Skriptum zur Analysis I

SS 2007 — TU Darmstadt

Karl – Hermann Neeb

I. Logik und Mengenlehre

Gegenstand der Analysis I ist die Menge $\mathbb{R}$ der reellen Zahlen und die Funktionen $f:\mathbb{R} \to \mathbb{R}$. Um mit diesen Begriffen systematisch und präzise umgehen zu können, benötigen wir eine Sprache. Die Sprache der Mathematik ist die *Mengenlehre*. Wie man mit mathematischen Sachverhalten umgeht, lehrt uns die *Logik*. Sie spielt die Rolle der *Grammatik* der Mathematik.

I.1 Quantoren und Aussagenlogik

Die Logik handelt von Aussagen, die nach gewissen Regeln aus bestimmten Zeichen aufgebaut werden. Wir betrachten eine Aussage als *wohlgeformt*, wenn sich „entscheiden" lässt, ob sie wahr oder falsch ist. Wohlgeformte Aussagen sind beispielsweise

1) 0 ist eine ganze Zahl.
2) $2+2=5$.
3) $a+a=2a$ gilt für jede ganze Zahl a.

Keine wohlgeformte Aussage hingegen ist etwa

$?!\,a = x + \diamond$.

Vorsicht: Wir stellen uns hiermit auf einen naiven Standpunkt. Die Wahrheit einer Aussage kann nämlich von gewissen Grundannahmen abhängen, die man *Axiome* nennt. Wenn im folgenden von Aussagen die Rede ist, sind damit immer wohlgeformte Aussagen gemeint.

Definition I.1.1. Seien p und q Aussagen. Wir bilden:

(i) *Negation:* $\neg p$ (nicht p) ist genau dann wahr, wenn p falsch ist.
(ii) *Konjunktion:* $p \wedge q$ (p und q) ist genau dann wahr, wenn p und q wahr sind.
(iii) *Disjunktion:* $p \vee q$ (p oder q) ist genau dann wahr, wenn p oder q wahr ist (dies ist kein ausschließliches „oder“).
(iv) *Implikation:* $p \Rightarrow q$ (p impliziert q; aus p folgt q) ist definiert als $(\neg p) \vee q$. Die Wahrheit dieser Aussage ist gleichbedeutend mit „Wenn p wahr ist, dann ist auch q wahr“ (Nachweis!)
(v) *Äquivalenz:* $p \Longleftrightarrow q$ (p ist äquivalent zu q) genau dann, wenn beide wahr oder beide falsch sind. ■

Die Wahrheitswerte der oben definierten verknüpften Aussagen sind in der folgenden Wahrheitstafel zusammengefasst:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Longleftrightarrow q$
W	W	F	W	W	W	W
W	F	F	F	W	F	F
F	W	W	F	W	W	F
F	F	W	F	F	W	W

■

Die folgenden Merkregeln verifiziert man direkt durch Aufstellen der jeweiligen Wahrheitstafel.

MERKREGELN FÜR DEN UMGANG MIT LOGISCHEN OPERATOREN

Bemerkung I.1.2.
(a) Doppelte Verneinung bejaht: $\neg(\neg p) \Longleftrightarrow p$. Diese Aussage ist unabhängig von p wahr. Solche Aussagen nennt man *allgemeingültig*.
(b) Negation vertauscht $\wedge$ und $\vee$: (*de Morgansche Regeln*):

$$\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q \quad \text{und} \quad \neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q.$$

(c) Wir schreiben **W** bzw. **F** für die Aussage, die immer wahr bzw. immer falsch ist. Dann gilt für jede Aussage p:

$$p \wedge \mathbf{F} \Longleftrightarrow \mathbf{F}, \quad p \vee \mathbf{F} \Longleftrightarrow p \quad \text{und} \quad p \wedge \mathbf{W} \Longleftrightarrow p, \quad p \vee \mathbf{W} \Longleftrightarrow \mathbf{W}.$$

Dies sind also 4 allgemeingültige Aussagen.
(d) Logische Distributivgesetze: Für Aussagen p, q, r gelten:

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r) \quad \text{und} \quad p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r).$$ ■

Bemerkung I.1.3. (Regeln für logisches Schließen)
(1) *Direkter Schluss:*

$$(p \wedge (p \Rightarrow q)) \Longrightarrow q$$

Ist p wahr und impliziert p die Aussage q (d.h. folgt aus der Wahrheit von p die Wahrheit der Aussage q), so ist q wahr. Die Allgemeingültigkeit dieser Aussage verifiziert man direkt anhand der Tabelle.
Beispiel: Es ist sehr instruktiv, sich diesen Schluß an einem Beispiel klarzumachen:
p: Es ist Montag.
q: Es regnet heute.
$p \Rightarrow q$: Es regnet an jedem Montag.

Die Schlussweise besagt also: „Wenn heute Montag ist" und „Wenn es jeden Montag regnet", dann „regnet es heute".
(2) $(\neg q \wedge (p \Rightarrow q)) \Longrightarrow \neg p$
Im Beispiel: „Wenn es heute nicht regnet und wenn es jeden Montag regnet, dann ist heute nicht Montag."
(3) *Kontraposition*:

$$(p \Rightarrow q) \Longleftrightarrow (\neg q \Rightarrow \neg p).$$

Im Beispiel: „Es regent jeden Montag" $\Longleftrightarrow$ „Wenn es nicht regnet, ist es nicht Montag".
(4) *Schlussketten*: In der Notation logischer Schlüsse verwenden wir zwei Typen von Schlussketten: In einer Schlusskette des Typs

$$p_1 \Longleftrightarrow p_2 \Longleftrightarrow \ldots \Longleftrightarrow p_n$$

verstehen wir das Zeichen $\Longleftrightarrow$ als ein Symbol, das uns signalisiert, dass alle Aussagen $p_1 \Longleftrightarrow p_2$, $p_2 \Longleftrightarrow p_3$ usw. wahr sind. Man sagt auch, dass die Aussagen durch *Äquivalenzumformungen* auseinander hervorgehen. Insbesondere gilt dann $p_1 \Longleftrightarrow p_n$. Zum Beispiel folgt die Gültigkeit von (3) unter Verwendung der doppelten Verneinung (I.1.2(a)) aus folgender Kette von Äquivalenzen:

$$(p \Rightarrow q) \Longleftrightarrow (\neg p) \vee q \Longleftrightarrow q \vee (\neg p) \Longleftrightarrow (\neg q \Rightarrow \neg p).$$

Entsprechend verwenden wir das Symbol $\Rightarrow$. In einer Schlusskette des Typs

$$p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n$$

bedeutet es, dass alle Aussagen $p_1 \Rightarrow p_2$, $p_2 \Rightarrow p_3$ usw. wahr sind. Insbesondere gilt dies dann für $p_1 \Rightarrow p_n$. ■

Bemerkung I.1.4. (Formale Struktur mathematischer Beweise) Typischerweise haben mathematische Sätze die Gestalt:

$$p \Longrightarrow q.$$

In einem Beweis geht es also um die Verifikation einer solchen Aussage. Es gibt mehrere Möglichkeiten des Vorgehens:
(1) *direkter Beweis:* Man nimmt an, die *Voraussetzung* p sei wahr und schließt hieraus, dass q wahr ist (siehe I.1.1(iv)).
(2) Für den *indirekten Beweis* gibt es zwei Varianten, die auf den Äquivalenzen

$$(p \Rightarrow q) \quad \Longleftrightarrow \quad (\neg q \Rightarrow \neg p) \Longleftrightarrow \neg(p \wedge \neg q)$$

beruhen.

(a) Man nimmt an, dass q falsch ist und leitet daraus ab, dass p falsch ist.

(b) Die andere Variante besteht darin anzunehmen, dass p wahr ist und q falsch und daraus einen Widerspruch herzuleiten. Hiermit ist die Wahrheit der Aussage $\neg(p \wedge \neg q)$ bewiesen und damit $p \Rightarrow q$. ■

Die *Menge der natürlichen Zahlen* sei mit

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

bezeichnet. (":= bedeutet hier *definierte Gleichheit*, oben wird also die Menge $\mathbb{N}$ definert.)

Wir betrachten ein erstes Beispiel für einen indirekten Beweis.

Satz I.1.5. *Ist n eine durch 4 teilbare natürliche Zahl, so ist $n + 3$ keine Quadratzahl.*

Beweis. (Indirekter Beweis) Wir nehmen an, $n+3$ sei eine Quadratzahl, d.h., es gibt eine natürliche Zahl k mit $n + 3 = k^2$.
1. Fall: k ist gerade, d.h., es gibt eine natürliche Zahl m mit $k = 2m$. Dann ist $k^2 = 4m^2$ durch 4 teilbar und folglich $n = k^2 - 3$ nicht durch 4 teilbar.
2. Fall: k ist ungerade, d.h., es gibt eine natürliche Zahl m mit $k = 2m + 1$. Dann ist $k^2 = 4m^2 + 4m + 1$, d.h. $k^2 - 1$ ist durch 4 teilbar, also $n = k^2 - 3 = (k^2 - 1) - 2$ nicht. ■

Definition I.1.6. (Quantoren)
(1) *Der Allquantor:* Sei J eine Menge (vgl. hierzu den nächsten Abschnitt) und $(p_j)_{j \in J}$ eine *Familie von Aussagen*, d.h., für jedes $j \in J$ ist p_j eine Aussage. Dann ist

$$(\forall j \in J)\, p_j$$

die Aussage, die genau dann wahr ist, wenn p_j für alle $j \in J$ wahr ist.

Beispiele:

(a) $(\forall n \in \mathbb{N})\, \underbrace{\text{„}n \text{ ist gerade“}}_{p_n}$ ist falsch, da 3 nicht gerade ist.

(b) $(\forall n \in \mathbb{N})\, n \leq n^2$ ist wahr.

(2) *Der Existenzquantor:* Ist $(p_j)_{j \in J}$ eine Familie von Aussagen, so ist

$$(\exists j \in J)\, p_j$$

die Aussage, die genau dann wahr ist, wenn ein $j_0 \in J$ so existiert, dass p_{j_0} wahr ist.

Beispiele:

(a) $(\exists n \in \mathbb{N})$ „ n ist gerade“ ist wahr.

(b) $(\exists n \in \mathbb{N})$ „ n ist Primzahl“ ist ebenfalls wahr.

(3) *Verschärfter Existenzquantor:* Die Aussage

$$(\exists! j \in J)\, p_j$$

bedeutet: Es existiert *genau* ein $j_0 \in J$, so dass p_{j_0} wahr ist.

Beispiele:

(a) $(\exists! n \in \mathbb{N})$ „ n ist gerade“ ist falsch.

(b) $(\exists! n \in \mathbb{N})$ $n^3 = 27$ ist wahr. ■

Bemerkung I.1.7. (Merkregeln für den Umgang mit Quantoren)

(a) Die Entsprechungen der *de Morganschen Regeln* für Quantoren sind

$$\neg\Big((\forall j \in J)\, p_j\Big) \iff (\exists j \in J)\, \neg p_j \quad \text{und} \quad \neg\Big((\exists j \in J)\, p_j\Big) \iff (\forall j \in J)\, \neg p_j .$$

(b) Man darf Existenz- und Allquantor im allgemeinen nicht vertauschen:

$$\underbrace{(\forall n \in \mathbb{N})(\exists k \in \mathbb{N})\, n \leq k}_{W} \;\not\Longleftrightarrow\; \underbrace{(\exists k \in \mathbb{N})(\forall n \in \mathbb{N})\, n \leq k}_{F} .$$

I.2 Mengenlehre

Dem Begriff der Menge stellen wir uns naiv gegenüber, d.h., wir stellen uns auf den Standpunkt, dass wir eine Menge kennen, wenn uns gesagt wird, welche Elemente sie enthält. Wie kann das aussehen?

Ist M eine Menge, so schreiben wir

$$x \in M$$

für die Aussage, die genau dann wahr ist, wenn x Element der Menge M ist, und

$$x \notin M :\Leftrightarrow \neg(x \in M).$$

Hierbei verwenden wir das Symbol $:\Leftrightarrow$ für *definierte Äquivalenz.* Durch obige Zeile wird die Bedeutung des Symbols $\notin$ definiert.

Definition I.2.1. (Beschreibung von Mengen)

(1) (Aufzählung der Elemente) Eine Menge kann durch Aufzählung ihrer Elemente beschrieben werden:

$M = \{4, 6, *\}$, $N = \{+, -, 8\}$.

$\mathbb{N} = \{1, 2, 3, \dots\}$ — Die Menge der *natürlichen Zahlen*

$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ — Die Menge der *ganzen Zahlen*

Beachte: $\{1, 2, 3, 2\} = \{1, 2, 3\}$.

Eine andere Möglichkeit besteht in der Beschreibung durch andere Mengen:

$\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}\}$ — Die Menge der *rationalen Zahlen*

(2) (Aussonderung) Die Elemente einer Menge können durch eine *Aussageform* spezifiziert werden: Zu jedem Element x einer Menge M sei uns eine Aussage $p(x)$ gegeben. Wir nennen das Symbol $p(x)$ dann eine *Aussageform* und x die *freie Variable* in $p(x)$. Wir können hiermit die Menge

$$N := \{x \in M : p(x)\} := \{x \in M : p(x) \text{ ist wahr}\}$$

bilden. Sie enthält genau die Elemente x von M, für die die Aussage $p(x)$ wahr ist. Genau wie bei der Definition der Quantoren, kann man $(p(x))_{x\in M}$ auch als eine Familie von Aussagen auffassen. ■

Beispiele:

a) Die Menge der geraden Zahlen

$$G = \{n \in \mathbb{N} : (\exists m \in \mathbb{N})\, n = 2m\} = \{n \in \mathbb{N} : n \text{ ist gerade}\}$$

Hier ist $p(n)$ die Aussage „ $(\exists m \in \mathbb{N})\, n = 2m$ “ bzw. „ n ist gerade“.

b) Die Menge aller Primzahlen

$$P = \{n \in \mathbb{N} : n \text{ ist Primzahl}\}.$$

Hier ist $p(n)$ die Aussage „ n ist Primzahl“. ■

Bemerkung I.2.2. Die Einschränkung $x \in M$ in Definition I.2.1(2) ist wesentlich, da sie unerlaubte Konstruktionen wie die folgende ausschließt:

$$R := \{x : x \notin x\} \text{ — die sogenannte } \textit{Russelsche Unmenge.}$$

Diese Definition führt zu einem Widerspruch (der Russelschen Antinomie[1]), wenn man fragt, ob die Menge R selbst Element von R ist:

- Ist $R \in R$, so folgt aus der definierenden Eigenschaft der Menge R, dass $R \notin R$ ist – Widerspruch; und

[1] Bertrand Russel (1872–1969), englischer Mathematiker, Logiker und Philosoph.

