verhalten solcher Objekte, wir nennen so etwas einen Beweis. Ein Beweis besteht typischerweise aus algebraischen Umformungen, also "Berechnungen", und logischen Schlüssen, also "Herleitungen". Der Mathematiker kann sich heutzutage sowohl beim Berechnen als auch beim logischen Schliessen von Softwaresystemen unterstützen lassen, etwa von Computeralgebra-Systemen wie Maple oder Mathematica.

Beweise in der Mathematik haben auch ihr Eigenleben. Sie werden meist in roher, ungeschliffener Form entdeckt. Im Laufe ihrer Entwicklung werden sie dann unzählige Male hin und her gewälzt, dadurch abgeschliffen und glatt poliert. Manche von ihnen verlieren schliesslich jede Ähnlichkeit mit ihrer ursprünglichen Form und strahlen eine blendende Eleganz aus. Ja, es gibt so etwas wie Ästhetik der Mathematik! Diese eherne Gültigkeit und Schönheit mathematischer Theorien hat wohl Carl Friedrich Gauß (1777 – 1855) zu folgendem Ausspruch veranlasst: *Mathematik ist die Königin der Wissenschaften und Arithmetik die Königin der Mathematik. Sie lässt sich oft herbei ihre Dienste der Astronomie und anderen Naturwissenschaften anzubieten, aber unter allen Umständen gebührt ihr der erste Platz.*

Nun aber genug der philosophischen und poetischen Betrachtungen. Wir wollen uns mit einem der Grundbausteine des Gebäudes der Mathematik befassen, mit der Linearen Algebra!

1.2 Zahlenbereiche

Die natürlichen Zahlen $\mathbb{N}$ und die ganzen Zahlen $\mathbb{Z}$

Die **natürlichen Zahlen** $\mathbb{N}$ bestehen aus $0, 1, 2, 3, \ldots$. Natürliche Zahlen können addiert $(m+n)$ und multipliziert $(m \cdot n)$ werden, sie sind linear der Grösse nach angeordnet $(m < n)$, und eine natürliche Zahl n kann von einer natürlichen Zahl m subtrahiert werden $(n - m)$, wenn $m \leq n$. Sowohl die Addition als auch die Multiplikation sind kommutativ, es gilt also

$$m + n = n + m \qquad \text{und} \qquad m \cdot n = n \cdot m.$$

Weiters sind Addition und Multiplikation assoziativ, es gilt also

$$(m + n) + k = m + (n + k) \qquad \text{und} \qquad (m \cdot n) \cdot k = m \cdot (n \cdot k).$$

Schliesslich gilt in $\mathbb{N}$ noch das Distributivitätsgesetz:

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

Unter *Arithmetik* versteht man die Theorie der natürlichen Zahlen mit den Operationen der Addition und Multiplikation.

Diese Definition der natürlichen Zahlen appelliert an den gemeinsamen Gebrauch der Umgangssprache, und wir hoffen dabei, uns auf gemeinsame Intuition berufen zu können. Um mathematisch exakt mit den natürlichen Zahlen umgehen zu können, hat man ausgehend vom 19. Jahrhundert versucht, die natürlichen Zahlen axiomatisch festzulegen. Das bekannteste Axiomensystem für $\mathbb{N}$ sind die sogenannten **Peano Axiome** (Giuseppe Peano, 1858–1932):

[P1] (Null) 0 ist eine natürliche Zahl.

[P2] (Nachfolger) Jede natürliche Zahl n hat genau einen Nachfolger (successor), bezeichnet als $S(n)$.

[P3] (Null minimal) 0 ist nicht Nachfolger einer natürlichen Zahl.

[P4] (verschiedene Nachfolger) Verschiedene natürliche Zahlen haben verschiedene Nachfolger.

[P5] (Induktion) Jede Eigenschaft, welche für 0 gilt und sich von jeder natürlichen Zahl n auf ihren Nachfolger $S(n)$ überträgt, gilt für alle natürlichen Zahlen.

Wegen [P5] gibt es ein eindeutiges Startelement, nämlich 0. Wir werden 1 für $S(0)$ schreiben, 2 für $S(S(0)) = S(1)$, usw. Die Peanoaxiome legen unmittelbar eine Ordnung auf den natürlichen Zahlen nahe, nämlich

$$0 < S(0) = 1 < S(S(0)) = 2 < S(S(S(0))) = 3 < \cdots \quad .$$

Das Axiom [P2] postuliert für $\mathbb{N}$ eine (einzige) Operation "S" bzw. "+1" Daraus können wir sofort die Addition wie folgt definieren:

Definition 1.2.1: *Die* **Addition** *"+" auf $\mathbb{N}$ ist wie folgt definiert für $n, m \in \mathbb{N}$:*
- $n + 0 = n$,

- $n + (m + 1) = (n + m) + 1$ *(also $n + S(m) = S(n + m)$).* □

Aus der Addition lässt sich die Subtraktion ableiten: ist $m < n$, so gibt es offensichtlich ein k mit $m + k = n$. Dieses k ist das Resultat der Subtraktion von m von n, geschrieben $k = n - m$.

Aus der Addition lässt sich die Multiplikation wie folgt definieren:

Definition 1.2.2: *Die* **Multiplikation** *"$\cdot$" auf $\mathbb{N}$ ist wie folgt definiert für $n, m \in \mathbb{N}$:*
- $n \cdot 0 = 0$,
- $n \cdot (m + 1) = n \cdot m + n$. □

Diese (und andere) Definition ist typischerweise "rekursiv", weil $\mathbb{N}$ rekursiv definiert ist.

Aus den Peanoaxiomen kann man nun durch logisches Schliessen mathematische Sätze über die natürlichen Zahlen herleiten, etwa die Kommutativität, Assoziativität und Distributivität von Addition und Multiplikation.

Häufig kommt es vor, dass wir Summen und Produkte mit einer variablen Anzahl von Summanden bzw. Faktoren schreiben wollen. Dazu benutzen wir die Schreibweise mittels "$\sum$" und "$\prod$". Seien etwa $l + 1$ natürliche Zahlen $m_0, \ldots, m_l$ gegeben. Mit $\sum_{i=0}^{l} m_i$ bezeichnen wir die Summe dieser Zahlen m_i, also

$$\sum_{i=0}^{l} m_i \;=\; m_0 + \cdots + m_l.$$

Ebenso bezeichnen wir mit $\prod_{i=0}^{l} m_i$ das Produkt dieser Zahlen m_i, also

$$\prod_{i=0}^{l} m_i \;=\; m_0 \cdot \cdots \cdot m_l.$$

In analoger Weise werden $\sum$ und $\prod$ für andere Indexbereiche definiert.

Schliesslich lässt sich aus der Multiplikation die Potenzierung wie folgt definieren:

Definition 1.2.3: *Die Operation der* **Potenzierung** *auf $\mathbb{N}$ ist wie folgt definiert für $n, m \in \mathbb{N}$:*
- $n^0 = 1$,
- $n^{(m+1)} = n^m \cdot n$. □

Das Induktionsaxiom [P5] bedeutet, dass wir für den Beweis einer Eigenschaft P natürlicher Zahlen das **Prinzip der vollständigen Induktion** verwenden können, also folgende Schlussregeln:

$$P(0) \wedge \forall n : (P(n) \Longrightarrow P(n+1)) \;\Longrightarrow\; \forall n : P(n)$$

und

$$\forall n : ((\forall k < n : P(k)) \Longrightarrow P(n)) \;\Longrightarrow\; \forall n : P(n)$$

Gilt eine Eigenschaft P für alle natürlichen Zahlen ab N, so kann man entweder eine neue Eigenschaft Q einführen mit $Q(n) = P(N + n)$ und Q für $\mathbb{N}$ beweisen, oder man zeigt $P(N)$ und $\forall n \geq N : P(n) \Longrightarrow P(n+1)$.

Beispiel 1.2.4: Wir wollen zeigen, dass für alle natürlichen Zahlen n gilt

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}. \tag{$*$}$$

$P(n)$ besagt, dass n die Eigenschaft (*) hat.
"Induktionsbasis": offensichtlich gilt $P(0)$, da $\sum_{i=0}^{0} i = 0$.
"Induktionshypothese": wir nehmen an, P gelte für ein beliebiges aber fix gewähltes $\overline{n}$, also

$$\sum_{i=0}^{\overline{n}} = \frac{\overline{n}(\overline{n}+1)}{2}. \tag{$**$}$$

"Schritt von $\overline{n}$ zu $\overline{n}+1$": wenn es uns nun gelingt, unter diesen Voraussetzungen zu zeigen, dass P auch für $\overline{n}+1$ gilt, so wissen wir, dass P für alle natürlichen Zahlen n gilt. Das ist aber tatsächlich der Fall, wie wir uns auf folgende Weise überzeugen:

$$\sum_{i=0}^{\overline{n}+1} i \;=\; \sum_{i=0}^{\overline{n}} i \;+(\overline{n}+1) \;=\; \frac{\overline{n}(\overline{n}+1)}{2}+(\overline{n}+1) \;=\; \frac{(\overline{n}+1)(\overline{n}+2)}{2}. \qquad \square$$

Beispiel: Etwas scherzhaft könnte man auch formulieren:
"*Es gibt keine uninteressate natürliche Zahl.*"
Wir "beweisen" diese Aussage durch Induktion.
$n = 0$: offensichtlich ist 0 eine höchst interessate Zahl, nämlich die kleinste.
Induktionshypothese: "*für alle n kleiner oder gleich einer beliebig aber fix gewählten Zahl $\overline{n}$ gilt: n ist eine interessante Zahl*"
$\overline{n} \longrightarrow \overline{n}+1$: wir betrachten also $\overline{n}+1$. $\overline{n}+1$ kann nicht uninteressant sein, sonst wäre es nämlich die kleinste uninteressante Zahl, was wiederum höchst interessant wäre. Also ist auch $\overline{n}+1$ interessant. Der "Satz" ist somit bewiesen.

Dazu eine Anekdote. Der berühmte Mathematiker G.H. Hardy hatte das indische Genie Ramanujan im Jahr 1914 nach Cambridge eingeladen. Ramanujan war krank, und Hardy besuchte ihn am Krankenbett: *It was on one of those visits that there happened the incident of the taxi-cab number. Hardy had gone out to Putney by taxi, as usual his chosen method of conveyance. He went into the room where Ramanujan was lying. Hardy, always inept about introducing a conversation, said, probably without a greeting, and certainly as his first remark: 'I thought the number of my taxi-cab was 1729. It seemed to me rather a dull number.' To which Ramanujan replied: 'No, Hardy! No, Hardy! It is a very interesting number. It is the smallest number expressible as the sum of two cubes in two different ways.'* [2] Tatsächlich gilt

$$1729 = 1^3 + 12^3 = 10^3 + 9^3. \qquad \square$$

Wir haben hier streng unterschieden zwischen der "Variablen" n, welche über den ganzen Bereich der natürlichen Zahlen $\mathbb{N}$ variiert, und der beliebig aber fix gewählten Konstanten $\overline{n}$. Macht man das nämlich nicht, so werden die zu zeigende Eigenschaft ($*$) und die Induktionshypothese ($**$) identisch; man nimmt also dann bereits die Gültigkeit

[2] Seite 37 im Vorwort von C.P.Snow zum Buch G.H.Hardy, "A Mathematician's Apology", Cambridge Univ. Press, Cambridge, 1992

von $(*)$ an und kann sie daraus offensichtlich unschwer herleiten. Die Unterscheidung zwischen Variablen und Konstanten ist also in einem Induktionsbeweis — wie übrigens immer in der Mathematik — von entscheidender Bedeutung. Dennoch schreibt man dann oft doch wieder einfach n auch für die Konstante. Man kann das aber nur machen, wenn man sich völlig im klaren ist über den verschiedenen Gebrauch des Symbols n — einmal als Variable, das andere Mal als Konstante.

In $\mathbb{N}$ kann eine Zahl m nur dann von n subtrahiert werden, wenn $m \leq n$. Die natürlichen Zahlen sind also nicht abgeschlossen bzgl. der Operation der Subtraktion. Dieser Mangel lässt sich beheben durch die Hinzunahme negativer Zahlen $-n$ mit den üblichen Rechenregeln. Diesen erweiterten Zahlenbereich nennen wir $\mathbb{Z}$, den Bereich der **ganzen Zahlen**.

Definition 1.2.5: *Seien $m, n \in \mathbb{Z}$. Wir sagen m* **teilt** *n, wenn es eine ganze Zahl k gibt, sodass $n = m \cdot k$. Für diesen Zusammenhang schreiben wir $m|n$.* □

Satz 1.2.6: *Sind $k, m, n \in \mathbb{Z}$, dann gilt*

(i) $k|m \ \wedge \ k|n \implies k|m+n \quad \wedge \quad k|m-n,$

(ii) $k|m \implies k|mn,$

(iii) $k|m \ \wedge \ m|k \implies k = \pm m,$

(iv) $k|m \ \wedge \ m|n \implies k|n.$

Sind a, b von 0 verschiedene natürliche Zahlen, dann gilt

(v) $a|b \implies a \leq b.$

0 teilt nur sich selbst. Offensichtlich teilt jede natürliche Zahl die 0, es gilt nämlich $0 = n \cdot 0$. Jede andere natürliche Zahl $n(\neq 0)$ hat nur endlich viele Teiler, welche bzgl. der Ordnung $<$ alle zwischen 1 und n liegen. Hat man also 2 natürliche Zahlen gegeben, welche nicht beide 0 sind, so macht es Sinn, vom "grössten gemeinsamen Teiler" dieser Zahlen zu sprechen. Der grösste gemeinsame Teiler kann natürlich auch für ganze Zahlen definiert werden. Das sei dem Leser überlassen.

