Jürgen Müller

Einführung in die Mathematik (plus)

Skript zur Vorlesung im Wintersemster 2024/25
Universität Trier
Fachbereich IV
Mathematik/Analysis

Inhaltsverzeichnis

1 Mengen, Abbildungen und Ringe

Mathematik ist einfach – bzw. zweifach. Im Grunde genommen befasst man sich mit lediglich zwei Arten von Objekten, nämlich Mengen und Abbildungen. Unsere Darstellung gründet auf dem von Georg Cantor geprägten (sogenannten naiven) Mengenbegriff:

> Eine **Menge** M ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Ein solches Objekt x heißt **Element** der Menge M (Schreibweise: $x \in M$; ist x nicht Element von M, so schreiben wir $x \notin M$). Die Menge ohne Elemente heißt die **leere Menge** (Schreibweise: $\varnothing$ oder $\{\}$).
Es gibt verschiedene Möglichkeiten der Darstellung von Mengen, etwa die aufzählende Schreibweise oder auch die beschreibende, also eine Charakterisierung der Elemente. Die beschreibende Variante hat allgemein die Form[1]

$$M := \{x : x \text{ hat die Eigenschaft } E\} := \{x \mid x \text{ hat die Eigenschaft } E\},$$

wobei E eine gegebene Eigenschaft ist. Wir stellen uns auf den Standpunkt, dass natürliche, ganze und rationale Zahlen bekannt sind, werden aber in der Plus-Vorlesung auf eine konstruktive Einführung eingehen.[2] Man schreibt

$$\begin{aligned}
\mathbb{N} &:= \{x : x \text{ natürliche Zahl}\},\\
\mathbb{N}_0 &:= \{x : x \text{ natürliche Zahl oder } x = 0\},\\
\mathbb{Z} &:= \{x : x \text{ ganze Zahl}\},\\
\mathbb{Q} &:= \{x : x \text{ rationale Zahl}\}.
\end{aligned}$$

Definition 1.1 Es seien A, B Mengen.

[1] Das Symbol := nennt man ein definierendes Gleichheitszeichen. Es bedeutet, dass das auf der linken Seite Stehende durch das auf der rechten Stehende bezeichnet wird. Manchmal schreibt man auch =:, wenn das links Stehende bekannt ist.

[2] Das Gleiche werden wir später für reelle Zahlen tun.

1. A heißt **Teilmenge** von B (Schreibweise: $A \subset B$ oder auch $A \subseteq B$), falls aus $x \in A$ auch $x \in B$ folgt. Man nennt dann B auch eine **Obermenge** von A und schreibt dafür $B \supset A$.
2. A und B heißen **gleich** (Schreibweise $A = B$), falls $A \subset B$ und $B \subset A$ gilt. Sind dabei speziell $A := \{x\}$ und $B := \{y\}$ einelementig, so nennen wir x und y **gleich** (Schreibweise: $x = y$; sind x und y ungleich, so schreibt man $x \neq y$).
3. Die Menge

$$A \cup B := \{x : x \in A \text{ oder } x \in B\}$$

heißt **Vereinigung** von A und B und die Menge

$$A \cap B := \{x : x \in A \text{ und } x \in B\}$$

Schnitt von A und B. Weiter nennt man

$$B \setminus A := \{x : x \in B \text{ und } x \notin A\}$$

Differenz von B und A. Ist $A \subset B$, so heißt

$$A^c := C_B(A) := B \setminus A$$

Komplement von A (bezüglich B).

Beispiel 1.2 Sind $A := \{2k : k \in \mathbb{Z}\}$ und $B := \{3k : k \in \mathbb{Z}\}$, so gilt

$$A \cap B = \{6k : k \in \mathbb{Z}\}.$$

Ähnlich wie bei der obigen Einführung von Mengen wollen wir auf eine eher informelle Definition des zweiten grundlegenden Begriffes der Mathematik zurückgreifen:
Es seien X und Y nichtleere Mengen.

> Eine **Funktion** oder **Abbildung** f von X nach Y ist eine Vorschrift, die jedem $x \in X$ *genau ein* Element $f(x) \in Y$ zuordnet. Alternativ schreibt man auch f_x.

Dabei heißen X der **Definitionsbereich** und Y der **Zielbereich** von f. Außerdem nennt man

$$W(f) := \{f(x) : x \in X\} = \{y \in Y : y = f(x) \text{ für ein } x \in X\}$$

den **Wertebereich** von f. Man schreibt $f : X \to Y$ beziehungsweise $(f_x)_{x\in X}$ (oder auch $X \ni x \mapsto f(x) \in Y$ oder kürzer $x \mapsto f(x)$). Im Fall der Schreibweise $(f_x)_{x\in X}$ spricht man auch von einer **Familie** in Y und nennt dann X die **Indexmenge**. Im Fall $X = \{1, \ldots, n\}$ schreibt man meist $(f_1, \ldots, f_n)$.[3]
Ist $\varnothing \neq A \subset X$, so heißt die Funktion $f|_A : A \to Y$, definiert durch $f|_A(x) := f(x)$ für alle $x \in A$, die **Einschränkung** von f auf A. Die Menge

$$f(A) := W(f|_A) = \{f(x) : x \in A\}$$

nennt man **Bild** von A unter f. Ergänzend setzt man noch $f(\varnothing) := \varnothing$.

Beispiel 1.3 1. Ist $X \neq \varnothing$, so nennt man $\mathrm{id}_X : X \to X$, definiert durch $\mathrm{id}_X(x) := x$ für $x \in X$, die **identische Abbildung** auf X.
2. Es seien $X := Y := \mathbb{Z}$, und es sei $f : \mathbb{Z} \to \mathbb{Z}$ definiert durch[4]

$$f(x) := x^2 \qquad (x \in \mathbb{Z}).$$

Dann ist $W(f) = f(\mathbb{N}_0)$ (und zwar die Menge der Quadratzahlen).

Definition 1.4 Es seien X, Y Mengen und $f : X \to Y$.

1. f heißt **surjektiv** (oder Abbildung von X **auf** Y), falls $W(f) = Y$ gilt, d. h. zu jedem $y \in Y$ existiert ein $x \in X$ mit $f(x) = y$. [5]
2. f heißt **injektiv**, falls aus $x_1, x_2 \in X$ und $f(x_1) = f(x_2)$ schon $x_1 = x_2$ folgt.
3. f heißt **bijektiv**, falls f injektiv und surjektiv ist.

Beispiel 1.5 Für jeden Mnege X ist die identische Abbildung id_X bijektiv. Ist f wie im Beispiel 1.3.2, so ist f weder surjektiv noch injektiv, dagegen ist $f|_{\mathbb{N}_0}$ injektiv.

[3] Man spricht dann auch von einem n-Tupel und im Fall $n = 2$ von einen geordneten Paar sowie im Fall $n = 3$ von einem Tripel.

[4] Die Schreibweise $(x \in X)$ ist im Weiteren als Kurzform von „für alle $x \in X$“ zu lesen.

[5] An dieser Stelle eine kleine Anmerkung zur Frage, ob *Abbildung* und *Funktion* unterschiedliche Begriffe sind: Gemäß obiger (informeller) Definition ist dies nicht der Fall. Man verwendet den Begriff Abbildung allerdings oft dann, wenn auch der Zielbereich eine wesentliche Rolle spielt, wie etwa im Fall der Surjektivität. Man spricht selten von einer surjektiven Funktion und so gut wie gar nicht von einer Funktion von X *auf* Y.

Definition 1.6 Es seien X, Y, Z Mengen und $f : X \to Y$ sowie $g : Y \to Z$ Abbildungen. Dann heißt die Funktion $g \circ f : X \to Z$, definiert durch

$$(g \circ f)(x) := g(f(x)) \qquad (x \in X) \,,$$

Komposition (oder **Hintereinanderausführung** oder **Verkettung**) von f und g.

Definition 1.7 Man setzt

$$Y^X := \mathrm{Abb}(X, Y) := \{f : f \text{ Abbildung von } X \text{ nach } Y\}$$

für Menge der Abbildungen von X nach Y. Sind $f, g \in Y^X$, so heißen f und g **gleich**, falls $f(x) = g(x)$ für alle $x \in X$ gilt.[6]

Beispiel 1.8 Ist f wie im Beispiel 1.3.2 und $g : \mathbb{Z} \to \mathbb{Z}$ definiert durch $g(y) := y + 1$ für $y \in \mathbb{Z}$, so ist $g \circ f : \mathbb{Z} \to \mathbb{Z}$ gegeben durch

$$(g \circ f)(x) = x^2 + 1 \quad (x \in \mathbb{Z}) \,.$$

Man beachte: Hier ist auch $f \circ g : \mathbb{Z} \to \mathbb{Z}$ definiert und es gilt

$$(f \circ g)(x) = (x + 1)^2 \quad (x \in \mathbb{N}).$$

Dabei ist $g \circ f \neq f \circ g$ (da etwa $(g \circ f)(1) = 2 \neq 4 = (f \circ g)(1)$).

Satz 1.9 *Es seien X, Y, Z, U Mengen und $f : X \to Y, g : Y \to Z$ und $h : Z \to U$ Abbildungen. Dann gilt*

$$h \circ (g \circ f) = (h \circ g) \circ f \,.$$

Beweis. Es gilt $h \circ (g \circ f) : X \to U$ sowie $(h \circ g) \circ f : X \to U$ und für alle $x \in X$ ist

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x) \,.$$

Damit sind die beiden Funktionen gleich. □

[6] Wir werden uns gelegentlich – so wie üblich und sehr praktisch – die Freiheit nehmen, zwei Funktionen $f : X \to Y$ und $g : X \to Z$ schon dann zu identifizieren, wenn $f(x) = g(x)$ für alle $x \in X$ gilt und der Zielbereich keine Rolle spielt.

Bemerkung und Definition 1.10 Sind X, Y nichtleere Mengen und ist $f : X \to Y$ bijektiv, so existiert zu jedem $y \in Y$ *genau* ein $x \in X$ mit $f(x) = y$. Dann ist durch

$$g(y) := x \qquad (y \in Y) \,,$$

wobei $y = f(x)$ eine Funktion $g : Y \to X$ definiert. Mann nennt g die **Umkehrfunktion** von f. Es gilt dann $g \circ f = \mathrm{id}_X$ sowie $f \circ g = \mathrm{id}_Y$ und außerdem ist auch $g : Y \to X$ bijektiv.

Definition 1.11 1. Es seien $X_1, \ldots, X_n$ Mengen. Dann schreibt man

$$X_1 \times \ldots \times X_n := \{(x_1, \ldots, x_n) : x_1 \in X_1, \ldots, x_n \in X_n\}.$$

2. Es sei M eine nichtleere Menge. Eine Funktion $f : M \times M \to M$ heißt **Verknüpfung** auf M. Man schreibt in diesem Kontext xfy statt $f((x, y))$ für $(x, y) \in M \times M$. Gewohnt aus der Schule sind Verknüpfungen auf Zahlenmengen, etwa die Addition $+$ und die Multiplikation $\cdot$. Wir werden diese Symbole auch in allgemeineren Situationen verwenden. Im Fall des Multiplikationszeichens $\cdot$ schreibt man meist kurz xy statt $x \cdot y$.