- ist $R \notin R$, so gilt die definierende Eigenschaft der Menge R für R, so dass $R \in R$ gilt – Widerspruch!

Diese Art von Konstruktion weist auf Probleme hin, die man erhält, wenn man Mengen von Mengen betrachtet. Insbesondere gilt:

Es gibt keine „Menge aller Mengen“! ■

Definition I.2.3. (1) $A \subseteq B$ (A ist *Teilmenge von* B) bedeutet $x \in A \Rightarrow x \in B$.
(2) $A = B :\iff \big((x \in A) \iff (x \in B)\big)$, d.h., zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten. Man beachte

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

(3) $\emptyset$: Die *leere Menge*. Sie enthält keine Elemente; die Aussage $x \in \emptyset$ ist immer falsch bzw. $x \in \emptyset \iff \mathbf{F}$. ■

In der folgenden Definition stellen wir zusammen, wie wir aus Mengen neue Mengen konstruieren dürfen. Dass hierbei Vorsicht geboten ist, zeigt die Russelsche Antinomie.

Definition I.2.4. (Konstruktion neuer Mengen) Seien X und Y Mengen.

(i) *Das Komplement von Y in X* beschreiben wir durch Aussonderung:

$$X \setminus Y := \{x \in X : x \notin Y\}$$

(ii) *Die Vereinigung zweier Mengen*

$$X \cup Y := \{x : x \in X \vee x \in Y\}$$

lässt sich nicht durch Aussonderung beschreiben.

(iii) *Den Durchschnitt zweier Mengen* beschreiben wir wieder durch Aussonderung:

$$X \cap Y := \{x \in X : x \in Y\} = \{x : x \in X \wedge x \in Y\}$$

(iv) *Beliebige Durchschnitte und Vereinigungen:* Ist $\{A_j : j \in J\}$ eine Menge von Mengen, so definieren wir

$$\bigcup_{j \in J} A_j := \{x : (\exists j \in J)\ x \in A_j\}$$

Dann ist $x \in \bigcup_{j \in J} A_j \Leftrightarrow (\exists j \in J)\ x \in A_j$. Ist $J = \emptyset$, so ist diese Aussage immer falsch und daher $\bigcup_{j \in J} A_j = \emptyset$. Analog definieren wir für eine nichtleere (Index-)Menge J:

$$\bigcap_{j \in J} A_j := \{x : (\forall j \in J)\ x \in A_j\}.$$

Für endliche Mengen $J = \{1, 2, 3, \dots, n\}$ schreibt man auch

$$\bigcup_{j=1}^{n} A_j = \bigcup_{j \in J} A_j = A_1 \cup A_2 \cup \dots \cup A_n$$

bzw.

$$\bigcap_{j=1}^{n} A_j = \bigcap_{j \in J} A_j = A_1 \cap A_2 \cap \dots \cap A_n.$$

(v) *Die Produktmenge:* Für $x \in X$ und $y \in Y$ nennt man eine geordnete Auflistung (x, y) ein *Paar*. Die Menge

$$X \times Y := \{(x, y) : x \in X \wedge y \in Y\}$$

heißt *Produktmenge* (kartesisches Produkt) von X und Y.

Folgende Konstruktion ist etwas allgemeiner. Sind $A_1, \dots, A_n$ Mengen und $a_1 \in A_1, \dots, a_n \in A_n$, so heißt die geordnete Liste $(a_1, a_2, \dots, a_n)$ ein n-*Tupel* (2-Tupel sind *Paare*; 3-Tupel werden *Tripel* genannt). Man definiert dann

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) : a_1 \in A_1 \wedge \dots \wedge a_n \in A_n\}.$$

Für $A_1 = A_2 = \dots = A_n$ schreibt man auch

$$A^n := A_1 \times \dots \times A_n = \underbrace{A \times \dots \times A}_{\text{n Faktoren}}.$$

Beispiele:

a) $\mathbb{Z}^3 := \{(n, m, k) : n, m, k, \in \mathbb{Z}\}$

b) Die Mengen $A := \{\star, \circ\}$ und $B := \{\bullet, 1\}$ liefern

$$A \times B = \{(\star, \bullet), (\star, 1), (\circ, \bullet), (\circ, 1)\}.$$

(vi) *Die Potenzmenge:* Ist A eine Menge, so heißt

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

die *Potenzmenge* von A. Sie enthält alle Teilmengen von A.

Beispiel: Für $A = \{0, 1\}$ ist $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Beachte: Für jede Menge A gilt $\emptyset \subseteq A$. ∎

I.3 Funktionen

Seien X und Y Mengen. Eine naive Definition einer Funktion bzw. Abbildung $f\colon X \to Y$ könnte beispielsweise so aussehen: „Eine *Funktion* $f\colon X \to Y$ ist eine Vorschrift, die jedem Element von X genau ein Element von Y zuordnet“. Hierbei haben wir zuerst zu klären, was man unter einer „Vorschrift“ versteht.

Definition I.3.1. Es seien X und Y Mengen. Eine *Funktion* (*Abbildung*) f ist ein Tripel (X, Y, Γ_f), bestehend aus den Mengen X, Y und einer Teilmenge $\Gamma_f \subseteq X \times Y$, für die gilt:

$$(\forall x \in X)(\exists! y \in Y)\,(x,y) \in \Gamma_f.$$

Bezeichnungen:

1) Ist $(x,y) \in \Gamma_f$, so heißt $f(x) := y$ *Funktionswert an der Stelle* x; man schreibt auch $x \mapsto f(x)$, womit suggeriert wird, dass dem Element $x \in X$ das Element $f(x)$ aus Y zugeordnet wird.
2) X heißt *Definitionsbereich.*
3) Y heißt *Werte-* oder *Bildbereich.*
4) Γ_f heißt *Graph* der Funktion.

Zwei Funktionen sind also genau dann gleich, wenn ihre Definitionsbereiche, Wertebereiche und Graphen übereinstimmen.

5) Man schreibt $f\colon X \to Y$ für Funktionen der Gestalt (X, Y, Γ_f), d.h. mit Definitionsbereich X und Bildbereich Y.
6) Die Menge $f(X) := \{y \in Y\colon (\exists x \in X)\, y = f(x)\}$ heißt *Bild von* f.
   Für eine Teilmenge $A \subseteq X$ heißt
   $$f(A) := \{y \in Y\colon (\exists x \in A)\, y = f(x)\}$$
   das *Bild von* A unter f.
   Für $B \subseteq Y$ heißt
   $$f^{-1}(B) := \{x \in X\colon f(x) \in B\}$$
   das *Urbild von* B.
   Für $B = \{y\} \subseteq Y$ schreiben wir kürzer $f^{-1}(y) := f^{-1}(\{y\})$. ■

Beispiel I.3.2. Sei $X = Y = \mathbb{Q}$.

(a) $f(x) = x^2 + 5$ hat den Graphen $\Gamma_f = \{(x,y) \in \mathbb{Q}^2\colon y = x^2 + 5\}$.
(b) $f(x) = x + 1$ hat den Graphen $\Gamma_f = \{(x,y)\colon y = x + 1\}$.
(c) Es gibt keine Funktion $f\colon \mathbb{Q} \to \mathbb{Q}$, deren Graph die Menge $\Gamma = \{(x,y) \in \mathbb{Q}^2\colon y^2 = x\}$ ist (Skizze!).

(d) Funktionen müssen nicht immer auf Zahlenmengen definiert sein; eine durchaus sinnvolle Funktion ist etwa:

$$f\colon \{\text{Menschen}\} \to \mathbb{N}_0, \quad x \mapsto \text{ Alter von } x. \qquad \blacksquare$$

Definition I.3.3. (1) *Die identische Funktion auf der Menge* X *:*

$$\mathrm{id}_X = (X, X, \Gamma_{\mathrm{id}_X}),$$

wobei der Graph $\Gamma_{\mathrm{id}_X} = \{(x,y) \in X \times X \colon x = y\}$ die *Diagonale* ist. Wir haben also $\mathrm{id}_X(x) = x$ für alle $x \in X$.

(2) *Die konstante Funktion/Abbildung* auf $y_0 \in Y$ ist durch $f\colon X \to Y, f(x) = y_0$ für alle $x \in X$ definiert. Ihr Graph ist die Menge $\Gamma_f = \{(x, y_0) \colon x \in X\}$ (Skizze!).

(3) Eine Möglichkeit, aus einer schon vorhandenen Funktion eine neue zu gewinnen, ist die *Restriktion* oder *Einschränkung* einer Funktion auf eine Teilmenge ihres Definitionsbereichs: Ist $f\colon X \to Y$ eine Funktion und $A \subseteq X$, so wird durch

$$f|_A\colon A \to Y, \quad x \mapsto f(x)$$

die *Einschränkung von* f *auf* A definiert. Der Graph dieser Funktion ist

$$\Gamma_{f|A} = \Gamma_f \cap (A \times Y) = \{(x,y) \in A \times Y \colon y = f(x)\} \subseteq \Gamma_f. \qquad \blacksquare$$

Bei einer Funktion $f\colon X \to Y$ wird jedem $x \in X$ *genau* ein $f(x) \in Y$ zugeordnet. Für ein $y \in Y$ kann es aber mehrere Urbilder geben. Man unterscheidet daher mehrere Typen von Funktionen:

Definition I.3.4. Eine Funktion $f\colon X \to Y$ heißt

(a) *injektiv*, wenn jedes $y \in Y$ höchstens ein Urbild hat, d.h.

$$(\forall x \in X)(\forall x' \in X)\, f(x) = f(x') \Longrightarrow x = x'.$$

(b) *surjektiv*, wenn jedes $y \in Y$ mindestens ein Urbild hat, d.h.

$$(\forall y \in Y)(\exists x \in X)\, y = f(x),$$

d.h. $f(X) = Y$.

(c) *bijektiv*, wenn jedes $y \in Y$ genau ein Urbild hat, d.h. wenn f injektiv und surjektiv ist. $\blacksquare$

Die Surjektivität von f besagt, dass die Gleichung $f(x) = y$ für jedes $y \in Y$ lösbar ist, wohingegen die Injektivität die Eindeutigkeit der Lösung bedeutet (sofern sie existiert).

Beispiel I.3.5.

(a) Die Funktion

$$f\colon \mathbb{N} \to \mathbb{N}, n \mapsto n+1$$

ist injektiv, aber nicht surjektiv.

(b) Die Funktion

$$f\colon \mathbb{N} \to \mathbb{N}, n \mapsto \begin{cases} n-1, & \text{falls } n \geq 2 \\ 1, & \text{falls } n = 1 \end{cases}$$

ist surjektiv, aber nicht injektiv (denn $f(2) = f(1) = 1$).

(c) Die Funktion

$$f\colon \mathbb{Z} \to \mathbb{Z}, n \mapsto n^2$$

ist weder injektiv noch surjektiv. ∎

Umkehrfunktionen

Sind X und Y zwei Mengen und ist $R \subseteq X \times Y$, so setzen wir

$$R^{-1} := \{(y,x) \in Y \times X\colon (x,y) \in R\}.$$

Eine Teilmenge $R \subseteq X \times Y$ nennt man eine *Relation* (zwischen X und Y).

Satz I.3.6. *Für eine Funktion $f\colon X \to Y$ sind die folgenden Aussagen äquivalent:*

(1) *f ist bijektiv.*

(2) *Die Relation $(\Gamma_f)^{-1} \subseteq Y \times X$ t der Graph einer Funktion $g\colon Y \to X$, d.h. das Tripel $\big(Y, X, (\Gamma_f)^{-1}\big)$ ist eine Funktion.*

Beweis. Das Tripel $(Y, X, (\Gamma_f)^{-1})$ ist genau dann eine Funktion, wenn es zu jedem $y \in Y$ genau ein $x \in X$ mit $(y,x) \in (\Gamma_f)^{-1}$ gibt. Dies ist nach der Definition von $(\Gamma_f)^{-1}$ genau dann der Fall, wenn es zu jedem $y \in Y$ genau ein $x \in X$ mit $(x,y) \in \Gamma_f$ gibt. Dies wiederum ist äquivalent zur Existenz genau eines $x \in X$ mit $y = f(x)$ für jedes $y \in Y$, was heißt, dass f bijektiv ist. ∎

Definition I.3.7. Erfüllt $f\colon X \to Y$ die Bedingungen von Satz I.3.6, so schreiben wir $f^{-1} := (Y, X, (\Gamma_f)^{-1})$ (bzw. $f^{-1}\colon Y \to X$) für die Funktion mit dem Graphen $\Gamma_{f^{-1}} = (\Gamma_f)^{-1}$. Sie heißt *Umkehrfunktion von f*.

