

Analysis I

Sebastian Baader

Herbstsemester 2020

Über dieses Dokument

Das ist eine Mitschrift der Vorlesung “Analysis 1” von Prof. Dr. Sebastian Baader im Herbstsemester 2020. Du darfst sie so verwenden, wie sie dir am meisten beim Verständnis des Materials hilft. Verantwortlich dafür was hier drin steht ist Levi Ryffel. Denke daran dass der Dozent dieses Dokument nicht schreibt (und vielleicht auch nicht liest). Ihn trifft keine Verantwortung, falls Unsinn steht.

Dein Beitrag

Diese Vorlesungsnotizen werden in Echtzeit während der Vorlesung mitgeschrieben und werden deshalb viele Probleme enthalten. Damit sind allerlei Missgeschicke gemeint wie zum Beispiel Symbolverwechslungen, unpräzise Aussagen und Argumente, alternative Rechtschreibung und Grammatik, oder unattraktives Layout. Falls dir so etwas auffällt, auch wenn es dich nicht stark stört, und auch wenn du es als etwas subjektiv empfindest, poste doch auf

<https://github.com/raw-bacon/ana1-notes>,

ein “Issue”, oder sende eine E-Mail an levi.ryffel@math.unibe.ch. Auf demselben Weg kannst du Wünsche und Verbesserungsvorschläge zu dieser Mitschrift anbringen.

Inhaltsverzeichnis

I	Konstruktion der Reellen Zahlen	3
1	Historische Motivation	3
2	Mengen im Vergleich	5
3	Gruppen und Körper	10
4	Konstruktion der reellen Zahlen	13

Kapitel I

Konstruktion der Reellen Zahlen

1 Historische Motivation

In der Antike war Mathematik praktisch synonym mit Geometrie. Der Zahlenbegriff war direkt an das Konzept der *Länge* gekoppelt.

Definition (Euklid, 300 vor Christus). Zwei Längen $a, b > 0$ heissen *kommensurabel*, falls eine Länge $L > 0$ existiert, so wie zwei natürliche Zahlen $m, n \in \mathbb{N}$, so dass $a = mL$ und $b = nL$.

Hier ist

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

die Menge der Natürlichen Zahlen.

Theorem (Euklid). *Die Seite und Diagonale eines ebenen Quadrats sind nicht kommensurabel.*

Beweis. Dieser Beweis ist geometrisch, nach Euklid. Wir nehmen an, es gäbe $L > 0$ und $m, n \in \mathbb{N}$ mit $x = mL$ und $d = nL$. Wir zeigen, dass das zu einem Widerspruch führt. Wir stellen fest, dass die Längen $x_1 = d - x$ und $d_1 = 2x - d$ ebenfalls die Seite und Diagonale eines Quadrats bilden, siehe Abbildung I.1.



Abbildung I.1: Euklids Konstruktion

Weiterhin gilt, dass sowohl x_1 als auch d_1 , ganze Vielfache von L sind:

$$\begin{aligned}x_1 &= d - x = (n - m)L \\d_1 &= 2x - d = (2m - n)L\end{aligned}$$

Nach Pythagoras gilt $d^2 = 2x^2$, und somit $d \leq 3/2 \cdot x$, da $(3/2)^2 > 2$. Daraus folgt, dass

$$x_1 = d - x \leq \frac{1}{2} \cdot x.$$

Iteriere dieses Verfahren und erhalte eine Serie von Quadraten mit Seiten x_2, x_3, \dots und Diagonalen d_2, d_3, \dots . Es gilt:

$$x_k \leq \frac{1}{2^k} \cdot x.$$

Ausserdem ist jedes x_k (und d_k) ein ganzes Vielfaches von L . Wähle nun k so gross, dass

$$x_k \leq \frac{1}{2^k} x < L.$$

Dies, zusammen mit dem Fakt, dass x_k ein ganzes Vielfaches von L ist, impliziert, dass $x_k = 0$, was unmöglich ist. Deshalb können x und d nicht kommensurabel sein. \square

Wir haben diese Aussage mit einem sogenannten *Widerspruchsbeweis* bewiesen. Hierfür haben wir eine Annahme getroffen, und diese zu einem Widerspruch geführt. Dies zeigt, dass unsere Annahme falsch war.