Definition 1.2.7: *Seien $m, n \in \mathbb{N}$, nicht beide 0. Dann ist k ein* **gemeinsamer Teiler** *von m und n, wenn gilt $k|m$ und $k|n$. Ist g maximal (bzgl. der Ordnung $<$) unter den (endlich vielen) gemeinsamen Teilern von m und n, so heisst g der* **grösste gemeinsame Teiler** *von m und n, geschrieben $g = \mathrm{ggT}(m, n)$. Falls $\mathrm{ggT}(m, n) = 1$, so sind m und n* **relativ prim**.

Neben der "exakten" Teilbarkeit $|$ betrachtet man in $\mathbb{N}$ auch die sogenannte "Teilung mit Quotient und Rest". Diese Beziehung lässt sich auch auf $\mathbb{Z}$ ausdehnen.

Definition 1.2.8: *Seien $m, n \in \mathbb{N}$, $n \neq 0$. Dann gibt es $q, r \in \mathbb{N}$, sodass:*

$$m = q \cdot n + r, \quad \text{und} \quad r < n.$$

q heisst der **Quotient** *und r der* **Rest** *der Teilung von m durch n, geschrieben $q = \mathrm{quot}(m, n)$, $r = \mathrm{rest}(m, n)$.*

Satz 1.2.9: *Für $m, n \in \mathbb{N}$, $n \neq 0$, gilt: $\mathrm{ggT}(m, n) = \mathrm{ggT}(\mathrm{rest}(m, n), n)$.*

Natürlich kann man den ggT zweier Zahlen bestimmen (berechnen), indem man aus den endlich vielen gemeinsamen Teilern den grössten auswählt. Der ggT kann aber auch mittels des obigen Satzes auf elegante Weise berechnet werden, durch den sogenannten Euklidschen Divisionsalgorithmus (Euklid, $\sim$ 300 v.Chr.).

Euklidscher Divisionsalgorithmus
Für gegebene positive natürliche Zahlen m und n wird $g = \text{ggT}(m, n)$ berechnet.

(1) setze $r_0 := m,\ r_1 := n,\ i := 1;$

(2) solange $r_i \neq 0$ ist, führe aus:

$$r_{i+1} := \text{rest}(r_{i-1}, r_i),\ i := i + 1;$$

(3) $(r_i = 0)$ $g := r_{i-1}$ ist der gesuchte ggT. □

Wegen des obigen Satzes gilt zu jedem Zeitpunkt der Ausführung des Euklidschen Divisionsalgorithmus:

$$\text{ggT}(m, n) = \text{ggT}(r_{i-1}, r_i).$$

In Schritt (3) gilt offensichlich $r_i = 0$, also ist $g = \text{ggT}(m, n) = \text{ggT}(r_{i-1}, 0) = r_{i-1}$.

Beispiel 1.2.10: Seien $m = 3641, n = 2827$ gegeben. Der Euklidsche Divisionsalgorithmus erzeugt die Folge von Resten

$$\begin{aligned} r_0 &= 3641 \\ r_1 &= 2827 \\ r_2 &= 814 \\ r_3 &= 385 \\ r_4 &= 44 \\ r_5 &= 33 \\ r_6 &= 11 \\ r_7 &= 0 \end{aligned}$$

Somit ist $11 = \text{ggT}(3641, 2827)$. □

Erweiterter Euklidscher Divisionsalgorithmus
Für gegebene positive natürliche Zahlen m und n wird $g = \mathrm{ggT}(m, n)$ berechnet, sowie ganze Zahlen a, b mit der Eigenschaft $g = am + bn$.

(1) setze $(r_0, r_1, s_0, s_1, t_0, t_1) := (m, n, 1, 0, 0, 1)$, $i := 1$;

(2) solange $r_i \neq 0$ ist, führe aus:

$q_i := \mathrm{quot}(r_{i-1}, r_i)$;

$(r_{i+1}, s_{i+1}, t_{i+1}) := (r_{i-1}, s_{i-1}, t_{i-1}) \;-\; q_i \cdot (r_i, s_i, t_i)$;

$i := i + 1$;

(3) $(r_i = 0)$ $g := r_{i-1}$ ist der gesuchte ggT, und die Kofaktoren sind $a := s_{i-1}, b := t_{i-1}$. □

Der Euklidsche Divisionsalgorithmus kann unschwer dahingehend erweitert werden, dass neben dem grössten gemeinsamen Teiler auch sogenannte Bézout-Kofaktoren $a, b \in \mathbb{Z}$ berechnet werden, sodass
$$\mathrm{ggT}(m, n) = am + bn \; .$$

Zu jedem Zeitpunkt der Ausführung des Erweiterten Euklidschen Algorithmus gilt
$$r_i = s_i m + t_i n.$$
In Schritt (3) gilt offensichtlich $g = \mathrm{ggT}(m, n) = am + bn$.

Die natürlichen Zahlen sind zunächst in den Peano Axiomen über ihre additive Struktur eingeführt, also jede natürliche Zahl lässt sich erzeugen aus der 0 durch mehrmalige Anwendung der Operation "+1". Andererseits lassen sich die natürlichen Zahlen auch eindeutig schreiben als Produkt von Primzahlpotenzen.

Definition 1.2.11: *Eine* **Primzahl** *ist eine natürliche Zahl p mit folgenden Eigenschaften:*
- $p \geq 2$,
- *wenn $p | m \cdot n$, dann $p | m$ oder $p | n$.* □

Satz 1.2.12: *Für von 0 verschiedene natürliche Zahlen a, b, c und eine Primzahl p gilt:*

(i) Aus $a | bc$ und $\mathrm{ggT}(a, b) = 1$ folgt $a | c$.

(ii) Aus $a | p$ folgt $a = 1$ oder $a = p$. □

Satz 1.2.13: *Es gibt unendlich viele Primzahlen.* □

Nun können wir die Tatsache der Darstellbarkeit natürlicher Zahlen als Produkt von Primzahlpotenzen ausdrücken:

Satz 1.2.14: *Für jede natürliche Zahl $n \geq 2$ gibt es verschiedene Primzahlen $p_1, \ldots, p_m$ und zugehörige Potenzen $e_1, \ldots, e_m$, sodass*

$$n = \prod_{i=1}^{m} p_i^{e_i}.$$

Diese Darstellung ist eindeutig bis auf Umreihung der Primzahlen. □

Die Theorie der natürlichen Zahlen (Arithmetik) betrifft wohl einen der grundlegendsten Bereiche der Mathematik. Dennoch ist diese Theorie äusserst reichhaltig und bis heute noch in grossen Teilen unverstanden. So beschäftigte etwa der berühmte *Satz von Fermat* (Pierre Fermat, 1601?–1665)

"Die Gleichung $x^n + y^n = z^n$ ist unlösbar für natürliche Zahlen $x, y, x \neq 0$ und $n > 2$" die Mathematik seit Jahrhunderten und konnte erst in den 1990er Jahren von Andrew Wiles bewiesen werden, und zwar mit Mitteln, welche weit über elementare Arithmetik hinausgehen. [3] Bisher unbewiesen ist die *Goldbachsche Vermutung* (C.Goldbach, 1690–1764), nämlich

"Jede gerade Zahl grösser als 2 lässt sich schreiben als Summe zweier Primzahlen".

Die rationalen Zahlen $\mathbb{Q}$

In den ganzen Zahlen $\mathbb{Z}$ kann man zwar beliebig subtrahieren, nicht aber dividieren (Division mit Quotient und Rest ist eine andere Operation). Dieser Mangel kann behoben werden durch den Übergang zu den **rationalen Zahlen** $\mathbb{Q}$: eine rationale Zahl q ist ein Paar (z, n) ganzer Zahlen (üblicherweise geschrieben als $q = \frac{z}{n}$), wobei $n \neq 0$ und

$$\frac{z}{n} = \frac{z'}{n'} \iff zn' = z'n.$$

Die beiden Komponenten einer rationalen Zahl heissen **Zähler** und **Nenner**. Offensichtlich kann jede ganze Zahl z auch als rationale Zahl $\frac{z}{1}$ interpretiert werden.

Addition und Multiplikation in $\mathbb{Q}$ folgen den herkömmlichen Regeln. In $\mathbb{Q}$ hat nun jede Zahl q ausser der 0 ein Inverses q^{-1} mit der Eigenschaft $q \cdot q^{-1} = 1$. Später werden wir davon sprechen, dass $\mathbb{Q}$ ein "Körper" ist.

Die rationalen Zahlen tragen auch eine natürliche Ordnung, welche mit der Ordnung der ganzen Zahlen verträglich ist. Wenn wir uns etwa o.B.d.A. (ohne Beschränkung der Allgemeinheit) rationale Zahlen mit positivem Nenner geschrieben denken, so hat man

$$q = \frac{z}{n} < q' = \frac{z'}{n'} \iff qnn' < q'nn'.$$

---

[3] Im Buch "Mathematical Apocrypha Redux" von S.G. Krantz findet sich dazu auf Seite 120 folgender scherzhafter Beitrag:
The television show *The Simpsons*, in the "Treehouse of Horror" episode from the sixth season, revealed the following counterexample to Fermat's Last Theorem: Take your TI-83 calculator and compute

$$[1782^{12} + 1841^{12}]^{1/12} .$$

You will find the answer to be 1922. Thus

$$1782^{12} + 1841^{12} = 1922^{12} .$$

We leave it as an exercise for you to make peace between this example and Andrew Wiles's celebrated proof (*Hint:* Think about roundoff error).

Rationale Zahlen lassen sich auch schreiben als “Dezimalzahlen”. Jede rationale Zahl entspricht dabei einer periodischen Dezimalzahl.

Satz 1.2.15: *Es gibt keine rationale Zahl q mit der Eigenschaft $q^2 = 2$.*
(Also $\sqrt{2}$ ist nicht rational, bzw. die polynomiale Gleichung $x^2 - 2 = 0$ ist in $\mathbb{Q}$ unlösbar.)

Nimmt man nun die Lösung einer polynomialen Gleichung (also etwa $\sqrt{2}$) zu $\mathbb{Q}$ hinzu zusammen mit allen Zahlen, die man daraus durch die üblichen Rechenoperationen erhält, so spricht man von einer algebraischen Erweiterung $\mathbb{Q}(\sqrt{2})$ von $\mathbb{Q}$.

Die reellen Zahlen $\mathbb{R}$

Zwischen zwei verschiedenen rationalen Zahlen gibt es stets eine dritte rationale Zahl, also

$$\forall q, q' : (q < q' \Longrightarrow \exists q'' : q < q'' < q')$$

Obwohl die rationalen Zahlen also “dicht” sind auf der Zahlengeraden, ist es doch möglich, beschränkte monoton wachsende (oder fallende) Folgen von rationalen Zahlen zu betrachten, etwa

$$1,\ 1,4,\ 1,41,\ 1,414,\ 1,4142,\ \ldots, 1,414213562,\ \ldots < 1,5\ ,$$

welche gegen keine rationale Zahl konvergieren, also keinen Limes in $\mathbb{Q}$ haben. Nimmt man nun alle solchen Limiten, also etwa $\sqrt{2}$, zu $\mathbb{Q}$ hinzu, so erhält man die **reellen Zahlen $\mathbb{R}$**.

Auf die Begiffe wie “konvergiert” oder “Limes” gehen wir an dieser Stelle nicht näher ein, sie werden ausführlich in der Vorlesung zur Analysis behandelt.

Reelle Zahlen lassen sich auch schreiben als (nicht notwendigerweise periodische) “Dezimalzahlen”. Diese Schreibweise ist aber nicht eindeutig, so gilt etwa $1,0000\ldots = 1 = 0,9999\ldots$. Das ist aber die einzige Art von Uneindeutigkeit in der Dezimaldarstellung.

Die komplexen Zahlen $\mathbb{C}$

Nicht jede polynomiale Gleichung mit ganzzahligen Koeffizienten hat eine Lösung in $\mathbb{R}$. Ein Beispiel dafür ist $x^2 + 1 = 0$. Also $\sqrt{-1} \notin \mathbb{R}$. Mit der Bezeichnung $i = \sqrt{-1}$ kann man nun Zahlen der Form

$$c = a + bi \quad \text{mit} \quad a, b \in \mathbb{R}$$

betrachten. Solche Zahlen nennt man **komplexe Zahlen** und der betreffende Zahlenbereich wird geschrieben als $\mathbb{C}$. In $\mathbb{C}$ hat nun tatsächlich jede polynomiale Gleichung eine Lösung, man nennt daher $\mathbb{C}$ **algebraisch abgeschlossen**.

Solche komplexen Zahlen lassen sich also interpretieren als Paare reeller Zahlen; das führt zur Darstellung komplexer Zahlen in der Gauß’schen Zahlenebene. In der Darstellung $c = a + bi$ heisst a der **Realteil** von c, $a = \mathrm{re}(c)$, und b heisst der **Imaginärteil** von c, $b = \mathrm{im}(c)$. Weiters ist $|c| = \sqrt{a^2 + b^2}$ der **Betrag** von c. Addition und Multiplikation sind klar (wobei $i^2 = -1$), Division ergibt sich aus $c^{-1} = (a/|c|^2) - (b/|c|^2)i$. Spiegelt man c in der Gauß’schen Zahlenebene um die reelle Achse, so erhält man die **komplex konjugierte** Zahl $\overline{c} = a - bi$.

Zusammenfassend haben wir also nun die folgenden ineinander enthaltenen Zahlbereiche: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
Wollen wir etwa nur die natürlichen Zahlen ohne die 0 bezeichnen, zu drücken wir das durch $\mathbb{N}^+$ aus. Analog verfahren wir mit anderen Zahlenbereichen.