Für $x \in X$ und $y \in Y$ ist $(x,y) \in \Gamma_f$ äquivalent zu $f(x) = y$ und $f^{-1}(y) = x$. Insbesondere gilt

$$f^{-1}(f(x)) = x \quad \text{und} \quad f(f^{-1}(y)) = y.$$

Beachte: Für jede Funktion $f\colon X \to Y$ und jede Teilmenge $B \subseteq Y$ ist die Urbildmenge $f^{-1}(B)$ immer definiert; ob f bijektiv ist oder nicht. In diesem Sinne verwenden wir das Symbol f^{-1} also auch, wenn keine Umkehrfunktion zu f existiert. ∎

Beispiel I.3.8. Für die Funktion $f\colon \mathbb{Q} \to \mathbb{Q}, f(x) = 3x+2$ ist die Umkehrfunktion f^{-1} gegeben durch $f^{-1} : \mathbb{Q} \to \mathbb{Q}, f^{-1}(y) = \frac{y-2}{3}$. ■

Definition I.3.9. Sind $f\colon X \to Y$ und $g\colon Y \to Z$ Funktionen, so wird durch

$$g \circ f\colon X \to Z, \quad x \mapsto g(f(x))$$

eine Funktion definiert (Nachweis!). Sie heißt die *Komposition* (*Verknüpfung*) der Funktionen f und g. ■

Bemerkung I.3.10. (a) Ist eine Funktion $f\colon X \to Y$ bijektiv, so gilt

$$f \circ f^{-1} = \mathrm{id}_Y \quad \text{und} \quad f^{-1} \circ f = \mathrm{id}_X .$$

Das folgt sofort aus den beiden Formeln in Definition I.3.7.

(b) Für

$$f\colon \mathbb{Q} \to \mathbb{Q}, \quad x \mapsto 3x+1 \quad \text{und} \quad g\colon \mathbb{Q} \to \mathbb{Q}, \quad x \mapsto x^2 - 1$$

ist

$$g \circ f\colon \mathbb{Q} \to \mathbb{Q}, \quad x \mapsto (3x+1)^2 - 1 = 9x^2 + 6x$$

und

$$f \circ g\colon \mathbb{Q} \to \mathbb{Q}, \quad x \mapsto 3(x^2 - 1) + 1 = 3x^2 - 2.$$

Insbesondere erkennt man an diesem Beispiel, dass für zwei Funktionen $f, g\colon \mathbb{Q} \to \mathbb{Q}$ im allgemeinen $f \circ g \neq g \circ f$ gilt. ■

Aufgabe I.3.1. (a) Sind $f\colon X \to Y$ und $g\colon Y \to Z$ injektive (surjektive) Funktionen, so ist auch deren Komposition $g \circ f\colon X \to Z$ injektiv (surjektiv).

(b) Ist $f\colon X \to \emptyset$ eine Funktion, so ist $X = \emptyset$.

(c) Für jede Menge Y ist $f = (\emptyset, Y, \emptyset)$ eine Funktion. Ihr Graph Γ_f ist die leere Menge. Man beachte, dass auch die Menge $\emptyset \times Y$ leer ist. ■

Aufgabe I.3.2. Seien X und Y Mengen sowie $f\colon X \to Y$ eine Funktion und

$$f^*\colon \mathcal{P}(Y) \to \mathcal{P}(X), \quad A \mapsto f^{-1}(A)$$

die Funktion, die jeder Teilmenge von Y ihr Urbild in X zuordnet. Zeigen Sie:

(1) f ist genau dann injektiv, wenn f^* surjektiv ist.

(2) f ist genau dann surjektiv, wenn f^* injektiv ist. ■

Aufgabe I.3.3. (a) Zeige: Sei X eine nichtleere Menge. Eine Funktion $f\colon X \to Y$ ist genau dann injektiv, wenn eine Funktion $g\colon Y \to X$ so existiert, dass

$$g \circ f = \mathrm{id}_X .$$

(b) Zeige: Eine Funktion $f\colon X \to Y$ ist genau dann surjektiv, wenn eine Funktion $g\colon Y \to X$ existiert, so dass

$$f \circ g = \mathrm{id}_Y .$$

(c) Zeige: Eine Funktion $f\colon X \to Y$ ist genau dann bijektiv, wenn eine Funktion $g\colon Y \to X$ existiert, so dass

$$f \circ g = \mathrm{id}_Y \quad \text{und} \quad g \circ f = \mathrm{id}_X . \qquad \blacksquare$$

Aufgabe I.3.4. (Komposition von Funktionen ist assoziativ) Zeige: Sind $f\colon X \to Y$, $g\colon Y \to Z$ und $h\colon Z \to U$ Funktionen, so gilt

$$(h \circ g) \circ f = h \circ (g \circ f). \qquad \blacksquare$$

Mächtigkeit von Mengen

Definition I.3.11. (a) Zwei Mengen X und Y heißen *gleichmächtig*, wenn es eine bijektive Funktion $F\colon X \to Y$ gibt. Zwei Mengen X und Y sind also genau dann gleichmächtig, wenn es möglich ist, jedem Element $x \in X$ genau ein Element $y \in Y$ derart zuzuordnen, dass jedes Element von Y genau einem Element von x zugeordnet ist. Man stellt sich vor, dass die beiden Mengen X und Y dann „gleichviele“ Elemente enthalten, wieviele es auch sein mögen.

(b) Eine Menge X heißt *endlich*, wenn sie leer ist oder ein $n \in \mathbb{N}$ existiert, so dass X gleichmächtig is zu $\{1, \ldots, n\}$, d.h., es existiert eine bijektive Funktion

$$f\colon \{1, 2, \ldots, n\} \to X.$$

Für $x_i := f(i)$ ist dann $X = \{x_1, \ldots, x_n\}$. In diesem Fall schreiben wir $|X| = n$ und nennen diese Zahl die *Kardinalität (Mächtigkeit) von* X.

Um einzusehen, dass die Definition der Kardinalität sinnvoll ist, hat man zu zeigen, dass n durch die Menge X eindeutig bestimmt ist, also dass aus der Existenz von Bijektionen

$$\{1, 2, \ldots, n\} \to X \to \{1, 2, \ldots, m\}$$

schon $n = m$ folgt (Nachweis als Übung! Hinweis: Man argumentiere, dass $n \leq m$ und $m \leq n$ gelten).

(c) Eine Menge X heißt *abzählbar*, wenn sie leer ist, oder es eine surjektive Funktion $f\colon \mathbb{N} \to X$ gibt, d.h. wenn man die Elemente von X „abzählen“ kann: $X = \{f(1), f(2), \ldots\}$ bzw. $X = \{x_1, x_2, x_3, \ldots\}$. Wenn X nicht abzählbar ist, so nennen wir X *überabzählbar*. ■

Bemerkung I.3.12. (a) Ist X eine abzählbare Menge und $f: X \to Y$ eine surjektive Funktion, so ist auch Y abzählbar. (Ist $g: \mathbb{N} \to X$ surjektiv, so ist $f \circ g: \mathbb{N} \to Y$ surjektiv. (Aufg. I.3.1(a)))

(b) Jede endliche Menge ist abzählbar (Nachweis!).

(c) Jede unendliche abzählbare Menge ist gleichmächtig zu $\mathbb{N}$. Hierzu muss man zeigen, dass aus der Existenz einer surjektiven Funktion $f: \mathbb{N} \to M$ die einer bijektiven Funktion $g: \mathbb{N} \to M$ folgt. Hierzu definiert man

$$h(n) := \min\{m \in \mathbb{N} \colon |\{f(1), \ldots, f(m)\}| = n\}.$$

Dann ist $h(n) \geq n$ für alle $n \in \mathbb{N}$ und man kann zeigen, dass $h: \mathbb{N} \to \mathbb{N}$ eine injektive Funktion ist, für die $g := f \circ h : \mathbb{N} \to M$ bijektiv ist. (Details als Übung!) ■

Satz I.3.13. *Die Mengen $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ sind gleichmächtig.*

Beweis. Wir definieren eine Funktion $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch

$$f(p, q) = \frac{(p + q - 1)(p + q - 2)}{2} + p.$$

Diese Funktion ist bijektiv (Nachweis als Übung; hierbei ist eine Skizze hilfreich). ■

Folgerung I.3.14. *Jede abzählbare Vereinigung abzählbarer Mengen ist abzählbar, d.h. ist $M = \bigcup_{n \in \mathbb{N}} M_n$ und sind alle Mengen M_n abzählbar, so auch M.*

Beweis. Seien die Mengen M_n für jedes $n \in \mathbb{N}$ abzählbar, d.h., wir können sie beschreiben als $M_n = \{x_{n,1}, x_{n,2}, \ldots\}$. Dann existiert für die Menge

$$\bigcup_{n \in \mathbb{N}} M_n = \{x_{n,m} \colon (n, m) \in \mathbb{N} \times \mathbb{N}\}$$

eine surjektive Funktion $\mathbb{N} \times \mathbb{N} \to \bigcup_{n \in \mathbb{N}} M_n, (n, m) \mapsto x_{n,m}$, sie ist also abzählbar (Bemerkung I.3.12(a)). ■

Folgerung I.3.15. *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.*

Beweis. Da die Menge $\mathbb{Z}$ abzählbar ist, ist für jedes $n \in \mathbb{N}$ die Menge $\frac{1}{n}\mathbb{Z} := \{\frac{p}{n} \colon p \in \mathbb{Z}\}$ abzählbar. Wegen

$$\mathbb{Q} = \bigcup_{n \in \mathbb{N}} \frac{1}{n}\mathbb{Z}$$

folgt die Abzählbarkeit von $\mathbb{Q}$ daher aus Folgerung I.3.14. ■

Satz I.3.16. (Cantor[1]-Russel) *Sei X eine Menge. Dann existiert keine surjektive Funktion $f: X \to \mathcal{P}(X)$, insbesondere auch keine bijektive.*

Beweis. Sei $f: X \to \mathcal{P}(X)$ eine Funktion. Wir zeigen, dass f nicht surjektiv ist, indem wir zeigen, dass die Menge $A := \{x \in X : x \notin f(x)\}$ nicht in $f(X)$ liegt. Wir führen einen indirekten Beweis; dazu nehmen wir an, dass $A = f(y)$ für ein $y \in X$ gilt.
1. Fall: $y \in A$. Dann ist $y \notin f(y) = A$; Widerspruch!
2. Fall: $y \notin A$. Dann ist $y \in f(y) = A$; Widerspruch!
Die Annahme ist also falsch, d. h. es gilt $A \notin f(X)$ und daher ist f nicht surjektiv. ■

Eine wichtige Folgerung aus Satz I.3.16 ist, dass es keine größte Menge gibt, denn für jede Menge X ist die Potenzmenge $\mathcal{P}(X)$ echt größer.

Folgerung I.3.17. *Die Menge $\mathcal{P}(\mathbb{N})$ aller Teilmengen der natürlichen Zahlen ist nicht abzählbar.* ■

I.4. Das Prinzip der vollständigen Induktion

In diesem Abschnitt werden wir die natürlichen Zahlen etwas genauer betrachten. Hierbei werden wir das zentrale Beweisprinzip der vollständigen Induktion kennenlernen.

Wir stellen uns hier auf den Standpunkt, dass wir die *natürlichen Zahlen*

$$\mathbb{N} = \{1, 2, 3, \ldots\} \quad \text{bzw.} \quad \mathbb{N}_0 = \{0, 1, 2, 3, \ldots\},$$

die *ganzen Zahlen*

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

und die *rationalen Zahlen* (Brüche)

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

kennen. Wir haben damit folgende Inklusionen von Mengen:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}.$$

Am Anfang unserer Überlegungen steht das:

Wohlordnungsprinzip/Induktionsprinzip

JEDE NICHTLEERE TEILMENGE $M \subseteq \mathbb{N}$ BESITZT EIN KLEINSTES ELEMENT.

[1] Georg Cantor (1845–1918), deutscher Math. in Halle, Begründer der Mengenlehre; besuchte 1859–1862 die Höhere Gewerbeschule in Darmstadt, studierte in Berlin.

Wir werden dieses Prinzip als ein Axiom über die Menge $\mathbb{N}$ der natürlichen Zahlen betrachten. Man sollte sich an dieser Stelle noch einmal bewusst machen, dass wir nicht axiomatisch präzisiert haben, was die natürlichen Zahlen sind, sondern von einer naiven Vorstellung der Menge $\mathbb{N}$ mit ihren arithmetischen Operationen ausgehen. Präzisiert man die Eigenschaften von $(\mathbb{N}, +, \cdot)$ axiomatisch (Peano-Axiome[1]), so ist das Wohlordnungsprinzip letztendlich in die Axiomatik eingebaut.

Aus dem Wohlordnungsprinzip leiten wir sogleich eine wichtige Folgerung ab:

Das Beweisprinzip der vollständigen Induktion

Satz I.4.1. *Sei $(p_n)_{n\in\mathbb{N}}$ eine Folge von Aussagen. Gilt*
(A) p_1 *und*
(S) $p_n \Rightarrow p_{n+1}$ *für alle* $n \in \mathbb{N}$,
so gilt: $(\forall n \in \mathbb{N})\, p_n$.

Beweis. (Indirekter Beweis) Wir betrachten die Menge $M := \{n \in \mathbb{N} \colon \neg p_n\}$. Ist M nicht leer, so besitzt M nach dem Wohlordnungsprinzip ein kleinstes Element m. Wegen (A) ist $m \neq 1$. Daher ist $m - 1$ eine natürliche Zahl mit $m - 1 \notin M$, d.h., p_{m-1} ist wahr. Wegen (S) ist dann auch p_m wahr; ein Widerspruch. ■

Möchte man für jede natürliche Zahl n eine Aussage p_n beweisen, so kann man also wie folgt vorgehen:
Induktionsanfang (A) Zeige die Aussage p_1.
Induktionsschritt (S) Zeige: $(\forall n \in \mathbb{N})\ p_n \Rightarrow p_{n+1}$, d.h., aus der *Induktionsannahme* p_n wird die Aussage p_{n+1} hergeleitet.
Anschaulich:

$$\begin{array}{ccccccccc} p_1 & \Rightarrow & p_2 & \Rightarrow & p_3 & \Rightarrow & p_4 & \Rightarrow & \dots \\ W & & W & & W & & W & & \end{array}$$

(Dominoprinzip!)
Man kann das Induktionsprinzip auch verwenden, um mathematische Objekte rekursiv zu definieren.