Wir betrachten nun Mengen und Verknüpfungen, die ein rudimentäres Rechnen zulassen.

Definition 1.12 Es seien M eine nichtleere Menge und $\cdot$ eine Verknüpfung auf M.
1. Die Verknüpfung $\cdot$ heißt **assoziativ**, falls $x\,(yz) = (xy)\,z$ für $x, y, z \in M$ gilt. In diesem Fall heißt $(M, \cdot)$ eine **Halbgruppe**. Bei assoziativen Verknüpfungen lässt man die Klammern meist weg, setzt also zum Beispiel $xyz := (xy)z = x(yz)$.
2. Die Verknüpfung heißt **kommutativ**, falls $xy = yx$ für $x, y \in M$ gilt. In diesem Fall heißt nennt man eine Halbgruppe **abelsch** oder auch **kommutativ**.
3. Ein $e \in M$ heißt **neutral** (bezüglich $\cdot$), falls

$$ex = xe = x \qquad (x \in M)$$

gilt. Existiert in einer Halbgruppe $(M, \cdot)$ ein neutrales Element e, so heißt das Tripel $(M, \cdot, e)$ ein **Monoid**.[7] Neutrale Elemente sind stets eindeutig, denn sind e und e' neutral, so ist $e' = ee' = e$.

[7] Man schreibt oft auch kurz M statt $(M, \cdot)$ im Falle einer Halbgruppe und M statt $(M, \cdot, e)$ im Falle eines Monoids.

Bemerkung und Definition 1.13 1. Das Paar $(\mathbb{N}, +)$ ist eine abelsche Halbgruppe, $(\mathbb{N}_0, +, 0)$, $(\mathbb{N}, \cdot, 1)$ und $(\mathbb{Z}, \cdot, 1)$ sind abelsche Monoide.
2. Es sei $X \neq \varnothing$ ein Menge. Nach Satz 1.9 ist

$$\mathrm{Abb}(X) := \mathrm{Abb}(X, X)$$

mit der Komposition $\circ$ von Funktionen als Verknüpfung ein Monoid mit neutralem Element id_X.
3. Ist X eine Menge, so heißt die Menge

$$\mathscr{P}(X) := \{A : A \subset X\}$$

aller Teilmengen von X die **Potenzmenge** von X.[8] Damit sind $(\mathscr{P}(X), \cup, \varnothing)$ und $(\mathscr{P}(X), \cap, X)$ kommutative Monoide ([Ü]).

Bemerkung und Definition 1.14 Es sei $(M, \cdot, e)$ ein Monoid. Ist $x \in M$, so heißt ein $y \in M$ **invers** zu x, falls

$$yx = xy = e$$

gilt.[9] Existiert ein Inverses, so nennt man x **invertierbar**. Ist jedes $x \in M$ invertierbar, so heißt M eine **Gruppe**.
Inverse Elemente sind im Falle der Existenz eindeutig, denn sind y, y' invers zu x, so gilt

$$y = ye = y(xy') = (yx)y' = ey' = y'.$$

Man bezeichnet das inverse Element zu x mit x^{-1}. Bei Verwendung des Verknüpfungszeichens $+$ schreibt man meist $-x$ und dann auch kurz $x - y$ statt $x + (-y)$.
Ist $a \in M$ invertierbar, so ist die Funktion $f_a : M \to M$ bijektiv mit Umkehrfunktion $g_a : M \to M$ gegeben durch $g_a(y) = a^{-1}y$, also mit anderen Worten: Für jedes $y \in M$ hat die Gleichung $ax = y$ genau ein Lösung, nämlich $a^{-1}y$. Entsprechendes gilt für die Gleichung $xa = y$.

Beispiel 1.15 Die Tripel $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$ und $(\mathbb{Q}\setminus\{0\}, \cdot, 1)$ sind abelsche Gruppen. Im Monoid $(\mathbb{Z}, \cdot, 1)$ sind nur ± 1 invertierbar.

[8] Stets ist $\varnothing \in \mathscr{P}(X)$.
[9] Allgemeiner heißt y **linksinvers** zu x, falls $yx = e$ gilt, und **rechtsinvers** zu x, falls $xy = e$ gilt.

Bemerkung 1.16 Es sei $(M, \cdot, e)$ ein Monoid. Sind $x, y \in M$ invertierbar, so ist wegen

$$xyy^{-1}x^{-1} = xx^{-1} = e = y^{-1}y = y^{-1}x^{-1}xy$$

auch xy invertierbar mit

$$(xy)^{-1} \;=\; y^{-1}x^{-1}$$

und damit die Menge U der invertierbaren Elemente ein Monoid. Wegen $x^{-1}x = xx^{-1} = e$ ist auch x^{-1} invertierbar mit $(x^{-1})^{-1} = x$, also insbesondere damit $(U, \cdot, e)$ eine Gruppe.[10]

Bemerkung und Definition 1.17 Nach Bemerkung 1.16 ist

$$S(X) \;:=\; \{f \in \mathrm{Abb}(X) : f \text{ invertierbar}\}$$

eine Gruppe, genannt **symmetrische Gruppe** von X. Ein Element $f \in S(X)$ heißt **Permutation** auf X. Für $n \in \mathbb{N}$ heißt speziell $S_n := S(\{1, \ldots, n\})$ die n-te symmetrische Gruppe. Für $n \geq 3$ ist S_n *nicht* abelsch ([Ü]).
Jede bijektive Funktion $f : X \to X$ ist invertierbar und umgekehrt kann leicht sehen ([Ü]), dass jedes $f \in S(X)$ bijektiv ist, und dass dann f^{-1} die Umkehrfunktion von f ist. Man schreibt daher üblicherweise auch f^{-1} für die Umkehrfunktion im Allgemeinen.

Wir wollen nun Produkte und Summen von mehr als zwei Faktoren beziehungsweise Summanden definieren.

Bemerkung und Definition 1.18 Es seien $(M, \cdot, e)$ ein Monoid, $m, N \in \mathbb{Z}$ mit $m \leq N$ und $x_m, \ldots, x_N \in M$. Dann setzt man $\prod_{k=m}^{m-1} x_k := e$ und definiert **rekursiv**

$$x_m \cdot \ldots \cdot x_n := \prod_{k=m}^{n} x_k := \Big(\prod_{k=m}^{n-1} x_k\Big) \cdot x_n$$

für $n = m, \ldots, N$. Außerdem schreibt man im Falle $x_1 = \ldots = x_n = x$ kurz

$$x^n := \prod_{k=1}^{n} x.$$

[10] mit $\cdot$ eingeschränkt auf $U \times U$ und Zielbereich U

Insbesondere ist damit $x^0 = e$. Ist x invertierbar, so setzt man auch $x^{-n} := (x^{-1})^n$ für $n \in \mathbb{N}$.
Im Falle des Pluszeichens als Verknüpfung schreibt man statt $\prod$ jeweils $\sum$. Außerdem schreibt man dann nx statt x^n. [11]

Eng verbunden mit dem eben verwendeten Prinzip der rekursiven Definition ist ein wichtiges Beweisverfahren: die **vollständige Induktion**.
Für ein $m \in \mathbb{Z}$ und alle $\mathbb{Z} \ni n \geq m$ sei eine Aussage $A(n)$ gegeben. Zum Beweis der Behauptung

$$\textit{für alle } n \in \mathbb{Z} \textit{ mit } n \geq m \textit{ gilt } A(n)$$

geht man oft folgendermaßen vor:

1. Man zeigt, dass $A(m)$ richtig ist (Induktionsanfang).
2. Man nimmt an, dass $A(n)$ oder auch $A(m), \ldots, A(n)$ für ein beliebiges $n \geq m$ richtig ist (Induktionsannahme) und zeigt, dass aus der Induktionsannahme die Richtigkeit der Aussage $A(n+1)$ folgt (Induktionsschritt).

Aus 1. und 2. ergibt sich, dass $A(n)$ für alle $n \geq m$ richtig ist. [12]

Beispiel 1.19 Wir illustrieren die Beweistechnik anhand eines Beispieles. Wir zeigen: Für alle $n \in \mathbb{N}$ gilt

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

Induktionsanfang: Für $n = 1$ sind rechte und linke Seite 0.
Induktionsannahme: Für ein $n \in \mathbb{N}$ gelte

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

Induktionsschritt: Nach Induktionsannahme gilt

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

und damit die Behauptung für $n + 1$.

[11] Man beachte, dass die Abbildung $(n, x) \mapsto nx$ im Allgemeinen keine Verknüpfung auf M ist.
[12] Denn es gilt ja dann $A(m) \Rightarrow A(m+1) \Rightarrow A(m+2) \ldots$.

Bemerkung und Definition 1.20 Es sei $(M, \cdot, e)$ ein Monoid. Induktiv kann man zeigen, dass für $x, y \in M$ und $m, n \in \mathbb{N}_0$ folgende Potenzgesetze gelten:

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn} .$$

Ist M abelsch, so gilt auch

$$x^n y^n = (xy)^n.$$

Allgemeiner kann man dann (induktiv und nicht leicht) zeigen, dass für $\varphi \in S_n$ und $x_1, \ldots, x_n \in M$

$$\prod_{k=1}^{n} x_{\varphi(k)} = \prod_{k=1}^{n} x_k$$

gilt, d. h. die Reihenfolge der Faktoren kann beliebig vertauscht werden. Damit werden Schreibweisen wie $\prod_{j \in I} x_j$ und $\sum_{j \in I} x_j$, wobei I eine beliebige endliche Menge ist und $x_j \in M$ für $j \in I$ gilt, sinnvoll.
Im Fall invertierbarer x bzw. y gelten die Potenzgesetze auch für $m, n \in \mathbb{Z}$.

Wir kommen jetzt zu algebraischen Strukturen mit zwei Verknüpfungen.

Bemerkung und Definition 1.21 Es sei R eine Menge und es seien $+$ und $\cdot$ Verknüpfungen auf R. Dann heißt $\cdot$ **distributiv** über $+$, falls für $x, y, z \in R$ gilt

$$x(y+z) = (xy) + (xz) \qquad \text{und} \qquad (x+y)z = (xz) + (yz).$$

Gilt

(R1) $(R, +, 0)$ ist eine abelsche Gruppe,

(R2) $(R, \cdot, 1)$ ist ein Monoid,

(R3) $\cdot$ ist distributiv über $+$,

so heißen $(R, +, \cdot)$ **Ring**, das neutrale Element 0 zu $+$ **Nullelement** oder kurz **Null** und das neutrale Element 1 zu $\cdot$ **Einselement** oder **Eins**.[13] Ist $(R, \cdot, 1)$ abelsch, so heißt der Ring **kommutativ**.
Standardbeispiele kommutativer Ringe sind $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$. Man verwendet wie dort auch in allgemeinen Ringen Punkt-vor-Strich-Schreibweisen, also zum Beispiel $x + yz := x + (yz)$.