1.3 Mengen

Die Mengentheorie begann mit Versuchen von Richard Dedekind (1831–1916) und Georg Cantor (1845–1918), unendliche Mengen in die Mathematik einzuführen. Cantor hatte erkannt, dass für eine Theorie der reellen Zahlen, wie sie vor allem von Dedekind und Karl Weierstrass (1815–1897) entwickelt worden war, unendliche Mengen unabdingbar waren. Diese heute allgemein anerkannte Sichtweise war Ende des 19. Jahrhunderts in keiner Weise akzeptiert. So teilten etwa Carl Friedrich Gauß und Leopold Kronecker (1823–1891) den von den alten Griechen überkommenen "Schrecken vor dem Unendlichen". Ihrer Meinung nach sollten unendliche Kollektionen nur als unvollständige, potentielle Objekte verstanden werden. Cantor betrachtete unendliche Mengen jedoch nicht nur als Objekte, er definierte auch Operationen auf ihnen und entwickelte eine detaillierte Theorie ihrer "Grösse" (Kardinalität). Die von Cantor entworfene "naive Mengentheorie" führt relativ schnell zu Widersprüchen, vergleiche das Russell'sche Paradoxon unten (Bertrand Russell, 1872–1970). Diese Probleme der naiven Mengentheorie konnten jedoch später durch die axiomatische Theorie der Zermelo-Fränkel-Mengentheorie behoben werden.

Definition 1.3.1: (naive Mengendefinition von Cantor) *Eine* **Menge** *ist eine Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.*

Definition 1.3.2: *Die Objekte x, welche in einer Menge A zusammengefasst werden, bezeichnet man als die* **Elemente** *der Menge A. Ist x ein Element der Menge A, so sagen wir auch, dass x in A* **enthalten** *ist, und wir schreiben diesen Sachverhalt als $x \in A$.*
Die Menge $\emptyset$, welche keine Elemente enthält, heisst die **leere Menge**.
Sind A und B zwei Mengen, und ist jedes Element x von A auch in B enthalten, so heisst A eine **Teilmenge** *von B. Wir schreiben $A \subseteq B$. Gibt es darüber hinaus mindestens ein Element $y \in B$, welches nicht in A enthalten ist, so ist A eine* **echte Teilmenge** *von B, geschrieben als $A \subset B$.*
Mengen sind einzig und allein durch ihre Elemente charakterisiert. Zwei Mengen A und B sind also **gleich**, *geschrieben als $A = B$, wenn sie dieselben Elemente enthalten.*

Satz 1.3.3: *Die Mengen A und B sind genau dann gleich, wenn sowohl A Teilmenge von B ist als auch B Teilmenge von A. Also*

$$A = B \iff A \subseteq B \wedge B \subseteq A.$$

Wie geben wir nun in der Mathematik Mengen an? Wir machen das, indem wir die Elemente der Menge zwischen Mengenklammern $\{$ und $\}$ schreiben, etwa

$$A = \{2, 3, 5\}.$$

In dieser aufzählenden Weise können wir natürlich nur endliche Mengen schreiben. Unendliche Mengen geben wir durch eine sogenannte "charakterische Eigenschaft" an, also mittels einer bestimmenden Eigenschaft P für die Elemente x der Menge A, etwa

$$A = \{x | \underbrace{x \text{ ist Primzahl}}_{P(x)}\}.$$

Hat man bereits eine Menge A, und will alle Elemente von A zusammenfassen, welche eine zusätzliche Eigenschaft P haben, so schreibt man dafür

$$B = \{x \in A | P(x)\}.$$

Häufig werden auch Familien von Mengen betrachtet. Dazu sei I eine Menge, genannt "Indexmenge". Für jedes $i \in I$ sei A_i eine Menge. Dann heisst

$$(A_i)_{i \in I} \quad \text{bzw.} \quad \{A_i | i \in I\}$$

eine **Familie von Mengen**.

Laut obiger Definition des Mengenbegriffes ist die Frage nach den Elementen ($x \in A$?) die einzige elementare Frage, die wir an eine Menge A stellen können. Insbesondere können wir nicht fragen, ob etwa x zweimal in A ist, oder ob x "vor" y in A ist. So gilt etwa

$$\{2, 3, 5\} = \{5, 3, 2\} = \{2, 2, 3, 5, 5, 5\}.$$

Die in Abschnitt 1.2 eingeführten Zahlenbereiche

$$\mathbb{N}, \ \mathbb{Z}, \ \mathbb{Q}, \ \mathbb{R}, \ \mathbb{C}$$

sind natürlich Mengen. Für manche speziellen Mengen gibt es auch spezielle Schreibweisen, so etwa für Intervalle reeller Zahlen. Seien $a, b \in \mathbb{R}$:

$$\begin{array}{rcll}
[a,b] & = & \{x \in \mathbb{R} \mid a \leq x \leq b\} & \ldots \text{ abgeschlossenes Intervall} \\
[a,b) & = & \{x \in \mathbb{R} \mid a \leq x < b\} & \ldots \text{ halb offenes Intervall} \\
(a,b] & = & \{x \in \mathbb{R} \mid a < x \leq b\} & \ldots \text{ halb offenes Intervall} \\
(a,b) & = & \{x \in \mathbb{R} \mid a < x < b\} & \ldots \text{ offenes Intervall} \\
[a,\infty) & = & \{x \in \mathbb{R} \mid a \leq x\} & \ldots \text{ offenes unendliches Intervall}
\end{array}$$

Operationen mit Mengen

Definition 1.3.4: *Seien A, B, U Mengen, mit $A \subseteq U$.*
Die **Vereinigung** *von A und B ($A \cup B$) enthält genaue jene Elemente, welche in A oder B enthalten sind, also*

$$A \cup B = \{x | x \in A \vee x \in B\}.$$

Der **Durchschnitt** *von A und B ($A \cap B$) enthält genau jene Elemente, welche sowohl in A als auch in B enthalten sind, also*

$$A \cap B = \{x | x \in A \wedge x \in B\}.$$

Gilt $A \cap B = \emptyset$, so heissen A und B **disjunkt**.
Die **Differenz** *von A und B ($A \setminus B$) enthält genau jene Elemente, welche in A aber nicht in B enthalten sind, also*

$$A \setminus B = \{x | x \in A \wedge x \notin B\}.$$

Die **symmetrische Differenz** *von A und B ($A \triangle B$) enthält genau jene Elemente, welche in A oder in B aber nicht in beiden Mengen enthalten sind, also*

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Das **Komplement** *von A bzgl. des* **Universums** *U ($Co_U(A)$) enthält genau jene Elemente von U, welche nicht in A enthalten sind, also*

$$Co_U(A) = \{x \in U | x \notin A\}.$$

Das Universum U ist gewöhnlich eine grosse Menge, in der sich alles bei einer Untersuchung abspielt. U wird daher oft als implizit gegeben betrachtet, man schreibt es nicht mehr extra an, und verwendet dann die Schreibweise

$$Co_U(A) = \overline{A}.$$

Definition 1.3.5: *Wir wollen die Operationen der Vereinigung und des Durchschnittes auch auf Familien von Mengen ausdehnen. Sei also $(A_i)_{i\in I}$ eine Familie von Mengen mit Indexmenge I. Dann ist*

$$\bigcup_{i\in I} A_i = \bigcup(A_i | i \in I) := \{x | \exists i \in I : x \in A_i\}$$

die **Vereinigung** *aller A_i für $i \in I$, und*

$$\bigcap_{i\in I} A_i = \bigcap(A_i | i \in I) := \{x | \forall i \in I : x \in A_i\}$$

der **Durchschnitt** *aller A_i für $i \in I$.*

Auf ähnliche Weise erklären wir Vereinigung und Durchschnitt von Mengen, welche eine Eigenschaft P besitzen:

$$\bigcup\{A | P(A)\} := \{x | \exists A : P(A) \wedge x \in A\},$$

$$\bigcap\{A | P(A)\} := \{x | \forall A : P(A) \Longrightarrow x \in A\}.$$

Als Varianten sind auch die folgenden (und ähnliche) Schreibweisen gebräuchlich:

$$\bigcup_{i\in\{0,1,2,\ldots,n\}} A_i = \bigcup_{i=0}^{n} A_i \quad \text{und} \quad \bigcup_{i\in\mathbb{N}} A_i = \bigcup_{i=0}^{\infty} A_i.$$

In analoger Weise auch für $\bigcap$.

Satz 1.3.6: *Es gelten folgende Beziehungen für Mengen A, B:*

- $A \cap B \subseteq A \subseteq A \cup B$,
- $A \setminus B \subseteq A$,
- $A \triangle B = (A \setminus B) \cup (B \setminus A)$,
- $A \subseteq B \iff A \cap B = A \iff A \cup B = B$.

Satz 1.3.7: *Es gelten folgende Beziehungen für Mengen A, B, C und Familien $(A_i)_{i\in I}$:*

- *(Kommutativgesetz)* $A \cup B = B \cup A$, $A \cap B = B \cap A$, $A \triangle B = B \triangle A$.
- *(Assoziativgesetz)* $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.
- *(Distributivgesetz)* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$,
  $A \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} (A \cap A_i)$, $A \cup \bigcap_{i \in I} A_i = \bigcap_{i \in I} (A \cup A_i)$.
- *(Idempotenzgesetz)* $A \cap A = A$, $A \cup A = A$.
- *(Verschmelzungsgesetz)* $A \cup (A \cap B) = A = A \cap (A \cup B)$.

Satz 1.3.8: *Es gelten folgende Beziehungen für Mengen A, B und Familien $(A_i)_{i \in I}$ in einer Universalmenge U:*

- $A \cap \overline{A} = \emptyset$, $A \cup \overline{A} = U$ *und* $\overline{\overline{A}} = A$,
- *(Gesetze von De Morgan)* $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\quad \overline{A \cap B} = \overline{A} \cup \overline{B}$,
  $\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}$, $\quad \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}$.

Häufig stellt man Mengen und ihre Verknüpfungen durch sogenannte **Venn-Diagramme** graphisch dar. Solche Diagramme können Argumente und Beweise anschaulich verdeutlichen.

Um später über Koordinaten von Punkten in der Ebene und im Raum sprechen zu können, also über Paare und Tripel von Zahlen, geben wir eine mengentheoretische Definition des Begriffes "Paar" an.

Definition 1.3.9: *Seien A und B Mengen. Für $a \in A$ und $b \in B$ heisst die Menge $\{a, \{a, b\}\}$ das* **geordnete Paar** *aus a und b. Gewöhnlich schreiben wir dieses geordnete Paar als (a, b). Das* **kartesische Produkt** *(René Descartes, 1596–1650) von A und B ist die Menge aller Paare aus Elementen von A und B, also*

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

Für $A \times A$ schreibt man auch A^2.

Ein Element von $(A \times B) \times C = A \times B \times C$ heisst **Tripel** und wir schreiben es als (a, b, c).
Ein Element von $A_1 \times A_2 \times \cdots \times A_n = \times_{i=1}^n A_i$ heisst ein **n-Tupel** und wir schreiben es als $(a_1, a_2, \ldots, a_n)$.

Man kann nun "kartesische Potenzen" von Mengen wie folgt betrachten:

$$\begin{aligned} A^1 &= A, \\ A^2 &= A^1 \times A = A \times A, \\ A^3 &= A^2 \times A, \\ &\vdots \\ A^{n+1} &= A^n \times A, \\ &\vdots \end{aligned}$$

So werden wir später die "reelle Ebene" mit $\mathbb{R}^2$ und den "reellen Raum" mit $\mathbb{R}^3$ identifizieren.

Eine weitere wichtige Operation zur Erzeugung neuer Mengen ist die Bildung der Potenzmenge.

Definition 1.3.10: *Sei A eine Menge. Die* **Potenzmenge** *$\mathcal{P}(A)$ von A ist die Menge aller Teilmengen von A, also*

$$\mathcal{P}(A) := \{B | B \subseteq A\}.$$

Manchmal schreiben wir für $\mathcal{P}(A)$ auch 2^A.

Beispiel 1.3.11: $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \quad \mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset.$

Satz 1.3.12: *$\mathcal{P}(\{1,\ldots,n\})$ hat genau 2^n Elemente.*

<u>Relationen</u>

Relationen sind die mathematische Modellierung von "Beziehungen" zwischen Elementen von Mengen. So könnte etwa A die Menge der Studenten in einer Vorlesung sein, und B die Menge der im Hörsaal verfügbaren Sitzplätze. Für $a \in A$ und $b \in B$ könnte dann etwa "$a \sim b$" bedeuten, dass Student a den Sitzplatz b einnimmt. Oder für $a_1, a_2 \in A$ könnte $a_1 \prec a_2$ bedeuten, dass a_2 öfter zur Vorlesung kommt als a_1.

Definition 1.3.13: *Seien A, B Mengen. Eine* **Relation** *R* **zwischen** *A und B ist eine Teilmenge von $A \times B$. Für $(a,b) \in R$ schreiben wir auch aRb.*
Ist $A = B$ so sprechen wir von einer **Relation auf** *A. Die Grundmenge A zusammen mit der Relation R auf A schreiben wir häufig als $\langle A, R\rangle$.*
Ist R eine Relation zwischen A und B, so ist die **inverse Relation**

$$R^{-1} := \{(b,a) | (a,b) \in R\}$$

eine Relation zwischen B und A.

Man kann natürlich auch Relationen zwischen mehreren Mengen $A_1, A_2, \ldots, A_n$ einführen als Teilmengen von $\times_{i=1}^n A_i$.