Definition I.4.2. Ist $n \in \mathbb{N}$ und sind $x_1, \dots, x_n \in \mathbb{Q}$, so setzen wir

$$x_1 + x_2 + \ldots + x_n := (x_1 + x_2 + \ldots + x_{n-1}) + x_n \qquad \text{für } n > 1.$$

dass man hiermit jede mögliche Anzahl von Summanden erfasst, folgt sofort aus dem Induktionsprinzip. Weiter definiert man

$$\sum_{j=1}^{n} x_j := \sum_{j\in\{1,2,\ldots,n\}} x_j := x_1 + x_2 + \ldots + x_n$$

[1] Guiseppe Peano (1858–1932), italienischer Mathematiker in Torino, formulierte 1892 das Peanosche Axiomensystem für die natürlichen Zahlen.

und

$$\sum_{j=1}^{0} x_j \; := \sum_{j \in \emptyset} x_j \; := 0$$

(die *leere Summe*).

Analog definiert man Mehrfachprodukte

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n := (x_1 \cdot x_2 \cdot \ldots \cdot x_{n-1}) \cdot x_n \qquad \text{für } n > 1$$

und weiter

$$\prod_{j=1}^{n} x_j := \prod_{j \in \{1,2,\ldots,n\}} x_j := x_1 \cdot x_2 \cdot \ldots \cdot x_n.$$

Hier setzen wir

$$\prod_{j=1}^{0} x_j \; := \prod_{j \in \emptyset} x_j \; := 1 \quad (\text{das } \textit{leere Produkt}).$$

Speziell definieren wir für $n \in \mathbb{N}_0$ die *n-te Potenz* von x durch

$$x^n := \prod_{j=1}^{n} x = \underbrace{x \cdots x}_{\text{n mal}} = x^{n-1}x, \quad x^1 := x, x^0 := 1.$$

Ist $x \neq 0$ und $n \in \mathbb{Z}$, $n < 0$, so setzen wir $x^n := \frac{1}{x^{-n}}$. ■

Wir schauen uns jetzt an einigen Beispielen an, wie das Induktionsprinzip für Beweise verwendet werden kann.

Satz I.4.3. (a) *Für alle $n \in \mathbb{N}$ gilt $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.*

(b) *Für alle $n, m \in \mathbb{N}$ und $q \in \mathbb{Q}$ gilt $q^m q^n = q^{n+m}$.*

(c) *Für alle $n, m \in \mathbb{N}$ und $q \in \mathbb{Q}$ gilt $(q^m)^n = q^{nm}$.*

Beweis. (a) (A) $(n = 1)$ $\sum_{k=1}^{1} k = 1 = \frac{1 \cdot (1+1)}{2}$ ist richtig.

(S) Es gelte $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Dann ist

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

(b) (A) $(n = 1)$ $q^m q^1 = q^{m+1}$ folgt für alle $m \in \mathbb{N}$ aus der Definition.

(S) Es gelte $q^m q^{n-1} = q^{m+(n-1)}$ für alle $m \in \mathbb{N}$. Dann ist

$$q^m q^n = q^m(q^{n-1}q) = (q^m q^{n-1})q = q^{m+(n-1)}q = q^{m+(n-1)+1} = q^{m+n}.$$

(c) (A) $(n = 1)$ $(q^m)^1 = q^m$ gilt trivialerweise.

(S) Es gelte $(q^m)^{n-1} = q^{(n-1)m}$ für alle $m \in \mathbb{N}$. Dann ist wegen (b)

$$(q^m)^n = (q^m)^{n-1} q^m = q^{(n-1)m} q^m \overset{(b)}{=} q^{(n-1)m+m} = q^{nm}. \qquad \blacksquare$$

Man beachte, dass der Induktionsanfang (A) sehr wesentlich ist, denn z.B. lässt sich für die Aussagen

$$p_n: \quad \sum_{k=1}^{n} k = \frac{n}{2}(n+1) + 5$$

zeigen, dass $p_n \Rightarrow p_{n+1}$ für alle $n \in \mathbb{N}$ gilt. Der Induktionsschluss wie im Beweis von Satz I.4.3(a) lässt sich also problemlos durchführen, obwohl keine der Aussagen p_n wahr ist.

Mit der Formel aus Satz I.4.3(a) verbindet sich eine berühmte Anekdote um *Carl Friedrich Gauß*[1]*. Dieser bekam im Alter von sieben Jahren von seinem Lehrer die Aufgabe gestellt, alle Zahlen von 1 bis 100 aufzusummieren. Carl Friedrich fing dies etwas anders an als seine Klassenkameraden, und zwar so:*

$$\begin{array}{cccccccccccc}
 & 1 & + & 2 & + & 3 & + & \dots & & + & 50 & + \\
 & 100 & + & 99 & + & 98 & + & \dots & + \; 52 & + & 51 & \\
= & 101 & + & 101 & + & 101 & + & \dots & & + & 101 & = \; 101 \cdot 50 = 5050
\end{array}$$

Dieser Ansatz steckt auch implizit in der soeben bewiesenen Formel:

$$\sum_{k=1}^{100} k = 101 \cdot \tfrac{100}{2} = 5050.$$

Satz I.4.4. *Seien M und N nichtleere Mengen mit n Elementen, also $|M| = |N| = n$. Dann existieren genau*

$$n! := 1 \cdot 2 \cdot 3 \cdots n \ (n\text{-Fakultät})$$

bijektive Funktionen von M nach N.

Beweis. (Induktion nach n).
(A) $n = 1$: Dann gilt $|M| = |N| = 1$ und es gibt genau eine Bijektion.
(S) Sei $M = \{x_1, \dots, x_{n+1}\}$ und $N = \{y_1, \dots, y_{n+1}\}$, wobei alle x_j bzw. y_k jeweils paarweise verschieden seien. Ist $f\colon M \to N$ eine Bijektion, so gibt es für $f(x_{n+1})$ genau $n+1$ Möglichkeiten. Ist $f(x_{n+1})$ gegeben, so ist die eingeschränkte Funktion

$$f|_{\{x_1,\dots,x_n\}} \to N \setminus \{f(x_{n+1})\}$$

eine Bijektion. Hierfür gibt es nach Induktionsannahme $n!$ Möglichkeiten, da $|\{x_1, \dots, x_n\}| = n$ und $|N \setminus \{f(x_{n+1})\}| = n$ gilt. Insgesamt ergeben sich so $(n+1) \cdot n! = (n+1)!$ Möglichkeiten. $\blacksquare$

[1] Carl Friedrich Gauß (1777–1855), Mathematiker und Physiker in Göttingen, leistete entscheidende Beiträge in vielen Bereichen der Mathematik.

Bemerkung I.4.5. (a) Eine Bijektion $f : M \to M$ der Menge M auf sich nennt man eine *Permutation.* Es gibt also $n!$ Permutationen einer n-elementigen Menge.

(b) Für den Spezialfall $M = \{1, 2, \dots, n\}$ ist eine Bijektion $f\colon M \to N$ eine Aufzählung der Menge N als $N = \{f(1), \dots, f(n)\}$. Es gibt nach Satz I.4.4 also genau $n!$ verschieden Anordnungen der Menge N. Konkret kann man dies folgendermaßen interpretieren: Hat man eine Menge N von n Büchern, so gibt es $n!$ Möglichkeiten, diese Bücher in einem Regal nebeneinander aufzustellen.

(c) Der Satz I.4.4 bleibt für $M = N = \emptyset$ richtig, wenn wir

$$0! := 1$$

setzen. ■

Definition I.4.6. Für $\alpha \in \mathbb{Q}$ und $n \in \mathbb{N}$ definieren wir die *Binomialkoeffizienten*

$$\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} \quad , \quad \binom{\alpha}{0} := 1.$$

Ist $\alpha \in \mathbb{N}_0$, so ist

$$\binom{\alpha}{n} = \begin{cases} \frac{\alpha!}{n!(\alpha-n)!} & \text{für } 0 \le n \le \alpha \\ 0 & \text{für } n > \alpha, \end{cases}$$

denn

$$\frac{\alpha!}{n!(\alpha-n)!} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} \, \frac{(\alpha-n)\cdots 2\cdot 1}{(\alpha-n)\cdots 2\cdot 1} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

■

Satz I.4.7. (Additionstheorem für Binomialkoeffizienten) *Für* $\alpha \in \mathbb{Q}$ *und* $n \in \mathbb{N}$ *gilt*

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

Beweis.

$$\begin{aligned} \binom{\alpha-1}{n-1} + \binom{\alpha-1}{n} &= \frac{(\alpha-1)\cdots(\alpha-1-(n-1)+1)}{(n-1)!} + \frac{(\alpha-1)\cdots(\alpha-n)}{n!} \\ &= \frac{(\alpha-1)\cdots(\alpha-n+1)}{(n-1)!} + \frac{(\alpha-1)\cdots(\alpha-n)}{n!} \\ &= \frac{(\alpha-1)\cdots(\alpha-n+1)}{(n-1)!} \left(1 + \frac{\alpha-n}{n}\right) \\ &= \frac{(\alpha-1)\cdots(\alpha-n+1)}{(n-1)!} \, \frac{\alpha}{n} \\ &= \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} = \binom{\alpha}{n} \end{aligned}$$

■

Eine leicht eingängige Möglichkeit, sich kleine Werte der Binomialkoeffizienten schnell zu besorgen, stellt das *Pascalsche Dreieck* dar. In ihm ergeben sich die Einträge nach der gerade bewiesenen Formel als Summe der diagonal darüberstehenden:

$$
\begin{array}{ccccccccccccc}
 & & & & & & & & \binom{n}{0} & & & & \\
 & & & & & & & \swarrow & & \binom{n}{1} & & & \\
 & & & & & & 1 & & \swarrow & & \binom{n}{2} & & \\
 & & & & & 1 & & 1 & & \swarrow & & \ddots & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\iddots & & & & & & & & & & & & \ddots
\end{array}
$$

Man sieht, wie die Binomialkoeffizienten angeordnet sind:

$$
\begin{array}{ccc}
\binom{n-1}{k-1} & & \binom{n-1}{k} \\
\searrow & + & \swarrow \\
 & \binom{n}{k} &
\end{array}
$$

Satz I.4.8. *Eine Menge M mit m Elementen hat $\binom{m}{n}$ Teilmengen mit n Elementen. Insbesondere ist $\binom{m}{n} \in \mathbb{N}_0$ für alle $m, n \in \mathbb{N}_0$.*

Beweis. (Durch Induktion nach m).
(A) Ist $m = 0$, so ist

$$\binom{m}{n} = \begin{cases} 1, & \text{falls } n = 0; \\ 0, & \text{sonst.} \end{cases}$$

Die Behauptung ist also richtig, da $M = \emptyset$ nur eine Teilmenge mit 0 Elementen besitzt.

(S) Wir nehmen nun an, dass die Behauptung für Mengen mit m Elementen gilt (Induktionsannahme). Sei jetzt $|M| = m + 1$ und $x_0 \in M$. Dann ist $M = \{x_0\} \cup (M \setminus \{x_0\})$ und $|M \setminus \{x_0\}| = m$. Für eine n-elementige Teilmenge $N \subseteq M$ gibt es zwei Fälle:

(1) $x_0 \in N$. Dann ist $N \cap (M \setminus \{x_0\})$ eine $(n-1)$-elementige Teilmenge. Nach Induktionsannahme gibt es hierfür $\binom{m}{n-1}$ Möglichkeiten.

(2) $x_0 \notin N$. Dann ist $N \subseteq M \setminus \{x_0\}$. Hierfür gibt es $\binom{m}{n}$ Möglichkeiten.

Insgesamt gibt es also

$$\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}$$

Möglichkeiten. ∎

Man kann den gerade bewiesenen Sachverhalt auch kombinatorisch interpretieren: Man betrachtet die verschiedenen Möglichkeiten, die Elemente einer Menge $M = \{x_1, \ldots, x_m\}$ anzuordnen. Das geht auf $m!$ Weisen. Ist die Menge der ersten n Elemente $N := \{x_1, \ldots, x_n\}$ festgelegt, so gibt es $n!(m-n)!$ Möglichkeiten der Anordnung, die auf die vorgegebene Menge N führt. Insgesamt ergeben sich also

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}$$

Möglichkeiten, n Elemente aus M herauszunehmen, da jeweils $n!(m-n)!$ Anordnungen die gleiche Teilmenge N liefern.

Satz I.4.9. (Binomischer Lehrsatz) *Für $x, y \in \mathbb{Q}$ und $n \in \mathbb{N}_0$ gilt*

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

Beweis. (durch vollständige Induktion nach m) (A) Für $n = 0$: $(x+y)^n = 1 = \sum_{k=0}^{0} \binom{n}{k} x^0 y^0$ ist wahr. Für den Induktionsschluss (S) rechnen wir:

$$\begin{aligned}
&(x+y)^{n+1} \\
&= (x+y)(x+y)^n \\
&\overset{\text{Ann.}}{=} (x+y)\left(\sum_{k=0}^{n} \binom{n}{k} x^k \cdot y^{n-k}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} \cdot y^{n-k} \;+\; \sum_{k=0}^{n} \binom{n}{k} x^k \cdot y^{n+1-k} \\
&= \binom{n}{n} x^{n+1} y^0 \;+\; \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} \cdot y^{n-k} \;+\; \sum_{k=1}^{n} \binom{n}{k} x^k \cdot y^{n+1-k} \;+\; \binom{n}{0} x^0 y^{n+1} \\
&= x^{n+1} \;+\; \sum_{k=1}^{n} \binom{n}{k-1} x^k \cdot y^{n+1-k} \;+\; \sum_{k=1}^{n} \binom{n}{k} x^k \cdot y^{n+1-k} \;+\; y^{n+1} \\
&= x^{n+1} \;+\; \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) x^k \cdot y^{n+1-k} \;+\; y^{n+1} \\
&= \binom{n+1}{n+1} x^{n+1} y^0 \;+\; \sum_{k=1}^{n} \binom{n+1}{k} x^k \cdot y^{n+1-k} \;+\; \binom{n+1}{0} x^0 y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k \cdot y^{n+1-k}.
\end{aligned}$$

∎

Auch hier kann man eine kombinatorische Interpretation finden. In der Summe

$$\begin{aligned}(x+y)^n &= (x+y)(x+y)\cdots(x+y) \quad (n \text{ Faktoren})\\ &= x^n + x^{n-1}y + \dots\end{aligned}$$

kommt der Term $x^k y^{n-k}$ genau $\binom{n}{k}$-mal vor, da es genau $\binom{n}{k}$ Möglichkeiten gibt, aus der n-elementigen Menge der Faktoren eine k-elementige auszuwählen.