[13] Manchmal schreibt man deutlicher 0_R und 1_R für die neutralen Elemente eines Ringes. Andererseits schreibt man oft kurz R statt $(R, +, \cdot)$.

Bemerkung 1.22 Es seien R ein Ring und X eine nichtleere Menge. Wir definieren für $f, g \in R^X$ die Funktionen $f \pm g \in R^X$ und $f \cdot g \in R^X$ argumentweise durch

$$(f \pm g)(x) := f(x) \pm g(x) \quad \text{und} \quad (f \cdot g)(x) := f(x) \cdot g(x) \quad (x \in X).$$

Damit ist $R^X = (R^X, +, \cdot)$ ein Ring mit Nullelement 0_{R^X} und Einselement 1_{R^X}, definiert durch $0_{R^X}(x) := 0_R$ und $1_{R^X}(x) := 1_R$ für $x \in X$. Ist R kommutativ, so ist auch R^X kommutativ.

Bemerkung und Definition 1.23 Es sei R ein Ring. Induktiv ergeben sich für $x \in R$ und endliche Familien $(x_j)_{j \in I}$ in R die allgemeinen **Distributivgesetze**

$$x \sum_{j \in I}^{n} x_j = \sum_{j \in I} x x_j \quad \text{und} \quad \Big(\sum_{j \in I} x_j \Big) x = \sum_{j \in I} x_j x.$$

Weiter ist 0 **absorbierend**, d. h. für $x \in R$ gilt

$$0x = x0 = 0.$$

Denn: Wegen $0x = (0+0)x = 0x+0x$ ist $0 = 0x-0x = (0x+0x)-0x = 0x$.
Entsprechend sieht man, dass $x0 = 0$ gilt.

Damit gilt für $x, y, z \in R$ ([Ü])

$$x(y-z) = xy - xz, \quad (x-y)z = xz - yz \quad \text{und} \quad (-x)(-y) = xy.$$

In der Schule lernt man die binomischen Formeln für reelle Zahlen in folgender Form kennen:

$$(a \pm b)^2 = a^2 \pm 2ab + b^2 \quad \text{und} \quad (a+b)(a-b) = a^2 - b^2.$$

Wir werden jetzt allgemeinere Formeln in Ringen herleiten, wobei er Exponent 2 durch ein beliebiges $n \in \mathbb{N}$ ersetzt wird.

Satz 1.24 *Es sei $(R, +, \cdot)$ ein kommutativer Ring. Dann gilt für alle $a, b \in R$ und alle $n \in \mathbb{N}$*

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} \,. \tag{1.1}$$

Beweis. Es gilt

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= \sum_{k=0}^{n-1} a a^k b^{n-1-k} - \sum_{k=0}^{n-1} b a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} a^{k+1} b^{n-(k+1)} - \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= \sum_{j=1}^{n} a^j b^{n-j} - \sum_{k=0}^{n-1} a^k b^{n-k} = a^n - b^n \ .\end{aligned}$$

□

Bemerkung 1.25 Als Spezialfall $b = 1$ ergibt sich die wichtige **geometrische Summenformel**: Für $a \in R$ und $n \in \mathbb{N}$ gilt

$$a^n - 1 \ = \ (a-1)\sum_{k=0}^{n-1} a^k = (a-1)(1 + a + \ldots + a^{n-1}), \tag{1.2}$$

die unter anderem eine zentrale Rolle im Zusammenhang mit der Binär-, Dezimal- bzw. Hexadezimaldarstellung natürlicher Zahlen spielt (siehe Anhang B).

Wir steuern nun auf eine Darstellung für Ausdrücke der Form $(a+b)^n$.

Bemerkung und Definition 1.26 Für $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$ setzen wir

$$\binom{n}{0} := 1 \quad \text{und} \quad \binom{0}{k} := 0.$$

Damit sind die **Binomialkoeffizienten** $\binom{n}{k}$ (gesprochen n über k) rekursiv bezüglich n definiert durch

$$\binom{n+1}{k} := \binom{n}{k-1} + \binom{n}{k} \qquad (n \in \mathbb{N}_0,\, k \in \mathbb{N}).$$

Aus der Defintion folgt, dass alle Binomialkoeffizienten nichtnegative ganze Zahlen sind mit

$$\binom{n}{k} = 0 \qquad (k > n).$$

Ordnet man die Binomialkoeffizienten $\binom{n}{k}$ in einem dreieckigen Schema an, wobei in der n-ten Zeile (mit Zeile 0 beginnend) die Koeffizienten $\binom{n}{0}, \ldots, \binom{n}{n}$ stehen, so entsteht das **Pascalsche Dreieck**:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & \vdots & & & & & & & & &
\end{array}
$$

Binomialkoeffizienten lassen sich geschlossen darstellen, jedenfalls unter Verwendung von Fakultäten.

Definition 1.27 Für $n \in \mathbb{N}_0$ definiert man n-**Fakultät** durch

$$
n! := \prod_{k=1}^{n} k = \begin{cases} 1\,, & \text{falls } n = 0 \\ 1 \cdot 2 \cdot \ldots \cdot n\,, & \text{falls } n \in \mathbb{N} \end{cases}.
$$

So ist etwa $6! = 1 \cdot 2 \cdots 6 = 720$.

Satz 1.28 *Für $n, k \in \mathbb{N}_0$ mit $k \leq n$ gilt*

$$
\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{1}{k!} \prod_{j=0}^{k-1} (n-j).
$$

Beweis. Wir zeigen die Darstellung per Induktion nach n.
Für $n = 0$ (und dann $k = 0$) sind nach den jeweiligen Definitionen beide Seiten 1. Gilt die Behauptung für $n \in \mathbb{N}_0$, so folgt für $k \in \{1, \ldots, n\}$

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

Außerdem ist $\binom{n+1}{n+1} = \binom{n}{n} + \binom{n}{n+1} = \binom{n}{n} + 0 = 1$. □

Mit der Darstellung sieht man insbesondere die Symmetrie der Binomialkoeffizienten:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k} . \tag{1.3}$$

Satz 1.29 (**binomischer Satz**)
Es sei $(R, +, \cdot)$ ein kommutativer Ring. Dann gilt für alle $a, b \in R$ und alle $n \in \mathbb{N}_0$

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

Beweis. 1. Für $n = 0$ gilt $(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$.

2. Für ein $n \in \mathbb{N}_0$ gelte $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. Dann folgt mit Satz 1.28

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

□

Beispiel 1.30 Für $n = 6$ gilt (siehe Pascalesches Dreieck)

$$(a+b)^6 = 1 \cdot b^6 + 6 \cdot ab^5 + 15a^2b^4 + 20a^3b^3 + 15a^4b^2 + 6a^5b + 1 \cdot a^6 .$$

Bemerkung 1.31 Als Spezialfälle aus Satz 1.29 ergeben sich interessante Beziehungen für das Pascalsche Dreieck: Für $R = \mathbb{Z}$ und $a = 1$, $b = 1$ ergibt sich

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

das heißt die Summe der Binomialkoeffizienten in der n-ten Zeile des Pascalschen Dreiecks ergibt stets 2^n. Für $a = -1$, $b = 1$ und $n \in \mathbb{N}$ ergibt sich

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

das heißt, versieht man die Binomialkoeffizienten in der n-ten Zeile jeweils abwechselnd mit dem Vorzeichen $+$ und $-$, so erhält man als Summe den Wert 0. Für $n = 6$ gilt etwa

$$1+6+15+20+15+6+1 = 64 = 2^6 \quad \text{und} \quad 1-6+15-20+15-6+1 = 0 .$$

Bemerkung und Definition 1.32 Ist $R = (R, +, \cdot)$ ein Ring mit Nullelement 0 und Einselement $1 \neq 0$, so setzen wir

$$R^* := R \setminus \{0\}.$$

Dann heißt R ein **Körper**, falls R kommutativ ist und jedes $x \in R^*$ invertierbar ist.[14] Nach Bemerkung 1.16 ist $(R^*, \cdot, 1)$ eine eine abelsche Gruppe und damit sind Körper **nullteilerfrei**, d. h. sind $x, y \in R$ mit $xy = 0$, so ist $x = 0$ oder $y = 0$. Man schreibt $y/x := yx^{-1}$ für $x \neq 0$ und wegen der Kommutativität auch $\dfrac{y}{x} := y/x$.

Beispiel 1.33 1. Der Ring $(\mathbb{Q}, +, \cdot)$ ist ein Körper, der Ring $(\mathbb{Z}, +, \cdot)$ nicht.
2. Es sei $\mathbb{F}_2 := \{\heartsuit, \clubsuit\}$, wobei die Addition und die Multiplikation durch die folgenden Verknüpfungstafeln (kommutativ) definiert sind:

$+$	$\heartsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\clubsuit$
$\clubsuit$	$\clubsuit$	$\heartsuit$

$\cdot$	$\heartsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$
$\clubsuit$	$\heartsuit$	$\clubsuit$

Man kann leicht nachrechnen, daß $(\mathbb{F}_2, +, \cdot)$ ein Körper ist, genannt der **Binärkörper**. Dabei gilt $\heartsuit = 0 = 0_{\mathbb{F}_2}$ und $\clubsuit = 1 = 1_{\mathbb{F}_2}$, also ist in der Binärarithmetik $1 + 1 = 0$.

[14] Verzichtet man auf die Forderung der Kommutativität, so spricht man von einem Schiefkörper.

2 Reelle und komplexe Zahlen

Bemerkung und Definition 2.1 Es sei $X \neq \varnothing$ eine Menge. Man nennt eine Teilmenge R von $X \times X$ auch eine **Relation** auf X und schreibt xRy falls $(x, y) \in R$.[15] Eine Relation $<$ auf X heißt (strenge) **Ordnung** auf X, falls gilt

(O1) Für alle $x, y \in X$ gilt entweder $x = y$ oder $x < y$ oder $y < x$ (Trichotomie).

(O2) Für $x, y, z \in X$ gilt: aus $x < y$ und $y < z$ folgt $x < z$ (Transitivität).

Das Paar $(X, <)$ heißt dann eine **geordnete Menge**. Außerdem bedeutet $x \leq y$, dass entweder $x < y$ oder $x = y$ gilt.[16] Wenig überraschend schreibt man auch $y > x$ statt $x < y$ und $y \geq x$ statt $x \leq y$.

Bemerkung und Definition 2.2 Es sei R ein kommutativer Ring mit $1 \neq 0$. Ist $<$ eine Ordnung auf R, so heißt $R = (R, +, \cdot, <)$ ein **geordneter Ring**, falls für $x, y \in R$ folgende Eigenschaften erfüllt sind:

(O3) Aus $x < y$ folgt $x + z < y + z$ für alle $z \in R$ (1. Monotoniegesetz).