Im folgenden werden wir einige wichtige Eigenschaften von Relationen untersuchen. Sie helfen uns, interessanten Typen von Relationen, wie etwa Funktionen (Zuordnung von Werten zu Daten), Äquivalenzrelationen (Ähnlichkeitsbeziehungen), oder Ordnungsrelationen (Hierarchiebeziehungen), zu definieren.

Definition 1.3.14: *Eine Relation R zwischen A und B heisst* **funktional**, *falls es zu jedem $a \in A$ genau ein $b \in B$ gibt sodass aRb, also*

$$\forall a \in A\ \exists! b \in B\ :\ aRb.$$

Definition 1.3.15: *Sei R eine Relation auf der Menge A.*

- *R heisst* **reflexiv** *wenn gilt:* $\quad \forall a \in A\ :\ aRa$.
- *R heisst* **symmetrisch** *wenn gilt:* $\quad \forall a, b \in A\ :\ aRb \Longrightarrow bRa$.
- *R heisst* **antisymmetrisch** *wenn gilt:* $\quad \forall a, b \in A\ :\ (aRb \wedge bRa) \Longrightarrow a = b$.

- *R heisst* **transitiv** *wenn gilt:* $\forall a, b, c \in A \;:\; (aRb \wedge bRc) \Longrightarrow aRc$.

Beispiel 1.3.16:

(i) Die Gleichheitsrelation bzw. Identitätsrelation auf einer Menge A ist

$$=_A = \{(a, a) | a \in A\}.$$

Offensichtlich ist $=_A$ funktional, reflexiv, symmetrisch, transitiv und antisymmetrisch.

(ii) Die Allrelation ist A^2, also jedes Element von A steht mit jedem anderen in Relation. Welche Eigenschaften hat die Allrelation?

(iii) Die Teilbarkeitsrelation $m|n$ auf $\mathbb{Z}$ ist reflexiv, und transitiv. Hat sie eine der anderen Eigenschaften?

(iv) Die Relation "quad" auf $\mathbb{Z}$ sei

$$\text{quad} = \{(n, n^2) | n \in \mathbb{Z}\}.$$

Die Relation quad ist funktional, aber quad^{-1} ist nicht funktional.

(v) Auf der Menge $A = \{1, 2, 3\}$ betrachten wir die Relation

$$R = \{(1, 1), (1, 2), (2, 3), (3, 2)\}.$$

Welche Eigenschaften hat R?

Definition 1.3.17: *Eine Relation R auf A heisst* **Äquivalenzrelation** *wenn sie reflexiv, symmetrisch und transitiv ist.*
Eine Relation R auf A heisst **Ordnungsrelation** *wenn sie reflexiv, antisymmetrisch und transitiv ist.*
Eine Relation R zwischen A und B heisst **Funktion** *wenn sie funktional ist.*

Beispiel 1.3.18: Gleichheit und Allrelation (Beispiel 1.3.16 (i) und (ii)) sind Äquivalenzrelationen.

Ein anderes typisches Beispiel einer Äquivalenzrelation ist

$$\langle \mathbb{Z}, \text{mod} n \rangle, \quad \text{für } n \in \mathbb{N}^+.$$

Also zwei ganze Zahlen a und b sind äquivalent, wenn sie denselben Rest bei Division durch n haben: $a = b \bmod n$.

Eine Äquivalenzrelation führt zu einer natürlichen Einteilung der Grundmenge in disjunkte Teilmengen. Das soll im folgenden präzisiert werden.

Definition 1.3.19: *Eine Familie von nichtleeren Teilmengen $\{A_i | i \in I\}$ einer Menge A heisst* **Partition** *oder* **Zerlegung** *von A, wenn gilt*

$$A_i \cap A_j = \emptyset \text{ für } i \neq j, \quad \text{und} \quad A = \bigcup_{i \in I} A_i \;.$$

Definition 1.3.20: *Sei $\sim$ eine Äquivalenzrelation auf A. Für $a \in A$ heisst die Menge*

$$K(a) := \{b \in A | a \sim b\}$$

die **Äquivalenzklasse** *von a. Die Menge aller Äquivalenzklassen*

$$A_{/\sim} := \{K(a) | a \in A\}$$

heisst die **Faktormenge** *von A nach $\sim$. Weiters heisst $S \subseteq A$ ein* **Repräsentantensystem** *von A bzgl. $\sim$, falls S aus jeder Äquivalenzklasse genau ein Element enthält.*

Satz 1.3.21: *Sei $\sim$ eine Äquivalenzrelation auf A. Dann gilt für $a, b \in A$:*

(i) $K(a) = K(b) \Longleftrightarrow a \sim b$,

(ii) $a \not\sim b \Longleftrightarrow K(a) \cap K(b) = \emptyset$,

(iii) $\bigcup_{a \in A} K(a) = A$.

Satz 1.3.22:

(i) Sei $\sim$ eine Äquivalenzrelation auf A. Dann bilden die verschiedenen Äquivalenzklassen eine Partition von A.

(ii) Sei $A = \bigcup_{i \in I} A_i$ eine Partition von A. Dann ist die Relation $\sim$ mit

$$a \sim b :\Longleftrightarrow a \text{ und } b \text{ liegen im selben } A_i$$

eine Äquivalenzrelation auf A.

Definition 1.3.23: *Seien $\sim$ und $\approx$ zwei Äquivalenzrelationen auf A. Dann heisst $\sim$* **feiner** *als $\approx$, und $\approx$* **gröber** *als $\sim$, wenn gilt: $\forall a, b \in A : a \sim b \Longrightarrow a \approx b$.*

Beispiel 1.3.24: Auf $\mathbb{Z}$ betrachten wir die beiden Äquivalenzrelationen

$$a \sim_5 b \Longleftrightarrow a = b \bmod 5 \quad \text{und} \quad a \sim_{10} b \Longleftrightarrow a = b \bmod 10\ .$$

Offensichtlich gilt $a \sim_{10} b \Longrightarrow a \sim_5 b$ für alle $a, b \in \mathbb{Z}$. $\sim_{10}$ ist also feiner als $\sim_5$.

Nun wollen wir uns den Ordnungsrelationen auf einer Menge A zuwenden. Ordnungsrelationen werden typischerweise mit $\leq$ oder ähnlichen Zeichen geschreiben. Gilt $a \leq b$ bzgl. einer Ordnungsrelation $\leq$, so heisst a **kleinergleich** b bzgl. $\leq$. Ist $a \leq b$ und $a \neq b$, so heisst a **kleiner** als b und wir schreiben dafür $a < b$. Eine endliche geordnete Menge $\langle A, \leq \rangle$ kann man graphisch dadurch darstellen, dass man die vergleichbaren Elemente von A mit Kanten verbindet, wobei eine Kante nach oben einen Aufstieg bzgl. der Ordnung $\leq$ bedeutet. Man spricht in diesem Zusammenhang von einem **Hasse-Diagramm**.

Definition 1.3.25: *Eine Ordnungsrelation $\leq$ auf A heisst* **linear**, *falls für je zwei Elemente $a, b \in A$ entweder $a \leq b$ oder $b \leq a$ gilt. $\langle A, \leq \rangle$ heisst dann eine* **linear geordnete Menge** *oder* **Kette**.

Beispiel 1.3.26: Die Teilbarkeitsrelation $|$ ist eine Ordnungsrelation auf $\mathbb{N}$, aber keine lineare Ordnungsrelation.

Auf $\mathbb{Z}$ ist $|$ keine Ordnungsrelation, da die Antisymmetrie verletzt ist.

Satz 1.3.27: *Sei M eine Menge, und $L = \mathcal{P}(M)$ ihre Potenzmenge. Dann ist die Relation*

$$A \leq B :\Longleftrightarrow A \subseteq B$$

eine Ordnungsrelation auf L, aber im allgemeinen (wenn M mehr als 1 Element enthält) keine lineare Ordnung.
Insbesondere sind dadurch alle Relationen $R \subseteq M_1 \times M_2$ zwischen zwei Mengen M_1, M_2 in natürlicher Weise geordnet.

Definition 1.3.28: *Sei $(A, \leq)$ eine geordnete Menge, und sei $B \subseteq A$.*

(i) $a \in A$ heisst **kleinstes Element** *von A g.d.w. (genau dann wenn) für alle $b \in A$ gilt: $a \leq b$.*

(ii) $a \in A$ heisst **grösstes Element** *von A g.d.w. für alle $b \in A$ gilt: $b \leq a$.*

(iii) $a \in A$ heisst **minimales Element** *von A g.d.w. für alle $b \in A$ gilt: $b \leq a \Longrightarrow b = a$.*

(iv) $a \in A$ heisst **maximales Element** *von A g.d.w. für alle $b \in A$ gilt: $a \leq b \Longrightarrow b = a$.*

(v) $a \in A$ heisst **untere Schranke** *von B (in A) g.d.w. für alle $b \in B$ gilt: $a \leq b$.*

(vi) $a \in A$ heisst **obere Schranke** *von B (in A) g.d.w. für alle $b \in B$ gilt: $b \leq a$.*

(vii) Besitzt die Menge aller unteren Schranken von B ein grösstes Element $a \in A$, so nennen wir a das **Infimum** *von B in A, $a = \inf_A(B)$.*

(viii) Besitzt die Menge aller oberen Schranken von B ein kleinstes Element $a \in A$, so nennen wir a das **Supremum** *von B in A, $a = \sup_A(B)$.*

Beispiel 1.3.29: In $\langle \mathbb{N} \setminus \{0, 1\}, |\rangle$ gibt es kein grösstes und kein kleinstes Element. Minimale Elemente sind genau die Primzahlen.
$\langle \mathbb{N}, |\rangle$ hat 1 als kleinstes und 0 als grösstes Element.
Für $\langle \mathbb{R}, \leq\rangle$ (übliche Ordnung) und $B =]0, 1]$ gilt:
die Menge der unteren Schranken von B ist $U = \{x \in \mathbb{R} | x \leq 0\}$, und $\inf_{\mathbb{R}} B = 0 \notin B$,
die Menge der oberen Schranken von B ist $O = \{x \in \mathbb{R} | x \geq 1\}$, und $\sup_{\mathbb{R}} B = 1 \in B$. □

Satz 1.3.30: *Sei $\langle A, \leq\rangle$ eine geordnete Menge.*

(i) A enthält höchstens ein kleinstes und höchstens ein grösstes Element.

(ii) Ist a kleinstes (grösstes) Element von A, so ist a das einzige minimale (maximale) Element von A.

Satz und Definition 1.3.31: *Sei $\langle A, \leq_A\rangle$ eine geordnete Menge, und sei $B \subseteq A$. Dann ist $\leq_B := \leq_A \cap B^2$ eine Ordnung auf B, die sogenannte* **induzierte Ordnung***. Ist $\langle A, \leq_A\rangle$ linear, dann auch $\langle B, \leq_B\rangle$.*

Satz und Definition 1.3.32: *Seien $\langle A_1, \leq_1\rangle$ und $\langle A_2, \leq_2\rangle$ geordnete Mengen. Auf $A = A_1 \times A_2$ definieren wir die Relation*

$$(a_1, a_2) \leq (b_1, b_2) \;:\Longleftrightarrow\; [a_1 <_1 b_1 \;\vee\; (a_1 = b_1 \wedge a_2 \leq_2 b_2)] \;.$$

Dann ist $\langle A, \leq\rangle$ auch geordnet. Die Ordnung $\leq$ heisst die **lexikographische Ordnung** *auf A. Sind $\leq_1$ und $\leq_2$ linear, dann auch $\leq$.*

Definition 1.3.33: *Eine Ordnung $\leq$ auf A heisst* **Wohlordnung**, *wenn jede nichtleere Teilmenge B von A ein kleinstes Element besitzt.*

Beispiel 1.3.34: Die übliche Ordnung $\leq$ ist eine Wohlordnung auf $\mathbb{N}$, nicht aber auf $\mathbb{Z}$. Jedoch kann $\mathbb{Z}$ durch $0 < 1 < 2 < \cdots < -1 < -2 < \cdots$ wohlgeordnet werden. □

Für Wohlordnungen (genauer Mengen A mit Wohlordnung $\leq$) gilt das **Prinzip der transfiniten Induktion**:

> *Ist $T \subseteq A$, und gilt:* $\quad \forall x \in A \;:\; \big(\{y \in A | y < x\} \subseteq T \implies x \in T\big)$,
> *dann ist $T = A$.*

Funktionen

Nun wollen wir einen Gundbegriff der Mathematik einführen, den der Funktion oder Abbildung. Wir haben bereits etliche Beispiele dafür kennenbelernt. Die Addition "+" bildet ein Paar von Zahlen ab auf ihre Summe, der Euklidsche Algorithmus bildet ein Paar natürlicher Zahlen ab auf ihren ggT.

Definition 1.3.35: *Seien A, B zwei nichtleere Mengen, und sei f eine funktionale Relation von A nach B, also $f \subseteq A \times B$ und zu jedem $a \in A$ gibt es genau ein $b \in B$ mit $(a, b) \in f$. Dann nennen wir f eine* **Funktion** *oder* **Abbildung** *von A nach B, und schreiben sie als*

$$\begin{array}{rccl} f : & A & \to & B \\ & a & \mapsto & f(a)\;. \end{array}$$

A heisst der **Definitionsbereich** *und B der* **Bildbereich** *von f. $f(a)$ heisst der* **Funktionswert** *von a unter f.*
Ist $A' \subset A$, so heisst $f(A') = \{f(a) | a \in A'\}$ das **Bild** *von A' unter f.*
Ist $B' \subset B$, so heisst $f^{-1}(B') = \{a \in A | f(a) \in B'\}$ das **Urbild** *von B' unter f.*
Die Menge $\{(a, f(a)) | a \in A\}$ heisst auch **Graph** *von f.*
Für $C \subseteq A$ ist $f_{/C} := f \cap (C \times B)$ eine Funktion von C nach B, genannt die **Einschränkung** *oder* **Restriktion** *von f auf C.*
Die Menge aller Funktionen von A nach B bezeichnet man durch B^A. □

Laut Definition ist also eine Funktion f bestimmt durch den Definitionsbereich, den Bildbereich, und die entsprechende Zuordnung. So haben die Funktionen

$$\begin{array}{rccl} f : & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & n^2 \end{array} \qquad\qquad \begin{array}{rccl} g : & \mathbb{Z} & \to & \mathbb{N} \\ & n & \mapsto & n^2 \end{array}$$

zwar denselben Graphen, sind aber verschiedene Funktionen, da die Bildbereiche nicht übereinstimmen.

