

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 population, 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 circumference 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

¹Communications 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 $0, 1, 2, 3, \dots$. 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

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

Weiters sind Addition und Multiplikation assoziativ, es gilt also

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

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

$$0 < S(0) = 1 < S(S(0)) = 2 < S(S(S(0))) = 3 < \dots$$

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, \dots, m_l gegeben. Mit $\sum_{i=0}^l m_i$ bezeichnen wir die Summe dieser Zahlen m_i . “ i ” heisst dabei der **Summationsindex**. Er durchläuft sukzessive die natürlichen Zahlen 0 bis l . Wird über einen leeren Laufbereich des Summationsindex summiert, also etwa von $i = 0$ bis $i = -1$, so ist der Wert der Summe 0, also das neutrale Element bzgl. der Addition.

$$\sum_{i=0}^l m_i = m_0 + \dots + m_l, \quad \sum_{i=0}^{-1} m_i = 0.$$

Ebenso bezeichnen wir mit $\prod_{i=0}^l m_i$ das Produkt dieser Zahlen m_i . “ i ” heisst in diesem Fall der **Multiplikationsindex**. Wird über einen leeren Laufbereich des Multiplikationsindex multipliziert, also etwa von $i = 0$ bis $i = -1$, so ist der Wert des Produkts 1, also das neutrale Element bzgl. der Multiplikation.

$$\prod_{i=0}^l m_i = m_0 \cdot \dots \cdot m_l, \quad \prod_{i=0}^{-1} m_i = 1.$$

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 Schlussregel:

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

Das heisst, wenn wir zeigen können, dass

- P für 0 gilt, und

• sich für jedes n die Eigenschaft P von n auf den Nachfolger $n + 1$ überträgt, dann können wir daraus schliessen, dass P für alle n gilt. Um also nachzuweisen, dass die Eigenschaft P für alle natürlichen Zahlen n gilt, weist man zunächst in der “Induktionsbasis” $P(0)$ nach. Sodann nimmt man in der “Induktionshypothese” an, dass $P(\bar{n})$ gilt für ein beliebig aber fix gewähltes \bar{n} ; und damit zeigt man dann, dass unter diesen Voraussetzungen auch $P(\bar{n} + 1)$ gilt. Gelingt das alles, so ist die Eigenschaft P für alle $n \in \mathbb{N}$ bewiesen.

Das Prinzip der vollständigen Induktion kann auch äquivalent wie folgt formuliert werden:

$$\forall n : ((\forall k < n : P(k)) \implies P(n)) \implies \forall n : P(n)$$

Das heisst, wenn wir zeigen können, dass sich für alle n die Eigenschaft P von allen Vorgängern von n auf n selbst überträgt, dann können wir daraus schliessen, dass P für alle n gilt.

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 $\forall n \geq N : P(n) \implies P(n + 1)$.

Beispiel 1.2.4: (a) Wir zeigen durch Induktion

$$\forall n : 0 + n = n$$

Induktionsbasis: offensichtlich gilt per definitionem die Behauptung für $n = 0$: $0 + 0 = 0$

Induktionshypothese: wir nehmen an, für ein beliebiges aber fix gewähltes \bar{n} gelte

$$0 + \bar{n} = \bar{n}$$

Induktionsschritt: wegen der Definition von “+” und der Induktionshypothese gilt

$$0 + (\bar{n} + 1) = (0 + \bar{n}) + 1 = \bar{n} + 1 .$$

Somit ist die Behauptung bewiesen.

(b) Als nächstes zeigen wir

$$\forall n, m : (n + m) + 1 = (n + 1) + m$$

Wir führen den Beweis durch Induktion über m .

Induktionsbasis: laut Definition von “+” gilt

$$(n + 0) + 1 = n + 1 = (n + 1) + 0 .$$

Induktionshypothese: wir nehmen an, für ein beliebiges aber fix gewähltes \bar{m} gelte

$$(n + \bar{m}) + 1 = (n + 1) + \bar{m} .$$

Induktionsschritt: wegen der Definition von “+”, der Induktionshypothese, und nochmals der Definition von “+” gilt dann

$$(n + (\bar{m} + 1)) + 1 = ((n + \bar{m}) + 1) + 1 = ((n + 1) + \bar{m}) + 1 = (n + 1) + (\bar{m} + 1) .$$

Somit ist die Behauptung bewiesen.

(c) Als nächstes weisen wir die Kommutativität der Addition nach, also

$$\forall m, n : m + n = n + m .$$

Wir führen den Beweis durch Induktion über n .

Induktionsbasis: wegen der Definition von “+” und wegen (a) gilt

$$m + 0 = m = 0 + m .$$

Induktionshypothese: wir nehmen an, für ein beliebiges aber fix gewähltes \bar{n} gelte

$$\forall m : m + \bar{n} = \bar{n} + m$$

Induktionsschritt: daraus schliessen wir

$$m + (\bar{n} + 1) \stackrel{\text{Def } +}{=} (m + \bar{n}) + 1 \stackrel{\text{IH}}{=} (\bar{n} + m) + 1 \stackrel{\text{(b)}}{=} (\bar{n} + 1) + m .$$

Somit ist die Behauptung bewiesen.

(d) Wir nehmen nun an, wir hätten schon alle üblichen arithmetischen Gesetzmässigkeiten für \mathbb{N} gezeigt.

Wir wollen nun zeigen, dass für alle natürlichen Zahlen n gilt

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

$P(n)$ 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 \bar{n} , also

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

Induktionsschritt: wenn es uns nun gelingt, unter diesen Voraussetzungen zu zeigen, dass P auch für $\bar{n} + 1$ 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:

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

Somit ist die Behauptung bewiesen. □

Beispiel: Etwas scherzhaft könnte man auch formulieren:

“Es gibt keine uninteressante natürliche Zahl.”