Aufgabe I.4.1. Zeigen Sie: Für eine Selbstabbildung $f\colon M \to M$ einer endlichen Menge M sind folgende Aussagen äquivalent:

(1) f ist bijektiv.

(2) f ist injektiv.

(3) f ist surjektiv. ■

Aufgabe I.4.2. Sei M eine k-elementige Menge und N eine n-elementige Menge. Zeigen Sie:

(1) Es gibt

$$\prod_{j=0}^{k-1}(n-j) = n(n-1)(n-2)\cdots(n-k+1)$$

injektive Funktionen $f\colon M \to N$. Was passiert für $k > n$?

(2) Es gibt n^k Funktionen $f\colon M \to N$. ■

II. Die reellen Zahlen

In diesem Kapitel wenden wir uns dem Hauptgegenstand der Analysis, der Menge $\mathbb{R}$ der reellen Zahlen, zu. Wir stellen uns die reellen Zahlen als eine "kontinuierliche Zahlengerade" vor, mit der wir messen und Geometrie treiben wollen. Die rationalen Zahlen sind dafür nicht ausreichend, denn mit ihnen lässt sich nicht einmal die Diagonale eines Einheitsquadrats messen, die bekanntlich die Länge $\sqrt{2}$ besitzt, und diese Zahl ist irrational. Wir werden im Verlauf der Vorlesung noch viele Gründe dafür kennenlernen, dass die reellen Zahlen einen minimalen Zahlbereich bilden, der den Anforderungen der Analysis gerecht wird. Es gibt durchaus größere Zahlbereiche, mit denen man Analysis treiben kann (Nonstandard Analysis), und andere Zahlbereiche (p-adische Zahlen), die zwar allen metrischen Anforderungen genügen, aber nicht zum Messen geeignet sind. Diese Zahlbereiche sind Gegenstand der p-adischen Analysis bzw. der Algebra.

Was sind die reellen Zahlen und welche Struktur tragen sie? Um dies zu verstehen, betrachten wir zunächst die bekannten Strukturen auf der Menge $\mathbb{Q}$ der rationalen Zahlen.

Die Menge $\mathbb{Q}$ der rationalen Zahlen trägt mehrere Strukturen:

(1) Die *Addition:*

$$\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ad + bc}{bd}$$

(2) Die *Multiplikation:*

$$\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ac}{bd}$$

(3) Eine dritte Struktur ist durch die *Ordnungsrelation* $<$ auf $\mathbb{Q}$ gegeben:

$$\frac{a}{b} < \frac{c}{d} \quad \Longleftrightarrow \quad bc - ad \in \mathbb{N}$$

(beachte: $b, d \in \mathbb{N}$).

Gegenstand dieses Abschnitts sind diese drei Strukturen, ihre Eigenschaften, und wie man sie auf die reellen Zahlen übertragen kann. Hierbei werden wir der axiomatischen Methode folgen, d.h., wir werden Eigenschaften bzw. Rechenregeln als *Axiome* formulieren, die in dem Bereich, den wir jeweils betrachten, gelten sollen. Dies führt uns zu vielen Strukturen, die in der Mathematik eine zentrale Rolle spielen. Die reellen Zahlen samt der drei Strukturen (Addition, Multiplikation und Ordnung) werden schließlich durch eine Liste von Axiomen, die sich auf diese Strukturen beziehen, (eindeutig) als *vollständig angeordneter Körper* charakterisiert.

II.1 Axiome der Arithmetik

Axiome der Addition

Wir betrachten zuerst die Axiome der Addition bzw. den Begriff der abelschen Gruppe.

Definition II.1.1. Ein Paar $(G, *)$ aus einer Menge G und einer Funktion

$$*\colon G \times G \to G, \ (x, y) \mapsto x * y$$

heißt *Gruppe*, wenn folgende Axiome erfüllt sind:

(A) *Assoziativgesetz:* $(\forall x, y, z \in G)\, x * (y * z) = (x * y) * z$.

(N) *Neutrales Element:* $(\exists e \in G)(\forall x \in G)\ x * e = e * x = x$.

(I) *Existenz eines Inversen:* $(\forall x \in G)(\exists y \in G)\, x * y = y * x = e$.

Man sagt dann auch, dass die (binäre) Operation $*$ auf G die Struktur einer Gruppe definiert.

Gilt zusätzlich das

(K) *Kommutativgesetz:* $(\forall x, y \in G)\, x * y = y * x$,

so spricht man von einer *abelschen Gruppe*. In diesem Fall schreiben wir in der Regel $+$ statt $*$ für die Gruppenoperation und 0 statt e für das neutrale Element, das man dann auch *Nullelement* nennt. ■

Beispiel II.1.2. (a) Einfache Beispiele für abelsche Gruppen sind $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$. Warum ist $(\mathbb{N}, +)$ keine abelsche Gruppe? Welche Axiome sind verletzt? Ein weiteres Beispiel ist $(\mathbb{Q}^\times, \cdot)$, wobei $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ ist.

(b) Wir betrachten die zweielementige Menge $\mathbb{F} := \{0, 1\}$ mit der Addition modulo 2:

$$0 + 0 := 1 + 1 := 0 \quad \text{und} \quad 0 + 1 := 1 + 0 := 1.$$

Dann ist $(\mathbb{F}, +)$ eine abelsche Gruppe. ■

Aus den 4 Axiomen (A),(N),(I) und (K) einer abelschen Gruppe lassen sich weitere Eigenschaften ableiten, die wir uns nun anschauen. Man kann sich überlegen, dass keines der 4 Axiome aus den drei anderen folgt. In diesem Sinn bilden sie ein minimales System.

Bemerkung II.1.3. Sei $(A, +)$ eine abelsche Gruppe. Wir halten einige Folgerungen aus den Axiomen fest:
(1) Eindeutigkeit des Nullelements: Sind 0 und $0'$ Nullelemente von A, so gilt $0 = 0 + 0' = 0'$ und folglich $0 = 0'$.
(2) Eindeutigkeit des Inversen: Sind y und y' invers zu x, so gilt

$$y \overset{\text{(N)}}{=} y + 0 \overset{\text{(I)}}{=} y + (x + y') \overset{\text{(A)}}{=} (y + x) + y' \overset{\text{(I)}}{=} 0 + y' \overset{\text{(N)}}{=} y'.$$

Da das Inverse des Elements $x \in A$ eindeutig bestimmt ist, ist es sinnvoll, dieses Element mit $-x$ zu bezeichnen. Weiter definieren wir

$$x - y := x + (-y).$$

(3) $0 = -0$: Dies folgt wegen $0 + 0 = 0$ aus (2).
(4) Für alle $x \in A$ gilt $-(-x) = x$ aufgrund der Symmetrie von (I).
(5) Für alle $x, y \in A$ gilt $-(x + y) = -y - x$:

$$\begin{aligned}(x + y) + (-y - x) &\overset{\text{(A)}}{=} x + (y + (-y - x)) \overset{\text{(A)}}{=} x + ((y - y) - x)\\ &\overset{\text{(I)}}{=} x + (0 - x) \overset{\text{(N)}}{=} x - x \overset{\text{(I)}}{=} 0.\end{aligned}$$

Aus (2) folgt somit $-y - x = -(x + y)$.
(6) (Subtraktion bei Gleichungen) Es gilt $x + a = b \Leftrightarrow x = b - a$:
„$\Rightarrow$“: Es gilt $x \overset{\text{(N)}}{=} x + 0 \overset{\text{(I)}}{=} x + (a - a) \overset{\text{(A)}}{=} (x + a) - a = b - a$.
„$\Leftarrow$“: Aus $x = b - a$ folgt $x + a = (b - a) + a \overset{\text{(A)}}{=} b + (-a + a) \overset{\text{(I)}}{=} b + 0 \overset{\text{(N)}}{=} b$. ■

Axiome der Multiplikation

Definition II.1.4. Ist K eine Menge mit zwei Verknüpfungen (Abbildungen)

$$K \times K \to K,\ (x, y) \mapsto x + y \quad \text{und} \quad K \times K \to K,\ (x, y) \mapsto x \cdot y,$$

so heißt K bzw. das Tripel $(K, +, \cdot)$ *Körper*, falls $(K, +)$ eine abelsche Gruppe ist und für die Multiplikation folgende Axiome gelten
(MA) *Assoziativgesetz:* $(\forall x, y, z \in K)\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(MK) *Kommutativgesetz:* $(\forall x, y \in K)\, x \cdot y = y \cdot x$
(E) *Einselement:* $(\exists 1 \in K)\big((1 \neq 0) \wedge (\forall x \in K)\ x \cdot 1 = 1 \cdot x = x\big)$
(MI) *Existenz eines Inversen:* $(\forall x \in K \setminus \{0\})\, (\exists y \in K)\, x \cdot y = y \cdot x = 1$.
Weiter seien Addition und Multiplikation verbunden durch das
(D) *Distributivgesetz*: $(\forall x, y, z \in K)\, x \cdot (y + z) = x \cdot y + x \cdot z$. ■

Man lässt bei der Multiplikation aus Bequemlichkeitsgründen üblicherweise den Punkt weg und schreibt xy anstatt $x \cdot y$.

Bemerkung II.1.5. Wir halten wieder einige Folgerungen aus den Körperaxiomen fest:
(7) Es gilt $0 \cdot x = 0 = x \cdot 0$ für alle $x \in K$:

$$x \cdot 0 \overset{(N)}{=} x \cdot (0+0) \overset{(D)}{=} x \cdot 0 + x \cdot 0 \overset{(6)}{\Longrightarrow} x \cdot 0 = x \cdot 0 - x \cdot 0 = 0.$$

(8) Wir schreiben $K^\times := K \setminus \{0\}$. Dann ist $(K^\times, \cdot)$ eine abelsche Gruppe: Zuerst müssen wir zeigen, dass die Multiplikation die Menge $K^\times \times K^\times$ nach $K^\times$ abbildet. Sind $x, y \in K^\times$ und x' bzw. y' jeweils multiplikative Inverse von x bzw. y, so erhalten wir wie in (6) zunächst

$$(xy)(y'x') \overset{(MA)}{=} x\big(y(y'x')\big) \overset{(MA)}{=} x\big((yy')x'\big) \overset{(MI)}{=} x\big(1x'\big) \overset{(E)}{=} xx' \overset{(MI)}{=} 1.$$

Wegen (7) und $0 \neq 1$ ist daher $xy \neq 0$. Also ist die Multiplikationsabbildung

$$\cdot \colon K^\times \times K^\times \to K^\times, \quad (x,y) \mapsto x \cdot y$$

definiert, da für $x, y \in K^\times$ das Produkt xy wieder in $K^\times$ liegt. Die Axiome (MA), (MK) und (E) liefern Assoziativität, Kommutativität und das neutrale Element (Nullelement), das in diesem Fall das Element 1 ist. Zur Existenz des Inversen: Ist $x \in K^\times$ und $y \in K$ mit $xy = 1$, so ist $y \neq 0$ wegen (7), da sonst $1 = x \cdot y = x \cdot 0 = 0$ gelten würde. Damit ist $y \in K^\times$, d.h., in $K^\times$ ist die Existenz eines Inversen gesichert.

Aus (1) bis (6) folgt jetzt: (9) Eindeutigkeit des Einselements (wegen (1)).
(10) Eindeutigkeit des multiplikativen Inversen. Man bezeichnet das multiplikative Inverse von $x \neq 0$ mit x^{-1} oder $\frac{1}{x}$. Weiter definieren wir für $y \neq 0$

$$\frac{x}{y} := xy^{-1}.$$

(11) $1 = 1^{-1}$ (wegen (3)).
(12) Für alle $x \neq 0$ gilt $(x^{-1})^{-1} = x$ (wegen (4)).
(13) Für $x, y \in K^\times$ ist $(xy)^{-1} = y^{-1}x^{-1}$: Das haben wir schon unter (8) gezeigt. Es folgt aber auch mit (8) aus (5).
(14) Für $a \neq 0$ gilt $xa = b \Leftrightarrow x = \frac{b}{a}$:
„$\Rightarrow$“: Aus $xa = b$ folgt $\frac{b}{a} = ba^{-1} = (xa)a^{-1} \overset{(MA)}{=} x(aa^{-1}) \overset{(MI)}{=} x1 \overset{(E)}{=} x$, also $x = \frac{b}{a}$.
„$\Leftarrow$“: Aus $x = \frac{b}{a}$ folgt umgekehrt $xa = (ba^{-1})a \overset{(MA)}{=} b(a^{-1}a) \overset{(MI)}{=} b1 \overset{(E)}{=} b$, also $xa = b$.
(15) Für alle $x, y \in K$ gilt $(-x)y = -(xy)$:

$$xy + (-x)y \overset{(D)}{=} (x + (-x))y \overset{(N)}{=} 0 \cdot y \overset{(7)}{=} 0,$$

also $(-x)y = -(xy)$.