Beispiel 1.3.36:

(i) Für jede Menge A ist id_A die Funktion, welche jedes Element $a \in A$ auf sich selbst abbildet. id_A heisst die **identische Funktion** auf A.

(ii) Sei A eine gegebene (Grund-)Menge. Für jede Menge $M \subseteq A$ heisst

$$\begin{array}{rcl} \chi_M : \quad A & \to & \{0,1\} \\ x & \mapsto & \begin{cases} 1 & \text{falls } x \in M \\ 0 & \text{sonst} \end{cases} \end{array}$$

die charakteristische Funktion von A.

(iii) ggT ist eine Funktion auf $\mathbb{N}^2 \setminus \{(0,0)\}$, nicht aber auf $\mathbb{Z}^2 \setminus \{(0,0)\}$.

(iv) $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$, $|\ | : \mathbb{R} \to \mathbb{R}^+$, $\sin, \cos : \mathbb{R} \to [-1,1]$ sind Funktionen.

Definition 1.3.37: *Sei $f : A \to B$ eine Funktion.*
f heisst **injektiv**, *wenn es zu jedem $b \in B$ höchstens ein $a \in A$ gibt mit $b = f(a)$, also $\forall a_1, a_2 \in A : (f(a_1) = f(a_2) \Longrightarrow a_1 = a_2)$.*
f heisst **surjektiv**, *wenn es zu jedem $b \in B$ ein $a \in A$ gibt mit $b = f(a)$, also $f(A) = B$.*
f heisst **bijektiv**, *wenn es zu jedem $b \in B$ genau ein $a \in A$ gibt mit $b = f(a)$, also wenn f sowohl injektiv als auch surjektiv ist.* □

Definition 1.3.38: *Sind $f : A \to B$ und $g : B \to C$ Funktionen, so wird die Zusammensetzung $g \circ f : A \to C$ definiert durch $(g \circ f)(a) = g(f(a))$. $g \circ f$ ist eine Funktion von A nach C.* □

Definition 1.3.39: *Eine Funktion $g : B \to A$ heisst eine zu $f : A \to B$* **inverse Funktion**, *wenn gilt $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Wenn es zu f eine inverse Funktion gibt, so ist diese eindeutig bestimmt (siehe Satz 1.3.40) und wir schreiben sie als f^{-1}.* □

Satz 1.3.40: *Seien $f : A \to B$, $g : B \to C$ und $h : C \to D$ Funktionen.*

(i) Es gilt $h \circ (g \circ f) = (h \circ g) \circ f$ (Assoziativität)

(ii) Sind die Funktionen f unf g beide injektiv (bzw. surjektiv bzw. bijektiv), so ist auch $g \circ f$ injektiv (bzw. surjektiv bzw. bijektiv).

(iii) Zu f gibt es höchstens eine inverse Funktion.

(iv) f besitzt genau dann eine inverse Funktion f^{-1}, wenn f bijektiv ist. In diesem Fall ist auch f^{-1} bijektiv.

(v) Wenn f bijektiv ist, dann ist $(f^{-1})^{-1} = f$.

(vi) Seien f und g bijektiv. Dann ist $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Satz 1.3.41: *Sei $f : A \to B$ eine Funktion.*

(i) f ist injektiv g.d.w. für alle Funktionen $g, h : C \to A$ gilt:

$$f \circ g = f \circ h \Longrightarrow g = h\ .$$

(ii) f *ist surjektiv g.d.w. für alle Funktionen* $g, h : B \to C$ *gilt:*

$$g \circ f = h \circ f \Longrightarrow g = h\ .$$

Mächtigkeit von Mengen

Mengen können aus völlig verschiedenen Elementen bestehen. Dennoch ist es natürlich, sie etwa ihrer Grösse nach vergleichen zu wollen. Das ist bei endlichen Mengen relativ unproblematisch, für unendliche Mengen brauchen wir dazu aber sorgfältige Überlegungen. Die wesentlichen Begriffsbildungen stammen von Cantor.

Definition 1.3.42: *Zwei Mengen* A, B *heissen* **gleichmächtig**, *falls es eine bijektive Abbildung* $f : A \to B$ *gibt.* □

Satz 1.3.43: *Sei* U *eine gegebene (Grund-)Menge von Mengen (etwa alle Teilmengen einer Menge* A*). Die Relation der Gleichmächtigkeit ist auf* U *eine Äquivalenzrelation.*

Definition 1.3.44: *Sei* U *eine Grundmenge. Die Äquivalenzklasse von* $A \subseteq U$ *bzgl. der Relation der Gleichmächtigkeit heisst die* **Kardinalzahl** $|A|$ *von* A*, also*

$$|A| := \{B \in U |\ A \text{ und } B \text{ sind gleichmächtig } \}. \qquad \square$$

Eigentlich sollten wir in obiger Definition $|A|_U$ schreiben. In der Praxis macht man das aber nicht, sondern geht von einer genügend grossen Grundmenge (Universum) U aus, welche alle in einer gegebenen Theorie betrachteten Mengen enthält.

Satz 1.3.45: *Für* $n \in \mathbb{N}$ *gilt:* $|\{1, \ldots, n\}| = |\{1, \ldots, m\}| \iff n = m$.

Deshalb spricht man gewöhnlich von n als der Kardinalzahl einer n-elementigen Menge. Als Spezialfall davon ist 0 die Kardinalzahl der leeren Menge $\emptyset$.

Definition 1.3.46: *Seien* A, B *zwei Mengen.*
Gibt es eine injektive Abbildung $f : A \to B$*, so bezeichnet man das durch* $|A| \leq |B|$.
Gibt es eine surjektive Abbildung $f : A \to B$*, so bezeichnet man das durch* $|A| \geq |B|$.

Eigentlich setzt diese Definition einen Satz voraus:

> *Wenn* $f : A \to B$ *injektiv ist, und* $|A| = |A'|, |B| = |B'|$*, dann gibt es eine injektive Funktion* $f' : A' \to B'$.

Das ist tatsächlich der Fall, man nennt daher die Relation $\leq$ für Kardinalzahlen wohldefiniert.

Satz 1.3.47: *Seien* A, B *zwei Mengen. Dann gilt:*

(i) $A \subseteq B \implies |A| \leq |B|$.

(ii) $\leq$ *ist eine Ordnungsrelation auf den Kardinalzahlen.*

(iii) $|A| \leq |B| \iff |B| \geq |A|$.

Definition 1.3.48: *Eine Menge A heisst* **endlich**, *wenn ihre Kardinalzahl eine natürliche Zahl ist. Ansonsten heisst A* **unendlich**.

Satz 1.3.49: *Eine Menge A ist unendlich g.d.w. es eine echte Teilmenge B von A gibt mit $|B| = |A|$.*

Satz 1.3.50: *Für jede unendliche Menge A gilt: $|\mathbb{N}| \leq |A|$.*

$|\mathbb{N}|$ ist also die kleinste Kardinalzahl einer unendlichen Menge. Man bezeichnet $|\mathbb{N}|$ auch als $\aleph_0$ ($\aleph$, Aleph, ist der erste Buchstabe im hebräischen Alphabet).

Definition1.3.51: *Eine unendliche Menge A heisst* **abzählbar** *bzw.* **abzählbar unendlich** *wenn $|A| = \aleph_0$. Ansonsten heisst A* **überabzählbar**.

Satz 1.3.52: *Die Zahlenmengen $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar.*

Satz 1.3.53: *Die Zahlenmenge $\mathbb{R}$ ist überabzählbar.*

Man bezeichnet $|\mathbb{R}|$ auch als c, abgeleitet von "Continuum". Es gilt also $\aleph_0 < c$.

Satz 1.3.54: *Seien $a, b \in \mathbb{R}$ mit $a < b$. Dann ist*

$$|[a, b]| = |(a, b]| = |[a, b)| = |(a, b)| = |\mathbb{R}| \ .$$

Satz 1.3.55 (Satz von Cantor): *Für jede Menge A ist $|A| < \mathcal{P}(A)$.*

Es gibt also unendlich viele Abstufungen von Unendlichkeit

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots \ .$$

Man kann übrigens zeigen, dass $|\mathbb{R}| = c = |\mathcal{P}(\mathbb{N})|$. Die **Kontinuumshypothese** besagt, dass es zwischen $\aleph_0$ und c keine Kardinalzahl gibt. Das kann aber aus den Axiomen der Mengenlehre weder bewiesen noch widerlegt werden. Die Kontinuumshypothese ist also unabhängig von den Axiomen der Mengenlehre und kann als zusätzliches Axiom aufgenommen werden (oder auch nicht).

Satz 1.3.56: *Seien A, B zwei Mengen, wobei B unendlich ist und $|A| \leq |B|$. Dann gilt:*

$$|A \cup B| = |A \times B| = |\bigcup_{n \geq 1} B^n| = |\{E \subseteq B | E \text{ endlich } \}| = B \ .$$

Satz 1.3.57 (Cantor-Schröder-Bernstein (CSB)): *Seien A, B Mengen. Dann gilt*

$$|A| \leq |B| \wedge |B| \leq |A| \Longrightarrow |A| = |B| \ .$$

Also die Relation $\leq$ auf Kardinalzahlen ist antisymmetrisch.

Beispiel 1.3.58: Mittels der Idee aus dem Beweis des CSB-Satzes konstruieren wir eine Bijektion zwischen den Intervallen $(-1, 1)$ und $[-1, 1]$. Wir gehen aus von den injektiven Funktionen

$$\begin{array}{rccc} f: & (-1,1) & \to & [-1,1] \\ & x & \mapsto & x \end{array} \qquad\qquad \begin{array}{rccc} g: & [-1,1] & \to & (-1,1) \\ & x & \mapsto & x/2 \end{array} \quad .$$

Mit den Bezeichnungen aus dem Beweis des CSB-Satzes haben wir $B \setminus C = \{-1, 1\}$. Daher müssen wir setzen: $h(1/2) = 1, h(1/4) = 1/2, h(1/8) = 1/4$, etc. Ebenso müssen wir setzen: $h(-1/2) = -1, h(-1/4) = -1/2, h(-1/8) = -1/4$, etc. Für alle anderen Elemente von $(-1, 1)$ setzen wir $h(x) = x$. Somit haben wir gezeigt, dass $|(-1, 1)| = |[-1, 1]|$. □

Mit dem Satz von CSB ist es leicht zu sehen, dass die Relation $\leq$ auf Kardinalzahlen eine Ordnungsrelation ist.

Axiomatisierung der Mengentheorie

Nach Einführung der naiven Mengentheorie durch Cantor wurde relativ schnell erkannt, dass sie widersprüchlich ist. Das Russell'sche Paradoxon lautet wie folgt:

"Sei A die Menge aller Mengen, welche sich nicht selbst als Element enthalten, also

$$A = \{B | B \notin B\}.$$

Daraus folgt sofort, dass $A \in A \iff A \notin A$, ein Widerspruch!"

Dieses Problem konnte dadurch gelöst werden, dass man strikte Regeln für die Definition von Mengen einführte, die sogenannten **Axiome der Zermelo-Fränkel-Mengentheorie (ZF):** [4]

[ZF1] **Extensionalitätsaxiom** Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten.

[ZF2] **Paarmengenaxiom** Zu je zwei Mengen x und y gibt es eine Menge $\{x, y\}$, die genau diese beiden Elemente enthält.

[ZF3] **Vereinigungsmengenaxiom** Zu jeder Menge von Mengen kann man die Vereinigungsmenge bilden.

[ZF4] **Leere Menge** Es gibt die leere Menge $\emptyset$.

[ZF5] **Unendlichkeitsaxiom** Es gibt eine Menge M, welche die leere Menge und mit jeder Menge x auch den sogenannten Nachfolger $x \cup \{x\}$ enthält.

[ZF6] **Potenzmengenaxiom** Zu jeder Menge existiert die Potenzmenge, die Menge aller Teilmengen.

[ZF7] **Ersetzungsaxiom** Ist A eine Menge und ist E eine zweistellige Eigenschaft derart, dass es zu jedem $a \in A$ genau ein b mit $E(a, b)$ gibt, dann bilden alle solchen b wieder eine Menge.

[ZF8] **Regularitätsaxiom** Jede nichtleere Menge X besitzt ein $x \in X$ mit leerem Schnitt $X \cap x = \emptyset$.

[ZF9] **Auswahlaxiom** Zu jeder Menge X nichtleerer Mengen gibt es eine Funktion f, welche jedem $x \in X$ ein $f(x) \in x$ zuordnet.

Aus den Axiomen der Zermelo-Fränkel-Mengentheorie (ZF), sogar ohne das Auswahlaxiom [ZF9], kann man das sogenannte **Aussonderungsaxiom** herleiten:

[4] R.S. Wolf, "A Tour Through Mathematical Logic", The Mathematical Association of America (MAA), (2005), Seite 69

Aussonderungsaxiom Aus jeder Menge kann man die Teilmenge jener Elemente bilden, die eine vorgegebene Eigenschaft besitzen.