Wir “beweisen” diese Aussage durch Induktion.

$n = 0$: offensichtlich ist 0 eine höchst interessante Zahl, nämlich die kleinste.

Induktionshypothese: “für alle n kleiner oder gleich einer beliebig aber fix gewählten Zahl \bar{n} gilt: n ist eine interessante Zahl”

$\bar{n} \rightarrow \bar{n} + 1$: wir betrachten also $\bar{n} + 1$. $\bar{n} + 1$ kann nicht uninteressant sein, sonst wäre

es nämlich die kleinste uninteressante Zahl, was wiederum höchst interessant wäre. Also ist auch $\bar{n} + 1$ 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

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

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 \bar{n} . Macht man das nämlich nicht, so werden die zu zeigende Eigenschaft (*) und die Induktionshypothese (***) identisch; man nimmt also dann bereits die Gültigkeit 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, vgl. dazu Kapitel 1.3 — 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**. Die Ordnung \leq kann auf die üblich Weise von \mathbb{N} auf \mathbb{Z} erweitert werden. In \mathbb{Z} haben wir auch die Betragsfunktion $|n| = \max\{n, -n\}$.

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 $m|n$.

$m \in \mathbb{Z}$ heisst **reduzibel**, wenn es $p, q \neq \pm 1$ gibt, sodass $m = p \cdot q$. Ist das nicht der Fall, so heisst m **irreduzibel**. □

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

²Seite 37 im Vorwort von C.P.Snow zum Buch G.H.Hardy, “A Mathematician’s Apology”, Cambridge Univ. Press, Cambridge, 1992

(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 $g = \text{ggT}(m, n)$. Falls $\text{ggT}(m, n) = 1$, 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 $q = \text{quot}(m, n)$, $r = \text{rest}(m, n)$.

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

Beweis: Wenn k sowohl m als auch n teilt, so sieht man aus Satz 1.2.6, dass k auch $\text{rest}(m, n) = m - qn$ und n teilt, und umgekehrt. Damit sind die Teiler dieser Zahlenpaare gleich, und somit auch der grösste gemeinsame Teiler. \square

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 Euklidischen Divisionsalgorithmus (Euklid, ~ 300 v.Chr.).

Euklidischer 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:

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

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

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

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

In Schritt (3) gilt offensichtlich $r_i = 0$, 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 Euklidische 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 $11 = \text{ggT}(3641, 2827)$. □

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 natürliche Zahl p ist eine **Primzahl** bzw. ist **prim**, wenn sie folgende Eigenschaften besitzt:

- $p \geq 2$,
- wenn $p|m \cdot n$, dann $p|m$ oder $p|n$.

Satz 1.2.12: Für von 0 verschiedene natürliche Zahlen a, b, c gilt:

- (i) Aus $a|bc$ und $\text{ggT}(a, b) = 1$ folgt $a|c$.
- (ii) Sei p eine Primzahl. Aus $a|p$ folgt $a = 1$ oder $a = p$.

Beweis: (i) Offensichtlich gibt es $s, t \in \mathbb{Z}$, sodass $1 = sa + tb$. Also $c = sac + tbc$ und somit $a|c$.

(ii) Sei $p = a \cdot b$ für ein b . Also $p|ab$. Wegen Satz 1.2.6(v) gilt $a, b \leq p$.

Somit muss entweder $p|a$ gelten, also $p = a, b = 1$, oder $p|b$, also $p = b, a = 1$. □

Satz 1.2.13: Sei $p \in \mathbb{N}$. Dann gilt: p ist Primzahl $\iff p$ ist irreduzibel.

Beweis: “ \implies ”: Sei p prim, und sei $p = ab$ für $a, b \in \mathbb{N}$. Dann $p|a$ oder $p|b$. O.B.d.A. gelte $p|a$. Dann gilt $p = pqb$ für ein $q \in \mathbb{N}$. Somit haben wir $qb = 1$, also $q = 1$ und $b = 1$. p ist also irreduzibel.

“ \impliedby ”: Sei p irreduzibel. Seien $a, b \in \mathbb{N}$ so, dass $p|ab$.

Angenommen $p \nmid a$. Dann ist $\text{ggT}(p, a) = 1$. Wegen Satz 1.2.12(i) ist daher p ein Teiler von b .

p ist also eine Primzahl. □

Satz 1.2.14: Es gibt unendlich viele Primzahlen.

Beweis: ang. es gibt nur endlich viele Primzahlen p_1, \dots, p_n . Sei $p := (\prod_{i=1}^n p_i) + 1$. Dann gibt es ein p_i , sodass

$$p_i|p \quad \text{und} \quad p_i|(p - 1).$$

Somit ist $p_i = 1$ (wegen Satz 1.2.6(i)), im Widerspruch dazu, dass p_i eine Primzahl ist. □

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

Satz 1.2.15: Für jede natürliche Zahl $n \geq 2$ gibt es verschiedene Primzahlen p_1, \dots, p_m und zugehörige Potenzen e_1, \dots, e_m , sodass

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

Diese Darstellung ist eindeutig bis auf Umreihung der Primzahlen.