Zeitgenössische Umformulierung

Seien $a, b > 0$ zwei kommensurable Längen. Das heisst, es existieren $L > 0$ und $m, n \in \mathbb{N}$ mit $a = mL$, $b = nL$. Dann gilt:

$$\frac{a}{b} = \frac{mL}{nL} = \frac{m}{n},$$

das heisst das Verhältnis a/b ist eine *rationale Zahl*. Zurück zum Quadrat mit Seite x und Diagonale d . Nach Pythagoras gilt $d^2 = 2x^2$. Falls $x = mL$ und $d = nL$ gilt, dann also

$$2 = \frac{d^2}{x^2} = \left(\frac{d}{x}\right)^2 = \left(\frac{n}{m}\right)^2,$$

und somit

$$2m^2 = n^2. \tag{1}$$

Die linke Seite dieser Gleichung ist durch 2 teilbar. Dies impliziert, dass n^2 , und somit auch n , durch 2 teilbar ist. Schreibe nun $n = 2k$. Schreibe $n = 2k$ mit $k \in \mathbb{N}$. Setze das in die Gleichung (1) ein und erhalte $2m^2 = (2k)^2 = 4k^2$, beziehungsweise

$$m^2 = 2k^2.$$

Die rechte Seite ist durch 2 teilbar, also auch m . Wir schliessen, dass sowohl n als auch m durch 2 teilbar sind. Schreibe noch $m = 2\ell$ mit $\ell \in \mathbb{N}$. Es gilt also

$$2 = \left(\frac{n}{m}\right)^2 = \left(\frac{k}{\ell}\right)^2.$$

In anderen Worten sind Zähler und Nenner beide gerade. Iteriere dieses Verfahren k mal, bis $n/2^k < 1$, Dann entsteht ein Widerspruch.

Korollar. Die Gleichung $z^2 = 2$ hat keine rationale Lösung, das heisst, keine Lösung der Form $z = p/q$ mit $p, q \in \mathbb{N}$ und $q > 0$.

Das Ziel für den Rest dieses Kapitels ist es, eine Zahlenmenge \mathbb{R} (die Menge der *reellen Zahlen*) zu konstruieren, in welcher die Gleichung $z^2 = 2$ eine Lösung hat.

Übung. Die Gleichung $z = \sqrt{2}x + \sqrt{3}y$ hat keine ganze Lösungen ausser $(0, 0, 0)$.

2 Mengen im Vergleich

Wir haben bereits einige Mengen erwähnt, nämlich die *natürlichen Zahlen*

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

die Menge der *ganzen Zahlen*,

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\},$$

und die Menge der *rationalen Zahlen*

$$\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q > 0\}.$$

Wir wollen eine weitere Menge, die Menge \mathbb{R} der *reellen Zahlen* einführen. Es gelten dann die Inklusionen

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Wichtige Grundbegriffe

Definition. Seien A, B zwei Mengen. Eine *Abbildung* zwischen A und B , in Symbolen, $f: A \rightarrow B$, ist eine Zuordnung $f(a) \in B$ für jedes $a \in A$. Eine Abbildung $f: A \rightarrow B$ heisst

- (i) *injektiv*, falls für alle $a_2, a_1 \in A$ mit $a_2 \neq a_1$ gilt, dass $f(a_1) \neq f(a_2)$,
- (ii) *surjektiv*, falls für alle $b \in B$ ein Element $a \in A$ existiert mit $f(a) = b$,
- (iii) *bijektiv*, falls f sowohl injektiv als auch surjektiv ist.

Beispiel.

- (i) Seien $A = B = \{0, 1\}$. Es gibt 4 Abbildungen $f: A \rightarrow B$:

- (a) $0 \mapsto 0$ und $1 \mapsto 0$,
- (b) $0 \mapsto 1$ und $1 \mapsto 1$,
- (c) $0 \mapsto 0$ und $1 \mapsto 1$,
- (d) $0 \mapsto 1$ und $1 \mapsto 0$.

Abbildungen (a) und (b) sind weder injektiv noch surjektiv. Abbildungen (c) und (d) sind beide bijektiv.