Das Auswahlaxiom spielt eine spezielle Rolle in der Mengentheorie. Es führt zu überraschenden Konsequenzen, und man stellte sich die Frage, ob es etwa schon aus den anderen Axiomen folgt. Tatsächlich ist es logisch unabhängig von [ZF1–8]. Kurt Gödel (1906–1978) bewies, dass Zermelo-Fränkel mit Auswahlaxiom konsistent (also widerspruchsfrei) ist, Paul Cohen bewies, dass [ZF1–8] zusammen mit der Negation des Auswahlaxioms ebenfalls konsistent ist. In der Mathematik ist es üblich geworden, das Auswahlaxiom als gültig zu verwenden

Das Auswahlaxiom ist äquivalent zu einigen anderen interessanten Aussagen der Mengentheorie; d.h. nimmt man zusätzlich zu den ersten 8 Axiomen der ZF auch das Auswahlaxiom an, so folgen diese anderen Aussagen, und nimmt man zu den ersten 8 Axiomen von ZF eine dieser anderen Aussagen hinzu, so folgt das Auswahlaxiom.

Lemma von Zorn: *Falls jede Kette in einer geordneten Menge $(A, \leq)$ eine obere Schranke (in A) besitzt, so besitzt A (mindestens) ein maximales Element.*

Axiom für kartesische Produkte: *Sind I und für alle $i \in I$ auch A_i nichtleere Mengen, so ist auch $\times_{i \in I} A_i \neq \emptyset$.*

Wohlordnungssatz: *Für jede Menge A gibt es eine Relation $\leq$, sodass $(A, \leq)$ eine Wohlordnung ist.*

Alle diese Aussagen sind also äquivalent zum Auswahlaxiom [ZF9]. Sie gelten also in der Mengentheorie ZF, wenn man das Auswahlaxiom annimmt. Bisher hat aber noch niemand eine Wohlordnung auf $\mathbb{R}$ finden können.

1.4 Logik

Häufig verwenden wir beim Sprechen über Mathematik die Umgangssprache, wenn diese nicht zu Missverständlichkeiten führt. Was aber soll man etwa von der Aussage "3 und 1/4 sind Inverse" halten? Ein Ziel mathematischer Logik ist die Elimination solcher Mehrdeutigkeiten. Wir brauchen beim Betreiben von Mathematik eine eindeutige Sprache und klare Schlussregeln.

Die grundlegenden Prinzipien der Logik und ihre Anwendung in der Mathematik waren den Philosophen und Mathematikern des klassischen griechischen Altertums wohl vertraut. Aristoteles (384–322 v.Chr.) erstellte die erste Abhandlung der Logik (das, was wir heute Aussagenlogik nennen). Aristoteles bediente sich dabei der Umgangssprache, wir sprechen von informeller im Gegensatz zu symbolischer Logik. Es dauerte ziemlich genau 2000 Jahre, bis die Aristotelische Logik durch Gottfried Wilhelm Leibniz (1646–1716), den Miterfinder der Differential- und Integralrechnung, eine Weiterentwicklung erfuhr. Sein Ziel war die Definition einer symbolischen Sprache des logischen Schliessens. Noch einmal 200 Jahre später bauten Augustus De Morgan (1806–1871) und George Boole (1815–1864) auf den Arbeiten von Leibniz auf und begannen die Entwicklung der modernen symbolischen Aussagenlogik. Schliesslich wurde die Bedeutung von Quantoren in der mathematischen Logik klar erkannt. Gottlob Frege (1848–1925) entwickelte die Prädikatenlogik, wie wir sie heute kennen. Viele der gebräuchlichen Symbole der Logik und Mengentheorie wurden von Giuseppe Peano (1858–1932) eingeführt. Am Ende des 19. Jahrhunderts wurden Widersprüchlichkeiten in der Mengentheorie gefunden (siehe Kapitel 1.3), und das führte zur Überzeugung, dass man die Umgangssprache in der Mathematik zurückdrängen und dafür den Gebrauch symbolischer Logik forcieren sollte. In ihrem monumentalen Werk *"Principia Mathematica"* gelang es Bertrand Russell und Alfred North Whitehead (1861–1947), einen Grossteil der Mathematik auf symbolischer Logik und Mengentheorie aufzubauen. David Hilbert (1862–1943) ging einen Schritt weiter. Laut seinem Programm sollte die ganze Mathematik in einem vollständig symbolischen, axiomatischen Rahmen aufgebaut werden. Mittels Metamathematik (Mathematik angewandt auf Mathematik), auch Beweistheorie genannt, sollte dann die Widerspruchsfreiheit der Mathematik bewiesen werden. Zu Beginn der 1930er Jahre zeigte aber der junge österreichische Logiker Kurt Gödel (1906–1978) in seinem berühmten Unvollständigkeitssatz, dass das Hilbertsche Programm undurchführbar ist. Schon die Theorie der natürlichen Zahlen $\mathbb{N}$ ist zu reichhaltig, um völlig axiomatisiert werden zu können. Jede Axiomatisierung der Theorie der natürlichen Zahlen ist notwendigerweise unvollständig in dem Sinn, dass es Aussagen gibt, welche zwar gültig sind aber nicht beweisbar. Dennoch waren zwei wichtige Vorhaben des Hilbertschen Programms — die Übersetzung der mathematischen *Sprache* und mathematischer *Beweise* in ein rein formales, symbolisches Format — extrem erfolgreich.

Im folgenden wollen wir die Grundkonzepte der mathematischen Logik, also der logischen Grundlage der Mathematik, einführend besprechen.

Aussagenlogik

Definition 1.4.1: *Unter einer* **Grundaussage** *verstehen wir einen deklarativen Satz, der entweder wahr (***t***) oder falsch (***f***) ist. Zur Bezeichnung von Aussagen verwenden wir sogenannte* **Aussagenvariable**, *wie etwa P, Q, R. Sowohl Grundaussagen als auch Aussagenvariable sind* **Aussagen**. *Ist A eine Grundaussage, so bezeichnen wir mit $T(A)$ den* **Wahrheitswert** *von A. Die Funktion T heisst die* **Wahrheitsfunktion**. *Auf Aus-*

sagenvariablen ist die Wahrheitsfunktion zunächst undefiniert, es sei denn, wir weisen der Variablen explizit einen Wahrheitswert zu.

Also Fragen oder Aufforderungen sind keine Aussagen, wohl aber sind "Schnee ist weiss" oder "$2+3=6$" Aussagen. Natürlich ist $T(2+3=6)=\mathbf{f}$.

Man beachte, dass wir hier davon ausgehen, dass eine Aussage nur einen der beiden Wahrheitswerte $\mathbf{t}$ oder $\mathbf{f}$ haben kann, die hier betrachtete Logik ist also zweiwertig. Man spricht in diesem Zusammenhang auch vom **Prinzip des ausgeschlossenen Dritten** (tertium non datur).

Definition 1.4.2: *Aussagen können mittels* **Junktoren** *zu neuen Aussagen verbunden werden. Seien P, Q Aussagen. Als Junktoren verwenden wir üblicherweise*

- *die* **Negation** $\neg P$*, "nicht P"; $T(\neg P)=\mathbf{t}$ genau dann wenn $T(P)=\mathbf{f}$;*
- *die* **Konjunktion** $P \wedge Q$*, "P und Q"; $T(P \wedge Q)=\mathbf{t}$ genau dann wenn sowohl $T(P)=\mathbf{t}$ als auch $T(Q)=\mathbf{t}$;*
- *die* **Disjunktion** $P \vee Q$*, "P oder Q"; $T(P \vee Q)=\mathbf{t}$ genau dann wenn entweder $T(P)=\mathbf{t}$ oder $T(Q)=\mathbf{t}$ (oder beide wahr sind, inklusives oder);*
- *die* **Implikation** $P \Longrightarrow Q$*, "wenn P dann Q"; $T(P \Longrightarrow Q)=\mathbf{f}$ genau dann wenn $T(P)=\mathbf{t}$ und $T(Q)=\mathbf{f}$, also wenn die Hypothese P wahr ist, aber die Konklusion Q falsch ist;*
- *die* **Äquivalenz** $P \Longleftrightarrow Q$*, "P ist äquivalent zu Q"; $T(P \Longleftrightarrow Q)=\mathbf{t}$ genau dann wenn $T(P)=T(Q)=\mathbf{t}$ oder $T(P)=T(Q)=\mathbf{f}$.*

Aussagen, welche keine Junktoren enthalten (also Grundaussagen und Aussagenvariable) heissen auch **atomare Aussagen**. *Alle übrigen sind* **zusammengesetzte Aussagen**.

Enthält eine Aussage mehrere Junktoren, so verwenden wir Klammern, um die Bedeutung festzulegen. Um die Klammernsetzung zu minimieren, legen wir folgende Priorität von Junktoren fest, von der höchsten zur niedrigsten:

$$\neg, \wedge, \vee, \Longrightarrow, \Longleftrightarrow \quad .$$

Also $P \Longrightarrow Q \wedge R$ bedeutet $P \Longrightarrow (Q \wedge R)$ und nicht $(P \Longrightarrow Q) \wedge R$.

Der Gebrauch der Implikation (wenn, dann) in der mathematischen Logik unterscheidet sich vom umgangssprachlichen Gebrauch. Während in der Umgangssprache meist ein ursächlicher Zusammenhang zwischen Hypothese und Konklusion hergestellt wird, ist das in der mathematischen Logik in keiner Weise so. Ist in $P \Longrightarrow Q$ die Hypothese P falsch, so ist die Aussage auf jeden Fall wahr.

Enthält eine Aussage aussagenlogische Variable, so wird ihr Wahrheitswert erst festgelegt, indem man diesen Variablen einen Wahrheitswert zuordnet. Dieser Zusammenhang wird gewöhnlich in einer sogenannten **Wahrheitstabelle** festgehalten.

Beispiel 1.4.3: Wir stellen die Wahrheitstabelle für die Aussage

$$(P \Longrightarrow Q) \Longleftrightarrow (R \wedge P)$$

auf.

P	Q	R	$P \Longrightarrow Q$	$R \wedge P$	$(P \Longrightarrow Q) \Longleftrightarrow (R \wedge P)$
t	**t**	**t**	**t**	**t**	**t**
t	**t**	**f**	**t**	**f**	**f**
t	**f**	**t**	**f**	**t**	**f**
t	**f**	**f**	**f**	**f**	**t**
f	**t**	**t**	**t**	**f**	**f**
f	**t**	**f**	**t**	**f**	**f**
f	**f**	**t**	**t**	**f**	**f**
f	**f**	**f**	**t**	**f**	**f**

Definition 1.4.4: *Sei P eine Aussage, welche ausser Grundaussagen nur die Variablen $P_1, \ldots, P_n$ enthält. Für die Grundaussagen seien Wahrheitswerte fix festgelegt. P heisst* **Tautologie** *(bzgl. der festgelegten Wahrheitswerte für die Grundaussagen), wenn bei jeder möglichen Belegung der Variablen $P_1, \ldots, P_n$ mit Wahrheitswerten die Aussage P den Wahrheitswert* **t** *erhält.*
Eine Aussage, deren Negation eine Tautologie ist, heisst **Kontradiktion**.
Zwei Aussagen P und Q heissen **(aussagenlogisch) äquivalent**, *wenn $P \Longleftrightarrow Q$ eine Tautologie ist.*
Eine Aussage ist eine **(aussagenlogische) Konsequenz** *der Aussagen $P_1, \ldots, P_n$, wenn $(P_1 \wedge \ldots \wedge P_n) \Longrightarrow Q$ eine Tautologie ist.*

Beispiel 1.4.5: Eine Implikation $P \Longrightarrow Q$ ist immer äquivalent zu $\neg Q \Longrightarrow \neg P$. Also

$$(P \Longrightarrow Q) \iff (\neg Q \Longrightarrow \neg P)$$

ist eine Tautologie.
Die **De Morgan'schen Gesetze** sind die folgenden Äquivalenzen:

$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q), \quad \neg(P \wedge Q) \iff (\neg P \vee \neg Q).$$

Die Definition einer aussagenlogischen Konsequenz kann auch auf folgende Weise ausgedrückt werden: Q ist eine Konsequenz von $P_1, \ldots, P_n$, wenn $T(Q) = \mathbf{t}$ sein muss unter der Voraussetzung $T(P_1) = \cdots = T(P_n) = \mathbf{t}$. In einem mathematischen Beweis können wir also jede Ausssage verwenden, welche eine Konsequenz bereits vorher bewiesener Aussagen ist. Auf diesem Prinzip bauen etliche "Beweismethoden" auf.

Bezeichnung 1.4.6: Beweismethoden der Aussagenlogik:

- **Modus Ponens:** aus P und $P \Longrightarrow Q$ können wir schliessen Q.
- **Modus Tollens:** aus $\neg Q$ und $P \Longrightarrow Q$ können wir schliessen $\neg P$.
- **Indirekter Beweis, Widerspruchsbeweis, "reductio ad absurdum":** aus $(\neg P) \Longrightarrow (Q \wedge \neg Q)$ können wir schliessen P.
- **Beweis durch Fallunterscheidung:** aus $P \vee Q$, $P \Longrightarrow R$ und $Q \Longrightarrow R$ können wir schliessen R.
- **Beweis der Äquivalenz durch beidseitige Implikation:** aus $P \Longrightarrow Q$ und $Q \Longrightarrow P$ können wir schliessen $P \Longleftrightarrow Q$. □

Weiters können wir in der Aussagenlogik das Prinzip des **bedingten Beweises** anwenden: wenn wir aus der Annahme von P einen Beweis für Q erzeugen können, dann können wir schliessen $P \Longrightarrow Q$.