(16) Für alle $x, y \in K$ gilt $(-x) \cdot (-y) = x \cdot y$: Wegen (15) gilt

$$(-x)(-y) \overset{(15)}{=} -(x \cdot (-y)) \overset{(MK)}{=} -((-y) \cdot x) \overset{(15)}{=} -(-(yx)) \overset{(5)}{=} yx \overset{(MK)}{=} xy. \qquad \blacksquare$$

Aufgabe II.1.1. Sei K ein Körper und

$$L := K^2 = \{(a, b): a, b \in K\}.$$

Auf L definieren wir Addition und Multiplikation durch

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

Weiter definieren wir eine Funktion

$$N: L \to K, \quad (a, b) \mapsto a^2 + b^2.$$

Zeigen Sie:
(1) $N(xy) = N(x)N(y)$ für $x, y \in L$.
(2) $(L, +)$ ist eine abelsche Gruppe.
(3) Für $x = (a, b)$ mit $N(x) \neq 0$ ist

$$x^{-1} := \Big(\frac{a}{N(x)}, -\frac{b}{N(x)}\Big)$$

ein multiplikatives Inverses von x, d.h. $xx^{-1} = x^{-1}x = 1$.
(4) $(L, +, \cdot)$ ist genau dann ein Körper, wenn $N(x) \neq 0$ für alle $x \neq (0, 0)$ in L gilt.
(5) $(L, +, \cdot)$ ist genau dann ein Körper, wenn $a^2 \neq -1$ für alle $a \in K$ gilt, d.h. wenn -1 in K kein Quadrat ist. ■

Aufgabe II.1.2. Wir betrachten die vier Axiome (A), (N), (I) und (K) für abelsche Gruppen. Finde Paare $(M, *)$, wobei $*$ eine Funktion $M \times M \to M, (x, y) \mapsto x * y$ ist, die jeweils folgenden Bedingungen genügen:
(1) (A), (N), (I), ¬ (K).
(2) (A), (N), (K), ¬ (I).
(3) (N), (K), (I), ¬ (A).

In diesem Sinn sind diese Bedingungen voneinander unabhängig, aber natürlich macht (I) nur Sinn, wenn (N) erfüllt ist. ■

II.2 Anordnung

Nachdem wir die Axiome für Addition und Multiplikation kennengelernt haben, wenden wir uns nun Anordnungen auf Körpern zu. Hierbei haben wir zu klären, in welchem Sinne diese Anordnungen mit Addition und Multiplikation verträglich sein sollen.

Definition II.2.1. Ein Paar (K, K_+) aus einem Körper K und einer Teilmenge K_+ heißt *angeordneter Körper*, wenn folgende Axiome gelten:

(O1) Für alle $x \in K$ gilt genau eine der Aussagen

$$x \in K_+, \quad -x \in K_+ \quad \text{oder} \quad x = 0.$$

(O2) Für alle $x, y \in K_+$ ist $x + y \in K_+$.

(O3) Für alle $x, y \in K_+$ ist $x \cdot y \in K_+$.

Die Elemente in K_+ heißen *positiv*. Wir schreiben für $x \in K_+$ auch $x > 0$. Weiter definieren wir folgende Relationen auf K:

- $x > y \quad :\Leftrightarrow \quad x - y > 0$,
- $x \geq y \quad :\Leftrightarrow \quad (x > y) \vee (x = y)$,
- $x < y \quad :\Leftrightarrow \quad y > x$ und
- $x \leq y \quad :\Leftrightarrow \quad y \geq x$. ■

Denkt man daran, dass K eingentlich nur die Menge ist, die dem Körper $(K, +, \cdot)$ unterliegt, so sollte man ausführlicher einen angeordneten Körper ausführlicher als Quadrupel $(K, +, \cdot, K_+)$ schreiben. Ein solcher *Bezeichnungsmissbrauch* ist oft bequem und daher in der Mathematik sehr gebräuchlich.

Beispiel II.2.2. Für $\mathbb{Q}_+ := \{x \in \mathbb{Q} : x > 0\}$ ist das Paar $(\mathbb{Q}, \mathbb{Q}_+)$ ein angeordneter Körper (Nachweis!). ■

Von nun an steht K bzw. (K, K_+) immer für einen angeordneten Körper.

Satz II.2.3. (Anordnungseigenschaften)

(Ver) *Vergleichbarkeit: Es gilt genau eine der Aussagen*

$$x < y, \quad x = y \quad \text{oder} \quad x > y.$$

(Tr) *Transitivität der Ordnung: Gilt $x < y$ und $y < z$, so auch $x < z$.*

(Ad) *Verträglichkeit mit der Addition:*

$$(x < y) \wedge (z \leq w) \Rightarrow x + z < y + w.$$

$(\mathrm{Mul})_+$ *Verträglichkeit mit der Multiplikation:*

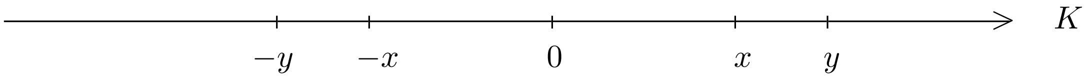
$$(x < y) \wedge (z > 0) \Rightarrow zx < zy.$$

(Neg) *Ist* $x < y$ *, so ist* $-x > -y$ *.*

Man erhält die gleichen Regeln für $\leq$ und $\geq$ statt $<$ und $>$ mit Ausnahme von (Ver); diese wird zu

(Verg) *Es gilt* $x \leq y$ *oder* $y \geq x$ *; gilt beides, so folgt daraus* $x = y$ *.*

Beweis. (Ver) wird durch Einsetzen der Definitionen zu $y - x > 0$ oder $y - x = 0$ oder $y - x < 0$; dies ist gerade (O1).
(Tr): Aus $y - x > 0$ und $z - y > 0$ folgt wegen (O2) $z - x = (z - y) + (y - x) > 0$, also $x < z$.
(Ad): Wir haben $y + w - (x + z) = (y - x) + (w - z) > 0$.
$(\mathrm{Mul})_+$: Aus $y - x > 0$ und $z > 0$ folgt wegen (O3) $z(y - x) = zy - zx > 0$, also $zx < zy$.
(Neg) folgt aus (Ad) Ist $x < y$, d.h. $y - x > 0$, so ist auch $(-x) - (-y) = -x + y = y - x > 0$, also $-x > -y$.
(Verg) ist klar. ■



Satz II.2.4. (Multiplikative Regeln) *Es gelten für alle* $x, y, z \in K$ *:*

(i) $x < y, z < 0 \quad \Rightarrow \quad zx > zy$.

(ii) *Für* $0 \neq x \in K$ *ist* $x^2 > 0$ *. Insbesondere ist* $1 > 0$ *.*

(iii) $x > 0 \Rightarrow x^{-1} > 0$.

(iv) $xy > 0 \Rightarrow (x < y \Leftrightarrow \frac{1}{x} > \frac{1}{y})$.

Beweis. (i) Wegen (Neg) ist $-z > 0$, also $(-z)x < (-z)y$ wegen $(\mathrm{Mul})_+$, d.h. $-zx < -zy$, also $zy < zx$ wegen (Neg).

(ii) Ist $x > 0$, so ist $x^2 > 0$. Andernfalls ist $-x < 0$ und $x^2 = (-x)^2 > 0$ wegen Bemerkung II.1.5(16).

(iii) Wegen $(x^{-1})^2 > 0$ ist $x^{-1} = x(x^{-1})^2 > 0$ wegen (O3).

(iv) Multiplikation mit $(xy)^{-1} > 0$ liefert

$$x < y \Leftrightarrow x \cdot (xy)^{-1} < y \cdot (xy)^{-1} \Leftrightarrow \frac{1}{y} < \frac{1}{x}$$ ■

Bemerkung II.2.5. Die Anordnung eines Körpers K hat auch arithmetische Konsequenzen. Insbesondere lässt sich nicht jeder Körper anordnen:

Wegen $1 > 0$ und (Neg) ist $-1 < 0$. Also ist $x^2 \neq -1$ für alle $x \in K$ und somit -1 kein Quadrat in K. Hieraus schließen wir insbesondere, dass die Konstruktion aus Aufgabe II.1 für jeden angeordneten Körper K einen Körper L liefert, dessen zugrundeliegende Menge K^2 ist. ■

Für $n \in \mathbb{N}_0$ und $x \in K$ setzen wir

$$nx := \sum_{j \in \{1,2,\ldots,n\}} x = \underbrace{x + \ldots + x}_{n \text{ mal}}.$$

Für $n \in \mathbb{Z}$ mit $n < 0$ setzen wir $nx := -(-nx)$.

Bemerkung II.2.6. (Einbettung von $\mathbb{Q}$ in angeordnete Körper) Ist K ein angeordneter Körper und $n \in \mathbb{N}$, so ist $n \cdot 1 = 1 + \ldots + 1$ (n mal) positiv und daher nie 0. Weiter gilt $(nm) \cdot 1 = (n \cdot 1)(m \cdot 1)$ $(n+m) \cdot 1 = n \cdot 1 + n \cdot 1$ für alle $n, m \in \mathbb{Z}$ (Nachweis durch vollständige Induktion für $n \in \mathbb{N}, m \in \mathbb{Z}$ und dann Berücksichtigung der Vorzeichen!). Sind $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}$ mit $\frac{a}{b} = \frac{c}{d}$, d.h. $ad = bc$, so ist $(a \cdot 1)(d \cdot 1) = (ad) \cdot 1 = (bc) \cdot 1 = (b \cdot 1)(c \cdot 1)$ und daher $(a \cdot 1) \cdot (b \cdot 1)^{-1} = (c \cdot 1) \cdot (d \cdot 1)^{-1}$. Wir erhalten daher eine Funktion

$$\varphi\colon \mathbb{Q} \to K, \quad \frac{a}{b} \mapsto (a \cdot 1) \cdot (b \cdot 1)^{-1},$$

denn die rechte Seite hängt nicht von der Darstellung des Bruches $\frac{a}{b}$ ab. Man rechnet leicht nach, dass

$$\varphi(x+y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y) \quad \text{für } x, y \in \mathbb{Q} \tag{2.1}$$

gelten. Ist $\varphi(\frac{a}{b}) = 0$, so ist $a \cdot 1 = 0$ und daher $a = 0$, denn für $a > 0$ ist $a \cdot 1 > 0$ und für $a < 0$ ist $-(a \cdot 1) = (-a) \cdot 1 > 0$. Hieraus schließen wir, dass φ injektiv ist, denn aus $\varphi(\frac{a}{b}) = \varphi(\frac{c}{d})$ folgt $0 = \varphi(\frac{a}{b} - \frac{c}{d}) = \varphi(\frac{ad-bc}{cd})$ und daher $ad = bc$, d.h. $\frac{a}{b} = \frac{c}{d}$. Eine injektive Funktion $\varphi\colon \mathbb{Q} \to K$ für die (2.1) gilt, nennt man eine *Körpereinbettung* oder einen *Homomorphismus von Körpern.* Wir haben also den Körper $\mathbb{Q}$ durch φ in K eingebettet und dürfen ihn uns in diesem Sinn als einen *Unterkörper* von K vorstellen, d.h. als eine Teilmenge von K, die unter Addition und Multiplikation abgeschlossen ist und diesbezüglich einen Körper bildet. In diesem Sinn schreiben wir auch kurz $\frac{a}{b}$ für $\frac{a \cdot 1}{b \cdot 1}$.

Obige Argumente zeigen also, dass jeder angeordenete Körper K den Körper $\mathbb{Q}$ der rationalen Zahlen als Unterkörper enthält. ■

Definition II.2.7. Wir wollen einige der in diesem Paragraphen eingeführten Operationen und Relationen auf Mengen erweitern.

(a) Zu diesem Zweck definieren wir für Mengen $M, N \subseteq K$ und Zahlen $x \in K$:

(1) $M + N := \{m + n \colon m \in M, n \in N\}$

(2) $M \cdot N := \{m \cdot n \colon m \in M, n \in N\}$ und $-M := (-1) \cdot M = \{-m \colon m \in M\}$.

(3) $x \leq M :\Leftrightarrow (\forall m \in M)\, x \leq m$

(4) $x \geq M$, $x < M$ und $x > M$ (analog)

Einige Eigenschaften der Addition und Multiplikation von Elementen von K übertragen sich auf die entsprechenden Operationen für Mengen; so gilt beispielsweise

$$M + N = N + M \quad \text{und} \quad (M+N) + U = M + (N + U).$$

Enthält M mehr als ein Element, so gibt es keine Menge N, für die $M + N = \{0\}$ gilt (Nachweis!).

(b) Ein $x \in K$ mit $x \leq M$ heißt *untere Schranke von* M und ein $x \in K$ mit $M \leq x$ *obere Schranke von* M (vgl. Definition II.2.11). Die Menge M heißt *nach oben* bzw. *nach unten beschränkt*, falls M eine obere bzw. untere Schranke hat. Ist M nach oben und nach unten beschränkt, so heißt M *beschränkt.* ■

Maximum und Minimum

In diesem Abschnitt sei K ein angeordneter Körper.

Definition II.2.8. Sei $M \subseteq K$. Ein Element $x \in M$ heißt *Maximum*, wenn $M \leq x$ gilt. Sind $x, y \in M$ Maxima, so gilt $x \leq y \leq x$, also $x = y$. In diesem Sinn sind Maxima eindeutig bestimmt. Wir schreiben daher

$$x = \max(M),$$

wenn x ein Maximum der Menge M ist. Analog bezeichnet man ein Element $y \in M$ als *Minimum*, wenn $y \leq M$ ist und schreibt $y = \min(M)$. ■

Beispiel II.2.9. (a) Sind $x, y \in K$, so gilt $\max\{x, y\} = \begin{cases} x & \text{für } x \geq y \\ y & \text{für } x \leq y. \end{cases}$ Insbesondere existiert das Maximum jeder zweielementigen Teilmenge von K.

(b) Nicht jede Teilmenge von K mit einer oberen Schranke besitzt ein Maximum. Wir betrachten hierzu die Menge

$$M := \{x \in K : x < 0\}.$$

Für jedes $x \in M$ ist $2x < x < 0$, also $x < \frac{x}{2} < 0$. Wir schließen hieraus, dass M kein Maximum besitzt, obwohl 0 eine obere Schranke ist. ■

Satz II.2.10. *Seien $M, N \subseteq K$ Teilmengen für die $\max M$ und $\max N$ existieren. Dann gilt:*

(1) $M \subseteq N \Longrightarrow \max(M) \leq \max(N)$

(2) $\max(M + N) = \max(M) + \max(N)$

(3) $M, N \geq 0 \Rightarrow \max(M \cdot N) = \max(M) \cdot \max(N)$.