Beweis: Sei $E(n)$ die Eigenschaft “ n ist Produkt von Primzahlen”. Wir beweisen E durch Induktion für $n \geq 2$. Offensichtlich gilt $E(2)$. In der Induktionshypothese nehmen wir an, dass E gilt für alle $n \leq \bar{n}$, also bis zur beliebig aber fix gewählten Konstanten \bar{n} . Dann ist $\bar{n} + 1$ entweder prim, oder $\bar{n} + 1 = mk$ für $m, k \leq \bar{n}$. In jedem Fall gilt E für $\bar{n} + 1$. Zum Beweis der Eindeutigkeit der Darstellung nimmt man an, dass die Primzahl p die Zahl n teilt, es aber eine Primzahldarstellung $p_1 \cdots p_l$ von n gäbe, in der p nicht vorkommt. Das ist aber sofort ein Widerspruch zur Tatsache, dass p einen der Faktoren p_i teilen muss (Satz 1.2.12(ii)). \square

Beispiel 1.2.16: In \mathbb{N} stimmen also die Begriffe “prim” und “irreduzibel” überein. Das ist aber nicht in jedem Zahlbereich so. Als Teilring der komplexen Zahlen \mathbb{C} betrachten wir $\mathbb{Z}[\sqrt{-5}]$, also Zahlen von der Form $a + b\sqrt{-5}$, wobei $a, b \in \mathbb{Z}$ (für den Zahlbereich \mathbb{C} und den Begriff eines “Ringes” sei auf spätere Kapitel verwiesen). In $\mathbb{Z}[\sqrt{-5}]$ können wir addieren und multiplizieren, etwa

$$(1 + \sqrt{-5}) + (2 - 3\sqrt{-5}) = 3 - 2\sqrt{-5}, \quad (1 + \sqrt{-5}) \cdot (2 - 3\sqrt{-5}) = 17 - \sqrt{-5}.$$

Zahlen $\alpha = a + b\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ haben eine Norm $N(\alpha) = a^2 + 5b^2$. Die Norm von α ist immer eine natürliche Zahl. Weiters ist die Norm multiplikativ, d.h. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$. Nur ± 1 haben die Norm 1. Nun lässt sich 9 auf prinzipiell verschiedene Arten zerlegen

$$3 \cdot 3 = 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}).$$

Alle diese Faktoren sind irreduzibel, da es keine Elemente von $\mathbb{Z}[\sqrt{-5}]$ mit Norm 3 gibt. Aber weder 3 noch $2 \pm \sqrt{-5}$ sind prim. \square

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 $x, y, z \neq 0$ 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.

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

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

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

Satz 1.2.17: *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.)*

Beweis: Ang. $(a/b)^2 = 2$. Dabei seien a, b teilerfremd. Dann folgt daraus

$$2b^2 = a^2 \implies 2|a^2 \implies 2|a \implies 2|b^2 \implies 2|b$$

im Widerspruch dazu, dass a, b teilerfremd sind. □

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

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

denn: seien $q = \frac{z}{n} < q' = \frac{z'}{n'}$, n positiv. Also $zn' < z'n$.

Falls $z < 0 < z'$, dann ist 0 dazwischen.

Sonst o.B.d.A. $0 < z, z'$. Also gibt $2zn' < zn' + z'n < 2z'n$, und somit

$$\frac{z}{n} < \frac{zn' + z'n}{2nn'} < \frac{z'}{n'}.$$

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

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

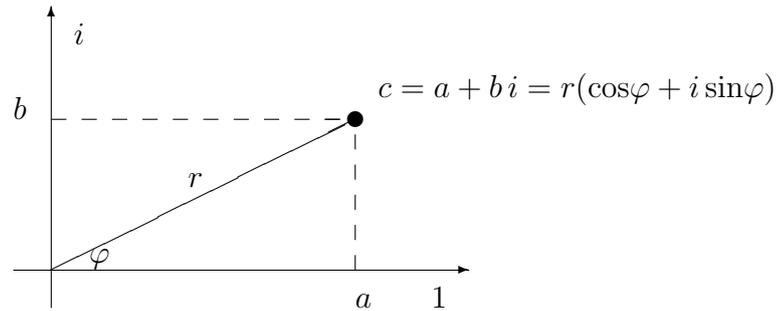


Figure 1: Gauß'sche Zahlenebene

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 Begriffe 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 $1,0000\dots = 1 = 0,9999\dots$. 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 $i = \sqrt{-1}$ (**imaginäre Einheit**) 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**.

Komplexe Zahlen lassen sich 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 , $a = \text{re}(c)$, und b heisst der **Imaginärteil** von c , $b = \text{im}(c)$. 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

$$c^{-1} = \frac{1}{a + bi} = \frac{(a - bi)}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i = \frac{a}{|c|^2} - \frac{b}{|c|^2}i.$$

Spiegelt man c in der Gauß'schen Zahlenebene um die reelle Achse, so erhält man die **komplex konjugierte** Zahl $\bar{c} = a - bi$.

In der Gauß'schen Zahlenebene kann c auch dargestellt werden als $c = r \cdot (\cos \varphi + i \cdot \sin \varphi)$.

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 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 1.3.1: *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 1.3.2: 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** $P \implies Q$, “wenn P dann Q ”; $T(P \implies Q) = \mathbf{f}$ 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** $P \iff Q$, “ P ist äquivalent zu Q ”; $T(P \iff Q) = \mathbf{t}$ 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 Klammersetzung zu minimieren, legen wir folgende Priorität von Junktoren fest, von der höchsten zur niedrigsten:

$$\neg, \wedge, \vee, \implies, \iff .$$

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

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 $P \implies Q$ 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 1.3.3: Wir stellen die Wahrheitstabelle für die Aussage

$$(P \implies Q) \iff (R \wedge P)$$

auf.

P	Q	R	$P \implies Q$	$R \wedge P$	$(P \implies Q) \iff (R \wedge P)$
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 1.3.4: Sei P eine Aussage, welche ausser Grundaussagen nur die Variablen P_1, \dots, 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, \dots, 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 $P \iff Q$ eine Tautologie ist.

Eine Aussage Q ist eine (**aussagenlogische**) **Konsequenz** der Aussagen P_1, \dots, P_n , wenn $(P_1 \wedge \dots \wedge P_n) \implies Q$ eine Tautologie ist. \square

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

Beweismethoden 1.3.5: (i) Die Aussage

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

ist eine Tautologie. Eine Implikation $P \implies Q$ ist also immer äquivalent zu $\neg Q \implies \neg P$. Anstatt die eine Implikation zu beweisen, reicht es immer aus, die andere zu beweisen.