(O4) Aus $x < y$ und $z > 0$ folgt $xz < yz$ (2. Monotoniegesetz).

$(\mathbb{Z}, +, \cdot, <)$ ist ein geordneter Ring und $(\mathbb{Q}, +, \cdot, <)$ ist ein geordneter Körper.
Ist R geordnet, nennt man $x \in R$ **positiv**, falls $x > 0$ gilt und **negativ**, falls $x < 0$ gilt. Aus (O3) folgt, dass x genau dann positiv ist, wenn $-x$ negativ ist.[17]

> Denn: Aus $0 < x$ folgt $-x = 0 + (-x) < x + (-x) = 0$. Entsprechend folgt aus $-x < 0$ auch $0 = x + (-x) < x + 0 = x$.

Wir setzen noch $R_+ := \{x \in R : x > 0\}$ und $R_- := \{x \in R : x < 0\}$.

Satz 2.3 *Es seien $R = (R, +, \cdot, <)$ ein geordneter Ring, $x, y \in R$ und $n \in \mathbb{N}$. Dann gilt:*

[15] Sind M eine Menge und $f : M \to X$ eine Funktion, so ist der **Graph** $\{(x, f(x)) : x \in M\} \subset M \times X$ von f im Fall $M \subset X$ eine Relation auf X.

[16] Die Relation $\leq$ ist dann eine sogenannte schwache Ordnung auf X.

[17] Insbesondere existiert damit im Binärkörper $\mathbb{F}_2$ keine Ordnungsrelation mit der Eigenschaft (O3).

1. *Aus* $x, y > 0$ *oder* $x, y < 0$ *folgt* $xy > 0$ *und aus* $x > 0$, $y < 0$ *folgt* $xy < 0$. *Speziell sind* $x^2 > 0$ *für* $x \neq 0$ *und* $1 > 0$.

2. *Ist* $x < y$, *so gilt* $nx < ny$ *und im Falle* $x > 0$ *auch* $0 < x^n < y^n$.

3. *Sind* $x > 0$ *und* $m \in \mathbb{N}$ *mit* $m > n$, *so ist* $mx > nx > 0$.[18]

Beweis. 1. Sind $x, y > 0$, so folgt mit (O4) sofort $0 = 0y < xy$. Sind andererseits $x, y < 0$, so sind $-y, -x > 0$ und damit $xy = (-x)(-y) > 0$. Sind $x, -y > 0$, so gilt $-(xy) = x(-y) > 0$. Ist $x \neq 0$, so ist $x > 0$ oder $x < 0$ nach (O1), also $x^2 > 0$. Wegen $1 \neq 0$ ist $1 = 1^2 > 0$.
2. und 3. als [Ü]. □

Satz 2.4 (Bernoulli-Ungleichung)
Sind R *ein geordneter Ring und* $n \in \mathbb{N}_0$, *so gilt* $(1 + x)^n \geq 1 + nx$ *für* $x \geq -1$.

Beweis. Denn: Für $n = 0$ sind beide Seiten 1. Gilt die Behauptung für ein $n \in \mathbb{N}_0$, so folgt wegen $x + 1 \geq 0$ mit (O4) und Satz 2.3

$$(1 + x)^{n+1} = (1 + x)(1 + x)^n \geq (1 + x)(1 + nx) = 1 + x + nx + nx^2 \geq 1 + (n + 1)x.$$

□

Satz 2.5 *Es seien* K *ein geordneter Körper und* $x, y \in K$. *Gilt* $0 < x < y$, *so ist* $0 < 1/y < 1/x$. *Außerdem ist die Menge* $\{z \in K : x < z < y\}$ *unendlich.*

Beweis. Zunächst folgt $1/x > 0$ aus Satz 2.3.1 (wäre $1/x < 0$, so wäre $1 = x/x < 0$). Genauso ist $1/y > 0$. Aus $x < y$ ergibt sich also $x/y < y/y = 1$ mit (O4) und wieder mit (O4)

$$1/y = (x/y) \cdot (1/x) < 1 \cdot (1/x) = 1/x \; .$$

Nach Satz 2.3 ist $m1 > n1 > 0$ für alle $n, m \in \mathbb{N}$ mit $m > n$, also $0 < 1/(m1) < 1/(n1)$ und folglich $x < x + (y - x)/(m1) < x + (y - x)/(n1) \leq y$. □

[18] Damit ist R_+ unendlich. Genauer enthält R_+ die natürlichen Zahlen in dem Sinne, dass man $n1$ mit n identifiziert.

Bemerkung und Definition 2.6 Ist K ein Körper und sind $a, b, c \in K$ mit $a \neq 0$, so hat die Gleichung $ax+b = 0$ genau eine Lösung, nämlich $x = -b/a$. Im Allgemeinen sind quadratische Gleichungen der Form[19]

$$0 = ax^2 + bx + c = a\Big(x + \frac{b}{2a}\Big)^2 + c - \frac{b^2}{4a}$$

nicht mehr lösbar (hier setzen wir $1+1 \neq 0$ und damit $2^n a \neq 0$ voraus). Ist K geordnet, so folgt aus Satz 2.3, dass notwendig die **Diskriminante**

$$\Delta := b^2 - 4ac$$

nicht-negativ ist. Aber auch in diesem Fall ist nicht stets Lösbarkeit garantiert. So haben etwa die Gleichungen $x^2 + x - 1 = 0$ und $x^2 - 2 = 0$ keine Lösung in $\mathbb{Q}$ ([Ü]) obwohl die Diskriminate in beiden Fällen positiv ist.

Wir erweitern nun $(\mathbb{Q}, +, \cdot, <)$ zu einem geordneten Körper $(\mathbb{R}, +, \cdot, <)$ so, dass quadratische Gleichungen mit nichtnegativer Diskriminante lösbar sind. Anschließend erweitern wir $(\mathbb{R}, +, \cdot)$ zu einem Körper $(\mathbb{C}, +, \cdot)$ so, dass *alle* quadratischen Gleichungen lösbar sind.

Bemerkung und Definition 2.7 Es seien $(X, <)$ geordnet und $M \subset X$.
1. M heißt **nach oben beschränkt**, wenn ein $s \in X$ existiert mit $x \leq s$ für alle $x \in M$. Ein solches s heißt dann eine **obere Schranke** von M. Ist dabei $s \in M$, so heißt s **Maximum** von M. Man schreibt dann

$$\max M := s.$$

Eine obere Schranke $s^* \in X$ von M heißt **kleinste obere Schranke** oder **Supremum** von M, falls $s \geq s^*$ für jede obere Schranke s von M gilt. Hieraus ergibt sich sofort, dass für jedes M höchstens ein Supremum und ein Infimum existieren. Wir schreiben im Falle der Existenz

$$\sup M := s^*$$

2. M heißt **nach unten beschränkt**, wenn ein $s \in X$ existiert mit $x \geq s$ für alle $x \in M$. Ein solches s heißt dann **untere Schranke** von M. Ist dabei $s \in M$, so heißt s **Minimum** von M. Man schreibt dann

$$\min M := s.$$

[19] die zweite Darstellung, die sich durch quadratische Ergänzung ergibt, nennt man Scheitelpunktform.

Eine untere Schranke $s_* \in X$ von M heißt **größte untere Schranke** oder **Infimum** von M, falls $s \leq s_*$ für jede untere Schranke s von M gilt. Wieder gibt es höchstens ein Infimum, bezeichnet mit

$$\inf M := s_* .$$

3. M heißt **beschränkt**, wenn M nach oben und nach unten beschränkt ist.

Bemerkung 2.8 Existiert $\max M$, so gilt $\sup M = \max M$ und im Falle der Existenz von $\min M$ ist $\inf M = \min M$. Außerdem existieren für endliche Mengen stets Maximum und Minimum. Weiter kann man zeigen ([Ü]), dass jede nach oben (bzw. unten) beschränkte Teilmenge von $\mathbb{Z}$ ein Maximum (bzw. Minimum) hat. In $\mathbb{Q}$ ist dies im Allgemeinen nicht der Fall: Für $M := \mathbb{Q}_+$ etwa gilt $\inf M = 0$.

> Denn: Zunächst ist 0 eine untere Schranke von M. Ist $s > 0$, so existieren nach Satz 2.5 Punkte $x \in \mathbb{Q}_+$ mit $x < s$. Also ist s keine untere Schranke von M. Damit ist jede untere Schranke $s \leq 0$.

Wegen $0 \notin M$ hat M kein Minimum.

Bemerkung und Definition 2.9 Eine geordnete Menge $(X, <)$ heißt **ordnungsvollständig** oder kurz **vollständig**, falls jede nichtleere, nach oben beschränkte Teilmenge M von X ein Supremum hat. Ein geordneter Körper $(K, +, \cdot, <)$ heißt **vollständig (geordnet)**, falls $(K, <)$ ordnungsvollständig ist.
Von fundamentaler Bedeutung für die Mathematik ist das folgende Ergebnis:

> *Es existiert ein vollständig geordneter Körper* $(\mathbb{R}, +, \cdot, <)$ *so, dass* $\mathbb{Q}$ *in* $\mathbb{R}$ *eingebettet ist.*

Man kann zeigen, dass in gewissem Sinne nur ein vollständig geordneter Körper existiert. Die Elemente von $\mathbb{R}$ heißen **reelle Zahlen**. Wir werden in der Vorlesung plus (im Anhang B) genauer auf eine mögliche Konstruktion der reellen Zahlen und einen Beweis zur obigen Aussage eingehen.

Bemerkung und Definition 2.10 Manchmal ist es praktisch und sinnvoll, die geordnete Menge $(\mathbb{R}, <)$ um zwei Punkte $+\infty$ (oder kurz ∞) und $-\infty$ so zu erweitern,

dass definitionsgemäß $-\infty < x < \infty$ für alle $x \in \mathbb{R}$ gilt. Für $M \subset \mathbb{R}$ ist damit $\sup M = \infty$, falls M nach oben unbeschränkt ist, und $\inf M = -\infty$, falls M nach unten unbeschänkt ist.
Eine nichtleere Menge $I \subset \mathbb{R}$ heißt **Intervall**, falls $x \in I$ für alle $x \in \mathbb{R}$ mit $\inf I < x < \sup I$ gilt. Für $a, b \in \mathbb{R} \cup \{\pm\infty\}$ setzt man

$$\begin{aligned}
(a,b) :=]a,b[&:= \{x \in \mathbb{R} : a < x < b\}, \text{ falls } -\infty \le a < b \le \infty,\\
[a,b) := [a,b[&:= \{x \in \mathbb{R} : a \le x < b\}, \text{ falls } -\infty < a < b \le \infty,\\
(a,b] :=]a,b] &:= \{x \in \mathbb{R} : a < x \le b\}, \text{ falls } -\infty \le a < b < \infty.\\
[a,b] &:= \{x \in \mathbb{R} : a \le x \le b\}, \text{ falls } -\infty < a \le b < \infty.
\end{aligned}$$

Jedes Intervall hat eine solche Form, wobei stets $a = \inf I$ und $b = \sup I$ gilt.