Prädikatenlogik

Mathematische Aussagen haben meist eine feinere Struktur als in der Aussagenlogik ausgedrückt werden kann. So ist etwa

"5 ist eine Primzahl"

eine Aussage, in welcher das **Prädikat** "ist eine Primzahl" auf das Subjekt "5" angewandt wird. Dasselbe Prädikat kann auf unendlich viele andere Subjekte (**Konstante**) angewandt werden. Steht P also für das Prädikat "ist eine Primzahl", so hat obige Aussage die Form

$$P(5) .$$

Ebenso könnten wir das Prädikat P auch auf eine mathematische Variable x anwenden, und etwa aussagen:

"nicht für alle x gilt $P(x)$."

Bezeichnung 1.4.7: Um solche Aussagen formal ausdrücken zu können, brauchen wir **Quantoren**. Meist findet man mit den folgenden zwei Quantoren das Auslangen:

- Der **Allquantor** $\forall$ drückt aus, dass eine Aussage "für alle" möglichen Werte einer Variablen gelten soll. So bedeutet also

  $$\forall x P(x) ,$$

  dass das Prädikat für alle möglichen x gilt. Der Wahrheitswert $T(\forall x P(x))$ ist also genau dann $\mathbf{t}$, wenn $T(P(x)) = \mathbf{t}$ für alle möglichen x.

- Der **Existenzquantor** $\exists$ drückt aus, dass eine Aussage für zumindest einen möglichen Wert gilt, also "es gibt" so ein x, bzw. "es existiert" so ein x. So bedeutet also

  $$\exists x P(x) ,$$

  dass es zumindest ein x gibt, für welches das Prädikat gilt. Der Wahrheitswert $T(\exists x P(x))$ ist also genau dann $\mathbf{t}$, wenn $T(P(x)) = \mathbf{t}$ für zumindest ein x. □

Definition 1.4.8: *Verbindet man Prädikate mit Quantoren und logischen Junktoren, so erhält man eine* **Formel**. *Die Variable x ist in der Formel $\forall x P(x)$* **gebunden**. *Ebenso ist x in der Formel $\exists x P(x)$ gebunden. Jede Variable, welche nicht durch einen Quantor gebunden wird, heisst* **frei**. □

Prädikate können natürlich nicht nur einstellig sein, wie $P(x)$, sondern auch mehrstellig, wie $Q(x_1, \ldots, x_n)$. So ist etwa die Aussage

"3 ist der grösste gemeinsame Teiler von 6 und 9"

mittels eines 3-stelligen Prädikates $GGT(3, 6, 9)$ ausdrückbar. Dass jedes Paar natürlicher Zahlen einen grössten gemeinsamen Teiler hat, schreiben wir dann als

$$\forall x \forall y \exists z \, GGT(z, x, y) .$$

Wollen wir eine Aussage nicht näher zerlegen, so verwenden wir dafür einfach ein 0-stelliges Prädikat P.

Häufig wollen wir den Bereich einer mathematischen Variablen auf eine Menge A, etwa $\mathbb{N}$ oder $\mathbb{R}$, einschränken. Das können wir natürlich ausdrücken als

$$\forall x(x \in A \Longrightarrow P(x)) \quad \text{bzw.} \quad \exists x(x \in A \wedge P(x)) \ ,$$

wir schreiben diesen Sachverhalt aber kürzer als

$$(\forall x \in A)P(x) \quad \text{bzw.} \quad (\exists x \in A)P(x)$$

oder

$$\forall x \in A : P(x) \quad \text{bzw.} \quad \exists x \in A : P(x) \ .$$

Wenn dieselbe Art von Quantor mehrmals hintereinander vorkommt, so fasst man das zusammen zu einem Quantor über mehrere Variablen; z.B. schreiben wir statt $\forall x \forall y P(x,y)$ auch $\forall x, y P(x,y)$.

Ebenso wie in der Aussagenlogik kann man auch in der Prädikatenlogik den Begriff der **logischen Konsequenz** einführen, und aufbauend darauf ergeben sich wiederum "Beweismethoden".

Bezeichnung 1.4.9: Beweismethoden der Prädikatenlogik:

- **Umwandlung von Quantoren:** die Formeln $\neg\forall x P(x)$ und $\exists x \neg P(x)$ sind äquivalent (also logische Konsequenzen von einander).
  Ebenso sind die Formeln $\neg\exists x P(x)$ und $\forall x \neg P(x)$ äquivalent.

- **Universelle Spezifikation:** aus $\forall x P(x)$ können wir schliessen $P(c)$, wobei c eine Konstante ist.

- **Universelle Generalisation:** wenn man ohne besondere Annahmen bzgl. x beweisen kann $P(x)$, dann können wir schliessen $\forall x P(x)$.

- **Existentielle Generalisation:** aus $P(c)$ für eine Konstante c können wir schliessen $\exists x P(x)$.

- **Vertauschung von Quantoren:** die Formeln $\forall x \forall y P(x,y)$ und $\forall y \forall x P(x,y)$ sind äquivalent. Ebenso sind die Formeln $\exists x \exists y P(x,y)$ und $\exists y \exists x P(x,y)$ äquivalent. □

Beispiel 1.4.10: Wir wollen an einigen Beispielen die Verwendung von Quantoren demonstrieren. Seien j, k, l, m, n Variablen über $\mathbb{Z}$.

- Die Aussage "n ist gerade" schreiben wir in der Prädikatenlogik als

  $$\exists m(n = 2m) \ .$$

  Die Aussage "n ist ungerade" schreiben wir in der Prädikatenlogik als

  $$\exists m(n = 2m + 1) \ .$$

- Die (wahre, aber durchaus nicht offensichtliche) Aussage, dass jede nichtnegative ganze Zahl ausgedrückt werden kann als die Summe von 4 Quadraten, schreiben wir als

  $$\forall n \geq 0 \, \exists j, k, l, m \ (n = j^2 + k^2 + l^2 + m^2) \ . \qquad \square$$

1.5 Algebraische Strukturen

Gruppen:

Definition 1.5.1: *Sei A eine nichtleere Menge. Eine* **binäre Operation** *oder* **Verknüpfung** $\circ$ *auf A ist eine Abbildung $\circ : A^2 \to A$, d.h. je zwei Elementen a, b von A wird ein Element $\circ(a, b)$ (auch geschrieben als $a \circ b$) zugeordnet.*
Das Paar $(A, \circ)$ heisst **algebraische Struktur** *oder* **Gruppoid**. *Statt $(A, \circ)$ schreiben wir oft nur A, wenn $\circ$ implizit klar ist.* □

Beispiel 1.5.2: Endliche Gruppoide können als Tabelle angegeben werden. Für $A = \{a_1, \ldots, a_n\}$ schreiben wir also

$\circ$	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$\cdots$	$a_1 \circ a_j$	$\cdots$	$a_1 \circ a_n$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_i	$a_i \circ a_1$	$\cdots$	$a_i \circ a_j$	$\cdots$	$a_i \circ a_n$
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	$a_n \circ a_1$	$\cdots$	$a_n \circ a_j$	$\cdots$	$a_n \circ a_n$

Ist etwa $+_3$ die Addition modulo 3, so beschreiben wir das Gruppoid $(\{0, 1, 2\}, +_3)$ als

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

Die Potenzmenge von $\{1, 2\}$ zusammen mit der Operation $\cap$ beschreiben wir als

$\cap$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\{1,2\}$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$

□

Definition 1.5.3: *Sei $\circ$ die Operation in einem Gruppoid $A = (A, \circ)$.*

(1) A (bzw. $\circ$) heisst **assoziativ**, *wenn gilt*

$$\forall a, b, c \in A: \ (a \circ b) \circ c = a \circ (b \circ c) \ .$$

(2) A besitzt ein **neutrales Element**, *wenn gilt*

$$\exists n \in A \forall a \in A: \ a \circ n = n \circ a = a \ .$$

(3) A besitze ein neutrales Element n. $a \in A$ besitzt ein **inverses Element** *bzw. a* **ist invertierbar**, *wenn gilt*

$$\exists a' \in A: \ a \circ a' = a' \circ a = n \ .$$

In diesem Fall ist a' das zu a inverse Element.

(4) A (bzw. $\circ$) heisst **kommutativ**, *wenn gilt*

$$\forall a, b \in A: \ a \circ b = b \circ a \ .$$

Schreibt man die Verknüpfung $\circ$ multiplikativ, also "$a \cdot b$", dann bezeichnet man das inverse Element von a auch durch a^{-1}, schreibt man die Verknüpfung $\circ$ additiv, also "$a + b$", dann bezeichnet man das inverse Element von a auch durch $-a$.

Definition 1.5.4: *Eine algebraische Struktur* $(A, \circ)$ *heisst*

- **Halbgruppe**, *wenn sie assoziativ ist,*
- **Monoid**, *wenn sie assoziativ ist und ein neutrales Element besitzt,*
- **Gruppe**, *wenn sie assoziativ ist, ein neutrales Element besitzt, und für jedes Element ein inverses Element besitzt.*

Ist ein Gruppoid, eine Halbgruppe, ein Monoid oder eine Gruppe auch kommutativ, so heisst eine solche Struktur auch **kommutative(s)** *Gruppoid, Halbgruppe, Monoid oder Gruppe. Eine kommutative Gruppe heisst auch* **abelsche** *Gruppe, nach dem Mathematiker Niels Henrik Abel (1802–1829).*

Satz 1.5.5: *In einer algebraischen Struktur* $(A, \circ)$ *gibt es höchstens ein neutrales Element.*
Ist $(A, \circ)$ *ein Monoid, so besitzt jedes* $a \in A$ *höchstens ein inverses Element.*
In einer Gruppe gilt für $a \neq 0$ *und beliebige* g, h*:* $a \circ g = a \circ h \Longrightarrow g = h$.

Es wird daher im folgenden nur mehr vom neutralen Element bzw. vom inversen Element gesprochen, sofern diese existieren.

Beispiel 1.5.6:

(1) $\mathbb{N}$ mit $a \circ b = a^b$ ist nur ein Gruppoid.

(2) $(\mathbb{N} \setminus \{0\}, +)$ ist eine Halbgruppe.

(3) $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ sind Monoide, aber keine Gruppen.

(4) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen.

(5) Sei M eine Menge. Dann bildet $(\mathcal{P}(M), \Delta)$, d.h. die Potenzmenge von M mit der symmetrischen Mengendifferenz, eine abelsche Gruppe. Das neutrale Element ist $\emptyset$ und jedes Element ist zu sich selbst invers.

(6) Sei $S(M)$ die Menge aller bijektiven Abbildungen $\sigma : M \to M$ auf einer nichtleeren Menge M. Ein Element von $S(M)$ heisst **Permutation** auf M. $S(M)$ zusammen mit der Hintereinanderausführung bildet die sogenannte **symmetrische Gruppe** oder **Permutationsgruppe** von M.

Satz 1.5.7: *Sei* $(G, \circ)$ *eine Gruppe. Dann gilt für alle* $g, h \in G$*:*

(1) $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$,

(2) $(g^{-1})^{-1} = g$.

Definition 1.5.8: *Eine nichtleere Teilmenge* $H \subseteq G$ *einer Gruppe* $(G, \circ)$ *heisst* **Untergruppe** *von* G*, wenn* $(H, \circ)$ *selbst eine Gruppe ist. Wir schreiben diesen Sachverhalt auch als* $(H, \circ) \leq (G, \circ)$ *oder einfach* $H \leq G$.

Satz 1.5.9: *Sei* $(G, \circ)$ *eine Gruppe und* H *eine nichtleere Teilmenge von* G*. Dann sind die folgenden drei Bedingungen äquivalent (FAÄ):*

(i) $H \leq G$,

(ii) $\forall a, b \in H: \; a \circ b \in H \;\wedge\; a^{-1} \in H$,

(iii) $\forall a, b \in H: \; a \circ b^{-1} \in H$.

Beispiel 1.5.10: So ist etwa $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$. □

Definition 1.5.10: *Sei $(G, \circ)$ eine Gruppe, H eine Untergruppe von G, und $a \in G$. Dann heisst*

$$a \circ H = \{a \circ b | b \in H\}$$

Linksnebenklasse *von G nach H (bzgl. a) und*

$$H \circ a = \{b \circ a | b \in H\}$$

Rechtsnebenklasse *von G nach H (bzgl. a).*

Satz 1.5.11: *Sei $(G, \circ)$ eine Gruppe und $H \leq G$. Dann gilt:*

(i) Für alle $a, b \in G$: $b \in a \circ H \iff b \circ H = a \circ H$.

(ii) Die Menge der Linksnebenklassen $\{a \circ H | a \in G\}$ bildet eine Partition von G. Die Relation $a \sim b \iff a \circ H = b \circ H$ ist die entsprechende Äquivalenzrelation. (Eine entsprechende Aussage gilt für die Rechtsnebenklassen $H \circ a$.)

(iii) Alle Links- und Rechtsnebenklassen sind gleich mächtig, d.h. für alle $a \in G$ gilt $|a \circ H| = |H \circ a| = |H|$.

Satz 1.5.12: *Ist $\{H_i | i \in I\}$ eine Familie von Untergruppen einer Gruppe G, so ist*

$$H := \bigcap_{i \in I} H_i$$

wieder eine Untergruppe von G.

Definition 1.5.13: *Sei G eine Gruppe und $K \subseteq G$ eine nichtleere Teilmenge von G. Die von K* **erzeugte Untergruppe** *$[K]$ ist der Durchschnitt aller Untergruppen $H \leq G$, die K enthalten. Also*

$$[K] := \bigcap \{H \leq G | K \subseteq H\} \; .$$

($[K]$ ist wegen Satz 1.5.12 eine Untergruppe von G.)