(ii) Die **De Morgan’schen Gesetze** beruhen auf den folgenden Tautologien:

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

Hat man also die Negation einer Disjunktion zu zeigen, so reicht es aus, in zwei (unabhängigen) Beweisschritten die Negation der einzelnen Teilaussagen zu zeigen. \square

In ähnlicher Weise gehen alle Beweismethoden der Aussagenlogik auf Tautologien zurück. Einige davon sind von besonderer Wichtigkeit und wurden deshalb mit Namen belegt.

Beweismethoden 1.3.6: Wir führen einige der wichtigsten Beweismethoden der Aussagenlogik an:

- **Modus Ponens:** aus P und $P \implies Q$ können wir schliessen Q .
Die zugehörige Tautologie ist $[P \wedge (P \implies Q)] \implies Q$.
- **Modus Tollens:** aus $\neg Q$ und $P \implies Q$ können wir schliessen $\neg P$.

- **Indirekter Beweis, Widerspruchsbeweis, “reductio ad absurdum”:** aus $(\neg P) \implies (Q \wedge \neg Q)$ können wir schliessen P .
Die zugehörige Tautologie ist $[(\neg P) \implies (Q \wedge \neg Q)] \implies P$.
- **Beweis durch Fallunterscheidung:** aus $P \vee Q$, $P \implies R$ und $Q \implies R$ können wir schliessen R .
- **Beweis der Äquivalenz durch beidseitige Implikation:** aus $P \implies Q$ und $Q \implies P$ können wir schliessen $P \iff Q$. \square

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 $P \implies Q$.

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 1.3.7: 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 **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 **t**, wenn $T(P(x)) = \mathbf{t}$ für zumindest ein x . \square

Definition 1.3.8: Verbindet man Prädikate mit Quantoren und logischen Junktoren, so erhält man eine **prädikatenlogische Aussage** oder **Formel**. Die Variable x ist in der Formel $\forall xP(x)$ **gebunden**. Ebenso ist x in der Formel $\exists xP(x)$ gebunden. Jede Variable, welche nicht durch einen Quantor gebunden wird, heisst **frei**. \square

Aussagen, in denen alle Variablen gebunden sind, haben einen Wahrheitswert.

Prädikate können natürlich nicht nur einstellig sein, wie $P(x)$, sondern auch mehrstellig, wie $Q(x_1, \dots, x_n)$. 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

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

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** bzw. **Äquivalenz** einführen. Eine Formel Q ist eine logische Konsequenz von P genau dann, wenn in jedem Modell (möglicher Welt), in dem P gilt, auch Q gelten muss. Ist Q logische Konsequenz von P und P logische Konsequenz von Q , so heissen P und Q logisch äquivalent. Logische Konsequenzen bzw. Äquivalenzen führen, ebenso wie Tautologien in der Aussagenlogik, zu Beweismethoden.

Beweismethoden 1.3.9: Wir führen einige der wichtigsten Beweismethoden der Prädikatenlogik an:

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

Beispiel 1.3.10: 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

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

1.4 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 1.4.1: (naive Mengendefinition von Cantor) *Eine Menge ist eine Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.*

Definition 1.4.2: *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 1.4.3: *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 “charakteristische Eigenschaft” an, also mittels einer bestimmenden Eigenschaft P für die Elemente x der Menge A , etwa

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

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

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

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

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

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 $a, b \in \mathbb{R}$:

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

Operationen mit Mengen

Definition 1.4.4: Seien A, B, U Mengen, mit $A \subseteq U$.

Die **Vereinigung** von A und B ($A \cup B$) enthält genau jene Elemente, welche in A oder B enthalten sind, also

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

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

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

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

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

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

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

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

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

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

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

Definition 1.4.5: 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

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

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

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

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

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

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

$$\bigcap \{A \mid P(A)\} := \{x \mid \forall A : P(A) \implies x \in A\}.$$

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

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

In analoger Weise auch für \bigcap .

Satz 1.4.6: Es gelten folgende Beziehungen für Mengen A, B :

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

Satz 1.4.7: Es gelten folgende Beziehungen für Mengen A, B, C und Familien $(A_i)_{i \in I}$:

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

Satz 1.4.8: Es gelten folgende Beziehungen für Mengen A, B und Familien $(A_i)_{i \in I}$ in einer Universalmenge U :

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

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 1.4.9: 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, \dots, 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 1.4.10: Sei A eine Menge. Die **Potenzmenge** $\mathcal{P}(A)$ von A ist die Menge aller Teilmengen von A , also

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

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

Beispiel 1.4.11: $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$.

Satz 1.4.12: Sei $n \in \mathbb{N}$. Die Potenzmenge $\mathcal{P}(\{1, \dots, n\})$ hat genau 2^n Elemente.

Beweis: Durch Induktion über n .

$n = 0$: offensichtlich gilt $\mathcal{P}(\emptyset) = \{\emptyset\}$, hat also $2^0 = 1$ Elemente.

$n \rightarrow n + 1$:

$$\mathcal{P}(\{1, \dots, n, n + 1\}) = \mathcal{P}(\{1, \dots, n\}) \cup \{A \mid \exists B \in \mathcal{P}(\{1, \dots, n\}) : A = B \cup \{n + 1\}\}.$$

Also wenn $\mathcal{P}(\{1, \dots, n\})$ 2^n Elemente enthält, dann enthält $\mathcal{P}(\{1, \dots, n + 1\})$ 2^{n+1} Elemente. □

Relationen

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 1.4.13: 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**

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

eine Relation zwischen B und A .

Man kann natürlich auch Relationen zwischen mehreren Mengen A_1, A_2, \dots, 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 1.4.14: 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 1.4.15: Sei R eine Relation auf der Menge A .