Satz 2.11 *Die Abbildung $f : [0,\infty) \to [0,\infty)$ mit $f(x) := x^2$ ist bijektiv. Für $y \ge 0$ schreibt man $\sqrt{y} := f^{-1}(y)$ und spricht von der Wurzel aus y.*

Beweis. Aus Satz 2.3 folgt, dass f injektiv ist.
Es seien $y \ge 0$ und $M := \{x \in [0,\infty) : x^2 \le y\}$. Ist $x \in \mathbb{R}$ mit $x > 1 + y$, so gilt $x^2 > (1+y)^2 > y$. Damit ist $1 + y$ obere Schranke vom M. Da $\mathbb{R}$ vollständig ist, existiert $s := \sup M$. Wir zeigen, dass weder $s^2 > y$ noch $s^2 < y$ gelten kann. Damit ist $s^2 = y$ nach (O1).[20]
Angenommen, es ist $s^2 > y$. Dann ist $\delta := (s^2 - y)/(2s) > 0$ und wegen $2\delta s = s^2 - y$

$$(s-\delta)^2 \ge s^2 - 2\delta s = y.$$

Ist $x \in M$, so folgt $x^2 \le y \le (s-\delta)^2$ und damit auch $x \le s - \delta$. Also ist $s - \delta$ obere Schranke von M im Widerspruch dazu, dass s kleinste obere Schranke ist.
Angenommen, es ist $s^2 < y$. Dann ist $\delta := \min\{1, (y^2 - s)/(2s+1)\} > 0$ und wegen $2s + \delta \le 2s + 1$ gilt

$$(s+\delta)^2 - s^2 = \delta(2s+\delta) \le \delta(2s+1) \le y - s^2,$$

also $(s+\delta)^2 \le y$. Damit ist $s + \delta \in M$ und folglich s keine obere Schranke von M. Also ergibt sich auch hier ein Widerspruch. □

[20] Der Beweis zeigt auch, dass $\mathbb{Q}$ kein vollständig geordneter Körper ist, da ansonsten etwa die Gleichung $x^2 = 2$ eine Lösung in $\mathbb{Q}$ hätte.

Bemerkung 2.12 Nach Satz 2.11 und Bemerkung und Definition 2.6 ist die quadratische Gleichung $ax^2 + bx + c = 0$ für $\Delta \geq 0$ lösbar und die Lösungen x_1, x_2 sind gegeben durch

$$x_{1,2} = \frac{1}{2a}\big(-b \pm \sqrt{b^2 - 4ac}\big).$$

Satz 2.13 *$\mathbb{N}$ ist unbeschränkt in $\mathbb{R}$[21] und für jedes nicht einpunktige Intervall I gilt*

$$I \cap \mathbb{Q} \neq \varnothing.$$

Beweis. 1. Angenommen, $\mathbb{N}$ sei nach oben beschränkt in $\mathbb{R}$. Dann existiert $s := \sup \mathbb{N} \in \mathbb{R}$. Da s kleinste obere Schranke von $\mathbb{N}$ ist, ist $s - 1/2$ keine obere Schranke von $\mathbb{N}$. Also existiert ein $n \in \mathbb{N}$ mit $n > s - 1/2$. Dann ist aber $s + 1/2 < n + 1 \in \mathbb{N}$. Widerspruch zu s obere Schranke von $\mathbb{N}$.
2. Sind $x, y \in I$ mit $x < y$ und $\delta := y - x$, so existiert nach 1. ein $q \in \mathbb{N}$ mit $q > 1/\delta$, also $1/q < \delta$. Ist nun $p := \max\{k \in \mathbb{N} : k < qy\}$, so ist $p/q < y$ und $(p+1)/q \geq y$, also auch $p/q \geq y - 1/q > y - \delta = x$. Damit ist $p/q \in I$. □

Unser Ziel ist es nun, den Körper der reellen Zahlen so zu erweitern, dass die quadratische Gleichung $x^2 = y$ auch für $y < 0$ lösbar ist.

Bemerkung und Definition 2.14 Wir betrachten die abelsche Gruppe

$$(\mathbb{R}^2, +, (0,0)) = (\mathbb{R}^{\{1,2\}}, +, 0)$$

aus Bemerkung 1.22. Mit der dort allgemein definierten argumentweisen Multiplikation ist $\mathbb{R}^2$ zwar ein kommutativer Ring, aber nicht nullteilerfrei und damit insbesondere kein Körper. Wir definieren alternativ für $x = (s,t)$ und $y = (u,v)$ in $\mathbb{R}^2$

$$x \cdot y = (s,t) \cdot (u,v) := (su - tv, sv + tu).$$

Man rechnet nach, dass damit $(\mathbb{R}^2, +, \cdot)$ ein Körper ist mit $1 = (1_\mathbb{R}, 0_\mathbb{R})$. Legt man diese Multiplikation zugrunde, so schreibt man $\mathbb{C}$ statt $\mathbb{R}^2$ und nennt die Elemente von $\mathbb{C}$ **komplexe Zahlen**.[22] Traditionell verwendet man meist z oder w als Bezeichnung für eine komplexe Zahl. Sind etwa $z = (3,-1)$ und $w = (1,2)$, so ist

$$z \cdot w = (3,-1) \cdot (1,2) = (3 - (-2), 6 - 1) = (5,5)\ .$$

[21] Geordnete Körper mit dieser Eigenschaft nennt man archimedisch geordnet.

[22] Damit ist $\mathbb{C}$ nichts anderes als der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ mit dem Bonus der Multiplikation $\cdot$, die bei erstem Faktor in $\mathbb{R}$ nichts anderes als die Skalarmultiplikation in $\mathbb{R}^2$ ist.

Für $z = (s,t) \neq 0$ gilt

$$\frac{1}{z} = \left(\frac{s}{s^2+t^2}, \frac{-t}{s^2+t^2} \right).$$

Aus der Definition der Addition und der Multiplikation ergibt sich

$$(s,0) + (u,0) = (s+u,0) \quad \text{und} \quad (s,0)(u,0) = (su,0),$$

das heißt, Addition und Multiplikation der komplexen Zahlen $(s,0)$ und $(u,0)$ entsprechen der Addition und der Multiplikation von s und u in $\mathbb{R}$. Indem wir die komplexe Zahl $(s,0)$ mit der reellen s identifizieren, können wir den Körper $\mathbb{C}$ damit als Erweiterung des Körpers $\mathbb{R}$ auffassen. Wir schreiben dann auch kurz s statt $(s,0)$. Man nennt weiterhin

$$i := (0,1) \in \mathbb{C}$$

die **imaginäre Einheit** in $\mathbb{C}$. Für i gilt

$$i^2 = (0,1) \cdot (0,1) = (-1,0) = -1\,.$$

Nach Bemerkung 2.6 gibt es keine Ordnung auf $\mathbb{C}$ so, dass $\mathbb{C}$ zu einem geordneten Körper wird.

Bemerkung und Definition 2.15 Unter Verwendung der imaginären Einheit kann man jedes $z = (s,t) \in \mathbb{C}$ in der Form

$$z = (s,t) = (s,0) + (0,1)(t,0) = s + it$$

schreiben. Diese Darstellung heißt **Normalform** (oder **kartesische Form**) von z. So gilt etwa

$$z = (3,-1) = 3 + i(-1) = 3 - i.$$

Weiter nennt man $\operatorname{Re} z := s$ **Realteil** von z und $\operatorname{Im} z := t$ **Imaginärteil** von z sowie

$$\overline{z} := s - it$$

konjugiert komplex zu z. Geometrisch entsteht $\overline{z}$ durch Spiegelung von z an der reellen Achse.
Für $z, w \in \mathbb{C}$ ergibt sich leicht

$$\overline{z+w} = \overline{z} + \overline{w}, \qquad \overline{zw} = \overline{z} \cdot \overline{w}, \qquad \overline{(\overline{z})} = z$$

sowie

$$\operatorname{Re}(z) = \frac{1}{2}(z + \overline{z}) \quad \text{und} \quad \operatorname{Im}(z) = \frac{1}{2i}(z - \overline{z}).$$

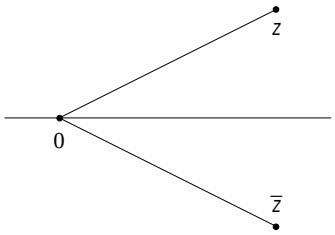


Abbildung 1: z und $\overline{z}$

Bemerkung und Definition 2.16 Die nichtnegative reelle Zahl

$$|z| := \sqrt{s^2 + t^2}$$

heißt **Betrag** von z. Insbesondere ist damit $|z| > 0$ falls $z \neq 0$ und $|s| = \sqrt{s^2}$. [23]

Satz 2.17 *Es seien $z, w \in \mathbb{C}$. Dann gilt*

1. $|z| = |\overline{z}| = |-z|$, $|\mathrm{Re}\, z| \leq |z|$ *und* $|\mathrm{Im}\, z| \leq |z|$.
2. $|z|^2 = z\overline{z}$ *und* $1/z = \overline{z}/|z|^2$, *falls* $z \neq 0$.
3. $|zw| = |z|\,|w|$
4. $|z \pm w|^2 = |z|^2 \pm 2\,\mathrm{Re}(z\overline{w}) + |w|^2$.
5. (**Dreiecksungleichung**) $|z \pm w| \leq |z| + |w|$.

Beweis. 1. ergibt sich unmittelbar aus der Definition des Betrages und 2. als [Ü].
3. Es gilt nach 2.

$$|zw|^2 = (zw)(\overline{zw}) = (z\overline{z})(w\overline{w}) = |z|^2|w|^2 = (|z||w|)^2 \ .$$

Durch Wurzelziehen folgt die Behauptung.
4. Wieder mit 2. gilt

$$|z \pm w|^2 = (z \pm w)(\overline{z} \pm \overline{w}) = z\overline{z} \pm z\overline{w} \pm w\overline{z} + w\overline{w} = |z|^2 \pm 2\,\mathrm{Re}\,(z\overline{w}) + |w|^2 \ .$$

[23] Der Betrag $|z|$ beschreibt nach dem Satz von Pythagoras anschaulich die Länge der Strecke von 0 nach z in der euklidschen Ebene.