Definition 1.5.14: *Eine Gruppe $(G, \circ)$ heisst* **zyklisch**, *wenn es ein $a \in G$ gibt, sodass jedes $b \in G$ sich schreiben lässt als Potenz von a, also $b = a \circ \ldots \circ a$ (n mal, für $n \in \mathbb{N}$).*

Definition 1.5.15: *Für jedes $i \in I$ (Indexmenge) sei $(G_i, \circ_i)$ eine Gruppe. Dann wird das kartesische Produkt $\prod_{i \in I} G_i$ mit der Operation*

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} := (a_i \circ_i b_i)_{i \in I}$$

zu einer Gruppe, dem **direkten Produkt** *der Gruppen $G_i, i \in I$.*

Definition 1.5.16: *Eine Untergruppe H einer Gruppe G heisst* **Normalteiler**, *bezeichnet als $H \trianglelefteq G$, wenn die Links- und Rechtsnebenklassen übereinstimmen.*

Satz 1.5.17: *Für eine Untergruppe H einer Gruppe G sind folgende Aussagen äquivalent:*

(i) $H \trianglelefteq G$,

(ii) $\forall a \in G: \; a \circ H = H \circ a$,

(iii) $\forall a \in G: \; a \circ H \circ a^{-1} \subseteq H$.

Ausserdem folgt aus $a_1 \circ H = a_2 \circ H$ *und* $b_1 \circ H = b_2 \circ H$ *auch* $(a_1 \circ b_1) \circ H = (a_2 \circ b_2) \circ H$.

Somit wird die Operation $\circ$ von der Gruppe G auf die Menge der Nebenklassen eines Normalteilers vererbt.

Definition 1.5.18: *Sei H Normalteiler einer Gruppe G und bezeichne G/H die Menge der Nebenklassen von G nach H. Dann wird durch*

$$(a \circ H) \circ (b \circ H) := (a \circ b) \circ H$$

eine Gruppenoperation auf G/H definiert. Die Gruppe $(G/H, \circ)$ heisst **Faktorgruppe** *von G nach H.*

Beispiel 1.5.19: Sei $G = \mathbb{Z}$ mit der Addition $+$ als Gruppenoperation. Sei $m \in \mathbb{Z}$. Die Untergruppe

$$H = m\mathbb{Z} = \{m \cdot n | n \in \mathbb{Z}\}$$

ist ein Normalteiler von $\mathbb{Z}$. Die Nebenklassen sind

$$\overline{0} = 0 + m\mathbb{Z}, \overline{1} = 1 + m\mathbb{Z}, \ldots, \overline{m-1} = (m-1) + m\mathbb{Z},$$

die sogenannten **Restklassen modulo** m. Die Faktorgruppe bezeichnen wir als

$$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$$

In $\mathbb{Z}_5$ gilt beispielsweise $\overline{3} + \overline{4} = \overline{2}$. □

Abbildungen zwischen zwei Gruppen, welche die Gruppenstruktur respektieren, bilden ihrerseits wiederum eine Gruppe.

Definition 1.5.20: *Eine Abbildung $\varphi : G \to H$ zwischen zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ heisst* **(Gruppen-) Homomorphismus**, *wenn für alle $a, b \in G$ gilt:*

$$\varphi(a \circ b) = \varphi(a) \diamond \varphi(b).$$

Die Menge aller Gruppenhomomorphismen von G nach H wird mit $\mathrm{Hom}(G, H)$ bezeichnet.
Ein injektiver Homomorphismus heisst auch **Monomorphismus**, *ein surjektiver Homomorphismus heisst auch* **Epimorphismus**.
Ein bijektiver Homomorphismus heisst auch **Isomorphismus**. *Zu einem Isomorphismus φ gibt es auch die inverse Abbildung $\varphi^{-1} : H \to G$, die ihrerseits auch in Isomorphismus ist. Existiert zwischen zwei Gruppen G und H ein Isomorphismus, so heissen G und H* **isomorph** *und wir schreiben dafür $G \cong H$.*
Ein Homomorphismus $\varphi : G \to G$ von G in sich selbst heisst **Endomorphismus** *und ein Isomorphismus von G in sich selbst heisst* **Automorphismus**. *Die Menge aller Endomorphismen von G bezeichnen wir mit $\mathrm{End}(G)$, die Menge aller Automorphismen auf G bezeichnen wir mit $\mathrm{Aut}(G)$.*

Satz 1.5.21: *Seien G und H Gruppen, und φ ein Homomorphismus von G nach H. Dann wird das neutrale Element e_G von G auf das neutrale Element e_H von H abgebildet, also $\varphi(e_G) = e_H$. Weiters gilt für alle $a \in G$: $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Satz und Definition 1.5.22: *Für eine Gruppe G ist* $\mathrm{Aut}(G)$ *ebenfalls eine Gruppe, die sogenannte* **Automorphismengruppe** *von G.*

Definition 1.5.23: *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Das Urbild $\varphi^{-1}(e_H)$ des neutralen Elements e_H wird als* **Kern** *von φ bezeichnet, also*

$$\mathrm{kern}(\varphi) := \{a \in G | \varphi(a) = e_H\}.$$

Weiters nennt man

$$\mathrm{im}(\varphi) = \varphi(G) := \{b \in H | \exists a \in G : \varphi(a) = b\}$$

das **Bild** *von G unter φ.*

Satz 1.5.24: *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist* $\mathrm{kern}(\varphi)$ *ein Normalteiler von G und* $\mathrm{im}(\varphi)$ *eine Untergruppe von H.*

Satz 1.5.25: (Homomorphiesatz der Gruppentheorie) *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist die Faktorgruppe $G/\mathrm{kern}(\varphi)$ mit dem Bild $\mathrm{im}(\varphi)$ isomorph:*

$$G/\mathrm{kern}(\varphi) \cong \mathrm{im}(\varphi) \ .$$

Dabei entspricht die Nebenklasse $a \circ \mathrm{kern}(\varphi) \in G/\mathrm{kern}(\varphi)$ dem Element $\varphi(a) \in \mathrm{im}(\varphi)$.

Für jeden Normalteiler N von G ist die Abbildung

$$\begin{array}{rccc} \varphi_N : & G & \to & G/N \\ & a & \mapsto & a \circ N \end{array}$$

ein Gruppenhomomorphismus. Die Faktorgruppen geben daher (bis auf Isomorphie) einen Überblick über die möglichen homomorphen Bilder von G.

<u>Ringe:</u>

Zahlenbereiche wie etwa $\mathbb{Z}$ besitzen eine Gruppenstruktur bzgl. "+", darüber hinaus aber noch eine weitere Operation "·". Wir nennen eine solche Struktur "Ring". In Anlehnung an die Operationen in $\mathbb{Z}$ bezeichnen wir die Operationen in einem Ring gewöhnlich wiederum durch "+" und "·".

Definition 1.5.26: *Eine Menge R mit zwei binären Operationen $+$ und $\cdot$, also eine algebraische Struktur der Form $(R, +, \cdot)$, heisst ein* **Ring**, *wenn gilt:*

(i) $(R, +)$ *ist eine abelsche Gruppe,*

(ii) $(R, \cdot)$ *ist eine Halbgruppe, also $\cdot$ ist assoziativ,*

(iii) $\cdot$ *ist distributiv bzgl. $+$, d.h.*

$$\forall a, b, c \in R: \ a \cdot (b + c) = a \cdot b + a \cdot c \ \wedge \ (a + b) \cdot c = a \cdot c + b \cdot c \ .$$

Statt $a \cdot b$ schreiben wir oft einfach ab. Das neutrale Element der abelschen Gruppe $(R, +)$ in einem Ring R nennen wir meist 0. Mit R^* bezeichnen wir R ohne die 0.

Beispiel 1.5.27: Die folgenden Zahlenbereiche sind Ringe:

$$(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot),\ (\mathbb{C}, +, \cdot)\ .$$

Definiert man auf $\mathbb{Z}_n$ die Multiplikation $\cdot$ als

$$\overline{a} \cdot \overline{b} = (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b) + n\mathbb{Z} = \overline{a \cdot b}\ ,$$

so wird dadurch

$$(\mathbb{Z}_n, +, \cdot)$$

zu einem Ring.
Aber auch für jede Menge A ist die Potenzmenge von A mit den Operationen der symmetrischen Differenz und des Durchschnitts ein Ring, also

$$(\mathcal{P}(A), \Delta, \cap)\ .$$

Beispiel 1.5.28: Sei R ein Ring. Eine formale Summe

$$a(x) = \sum_{i=0}^{\infty} a_i x^i, \qquad a_i \in R,$$

heisst eine **(formale) Potenzreihe** über R. a_i heisst der **Koeffizient** der **Potenz** x^i. Wir bezeichnen die Menge der Potenzreihen über R durch $R[[x]]$. Definieren wir für zwei Potenzreihen $a(x) = \sum_{i=0}^{\infty} a_i x^i$ und $b(x) = \sum_{i=0}^{\infty} b_i x^i$ die Operationen $+$ und $\cdot$ als

$$a(x) + b(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i\ , \quad a(x) \cdot b(x) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j \cdot b_{i-j} \right) x^i\ ,$$

so ist $(R[[x]], +, \cdot)$ ein Ring, der **Ring der formalen Potenzreihen über** R. Die 0 in $R[[x]]$ ist offensichtliche die Potenzreihe, in welcher alle Koeffizienten 0 sind. □

Beispiel 1.5.29: Sind in der Potenzreihe $a(x) = \sum_{i=0}^{\infty} a_i x^i$ über R nur endlich viele Koeffizienten verschieden von 0, so heisst $a(x)$ ein **Polynom** über R. Die Menge der Polynome über R bezeichnen wir durch $R[x]$. Die Operationen $+$ und $\cdot$ (auf Potenzreihen) führen nicht aus $R[x]$ hinaus, $(R[x], +, \cdot)$ ist also ebenfalls ein Ring.
Ist $a(x) \neq 0$ (also verschieden vom Nullpolynom, in dem alle Koeffizienten 0 sind), so heisst das grösste i mit $a_i \neq 0$ der **Grad** von a, geschrieben als $\mathrm{grad}(a)$. □

Definition 1.5.30: *Falls in einem Ring $(R, +, \cdot)$ die Operation $\cdot$ ein neutrales Element besitzt, so heisst es* **Einselement** *und wird mit 1 bezeichnet. Ist $\cdot$ kommutativ, so heisst R ein* **kommutativer Ring**.

Satz 1.5.31: *In jedem Ring R gilt $a \cdot 0 = 0 \cdot a = 0$.*

Definition 1.5.32: *Sei R ein Ring. Ein Element $a \in R^*$ (also $a \neq 0$) heisst* **Nullteiler**, *wenn es ein $b \in R^*$ gibt, sodass $a \cdot b = 0$ oder $b \cdot a = 0$ (damit ist natürlich auch b ein Nullteiler).*

Beispiel 1.5.33: In $\mathbb{Z}_6$ haben wir $\overline{2} \cdot \overline{3} = \overline{0}$. $\overline{2}$ und $\overline{3}$ sind also Nullteiler.
In den Ringen $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ gibt es keine Nullteiler. □

Definition 1.5.34: *Ein kommutativer Ring mit Einselement ohne Nullteiler heisst* **Integritätsbereich**.

Beispiel 1.5.35: Die Ringe $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind also Integritätsbereiche.
$\mathbb{Z}_n$ ist genau dann ein Integritätsbereich, wenn n eine Primzahl ist. □

Satz 1.5.36: *Ist R ein Integritätsbereich, so sind auch der Polynomring $R[x]$ über R und der Ring der formalen Potenzreihen $R[[x]]$ über R wiederum Integritätsbereiche.*

Definition 1.5.37 *Ein Element a eines kommutativen Ringes mit Einselement 1 heisst* **Einheit**, *wenn es bzgl. der Multiplikation $\cdot$ ein inverses Element a^{-1} besitzt, also $a \cdot a^{-1} = 1$.*

Beispiel 1.5.38: Die Einheiten in $\mathbb{Z}$ sind 1 und -1.
Die Einheiten in $\mathbb{Q}$ sind $\mathbb{Q}^*$.
Die Einheiten in $\mathbb{Q}[x]$ sind die von 0 verschiedenen Konstanten, also $\mathbb{Q}^*$. □

Körper:

Definition 1.5.39: *Ein Ring $(R, +, \cdot)$ ist ein* **Körper**, *wenn $(R^*, \cdot)$ eine abelsche Gruppe ist.*

Jeder Körper hat also mindestens 2 Elemente, nämlich 0 und 1.

Beispiel 1.5.40: Die Identitätsbereiche $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.
$\mathbb{Z}_n$ ist genau dann eine Körper, wenn n eine Primzahl ist. □

Satz 1.5.41: *Jeder Körper ist ein Identitätsbereich.*

Satz und Definition 1.5.42: *Ist I ein Integritätsbereich, so ist*

$$Q(I) := (I \times I^*)_{/\sim}, \quad \text{für } (a, b) \sim (c, d) \Longleftrightarrow ad = bc$$

mit den Operationen

$$(a, b) + (c, d) := (ad + bc, bd), \quad (a, b) \cdot (c, d) := (ac, bd)$$

ein Körper, der sogenannte **Quotientenkörper** *von I.*

Die Elemente von $Q(I)$ schreiben wir gewöhnlich als a/b anstatt (a, b).

Beispiel 1.5.43: $\mathbb{Q}$ ist der Quotientenkörper von $\mathbb{Z}$. □