- R heisst **reflexiv** wenn gilt: $\forall a \in A : aRa$.
- R heisst **symmetrisch** wenn gilt: $\forall a, b \in A : aRb \implies bRa$.
- R heisst **antisymmetrisch** wenn gilt: $\forall a, b \in A : (aRb \wedge bRa) \implies a = b$.
- R heisst **transitiv** wenn gilt: $\forall a, b, c \in A : (aRb \wedge bRc) \implies aRc$.

Beispiel 1.4.16:

(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 1.4.17: 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 1.4.18: 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: $a = b \text{ mod } n$.

Äquivalenzrelationen

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

Definition 1.4.19: 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 1.4.20: Sei \sim eine Äquivalenzrelation auf A . Für $a \in A$ heisst die Menge

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

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

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

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

- (i) $K_{\sim}(a) = K_{\sim}(b) \iff a \sim b$,
- (ii) $a \not\sim b \iff K_{\sim}(a) \cap K_{\sim}(b) = \emptyset$,
- (iii) $\bigcup_{a \in A} K_{\sim}(a) = A$.

Satz 1.4.22:

- (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

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

eine Äquivalenzrelation auf A .

Definition 1.4.23: Seien \sim und \approx zwei Äquivalenzrelationen auf A . Dann heisst \sim **feiner** als \approx , und \approx **größer** als \sim , wenn gilt: $\forall a, b \in A : a \sim b \implies a \approx b$.

Beispiel 1.4.24: Auf \mathbb{Z} betrachten wir die beiden Äquivalenzrelationen

$$a \sim_5 b \iff a = b \pmod{5} \quad \text{und} \quad a \sim_{10} b \iff a = b \pmod{10} .$$

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

Ordnungsrelationen

Nun wollen wir uns den Ordnungsrelationen auf einer Menge A zuwenden. Ordnungsrelationen werden typischerweise mit \leq oder ähnlichen Zeichen geschrieben. 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 1.4.25: 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 1.4.26: Die Teilbarkeitsrelation $|$ ist eine Ordnungsrelation auf \mathbb{N} , aber keine lineare Ordnungsrelation.

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

Satz 1.4.27: Sei M eine Menge, und $L = \mathcal{P}(M)$ ihre Potenzmenge. Dann ist die Relation

$$A \leq B : \iff A \subseteq B$$

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 1.4.28: Sei $\langle A, \leq \rangle$ 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: $b \leq a \implies b = a$.
- (iv) $a \in A$ heisst **maximales Element** von A g.d.w. für alle $b \in A$ gilt: $a \leq b \implies b = a$.
- (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 1.4.29: 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 $\sup_{\mathbb{R}} B = 1 \in B$. \square

Satz 1.4.30: 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 .

Beweis: (i) Seien a, a' kleinste Elemente von (A, \leq) . Dann gilt $a \leq a'$ und $a' \leq a$, also wegen der Antisymmetrie $a = a'$.

(ii) Sei a kleinstes Element von (A, \leq) , also

$$\forall b \in A : a \leq b . \quad (*)$$

Für beliebiges $b \in A$ gilt also

$$b \leq a \implies a = b$$

wegen der Antisymmetrie. Somit ist a minimal.

Sei auch a' minimal. Dann haben wir $a \leq a'$ (wegen $(*)$) und somit wegen der Minimalität von a' : $a = a'$. □

Funktionen

Nun wollen wir einen Grundbegriff der Mathematik einführen, den der Funktion oder Abbildung. Wir haben bereits etliche Beispiele dafür kennenbelehrt. Die Addition “+” bildet ein Paar von Zahlen ab auf ihre Summe, der Euklidische Algorithmus bildet ein Paar natürlicher Zahlen ab auf ihren ggT.

Definition 1.4.35: 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

$$\begin{aligned} f : A &\rightarrow B \\ a &\mapsto f(a) . \end{aligned}$$

A heisst der **Definitionsbereich** und B der **Bildbereich** von f . $f(a)$ heisst der **Funktionswert** von a unter f .

Ist $A' \subseteq A$, so heisst $f(A') = \{f(a) | a \in A'\}$ das **Bild** von A' unter f .

Ist $B' \subseteq B$, 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

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z} & g : \mathbb{Z} &\rightarrow \mathbb{N} \\ n &\mapsto n^2 & n &\mapsto n^2 \end{aligned}$$

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

Beispiel 1.4.36:

- (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

$$\chi_M : A \rightarrow \{0, 1\}$$

$$x \mapsto \begin{cases} 1 & \text{falls } x \in M \\ 0 & \text{sonst} \end{cases}$$

die charakteristische Funktion von M in A .

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

Definition 1.4.37: Sei $f : A \rightarrow B$ eine Funktion.

f heisst **injektiv**, wenn es zu jedem $b \in B$ höchstens ein $a \in A$ gibt mit $b = f(a)$, also $\forall a_1, a_2 \in A : (f(a_1) = f(a_2) \implies a_1 = a_2)$.

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. \square

Definition 1.4.38: Sind $f : A \rightarrow B$ und $g : B \rightarrow C$ Funktionen, so wird die **Hintereinanderausführung** oder **Zusammensetzung** $g \circ f : A \rightarrow C$ definiert durch $(g \circ f)(a) = g(f(a))$. $g \circ f$ ist eine Funktion von A nach C . \square

Definition 1.4.39: Eine Funktion $g : B \rightarrow A$ heisst eine zu $f : A \rightarrow B$ **inverse Funktion**, wenn gilt $g \circ f = \text{id}_A$ und $f \circ g = \text{id}_B$. Wenn es zu f eine inverse Funktion gibt, so ist diese eindeutig bestimmt (siehe Satz 1.4.40) und wir schreiben sie als f^{-1} . \square

Satz 1.4.40: Seien $f : A \rightarrow B$, $g : B \rightarrow C$ und $h : C \rightarrow D$ Funktionen.