5. Nach 4. sowie 1. und 3. ist

$$|z \pm w|^2 \leq |z|^2 + 2|z\overline{w}| + |w|^2 = |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2 .$$

Durch Wurzelziehen folgt die Behauptung. □

Beispiel 2.18 Für $z = 3 - i$ gilt $|z| = \sqrt{9+1} = \sqrt{10}$, $\overline{z} = 3 - i(-1) = 3 + i$ und

$$z\overline{z} = (3 - i)(3 + i) = 9 + 1 = |z|^2.$$

Bemerkung und Definition 2.19 Wir schreiben

$$\mathbb{S} := \{z \in \mathbb{C} : |z| = 1\}$$

für den **Einheitskreis** in $\mathbb{C}$. Ist $z \in \mathbb{C}^*$, so gilt $z = r\zeta$ mit $r = |z| > 0$ und $\zeta = z/|z| \in \mathbb{S}$. Sind $r' > 0$ und $\zeta' \in \mathbb{S}$ mit $z = r'\zeta'$, so ist $r' = r$ und $\zeta' = \zeta$. Also hat jedes $z \in \mathbb{C}^*$ genau eine multiplikative Zerlegung $z = r\zeta$ mit $r > 0$ und $\zeta \in \mathbb{S}$. Diese Darstellung von z nennt man die **Polarform** von z.

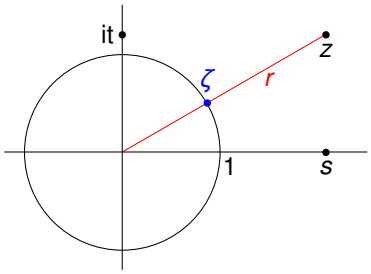


Abbildung 2: Polarform $z = r\zeta$.

A Weiteres zu Mengen und Abbildungen

Definition A.1 Es seien $I \neq \varnothing$ eine Menge, X eine Menge und $(A_\alpha)_{\alpha\in I}$ eine Familie von Teilmengen von X. Dann heißen

$$\bigcup_{\alpha\in I} A_\alpha := \{x : x \in A_\alpha \text{ für ein } \alpha \in I\}$$

Vereinigung von (A_α) und

$$\bigcap_{\alpha\in I} A_\alpha := \{x : x \in A_\alpha \text{ für alle } \alpha \in I\}$$

Durchschnitt von (A_α). Insbesondere sind damit für eine Menge von Mengen (einem sogenannten Mengensystem) $\mathcal{F}$ auch

$$\bigcup_{M\in\mathcal{F}} M \qquad \text{und} \qquad \bigcap_{M\in\mathcal{F}} M$$

definiert (hier ist speziell $I = \mathcal{F}$ und $A_M = M$). Man schreibt dann auch kurz $\bigcup\mathcal{F}$ beziehungsweise $\bigcap\mathcal{F}$.

Nach Definition sind zwei Mengen gleich, wenn die erste Teilmenge der zweiten und die zweite Teilmenge der ersten ist. Daher beweist man üblicherweise die Gleichheit, indem man die beiden Inklusionen getrennt nachweist. Wir deuten dies im Weiteren durch die Schreibweise $\subset$: und $\supset$: in den entsprechenden Beweisen an.

Satz A.2 *Es seien X eine Menge, $(A_\alpha)_{\alpha\in I}$ eine Familie von Mengen in X und $B \subset X$. Dann gilt*

$$B \cap \Big(\bigcup_{\alpha\in I} A_\alpha\Big) = \bigcup_{\alpha\in I}(B \cap A_\alpha) \quad \textit{und} \quad B \cup \Big(\bigcap_{\alpha\in I} A_\alpha\Big) = \bigcap_{\alpha\in I}(B \cup A_\alpha).$$

und (**De Morgansche Regeln**)

$$B \setminus (\bigcup_{\alpha\in I} A_\alpha) = \bigcap_{\alpha\in I}(B \setminus A_\alpha) \quad \textit{und} \quad B \setminus (\bigcap_{\alpha\in I} A_\alpha) = \bigcup_{\alpha\in I}(B \setminus A_\alpha).$$

Beweis. Wir werden exemplarisch die Beweise der links stehenden Aussage führen. Die rechten ergeben sich in ähnlicher Weise. Wir schreiben dabei kurz $\bigcup$ statt $\bigcup_{\alpha\in I}$.

$\subset$: Es sei $x \in B \cap (\bigcup A_\alpha)$. Dann ist $x \in B$ und $x \in \bigcup A_\alpha$, also $x \in B$ und $x \in A_\beta$ für ein $\beta \in I$. Damit ist $x \in B \cap A_\beta$, also auch $x \in \bigcup(B \cap A_\alpha)$.
$\supset$: Es sei $x \in \bigcup(B \cap A_\alpha)$. Dann existiert ein $\beta \in I$ mit $x \in B \cap A_\beta$. Damit ist $x \in B$ und $x \in A_\beta$, also auch $x \in B$ und $x \in \bigcup A_\alpha$, das heißt $x \in B \cap (\bigcup A_\alpha)$.
$\subset$: Es sei $x \in B \setminus (\bigcup A_\alpha)$. Dann ist $x \in B$ und $x \notin \bigcup A_\alpha$, also $x \in B$ und $x \notin A_\alpha$ für alle $\alpha \in I$. Damit ist $x \in B \setminus A_\alpha$ für alle $\alpha \in I$, also $x \in \bigcap(B \setminus A_\alpha)$.
$\supset$: Es sei $x \in \bigcap(B \setminus A_\alpha)$. Dann ist $x \in B \setminus A_\alpha$ für alle $\alpha \in I$, also $x \in B$ und $x \notin A_\alpha$ für alle $\alpha \in I$. Damit ist $x \in B$ und $x \notin \bigcup A_\alpha$, das heißt $x \in B \setminus (\bigcup A_\alpha)$. □

Definition A.3 Sind X, Y Mengen und ist $f : X \to Y$, so heißt für $B \subset Y$

$$f^{-1}(B) := \{x \in X : f(x) \in B\}$$

Urbildmenge von B unter f.

Satz A.4 *Es seien X, Y Mengen und $f : X \to Y$.*

1. *Ist $(B_\alpha)_{\alpha \in I}$ eine Familie von Mengen in Y, so gilt*

$$f^{-1}\Big(\bigcup_{\alpha \in I} B_\alpha\Big) = \bigcup_{\alpha \in I} f^{-1}(B_\alpha) \quad \textit{und} \quad f^{-1}\Big(\bigcap_{\alpha \in I} B_\alpha\Big) = \bigcap_{\alpha \in I} f^{-1}(B_\alpha).$$

2. *Ist $(A_\alpha)_{\alpha \in I}$ eine Familie von Mengen in X, so gilt*

$$f\Big(\bigcup_{\alpha \in I} A_\alpha\Big) = \bigcup_{\alpha \in I} f(A_\alpha) \quad \textit{und} \quad f\Big(\bigcap_{\alpha \in I} A_\alpha\Big) \subset \bigcap_{\alpha \in I} f(A_\alpha).$$

Beweis.
1. Wir beschränken uns wieder auf die links stehende Aussage.
$\subset$: Es sei $x \in f^{-1}\big(\bigcup B_\alpha\big)$. Dann ist $f(x) \in \bigcup B_\alpha$, das heißt, es existiert ein $\beta \in I$ mit $f(x) \in B_\beta$. Also ist $x \in f^{-1}(B_\beta)$ und damit auch $x \in \bigcup f^{-1}(B_\alpha)$.
$\supset$: Ist $\beta \in I$, so ist $B_\beta \subset \bigcup B_\alpha$, also auch $f^{-1}(B_\beta) \subset f^{-1}\big(\bigcup B_\alpha\big)$. Da $\beta \in I$ beliebig war, gilt $\bigcup f^{-1}(B_\alpha) \subset f^{-1}\big(\bigcup B_\alpha\big)$.
2. Zur linken Aussage:
$\subset$: Es sei $y \in f\big(\bigcup A_\alpha\big)$. Dann existiert ein $x \in \bigcup A_\alpha$ mit $f(x) = y$. Ist $\beta \in I$ mit $x \in A_\beta$, so ist also $y = f(x) \in f(A_\beta)$. Damit ist $y \in \bigcup f(A_\alpha)$.

$\supset$: Ist $\beta \in I$, so ist $A_\beta \subset \bigcup A_\alpha$, also auch $f(A_\beta) \subset f\big(\bigcup A_\alpha\big)$. Da $\beta \in I$ beliebig war, gilt $\supset$.
Zur rechten Aussage: Es sei $y \in f\big(\bigcap A_\alpha\big)$. Dann existiert ein $x \in \bigcap A_\alpha$ mit $f(x) = y$. Damit ist $y = f(x) \in f(A_\alpha)$ für jedes $\alpha \in I$, d. h. $y \in \bigcap f(A_\alpha)$. □

Bemerkung A.5 Man beachte, dass in der letzten Aussage des zweiten Teils von Satz A.4 kein Gleichheitszeichen steht. Ist etwa $f : \mathbb{Z} \to Z$ definiert durch $f(x) := x^2$ für $x \in \mathbb{Z}$, so gilt

$$f(\{1\} \cap \{-1\}) = f(\varnothing) = \varnothing \quad \text{und} \quad f(\{1\}) \cap f(\{-1\}) = \{1\}.$$

Damit gilt hier keine Gleichheit. Tatsächlich liegt Gleichheit für alle Familien (A_α) genau dann vor, wenn f injektiv ist ([Ü]).

Definition A.6 Es seien A, B beliebige Mengen.
1. A und B heißen **gleichmächtig**, falls eine bijektive Abbildung $\varphi : A \to B$ existiert.[24]
2. Ist A gleichmächtig zu $\{1, \ldots, n\}$ für ein $n \in \mathbb{N}$, so sagt man, dass A die **Mächtigkeit** n hat (man kann zeigen, dass n eindeutig ist). Der leeren Menge wird die Mächtigkeit 0 zugeordnet. Damit heißt A **endlich**, falls A eine Mächtigkeit $n \in \mathbb{N}_0$ hat und **unendlich**, falls dies nicht der Fall ist. Wir schreiben dann $\#A := n$.[25]

Beispiel A.7 Man kann zeigen ([Ü]), dass etwa $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$ gleichmächtig zu $\mathbb{N}$ sind.

Bemerkung und Definition A.8 Es sei X eine Menge. Eine Familie $(A_\alpha)_{\alpha \in I}$ von Mengen in X heißt **disjunkt**, falls $A_\alpha \cap A_\beta = \varnothing$ für $\alpha, \beta \in I$, $\alpha \neq \beta$ gilt. Ist A eine Menge und ist $(A_\alpha)_{\alpha \in I}$ eine disjunkte Familie nichtleerer Mengen mit $A = \bigcup_{\alpha \in I} A_\alpha$, so nennt man $(A_\alpha)_{\alpha \in I}$ eine **Zerlegung** von A. Ist A endlich und $(A_1, \ldots, A_n)$ eine Zerlegung von A, so gilt

$$\#A = \#A_1 + \ldots + \#A_n.$$

[24] d. h. es existiert eine eins-zu-eins Zuordnung zwischen den Elementen aus A und denen aus B.
[25] Ist A unendlich, so schreibt man auch $\#A = \infty$.