(4) $\max(M \cup N) = \max\{\max(M), \max(N)\}$.

(5) $\min(M) = -\max(-M)$, *falls* $\max(-M)$ *existiert.*

(6) $\min(M \cup N) = \min\{\min(M), \min(N)\}$, *falls* $\min(M)$ *und* $\min(N)$ *existieren.*

Beweis. (1) Wegen $M \leq \max(N)$ ist auch $\max(M) \leq \max(N)$.

(2) Sei $m := \max(M)$ und $n := \max(N)$. Für $a \in M$ und $b \in N$ ist dann $a \leq m$ und $b \leq n$, also $a + b \leq m + n$, d.h. $M + N \leq m + n$. Aus $m + n \in M + N$ folgt somit $m + n = \max(M + N)$.

(3) Analog zu (2).

(4) Seien wieder $m := \max(M)$ und $n := \max(N)$. Dann ist $\max\{m, n\} \in M \cup N$ und für $a \in M, b \in N$ gilt $a, b \leq \max\{m, n\}$; daher ist

$$\max\{m, n\} = \max(M \cup N).$$

(5) Es gilt $-\max(-M) \in -(-M) = M$. Zu zeigen ist noch

$$-\max(-M) \leq M.$$

Sei also $n \in M$. Dann ist $-n \in -M$, also $\max(-M) \geq -n$. Also ist $-\max(-M) \leq n$.

(6) zeigt man analog zu (4). ■

Satz II.2.11. *Jede endliche Teilmenge $M \subseteq K$ besitzt ein Maximum.*

Beweis. Wir beweisen diese Behauptung über vollständige Induktion nach der Anzahl n der Elemente von M.
(A) Induktionsanfang: $|M| = 1$, d.h. $M = \{x\}$. Dann ist $\max M = x$.
(S) Induktionsannahme: Die Behauptung gelte für Mengen N mit n Elementen und M habe $n+1$ Elemente. Dann ist $M \neq \emptyset$ und folglich gibt es ein $x \in M$. Sei $M' := M \setminus \{x\}$. Dann ist $|M'| = n$, so dass nach der Induktionsannahme das Maximum $\max(M')$ existiert. Dann existiert auch $\max(M) = \max(M' \cup \{x\}) = \max\{\max(M'), x\}$ (Satz II.2.10(4)). ■

Wendet man Satz II.2.11 auf die endliche Menge $-M$ an, so sieht man natürlich auch, dass jede endliche Menge M ein Minimum besitzt (Satz II.2.10(5)). Im folgenden schreiben wir daher

$$\max(x_1, \ldots, x_n) := \max\{x_1, \ldots, x_n\}, \qquad \min(x_1, \ldots, x_n) := \max\{x_1, \ldots, x_n\}.$$

Satz II.2.12. (Bernoullische[1] Ungleichung) *Für $x \in K$ mit $x \geq -1$ und $n \in \mathbb{N}$ gilt*

$$1 + nx \leq (1+x)^n.$$

Beweis. Wir zeigen die Behauptung über Induktion nach n.
(A) Für $n = 1$ gilt $1 + x = (1+x)^1$.
(S)

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \\ &\overset{\text{Ann.}}{\geq} (1+x)(1+nx) \qquad \text{wegen } 1+x \geq 0 \\ &= 1 + x + nx + nx^2 = 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x.\end{aligned}$$

■

Für $x \geq 0$ erhalten wir direkter

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = 1 + \binom{n}{1} x + \binom{n}{2} x^2 + \ldots + x^n \geq 1 + \binom{n}{1} x = 1 + nx.$$

Aufgabe II.2.1. (a) Zeigen Sie die *Ungleichung vom arithmetischen Mittel*: Für Elemente x, y eines angeordneten Körpers K gilt

$$x < y \quad \Rightarrow \quad x < \frac{x+y}{2} < y.$$

[1] Jacob Bernoulli (1654–1705), Schweizer Mathematiker und Physiker in Basel.

Hinweis: Zeige, dass für $2 := 1 + 1$ die Beziehung $1 > \frac{1}{2} > 0$ gilt.

(b) Für $0 < x < y$ und alle $k \in \mathbb{N}$ gilt $0 < x^k < y^k$. Hinweis: Vollständige Induktion. ■

Aufgabe II.2.2. (a) Zeigen Sie: Für $n \in \mathbb{N}$ und $a, b \in K$ mit $a \geq 0$ und $a + b \geq 0$ gilt $(a+b)^n \geq a^n + na^{n-1}b$.

(b) Aus $a, b \geq 0$ und $n \in \mathbb{N}$ folgt $(a+b)^n \geq a^n + b^n$. ■

Das Vollständigkeitsaxiom

Das folgenden Konzept liefert einen Ersatz für fehlende Maxima und Minima von Mengen.

Definition II.2.13. (a) Für eine nach oben beschränkte Teilmenge $M \subseteq K$ definieren wir ihr *Supremum* (*obere Grenze*, *kleinste obere Schranke*)

$$\sup(M) := \min\{x : M \leq x\},$$

falls es existiert. Für nach unten beschränkte Teilmengen $M \subseteq K$ definieren wir ihr *Infimum* (*untere Grenze*, *größte untere Schranke*)

$$\inf(M) := \max\{x : x \leq M\},$$

falls es existiert.

Existiert $\max(M)$ und ist $M \leq x$, so ist auch $\max(M) \leq x$ und daher $\sup(M) = \max(M)$, d.h., das Maximum einer Menge ist eine kleinste obere Schranke, falls es existiert.

(b) Eine Menge, die keine obere Schranke besitzt, heißt *nach oben unbeschränkt*; wir schreiben dann $\sup(M) := \infty$. Analog setzt man $\inf(M) := -\infty$, wenn M *nach unten unbeschränkt* ist. Für die leere Menge setzt man

$$\sup(\emptyset) = -\infty \quad \text{und} \quad \inf(\emptyset) = \infty$$

(jedes Element ist obere und untere Schranke von $\emptyset$). ■

Lemma II.2.14. [1] *Sei $\emptyset \neq M \subseteq K$ nach oben beschränkt und $s \in K$. Dann ist $s = \sup(M)$ genau dann, wenn*

$$M \leq s \quad \textit{und} \quad (\forall \varepsilon > 0)(\exists m \in M) \ \ m > s - \varepsilon.$$

[1] Zur Terminologie: Mathematische Sachverhalte werden typischerweise in Sätzen formuliert. Sätze, die vorbereitender Natur sind, werden *Lemma* genannt. Das Wort Lemma (Pural: Lemmata) ist griechisch und bedeuetet Horn (weist in eine Richtung; vgl. Dilemma). Dagegen heißen Sätze, die mehr oder minder Konsequenzen eines vorausgegangenen Satzes sind, oft *Folgerung* oder *Korollar*. Besonders wichtige Sätze heißen *Theorem*.

Beweis. $\Rightarrow$: Sei zunächst $s = \sup(M)$. Dann gilt trivialerweise $M \leq s$. Ist $\varepsilon > 0$, so ist $s - \varepsilon$ keine obere Schranke von M. Also existiert ein $m \in M$ mit $m > s - \varepsilon$.

$\Leftarrow$: Erfüllt s die angegebenen Bedingungen, so ist s eine obere Schranke von M und für kein $\varepsilon > 0$ ist $s - \varepsilon$ eine obere Schranke. Ist $x < s$, so ist $\varepsilon := s - x$ und $x = s - \varepsilon$, also ist x keine obere Schranke von M. Folglich ist s die kleinste obere Schranke von M, d.h. $s = \sup(M)$. ■

Aufgabe II.2.3. Verallgemeinern Sie Satz II.2.10, indem Sie die entsprechenden Aussagen für Suprema bzw. Infima zeigen. Z.B. gilt

$$\sup(M + N) = \sup(M) + \sup(N),$$

falls alle Suprema existieren. ■

Definition II.2.15. (Vollständigkeitsaxiom) Ein angeordneter Körper $(K, +, \cdot, K_+)$ heißt *(ordnungs-)vollständig* oder *vollständig angeordnet*, wenn für jede nichtleere nach oben beschränkte Menge $M \subseteq K$ das Supremum existiert.■

Definition II.2.16. Eine Teilmenge $I \subseteq K$ heißt *Intervall*, wenn

$$x, z \in I, \quad x \leq y \leq z \quad \Rightarrow \quad y \in I$$

gilt, d.h., mit zwei Elementen x und z enthält I auch alle Elemente dazwischen. Für $a, b \in K$ erhält man spezielle Beispiele von Intervallen wie folgt:

$[a, b] := \{x \in K : a \leq x \leq b\}$ (*abgeschlossenenes* Intervall)
$[a, b[:= \{x \in K : a \leq x < b\}$ (*rechtsoffenes* Intervall)
$]a, b] := \{x \in K : a < x \leq b\}$ (*linksoffenes* Intervall)
$]a, b[:= \{x \in K : a < x < b\}$ (*offenes* Intervall).

Die Intervalleigenschaft dieser Mengen ergibt sich sofort aus der Transitivität der Ordnung (Satz II.2.3). Man beachte, dass diese Intervalle für $b < a$ alle leer sind. Für $b = a$ ist lediglich das abgeschlossene Intervall $[a, b] = \{a\}$ nicht leer. Weitere Beispiele für Intervalle sind

$]a, \infty[:= \{x \in K : a < x\}$.
$[a, \infty[:= \{x \in K : a \leq x\}$.
$]-\infty, b] := \{x \in K : x \leq b\}$.
$]-\infty, b[:= \{x \in K : x < b\}$. ■

Bemerkung II.2.17. Sei $a < b$ in K. Alle Intervalle $[a, b]$, $[a, b[$, $]a, b]$, $]a, b[$ sind durch b nach oben beschränkt, d.h., b ist eine obere Schranke. Weiter ist

$$\max([a, b]) = \max(]a, b]) = b,$$

aber $\max([a, b[)$ und $\max(]a, b[)$ existieren nicht. In der Tat haben wir für $x \in]a, b[$ wegen der Ungleichung vom arithmetischen Mittel:

$$x < \frac{x + b}{2} < b,$$

so dass kein Element maximal ist. Allerdings ist

$$\sup([a,b[) = \sup(]a,b[) = b,$$

denn b ist die kleinste obere Schranke dieser Intervalle. Analog gilt

$$\min([a,b]) = \min([a,b[) = a = \inf(]a,b[) = \inf(]a,b[). \qquad \blacksquare$$

Im weiteren werden wir einige Eigenschaften vollständig angeordneter Körper studieren. In folgenden steht K daher immer für einen vollständig angeordneten Körper.

Bemerkung II.2.18. (a) Ist die nichtleere Menge M nach unten beschränkt, so existiert $\inf(M)$: Ist M nach unten beschränkt, so ist $-M$ nach oben beschränkt und $x \leq M$ ist äquivalent zu $-M \leq -x$. Wegen dem Vollständigkeitsaxiom existiert $\sup(-M)$. Die Behauptung folgt nun aus

$$\begin{aligned} -\sup(-M) &= -\min\{a: a \geq -M\} \overset{\text{II.2.10}}{=} \max\{-a: a \geq -M\} \\ &= \max\{b: b \leq M\} = \inf(M). \end{aligned}$$

(b) Wir erinnern uns daran, dass wir $\mathbb{Z}$ mit der Teilmenge $\mathbb{Z} \cdot 1 \subseteq K$ identifizieren (Bemerkung II.2.6). Ist eine nichtleere Teilmenge $M \subseteq \mathbb{Z}$ nach oben bzw. nach unten beschränkt, so besitzt sie ein Maximum bzw. ein Minimum: Zunächst existiert $m := \sup(M)$. Gemäß Lemma II.2.14 existiert ein $x \in M$ mit $x > m - 1$. Für $y \in M$ ist nun $y \leq m < x + 1$ und daher $y \leq x$, wegen $x, y \in \mathbb{Z}$. Somit ist $x = \max(M) = m$. Analog zeigt man, dass eine nach unten beschränkte Teilmenge von $\mathbb{Z}$ ein Minimum besitzt. ■

Satz von Archimedes

Satz II.2.19. *Ist K ein vollständig angeordneter Körper und $a, b, \in K$ mit $b > 0$, so existiert ein $n \in \mathbb{N}$ mit $nb > a$.*

Beweis. Sei $M := \{nb: n \in \mathbb{N}\}$. Wir führen einen indirekten Beweis. Ist die Behauptung falsch, so ist $M \leq a$, die Menge M hat also nach dem Vollständigkeitsaxiom ein Supremum $s = \sup(M)$. Wegen Lemma II.2.14 existiert ein $n \in \mathbb{N}$ mit $nb > s - b$. Dann ist $(n+1)b > s$, was der Annahme widerspricht. ■

Einen Körper, in dem der Satz von Archimedes gilt, nennt man *archimedisch geordnet*, z.B. ist der geordnete Körper $(\mathbb{Q}, \mathbb{Q}_+)$ archimedisch geordnet. Obiger Satz wird oft „Axiom des Archimedes“ genannt, da er als Axiom in der Geometrie der Griechen eine zentrale Rolle spielte. Bei uns folgt er aus dem Vollständigkeitsaxiom. Denkt man sich a und b als die Länge von Streckenstücken, so besagt er, dass man durch Aneinanderlegen einer ausreichend großen Zahl von Strecken der Länge b eine Strecke erhält, die länger als a ist. Da sich die Griechen positive Zahlen als etwas vorstellten, womit man Strecken messen kann, ist das Archimedische Axiom eine sehr natürliche Anforderung an diese „Meßzahlen“. Man kann zeigen, dass vollständig angeordnete Körper in einem gewissen Sinn maximal archimedisch angeordnet sind. Man kann sich das so vorstellen, dass sie die größtmöglichen Körper sind, deren positive Elemente Streckenlängen entsprechen.