- (i) Es gilt $h \circ (g \circ f) = (h \circ g) \circ f$ (Assoziativität)
- (ii) Sind die Funktionen f und 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 1.4.41: Sei $f : A \rightarrow B$ eine Funktion.

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

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

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

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

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 1.4.42: Zwei Mengen A, B heissen **gleichmächtig**, falls es eine bijektive Abbildung $f : A \rightarrow B$ gibt. \square

Satz 1.4.43: Sei U eine gegebene (Grund-)Menge von Mengen (etwa alle Teilmengen einer Menge A). Die Relation der Gleichmächtigkeit ist auf U eine Äquivalenzrelation.

Definition 1.4.44: Sei U eine Grundmenge. Die Äquivalenzklasse von $A \subseteq U$ bzgl. der Relation der Gleichmächtigkeit heisst die **Kardinalzahl** $|A|$ von A , also

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

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 1.4.45: Für $n \in \mathbb{N}$ gilt: $|\{1, \dots, n\}| = |\{1, \dots, m\}| \iff n = m$.

Beweis: “ \Leftarrow ”: trivial

“ \Rightarrow ”: wir zeigen “ $n \neq m \implies |\{1, \dots, n\}| \neq |\{1, \dots, m\}|$ ”.

o.B.d.A. sei $n > m$. Für jede Funktion $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ gibt es $k, l \in \{1, \dots, n\}$, $k \neq l$, sodass $f(k) = f(l)$. Es gibt also keine Bijektion, die Mengen sind also nicht gleichmächtig. \square

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 1.4.46: Seien A, B zwei Mengen.

Gibt es eine injektive Abbildung $f : A \rightarrow B$, so bezeichnet man das durch $|A| \leq |B|$.

Gibt es eine surjektive Abbildung $f : A \rightarrow B$, so bezeichnet man das durch $|A| \geq |B|$.

Eigentlich setzt diese Definition einen Satz voraus:

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

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

Satz 1.4.47: Seien A, B zwei Mengen. Dann gilt:

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

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

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

Beweis: (i) id_A ist injektiv.

(ii) Reflexivität ist klar. Die Antisymmetrie folgt aus CSB (Satz 1.4.57) Die Hintereinanderausführung injektiver Funktionen ist injektiv, daraus folgt die Transitivität.

(iii) Sei $f : A \rightarrow B$ injektiv. Sei $g : B \rightarrow A$ definiert als $g(b) = a$ für $b = f(a)$, und $g(b)$ beliebig sonst. Dann ist g surjektiv.

Sei andererseits $g : B \rightarrow A$ surjektiv. Sei $f : A \rightarrow B$ definiert als $f(a) = b$ für ein $b \in g^{-1}(\{a\})$. Dann ist f injektiv. \square

Definition 1.4.48: Eine Menge A heisst **endlich**, wenn ihre Kardinalzahl eine natürliche Zahl ist. Ansonsten heisst A **unendlich**.

Satz 1.4.49: Eine Menge A ist unendlich g.d.w. es eine echte Teilmenge B von A gibt mit $|B| = |A|$.

Beweis: “ \Leftarrow ”: mit Satz 1.4.45.

“ \Rightarrow ”: Sei $|A| \neq |\{1, \dots, n\}|$ für $n \in \mathbb{N}$.

Wir wählen $a_0, a_1, a_2, \dots \in A$ verschieden. Sei $B := A \setminus \{a_0\}$. Dann ist

$$\begin{aligned} f : A &\longrightarrow B \\ a &\mapsto a \text{ für } a \neq a_i \\ a_i &\mapsto a_{i+1} \end{aligned}$$

bijektiv. \square

Satz 1.4.50: Für jede unendliche Menge A gilt: $|\mathbb{N}| \leq |A|$.

Beweis: wähle $a_0, a_1, \dots \in A$ verschieden. Dann ist $|\mathbb{N}| = |\{a_0, a_1, \dots\}| \leq |A|$. \square

$|\mathbb{N}|$ 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).

Definition 1.4.51: Eine unendliche Menge A heisst **abzählbar** bzw. **abzählbar unendlich** wenn $|A| = \aleph_0$. Ansonsten heisst A **überabzählbar**.

Satz 1.4.52: Die Zahlenmengen \mathbb{Z} und \mathbb{Q} sind abzählbar.

Satz 1.4.53: Die Zahlenmenge \mathbb{R} ist überabzählbar.

Beweis: Wir zeigen, dass es keine surjektive Abbildung $f : \mathbb{N} \rightarrow [0, 1] (\subset \mathbb{R})$ gibt.

Jedes $x \in [0, 1]$ lässt sich schreiben als Dezimalzahl der Form $0, x_1 x_2 \dots$ (vergleiche Kapitel 1.2). Weiters vereinbaren wir, dass wir eine Zahl $0, \dots 1000 \dots = 0, \dots 0999 \dots$ immer in der zweiten Form schreiben.

Sei f eine beliebig aber fix gewählte Abbildung von \mathbb{N} nach $[0, 1]$. Für jedes $n \in \mathbb{N}$ sei a_n die n -te Dezimalstelle nach dem Komma von $f(n)$. Sei

$$b_n := \begin{cases} a_n + 1 & \text{falls } a_n < 9 \\ 0 & \text{falls } a_n = 9 \end{cases} .$$

Dann wird die reelle Zahl $0, b_1 b_2 \dots$ von der Funktion f nicht getroffen. \square

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

Satz 1.4.55 (Satz von Cantor): Für jede Menge A ist $|A| < |\mathcal{P}(A)|$.

Beweis: Offensichtlich gilt $|\emptyset| = 0 < 1 = |\{\emptyset\}| = |\mathcal{P}(\emptyset)|$.

Sei also nun $A \neq \emptyset$. Angenommen $f : A \rightarrow \mathcal{P}(A)$ wäre surjektiv.