B Von den natürlichen zu den reellen Zahlen

In diesem Anhang werden wir auf die axiomatische Einführung der natürlichen Zahlen eingehen und einen darauf basierenden konstruktiven Zugang über die ganzen und die rationalen Zahlen zu den reellen *skizzieren*.
Die **natürlichen Zahlen** können axiomatisch beschrieben werden als Tripel $(\mathbb{N}, 1, \nu)$ mit den drei Eigenschaften (**Peano-Axiome**):

(N1) $\mathbb{N}$ ist eine Menge mit $1 \in \mathbb{N}$.

(N2) $\nu : \mathbb{N} \to \mathbb{N}$ ist eine injektive Funktion mit $1 \notin \nu(\mathbb{N})$.[26]

(N3) (Prinzip der vollständigen Induktion) Ist $A \subset \mathbb{N}$ mit $1 \in A$ und $\nu(A) \subset A$, so ist $A = \mathbb{N}$.

Damit definiert man die arabischen Ziffern durch $2 := \nu(1)$, $3 := \nu(2)$, $4 := \nu(3)$, $5 := \nu(4)$, $6 := \nu(5)$, $7 := \nu(6)$, $8 := \nu(7)$ und $9 := \nu(8)$. Weiter kann man – mit viel Aufwand – zeigen:
Auf $\mathbb{N}$ ist durch $n+1 := \nu(n)$ und $n+\nu(m) := \nu(n+m)$ für $n, m \in \mathbb{N}$ eine assoziative und kommutative Verknüpfung $+$ rekursiv definiert. Unter Verwendung der Addition ist durch $n < m$ falls $m = n + k$ für ein $k \in \mathbb{N}$ zudem eine Ordnungsrelation $<$ auf $\mathbb{N}$ gegeben. Damit kann man wiederum zeigen: Auf $\mathbb{N}$ ist durch $n \cdot 1 := 1$ und $n(m+1) := nm + n$ für $n, m \in \mathbb{N}$ eine assoziative und kommutative Verknüpfung $\cdot$ rekursiv definiert. So wird $(\mathbb{N}, \cdot, 1)$ zu einem abelschen Monoid.
Erweitert man $\mathbb{N}$ um ein Element 0 zu $\mathbb{N}_0$ mit $0 < n$ für alle $n \in \mathbb{N}$ und so, dass $n + 0 := 0 + n := n$ und $n \cdot 0 := 0 \cdot n := 0$ für alle $n \in \mathbb{N}_0$, so ist auch $(\mathbb{N}_0, +, 0)$ ein abelsches Monoid.

Bemerkung B.1 Aus dem Prinzip der vollständigen Induktion folgt die wichtige **Wohlordnungseigenschaft** von $\mathbb{N}_0$ ([Ü]):

Jede nichtleere Menge $M \subset \mathbb{N}_0$ hat ein minimales Element.

Hiermit kann man leicht zeigen: Zu jedem Paar $(n, p) \in \mathbb{N} \times \mathbb{N}$ existiert genau ein Paar $(a, r) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $r < p$ und $n = ap + r$ (Division mit Rest).

Ist $A \subset \mathbb{N}_0$, so heißt ein Tupel $(a_j) = (a_j)_{j \in \mathbb{N}_0} \in A^{\mathbb{N}_0}$ eine **abbrechende Folge** in A, falls ein $d \in \mathbb{N}_0$ existiert mit $a_j = 0$ für $j > d$. Man nennt das kleinste solche d die

[26] Die Zahl $\nu(n)$ nennt man Nachfolger von n. (N2) besagt, dass 1 kein Nachfolger eines $n \in \mathbb{N}$ ist.

Länge von (a_j). Damit gilt folgende wichtige Aussage über die *Darstellung* natürlicher Zahlen:

Satz B.2 *Es seien $q \in \mathbb{N}$ mit $q \geq 2$ und $A := \{a \in \mathbb{N}_0 : a \leq q-1\}$.*[27] *Dann existiert zu jedem $n \in \mathbb{N}_0$ genau ein abbrechende Folge $(a_j(n))$ in A mit*

$$n = \sum_{j=0}^{d(n)} a_j(n) q^j,$$

wobei $d(n)$ die Länge von $(a_j(n))$ ist.

Beweis. 1. Eindeutigkeit: Es seien (b_j), (a_j) abbrechende Folgen in A mit

$$n = \sum_{j=0}^{m} a_j q^j = \sum_{j=0}^{m} b_j q^j.$$

Angenommen es ist $(a_j) \neq (b_j)$, also $J := \{j : a_j \neq b_j\} \neq \varnothing$ (und endlich). Ohne Einschränkung sei $b_N > a_N$, wobei N das maximale $j \in J$ ist. Es gilt ([Ü])

$$\sum_{j=0}^{N-1} a_j q^j < q^N$$

und damit wegen $a_j = b_j$ für $j > N$ und $a_N + 1 \leq b_N$

$$\sum_{j=0}^{m} a_j q^j = \sum_{j=0}^{N-1} a_j q^j + a_N q^N + \sum_{j>N} a_j q^j < (a_N+1) q^N + \sum_{j>N}^{N-1} b_j q^j \leq \sum_{j=0}^{m} b_j q^j.$$

Widerspruch!
2. Wir zeigen die Existenz per Induktion nach n.
Induktionsanfang $n = 0$: Man setze $a_j(0) := 0$ für $j \in \mathbb{N}_0$.
Induktionsschritt $r < n \to n$: Es sei $k \in \mathbb{N}_0$ mit $q^k \leq n < q^{k+1}$. Nach Division mit Rest existieren $0 < a < q$ und $0 \leq r < q^k$ mit

$$n = aq^k + r,$$

[27] A kann als Menge der Ziffern interpretiert werden, eine Art Alphabet der Zahlen.

also insbesondere $r < n$. Nach Induktionsvoraussetzung (die Behauptung gilt für jedes $r < n$) existiert eine Folge $\big(a_j(r)\big)$ mit

$$r = \sum_{j=0}^{d(r)} a_j(r) q^j.$$

Wegen $r < q^k$ ist $d(r) < k$. Setzt man $a_j(n) := a_j(r)$ für $j \neq k$ und $a_k(n) := a$, so ist $n = \sum_{j=0}^{d(n)} a_j(n) q^j$ mit $d(n) = k$. □

Man nennt $(a_{d(n)}(n) a_{d(n)-1}(n) \dots a_0(n))_q$ die **q-adische Darstellung** von n. Im Falle $q = 2$ spricht man dann von der **Binärdarstellung**, im Falle $q = 2{\cdot}5$ von der **Dezimaldarstellung** und im Falle $q = 2^4$ von der **Hexadezimaldarstellung**.[28] Schließlich schreibt man im Dezimalfall auch kurz $a_{d(n)}(n) \dots a_0(n)$ statt $(a_{d(n)}(n) \dots a_0(n))_{2\cdot5}$. So ist etwa für $n = 8 + 8 + 7$

$$n = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (10111)_2$$

und

$$n = 2 \cdot (2 \cdot 5)^1 + 3 \cdot (2 \cdot 5)^0 = (23)_{2\cdot5} = 23\ .$$

Definition B.3 Eine Relation $\sim$ auf X heißt **Äquivalenzrelation**, falls für alle $x, y, z \in X$ gilt

(A1) $x \sim x$ (Reflexivität),

(A2) aus $x \sim y$ folgt $y \sim x$ (Symmetrie),

(A3) aus $x \sim y$ und $y \sim z$ folgt $x \sim z$ (Transitivität).

Ist $\sim$ eine Äquivalenzrelation, so heißt $[x] := [x]_\sim := \{x' \in X : x \sim x'\}$ die von x erzeugte **Äquivalenzklasse** und jedes $x' \in [x]$ ein **Repräsentant** der Äquivalenzklasse $[x]$. Außerdem heißt $X/_\sim := \big\{[x] : x \in X\big\}$ **Quotientenmenge** von X (**modulo** $\sim$).

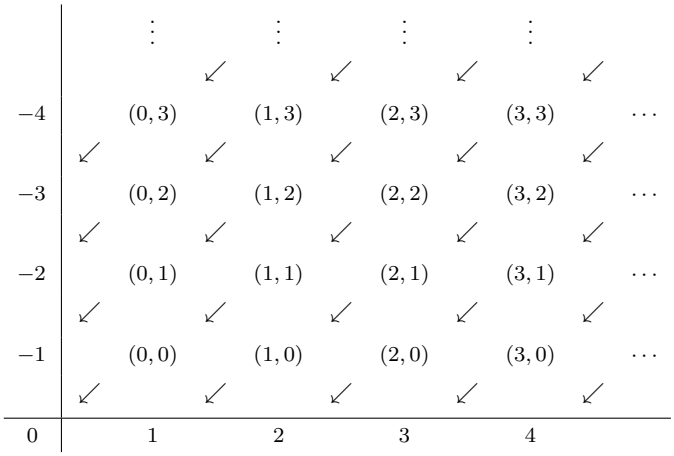
[28] Die Schreibweise $q = 2 \cdot 5$ beziehungsweise $q = 2^4$ mag umständlich erscheinen, ist aber nicht durch $q = 10$ beziehungsweise $q = 16$ ersetzbar, da dies schon die zu definierende Dezimaldarstellung vorwegnehmen würde.

Bemerkung und Definition B.4 Es sei $X = \mathbb{N}_0 \times \mathbb{N}_0$. Durch $(a, b) \sim (a', b')$ falls $a + b' = b + a'$ für $a, b, a', b' \in \mathbb{N}_0$ ist $\sim$ eine Äquivalenzrelation auf X definiert. Ist $a \geq b$, so existiert (genau) ein $n \in \mathbb{N}_0$ mit $a = b + n$ und es gilt damit

$$[(a, b)] = \{(k + n, k) : k \in \mathbb{N}_0\} = [(n, 0)] \ .$$

Ist $a < b$, so ist $b = a + m$ für ein $m \in \mathbb{N}$ und damit

$$[(a, b)] = \{(k, k + m) : k \in \mathbb{N}_0\} = [(0, m)].$$



Definiert man die Menge $\mathbb{Z}$ der **ganzen Zahlen** als

$$\mathbb{Z} := X/_\sim = (\mathbb{N}_0 \times \mathbb{N}_0)/_\sim \ ,$$

so sind durch

$$[(a, b)] + [(c, d)] := [(a + c, b + d)] \quad \text{und} \quad [(a, b)] \cdot [(c, d)] := [(ac + bd, ad + bc)]$$

Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}$ (unabhängig von der Wahl der jeweiligen Repräsentanten) definiert, mit denen $(\mathbb{Z}, +, \cdot)$ zu einem kommutativen Ring wird. Dabei gilt $[(0, n)] = -[(n, 0)]$ für $n \in \mathbb{N}_0$. Indem man n mit $[(n, 0)]$ identifiziert, ist $\mathbb{N}_0$ in $\mathbb{Z}$ eingebettet, und es ergibt sich

$$[(a, b)] = a - b \quad (a, b \in \mathbb{N}_0).$$

Außerdem ist damit durch $a-b < c-d$ definitionsgemäß genau dann, wenn $a+d < b+c$ für $a, b, c, d \in \mathbb{N}_0$ eine Erweiterung der Ordnung $<$ von $\mathbb{N}_0$ auf $\mathbb{Z}$ definiert.