Folgerung II.2.20. *Ist $a < b$, so enthält das Intervall $]a, b[$ eine rationale Zahl (vgl.* Bemerkung II.2.6*).*

Beweis. Wegen $b - a > 0$ existiert nach Archimedes (Satz II.2.19) eine natürliche Zahl $n \in \mathbb{N}$ mit $n(b-a) > 1$, also $\frac{1}{n} < b - a$. Weiter existiert $m := \max\{x \in \mathbb{Z} \colon x \leq na\}$ nach Bemerkung II.2.18(b). Dann ist $\frac{m}{n} \leq a$ und $\frac{m+1}{n} > a$, wegen der Maximalität von m. Andrerseits ist

$$\frac{m+1}{n} = \frac{m}{n} + \frac{1}{n} < a + (b-a) = b$$

und somit $a < \frac{m+1}{n} < b$. Da offensichtlich $\frac{m+1}{n} \in \mathbb{Q}$ gilt, haben wir die Behauptung gezeigt. ■

Wir kommen nun zur Existenz von Wurzeln aus positiven Elementen eines vollständig angeordneten Körpers K.

Satz II.2.21. (Existenz k-ter Wurzeln) *Sei K ein vollständig angeordneter Körper. Für jedes $k \in \mathbb{N}$ und $a \geq 0$ existiert genau ein $b \geq 0$ mit $b^k = a$.*

Beweis. Der Fall $a = 0$ ist trivial (Nachweis!). Wir dürfen daher $a > 0$ annehmen.
Eindeutigkeit: Für $0 \leq b < c$ gilt nach Aufgabe II.2.1(b) die Beziehung $b^k < c^k$. Also existiert höchstens ein $b \geq 0$ mit $b^k = a$.
Existenz: Wir betrachten die Menge

$$M := \{x \in [0, \infty[\colon x^k \leq a\}.$$

Dann ist $0 \in M$ und daher $M \neq \emptyset$. Für $y := \max(1, a)$ und $x > y$ gilt

$$x^k > y^k \geq y \geq a$$

(vgl. Aufgabe II.2.1(b)). Also ist $M \leq y$, d.h., M ist nach oben beschränkt. Wegen dem Vollständigkeitsaxiom existiert daher

$$b := \sup M.$$

Wie zeigen $b^k = a$. Sei dazu

$$C := k \cdot \max\Big\{\binom{k}{j} b^{k-j} \colon j = 1, \ldots, k\Big\}.$$

Aus dem Binomischen Lehrsatz folgt dann für $0 < h < 1$:

$$(b+h)^k = b^k + \sum_{j=1}^{k} \binom{k}{j} b^{k-j} h^j \leq b^k + \sum_{j=1}^{k} \frac{1}{k} C h^j \leq b^k + hC$$

und entsprechend

$$(b-h)^k = b^k + \sum_{j=1}^{k} \binom{k}{j} (-1)^j h^j b^{k-j} \geq b^k - \sum_{j=1}^{k} \binom{k}{j} h^j b^{k-j} \geq b^k - hC.$$

Ist $b^k < a$, so setzen wir $h := \frac{1}{2}\min\left(1, \frac{a-b^k}{C}\right)$. Für dieses h erhalten wir mit obiger Abschätzung

$$(b+h)^k \leq b^k + hC < b^k + a - b^k = a,$$

im Widerspruch zur Definition von b, denn $b + h > b$. Gilt $b^k > a$, so erhalten wir für $0 < h < \min\left(1, \frac{b^k-a}{C}\right)$ entsprechend

$$(b-h)^k \geq b^k - hC > b^k + a - b^k = a,$$

im Widerspruch zur Definition von b. Da die Annahme $b^k \neq a$ zu einem Widerspruch führt, ist daher $b^k = a$ und somit die Existenz eines $b > 0$ mit $b^k = a$ gezeigt. ■

Definition II.2.22. Ist $a \in K$ mit $a \geq 0$ und $k \in \mathbb{N}$, so schreiben wir $\sqrt[k]{a}$ für die k-te Wurzel aus a. Für $\frac{p}{q} \in \mathbb{Q}$ mit $q \in \mathbb{N}$ und $a > 0$ setzen wir

$$a^{\frac{p}{q}} := \sqrt[q]{a^p} = (\sqrt[q]{a})^p \quad \text{und} \quad 0^{\frac{p}{q}} := 0 \quad \text{für } p > 0.$$ ■

Aufgabe II.2.4. Zeigen Sie:

(a) Für $0 < x < y$ in K und $q \in \mathbb{Q}_+$ gilt $x^q < y^q$.

(b) Für $0 < x, y$ in K und $q \in \mathbb{Q}_+$ gilt $(xy)^q = x^q y^q$. Hinweis: Man betrachte zuerst den Fall $q \in \mathbb{N}$ bzw. $\mathbb{Z}$ und dann den Fall $q = \frac{1}{k}$, $k \in \mathbb{N}$. Schließlich setze man beides zusammen. ■

Aufgabe II.2.5. Zeigen Sie: Der angeordnete Körper $\mathbb{Q}$ ist nicht vollständig. Hierzu betrachte man die Menge

$$M := \{x \in \mathbb{Q} \colon 0 \leq x, x^2 \leq 2\}$$

und zeige wie im Beweis von Satz II.2.11, dass M beschränkt ist. Welche Eigenschaft hätte $s = \sup(M)$, wenn solch ein Element in $\mathbb{Q}$ existieren würde? ■

Die rellen Zahlen

Für die Zwecke der Analysis ist es sekundär, wie man die reellen Zahlen konstruiert, denn hierzu gibt es viele Methoden, die alle zum gleichen Ziel führen. Wir müssen von den reellen Zahlen nur ihre arithmetischen und die Ordnungseigenschaften kennen. Wie wir sogleich präzisieren werden, sind all diese Eigenschaften vollständig dadurch bestimmt, dass die reellen Zahlen einen vollständig angeordneten Körper bilden, d.h. je zwei vollständig angeordnete Körper lassen sich nicht durch Eigenschaften der Ordnung oder ihrer Arithmetik unterscheiden. Man spricht dann von *isomorphen* angeordneten Körpern.

Definition II.2.23. Seien (K, K_+) und (L, L_+) angeordnete Körper. Eine Abbildung $f : K \to L$ heißt *Homomorphismus von angeordneten Körpern*, wenn die Bedingungen

(a) $(\forall x, y \in K)\ f(x + y) = f(x) + f(y)$

(b) $(\forall x, y \in K)\ f(xy) = f(x) \cdot f(y)$

(c) $f(K_+) \subseteq L_+$

gelten. Die Abbildung f heißt *Isomorphismus von angeordneten Körpern*, wenn f zusätzlich bijektiv ist. Existiert solch ein Isomorphismus, so nennen wir (K, K_+) und (L, L_+) *isomorph.* ∎

Man sollte sich dies so vorstellen, dass sich isomorphe angeordnete Körper nur durch die Bezeichnung ihrer Elemente unterscheiden, und dass sie durch die Umbenennung ihrer Elemente, die durch einen Isomorphismus realisiert wird, auseinander hervorgehen. In diesem Sinne stellen wir uns isomorphe angeordnete Körper als im wesentlichen gleiche mathematische Objekte vor.

Theorem II.2.24. (Eindeutigkeitssatz) *Zwei vollständig angeordnete Körper sind zueinander isomorph.*

Beweis. Für einen schönen, gut lesbaren Beweis verweisen wir auf das schöne Buch von B. Artmann, „Der Zahlbegriff“.

Wir schildern hier nur kurz die Grundidee des Beweises. Seien K und L vollständig angeordneter Körper. Für eine nach oben beschränkte Teilmenge $M \subseteq K$ schreiben wir $\sup_K M$ für deren Supremum und analog $\sup_L M$ für eine Teilmenge M von L. Wir haben schon gesehen, dass wir $\mathbb{Q}$ als Unterkörper von K und L auffassen können (Bemerkung II.2.6). Wir betrachten nun die Abbildung

$$\Phi\colon K \to L, \quad \Phi(x) := \sup_L\{q \in \mathbb{Q}\colon q < x\}.$$

Hierbei existiert $\Phi(x)$, da $\mathbb{N}$ in L unbeschränkt ist, und die Existenz eines $q \in \mathbb{Q}$ mit $q < x$ erhalten wir aus Folgerung II.2.20, die zeigt, dass das Intervall $]x - 1, x[\subseteq K$ eine rationale Zahl enthält.

Sind $x, y \in K$ mit $x < y$, so enthält das Intervall $]x, y[$ ebenfalls eine rationale Zahl. Also ist $\Phi(x) \neq \Phi(y)$, d.h., Φ ist injektiv.

Wir zeigen noch, dass Φ surjektiv ist. Sei dazu $s \in L$ und

$$x := \sup_K\{q \in \mathbb{Q}\colon q < s\}.$$

Wir zeigen $s = \Phi(x)$. In der Tat ist $\{q \in \mathbb{Q}\colon q < s\} = \{q \in \mathbb{Q}\colon q < x\}$, so dass die Behauptung aus

$$\Phi(x) = \sup_L\{q \in \mathbb{Q}\colon q < x\} = \sup_L\{q \in \mathbb{Q}\colon q < s\} = s$$

folgt. Die letzte Gleichheit ist wieder eine Konsequenz aus Folgerung II.2.20. Wir haben damit eingesehen, dass $\Phi\colon K \to L$ bijektiv ist.

Jetzt hat man sich nur noch davon zu überzeugen, dass Φ Addition, Multiplikation und Ordnung respektiert. Das ist wieder etwas technisch und wir verweisen auf das Artmannsche Buch. ∎

Mit dem Eindeutigkeitssatz wird klar, dass es bis auf Isomorphie höchstens einen vollständig angeordneten Körper gibt. Daher ist das folgende Axiom sinnvoll.

Axiomatische Beschreibung der reellen Zahlen

$(\mathbb{R}, +, \cdot, \mathbb{R}_+)$ IST EIN VOLLSTÄNDIG ANGEORDNETEN KÖRPER

Damit ist sehr präzise zusammengefasst, als was wir die reellen Zahlen verstehen wollen. Die Gesamtheit der Axiome eines vollständig angeordneten Körpers bilden die Regeln, die wir beim Umgang mit reellen Zahlen einhalten müssen. Ausgehend von dieser axiomatischen Fixierung werden wir nun darangehen, die reellen Zahlen zu studieren. Hierbei wird sich schnell herausstellen, dass die Bilder, die man sich von den reellen Zahlen macht, ihre Eigenschaften sehr gut wiedergeben.

Die komplexen Zahlen

Da die reellen Zahlen einen angeordneten Körper bilden, sind alle Quadrate nichtnegativ und die Zahl -1 ist in $\mathbb{R}$ kein Quadrat. Insbesondere können wir die Konstruktion aus Aufgabe II.1 anwenden und erhalten einen Körper

$$\mathbb{C} := \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$$

dessen Addition und Multiplikation wie folgt aussehen:

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

Wir nennen die Elemente von $\mathbb{C}$ *komplexe Zahlen.*

Der Nachweis der Körperaxiome ist eine elementare Verifikation (Aufgabe II.1). Das Einselement ist $1 = (1,0)$. Wir schreiben

$$i := (0,1).$$

Dann gilt $i^2 = (-1,0) = -1$, d.h., in $\mathbb{C}$ ist -1 ein Quadrat.

Die reellen Zahlen finden wir in $\mathbb{C}$ leicht wieder, da

$$(a,0) + (c,0) := (a+c, 0), \quad \text{und} \quad (a,0) \cdot (c,0) := (ac, 0)$$

für alle $a, c \in \mathbb{R}$ gilt, d.h., die Abbildung

$$\varphi\colon \mathbb{R} \to \mathbb{C}, \quad x \mapsto (x,0)$$

ist eine Einbettung von Körpern. In diesem Sinne dürfen wir $\mathbb{R}$ als Unterkörper von $\mathbb{C}$ auffassen, was wir von nun an tun werden.

Jede komplexe Zahl (x, y) lässt sich in eindeutiger Weise schreiben als

$$(x, y) = x + iy, \quad x, y \in \mathbb{R}.$$

Von nun an wollen wir uns komplexe Zahlen immer in dieser Form vorstellen. Wir rechnen in dieser Darstellung wie folgt:

$$(a+ib)+(c+id) = (a+c)+i(b+d) \quad \text{und} \quad (a+ib)(c+id) = (ac-bd)+i(bc+ad).$$

Definition II.2.25. Für $z = x + iy \in \mathbb{C}$ definieren wir:

(a) die *konjugierte Zahl* durch $\overline{z} := x - iy$.

(b) den *Betrag von* z durch $|z| := \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$. Man beachte, dass die Wurzel wegen $x^2 + y^2 \geq 0$ existiert.

(c) den *Realteil von* z*:* $\operatorname{Re} z := \frac{z+\overline{z}}{2} = x$.

(d) den *Imaginärteil von* z*:* $\operatorname{Im} z := \frac{z-\overline{z}}{2i} = y$. ■

Lemma II.2.26. *Für* $z, w \in \mathbb{C}$ *gilt:*

(i) $\overline{zw} = \overline{z} \cdot \overline{w}$.

(ii) *Für* $z \neq 0$ *ist* $z^{-1} = \frac{\overline{z}}{|z|^2}$.

(iii) $|zw| = |z| \cdot |w|$.

Beweis. (i) rechnet man sofort nach.

(ii) Wegen $z \neq 0$ ist $|z| > 0$, und die Behauptung ergibt sich aus (i) und $|z|^2 = z\overline{z}$ (vgl. Aufgabe II.1).

(iii) ergibt sich direkt aus (i), da:

$$|zw| = \sqrt{zw\overline{zw}} = \sqrt{z\overline{z}w\overline{w}} = \sqrt{z\overline{z}}\sqrt{w\overline{w}} = |z| \cdot |w|$$

(vgl. Aufgabe II.2.3(b)). ■