Sei $B := \{a \in A \mid a \notin f(a)\}$. Sei $b \in A$ mit $f(b) = B$. Dann haben wir den Widerspruch $b \in B \iff b \notin f(b) = B$. \square

Es gibt also unendlich viele Abstufungen von Unendlichkeit

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

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).

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 $\circ : A^2 \rightarrow A$, 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. \square

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

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

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	$\{1\}$	$\{2\}$	$\{1, 2\}$

\square

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: Sei (A, \circ) eine algebraische Struktur.

- (i) In (A, \circ) gibt es höchstens ein neutrales Element.
- (ii) Ist (A, \circ) ein Monoid, so besitzt jedes $a \in A$ höchstens ein inverses Element.
- (iii) In einer Gruppe gilt für beliebige a, b, c : $a \circ b = a \circ c \implies b = c$.

Beweis: (i) Seien n, n' neutral. Dann haben wir $n = n \circ n' = n'$.

(ii) Seien b, c invers zu a . Dann haben wir

$$b = n \circ b = (c \circ a) \circ b = c \circ (a \circ b) = c \circ n = c .$$

(iii) Aus $a \circ b = a \circ c$ erhalten wir $(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$, also $b = c$. □

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 $\sigma : M \rightarrow M$ 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 $g, h \in G$:

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

Beweis: (i) einfach ausrechnen $(g \circ h) \circ (h^{-1} \circ g^{-1}) = n = (h^{-1} \circ g^{-1}) \circ (g \circ h)$.

(ii) offensichtlich. □

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 Aussagen äquivalent (FAÄ):

- (i) $H \leq G$,
- (ii) $\forall a, b \in H : a \circ b \in H \wedge a^{-1} \in H$,
- (iii) $\forall a, b \in H : a \circ b^{-1} \in H$.

Beweis: (i) \implies (ii): trivial.

(ii) \implies (iii): seien $a, b \in H$; dann auch $b^{-1} \in H$, also $a \circ b^{-1} \in H$.

(iii) \implies (i): neutrales Element: sei $a \in H$, dann ist auch $n = a \circ a^{-1} \in H$.

inverses Element: Sei $a \in H$, dann auch $a^{-1} = n \circ a^{-1} \in H$.

\circ führt nicht aus H hinaus: seien $a, b \in H$; dann $a \circ b = a \circ (b^{-1})^{-1} \in H$. □

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

Definition 1.5.11: Sei (G, \circ) eine Gruppe, H eine Untergruppe von G , und $a \in G$. Dann heisst

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

Linksnebenklasse von G nach H (bzgl. a) und

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

Rechtsnebenklasse von G nach H (bzgl. a).

Satz 1.5.12: 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 $\{a \circ H \mid a \in G\}$ 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 $|a \circ H| = |H \circ a| = |H|$.

Beweis: zu (i): sei $b \in a \circ H$, also $b = a \circ b'$ für ein $b' \in H$. Somit

$$b \circ H = a \circ b' \circ H \subseteq a \circ H.$$

Weiters $b \circ (b')^{-1} = a$, also $a \circ H \subseteq b \circ H$.

zu (ii): klar wegen (i).

zu (iii): die Abbildung $\varphi : H \rightarrow a \circ H, b \mapsto a \circ b$ ist sowohl surjektiv (per Def. von $a \circ H$) als auch injektiv (wegen Satz 1.5.5(c)). \square

Satz 1.5.13: 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 .

Beweis: das folgt sofort aus Satz 1.5.9. \square

Definition 1.5.14: 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 1.5.15: 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 $b = a \circ \dots \circ a$ (n mal, für $n \in \mathbb{Z}$).

Definition 1.5.16: 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 1.5.17: Eine Untergruppe H einer Gruppe G heisst **Normalteiler**, bezeichnet als $H \trianglelefteq G$, wenn die Links- und Rechtsnebenklassen übereinstimmen.

Satz 1.5.18: Sei H ein Normalteiler der Gruppe G . Dann gilt

$$a_1 \circ H = a_2 \circ H \wedge b_1 \circ H = b_2 \circ H \implies (a_1 \circ b_1) \circ H = (a_2 \circ b_2) \circ H.$$

Beweis: $a_1 \circ b_1 \circ H = a_1 \circ b_2 \circ H = a_1 \circ H \circ b_2 = a_2 \circ H \circ b_2 = a_2 \circ b_2 \circ H$. \square

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

Definition 1.5.19: 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 1.5.20: 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

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

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

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

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

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

Definition 1.5.21: Eine Abbildung $\varphi : G \rightarrow H$ 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 $\text{Hom}(G, H)$ 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 $\varphi^{-1} : H \rightarrow G$, die ihrerseits auch ein 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 $\varphi : G \rightarrow G$ 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 $\text{End}(G)$, die Menge aller Automorphismen auf G bezeichnen wir mit $\text{Aut}(G)$.

Satz 1.5.22: Seien (G, \circ) und (H, \diamond) Gruppen, und φ ein Homomorphismus von G nach H .

(i) Das neutrale Element n_G von G wird auf das neutrale Element n_H von H abgebildet, also $\varphi(n_G) = n_H$.

(ii) Für alle $a \in G$ gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Beweis: zu (i): $\varphi(n_G) = \varphi(n_G \circ n_G) = \varphi(n_G) \diamond \varphi(n_G)$. Wir kürzen durch $\varphi(n_G)$ (Satz 1.5.5(c)) und erhalten $n_H = \varphi(n_G)$.

zu (ii): $\varphi(a^{-1}) \diamond \varphi(a) = \varphi(a^{-1} \circ a) = n_H = \varphi(a \circ a^{-1}) = \varphi(a) \diamond \varphi(a^{-1})$. □

Satz und Definition 1.5.23: Für eine Gruppe G ist $\text{Aut}(G)$ ebenfalls eine Gruppe, die sogenannte **Automorphismengruppe** von G . Die Verknüpfung \circ ist die Hintereinanderausführung.