Bemerkung und Definition B.5 Es sei $X := \mathbb{Z} \times \mathbb{Z}^*$. Definiert man $(a, b) \sim (a', b')$ falls $ab' = ba'$ für $(a, b), (a', b') \in X$, so ist $\sim$ eine Äquivalenzrelation auf X. Man kann zeigen: Für $(a, b) \in X$ existieren teilerfremde $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit

$$[(a, b)] = \{(mp, mq) : m \in \mathbb{Z}^*\} = [(p, q)].$$

Definiert man die Menge $\mathbb{Q}$ der **rationalen Zahlen** als

$$\mathbb{Q} := X/_\sim = \big(\mathbb{Z} \times \mathbb{Z}^*\big)/_\sim$$

und Verknüpfungen $+$ und $\cdot$ durch

$$[(a, b)] + [(c, d)] := [(ad + cb, bd)] \quad \text{und} \quad [(a, b)] \cdot [(c, d)] := [(ac, bd)],$$

so wird $(\mathbb{Q}, +, \cdot)$ zu einem Körper. Dabei gilt $1/[(a, b)] = [(b, a)]$ für $a \neq 0$. Durch Identifikation von a und $[(a, 1)]$ ist wieder $\mathbb{Z}$ in $\mathbb{Q}$ eingebettet und es gilt

$$[(a, b)] = [(a, 1)] \cdot [(1, b)] = \frac{[(a, 1)]}{[(b, 1)]} = \frac{a}{b} \qquad ((a, b) \in X).$$

Schließlich erweitert die Definition $a/b < c/d$ falls $ad < bc$ für $a, b \in \mathbb{Z}$ und $b, d \in \mathbb{N}$ (also $b, d > 0$) die Ordnung $<$ von $\mathbb{Z}$ auf $\mathbb{Q}$.

Wir skizzieren zum Abschluss einen möglichen konstruktiven Zugang zu den reellen Zahlen, der an die q-adische Darstellung natürlicher Zahlen anschließt. Basis ist die folgende Beobachtung ([Ü]): Ist $k \in \mathbb{Z}$ und ist $n \geq k$, so gilt

$$\sum_{j=k}^{n-1} a_j q^j \leq q^n - q^k \tag{B.1}$$

für beliebige $a_j \in \{0, \ldots, q - 1\}$.

Bemerkung und Definition B.6 Es seien $q \in \mathbb{N}$, $q \geq 2$ und $A := \{0, 1, \ldots, q - 1\}$. Wir betrachten die Menge der nach oben abbrechenden zweiseitigen Folgen

$$A^{\mathbb{Z})} := \{(a_j) = (a_j)_{j \in \mathbb{Z}} \in A^{\mathbb{Z}} : \text{es existiert ein } d \in \mathbb{N}_0 \text{ mit } a_j = 0 \text{ falls } j > d\}.$$

Man schreibt statt $(a_j) \in A^{\mathbb{Z})}$ komprimierter und suggestiver

$$(a_d a_{d-1} \ldots a_0, a_{-1} a_{-2} \ldots)_q = a_d a_{d-1} \ldots a_0, a_{-1} a_{-2} \ldots .$$

und spricht von einer q-adischen Folge. Im Fall $q = 2$ spricht man von **Binärfolge** und im Fall $q = 2 \cdot 5$ von **Dezimalfolge**. Wir setzen

$$A^{(\mathbb{Z})} := \{(a_j)_{j\in\mathbb{Z}} \in A^{\mathbb{Z})} : \text{es existiert ein } m \in \mathbb{N}_0 \text{ mit } a_j = 0 \text{ falls } j < -m\}$$

und nennen (a_j) **abbrechend**, falls $(a_j) \in A^{(\mathbb{Z})}$ gilt. Aus (B.1) sieht man wie beim Beweis der Eindeutigkeit in Satz B.2, dass die Abbildung

$$A^{(\mathbb{Z})} \ni (a_j) \mapsto \sum_{j=-m}^{d} a_j q^j \in \mathbb{Q}_+ \cup \{0\}$$

injektiv ist. Wir identifizieren im Weiteren die abbrechende Folge (a_j) mit der entsprechenden rationalen Zahl. Weiter definiert man auf $A^{\mathbb{Z})}$ eine Äquivalenzrelation durch $(a_j) \sim (b_j)$ genau dann, wenn $(a_j) = (b_j)$ oder wenn ein $k \in \mathbb{Z}$ so existiert, dass $a_j = b_j$ für $j > k$, $a_k = b_k + 1$ sowie $a_j = 0$ und $b_j = q - 1$ für $j < k$ (oder entsprechend mit vertauschten Rollen von a_j und b_j). Damit sind alle Äquivalenzklassen entweder ein- oder zweielementig, wobei im zweielementigen Fall eine der beiden Folgen abbrechend ist.

Bemerkung B.7 Wir betrachten ab jetzt den Fall $q = 2$ und definieren

$$X := \{x = [(a_j)] : (a_j) \in \{0, 1\}^{\mathbb{Z})}\}.$$

Wählt man im Fall zweielementiger $[(a_j)]$ die abbrechende Folge als Repräsentant, so entspricht jedem $x \in X$ genau eine Binärfolge (a_j). Wenn nichts anderes gesagt ist, legen wir uns auf diese Darstellung fest und schreiben dann auch $x = (a_j)$.
Ist $x = (a_j)$ (in diesem Sinne), so nennen wir für $k \in \mathbb{Z}$ [29]

$$\lfloor x \rfloor_k := \sum_{j\geq k} a_j 2^j \in 2^k \mathbb{N}_0$$

die k-te Abschneidung von x. Unter Verwendung der Relation $<$ auf $\mathbb{Q}_+ \cup \{0\}$ definieren wir eine Relation $<$ auf X durch $x < y$ genau dann, wenn $\lfloor x \rfloor_k < \lfloor y \rfloor_k$ für ein k $\in \mathbb{N}_0$ gilt. Ist dies der Fall, so folgt $\lfloor x \rfloor_n < \lfloor y \rfloor_n$ für alle $n \leq k$ aus (B.1). Man kann zeigen, dass damit $(X, <)$ geordnet ist.
Wesentlich ist nun, dass $(X, <)$ *vollständig* ist.

[29] Ist $\cdot$ eine Verknüpfung auf einer Menge M, so schreiben wir für $B \subset M$ und $a \in M$ kurz $aB := \{ab : b \in B\}$.

Wir deuten den Beweis der Vollständigkeit an. Es sei dazu $M \subset X$ nichtleer und nach oben beschränkt und ohne Einschränkung $M \neq \{0\}$. Wir definieren rekursiv eine Binärfolge (b_j): Zunächst folgt aus der Beschränktheit nach oben von M die Beschränktheit nach oben von

$$\{k \in \mathbb{Z} : \lfloor x \rfloor_k \neq 0 \text{ für ein } x \in M\}$$

in $\mathbb{Z}$. Ist d das Maximum dieser Menge, so setzen wir $b_d := 1$ und $b_j := 0$ für $j > d$. Weiter definieren wir

$$b_{d-1} := \begin{cases} 1, & \text{falls } \lfloor x \rfloor_{d-1} > 2^d \text{ für ein } x \in M \\ 0, & \text{sonst} \end{cases}$$

und entsprechend für $n \in \mathbb{N}$

$$\xi_{d-n-1} := \begin{cases} 1, & \text{falls } \lfloor x \rfloor_{d-n-1} > 2^d + b_{d-1}2^{d-1} + \ldots + b_{d-n}2^{d-n} \text{ für ein } x \in M \\ 0, & \text{sonst} \end{cases}.$$

Ist $s := [(\xi_j)]$, so ergibt sich $s = \sup M$ aus der Konstruktion von s.

Bemerkung B.8 Nun wollen wir in X rechnen. Zunächst setzt man $0 := [(0)_{j\in\mathbb{Z}}]$ und $1 := [(\delta_{j,0})_{j\in\mathbb{Z}}]$. Die Existenz von Suprema ermöglicht es, die Verknüpfungen $+$ und $\cdot$ von $A^{(\mathbb{Z})}$ auf X zu erweitern: Für $x, y \in X$ existieren nämlich

$$x + y := \sup\left\{\lfloor x \rfloor_k + \lfloor y \rfloor_k : k \in \mathbb{Z}\right\} \in X$$

und

$$x \cdot y := \sup\left\{\lfloor x \rfloor_k \cdot \lfloor y \rfloor_k : k \in \mathbb{Z}\right\} \in X,$$

so besteht das Hauptproblem besteht darin, zu zeigen, dass $(X, +, 0)$ ein Monoid und $(X \setminus \{0\}, \cdot, 1)$ eine Gruppe sind. Ist dies getan, so sieht man wie bei der Erweiterung von $\mathbb{N}_0$ zu $\mathbb{Z}$, dass durch

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad a + d = b + c$$

für $(a, b), (c, d) \in X \times X$ eine Äquivalenzrelation auf $X \times X$ definiert ist. Damit setzt man

$$\mathbb{R} := (X \times X)/_\sim$$

und schreibt wieder $a - b$ statt $[(a, b)]$ und im Falle $b = 0$ kurz a sowie im Falle $a = 0$ kurz $-b$. Die Rechenoperationen $+$ und $\cdot$ sowie die Relation $<$ lassen sich auf $\mathbb{R}$ übertragen, und zwar so, dass damit $(\mathbb{R}, +, \cdot, <)$ ein vollständig geordneter Körper wird.[30] Dabei ist $\mathbb{Q}$ monoton eingebettet in $\mathbb{R}$, das heißt, es existiert eine injektive Abbildung $j : \mathbb{Q} \to \mathbb{R}$ so, dass $j(x + y) = j(x) + j(y)$ und $j(xy) = j(x)j(y)$ für alle $x, y \in \mathbb{Q}$ gilt und dass $j(x) < j(y)$ genau dann gilt, wenn $x < y$ ist. Indem man $j(x)$ mit x identifiziert, kann man $\mathbb{Q}$ als Teilmenge von $\mathbb{R}$ auffassen. Man kann zeigen, dass in diesem Sinne den rationalen Zahlen die sogenannten periodischen Binärfolgen entsprechen.

[30] In der Literatur findet man neben axiomatischen Zugängen oft den konstruktiven Zugang über *Dedekindsche Schnitte*. Der Vorteil dieses Zugangs liegt in einer einfacheren Definition des Supremums und einem weniger aufwändigen Nachweis der Körperaxiome, allerdings sind die dabei betrachteten Objekte, die am Ende als reelle Zahlen bezeichnet werden, weniger instruktiv als die oben eingeführten Binärfolgeen. Außerdem knüpft die Vorstellung einer reellen Zahl als Binärfolge meist an die Vorkenntnisse aus der Schule an und deutet zudem Problematiken der Gleitkommaarithmetik und der Struktur der Maschinenzahlen an.

Index