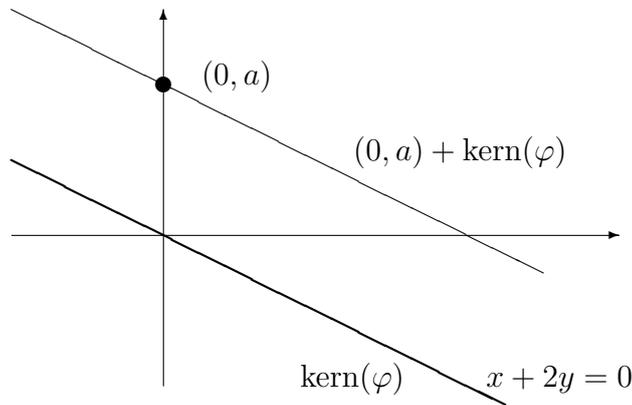


Figure 2: Beispiel 1.5.27: Homomorphismus $\varphi(x, y) = x + 2y$

Beweis: \circ ist assoziativ, id_G ist das neutrale Element, die Inverse φ^{-1} eines Automorphismus ist ebenfalls bijektiv und auch ein Homomorphismus. \square

Definition 1.5.24: Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Das Urbild $\varphi^{-1}(e_H)$ des neutralen Elements e_H wird als **Kern** von φ bezeichnet, also

$$\text{kern}(\varphi) := \{a \in G \mid \varphi(a) = e_H\}.$$

Weiters nennt man

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

das **Bild** von G unter φ .

Satz 1.5.25: Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist $\text{kern}(\varphi)$ ein Normalteiler von G und $\text{im}(\varphi)$ eine Untergruppe von H .

Beweis: $\text{kern}(\varphi)$ ist eine Untergruppe. $a \circ \text{kern}(\varphi) \circ a^{-1} \subseteq \text{kern}(\varphi)$, also $a \circ \text{kern}(\varphi) \subseteq \text{kern}(\varphi) \circ a$. Die andere Teilmengenbeziehung zeigt man analog.

Dass $\text{im}(\varphi)$ eine Untergruppe von H ist folgt aus Satz 1.5.22. \square

Satz 1.5.26: (Homomorphiesatz der Gruppentheorie) Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist die Faktorgruppe $G/\text{kern}(\varphi)$ mit dem Bild $\text{im}(\varphi)$ isomorph:

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

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

Beispiel 1.5.27: Wir demonstrieren diese Zusammenhänge anhand eines geometrischen Beispiels. Die Abbildung

$$\begin{aligned} \varphi : \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x + 2y \end{aligned}$$

ist ein Homomorphismus von $(\mathbb{R}^2, +)$ nach $(\mathbb{R}, +)$.

Offensichtlich ist

$$\text{im}(\varphi) = \mathbb{R} , \text{ und } \text{kern}(\varphi) = \{(x, y) \mid x + 2y = 0\} .$$

Die Nebenklassen von $\text{kern}(\varphi)$ sind

$$\overline{(0, a)} = (0, a) + \text{kern}(\varphi),$$

denn $\overline{(c, a - \frac{1}{2}c)} = \overline{(0, a)}$.

Der laut Homomorphiesatz existierende Isomorphismus ist

$$\begin{aligned} \psi : \mathbb{R}^2 / \ker(\varphi) &\longrightarrow \mathbb{R} = \text{im}(\varphi) \\ (0, a) &\mapsto 2a = \varphi(0, a) , \end{aligned}$$

wie man leicht nachrechnet (Bijektion und Homomorphismus). □

Für jeden Normalteiler N von G ist die Abbildung

$$\begin{aligned} \varphi_N : G &\rightarrow G/N \\ a &\mapsto a \circ N \end{aligned}$$

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

Ringe:

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 1.5.28: 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 1.5.29: 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

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

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 1.5.30: Sei R ein Ring. Eine formale Summe

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

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 offensichtlich die Potenzreihe, in welcher alle Koeffizienten 0 sind. \square

Beispiel 1.5.31: 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 $\text{grad}(a)$. \square

Definition 1.5.32: 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 1.5.33: In jedem Ring R gilt $a \cdot 0 = 0 \cdot a = 0$.

Beweis: Sei $a \in R$. Dann gilt

$$a \cdot a + a \cdot 0 = a \cdot (a + 0) = a \cdot a.$$

Durch Subtraktion von aa auf beiden Seiten dieser Gleichung erhalten wir $a \cdot 0 = 0$.

Analog zeigt man $0 \cdot a = 0$. \square

Definition 1.5.34: 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 1.5.35: In \mathbb{Z}_6 haben wir $\bar{2} \cdot \bar{3} = \bar{0}$. $\bar{2}$ und $\bar{3}$ sind also Nullteiler.

In den Ringen $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ gibt es keine Nullteiler. \square

Definition 1.5.36: Ein kommutativer Ring mit Einselement ohne Nullteiler heisst **Integritätsbereich**.

Beispiel 1.5.37: 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. \square

Satz 1.5.38: 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.

Beweis: betrachte den kleinsten nichtverschwindenden Koeffizienten. \square

Definition 1.5.39 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 1.5.40: 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 1.5.41: 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 1.5.42: Die Integritätsbereiche $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.

\mathbb{Z}_n ist genau dann ein Körper, wenn n eine Primzahl ist. □

Satz 1.5.43: Jeder Körper ist ein Integritätsbereich.

Beweis: Sei $a \cdot b = 0$ und $a \neq 0$. Dann ist $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$. □

Satz und Definition 1.5.44: Ist I ein Integritätsbereich, so ist

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

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 .

Beweis: einfach nachrechnen. □

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

Beispiel 1.5.45: \mathbb{Q} ist der Quotientenkörper von \mathbb{Z} . □