- (ii) Seien $A = B = \mathbb{N}$. Betrachte die Abbildung

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

Diese Abbildung ist injektiv, aber nicht surjektiv. Die Abbildung

$$\begin{aligned} g: \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto \frac{2n - 1 + (-1)^n}{4}, \end{aligned}$$

also die Abbildung die durch 2 dividiert und dann abrundet, ist nicht injektiv, aber surjektiv. Um zu sehen, dass $g(n) = \lfloor n/2 \rfloor$, betrachte zwei Fälle:

- (a) $n = 2k$ ist gerade. Dann ist $g(n) = (4k + 1 - 1)/4 = k$.
- (b) $n = 2k + 1$ ist ungerade. Dann ist $g(n) = (4k + 2 - 1 - 1)/4 = k$.

Bemerkung.

- (1) Bijektive Abbildungen $f: A \rightarrow B$ haben eine eindeutige *Umkehrabbildung* $f^{-1}: B \rightarrow A$. Die Konstruktion dafür ist wie folgt. Sei $b \in B$. Da f surjektiv ist, existiert $a \in A$ mit $f(a) = b$. Da f injektiv ist, ist dieses a eindeutig. Setze $f^{-1}(b) = a$. Es gilt dann

$$f^{-1}(f(a)) = a$$

für alle $a \in A$, und ebenso

$$f(f^{-1}(b)) = b$$

für alle $b \in B$. Wir schreiben häufig

$$\begin{aligned} f^{-1} \circ f &= \text{Id}_A, \\ f \circ f^{-1} &= \text{Id}_B, \end{aligned}$$

in Worten, “ f^{-1} verknüpft mit f ist die Identitätsabbildung auf A ” und ähnlich, “ f verknüpft mit f^{-1} ist die Identitätsabbildung auf B ”

- (2) Für endliche Mengen A und B gilt: Es existiert eine bijektive Abbildung $f: A \rightarrow B$, genau dann, wenn A und B gleich viele Elemente haben.

Definition. Eine Menge A heisst

- (i) *unendlich*, falls eine injektive, nicht surjektive Abbildung $f: A \rightarrow A$ existiert,
- (ii) *abzählbar*, falls eine bijektive Abbildung $f: \mathbb{N} \rightarrow A$ existiert.

Beispiel. Sei $A = \mathbb{N}$. Die Abbildung f aus Beispiel (ii) ist injektiv, aber nicht surjektiv. Also ist \mathbb{N} eine unendliche Menge.

Beispiel. Sei M eine Menge, welche \mathbb{N} als Teilmenge enthält (zum Beispiel $M = \mathbb{Q}$). Dann ist M unendlich. Betrachte dazu die Abbildung

$$f: M \rightarrow M$$

$$x \mapsto \begin{cases} x+1 & \text{falls } x \in \mathbb{N} \subset M, \\ x & \text{falls } x \in M \setminus \mathbb{N} \end{cases}$$

Folgende Proposition zeigt in einem gewissen Sinn, dass es gleich viele Brüche wie natürliche Zahlen gibt. Dies ist unser erstes potentiell überraschendes Resultat.

Proposition 1. Die Menge \mathbb{Q} der rationalen Zahlen ist abzählbar.

Beweis. Wir konstruieren eine Bijektion $\varphi: \mathbb{N} \rightarrow \mathbb{Q}$. Für $k \in \mathbb{N}$ mit $k \geq 1$ definiere

$$A_k = \{p/q \mid p, q \in \mathbb{Z}, q \geq 1, p/q \text{ ist gekürzt}, |p| + |q| = k\}.$$

Alle solchen $A_k \subset \mathbb{Q}$ sind endlich und

$$\mathbb{Q} = \bigcup_{k \geq 1} A_k$$

ist die *disjunkte Vereinigung* dieser Mengen. Wir haben

$$A_1 = \{0/1\}, A_2 = \{\pm 1/1\}, A_3 = \{\pm 1/2, \pm 2/1\}, \dots$$

Sei $a_k = |A_k|$ die Anzahl Elemente von A_k . Definiere Teilmengen $B_k \subset \mathbb{N}$ mit $|B_k| = a_k$. Dazu setze $B_1 = \{0\}$, und für $k \geq 2$ setze

$$B_k = \{a_1 + \dots + a_{k-1}, a_1 + \dots + a_{k-1} + 1, \dots, a_1 + \dots + a_{k-1} + a_k - 1\}.$$

Es gilt dann

$$B_1 = \{0\}, B_2 = \{1, 2\}, B_3 = \{3, 4, 5, 6\}, \dots$$

Wähle eine Bijektion $\varphi_k: B_k \rightarrow A_k$ für alle $k \geq 1$. Definiere nun

$$\varphi: \mathbb{N} \rightarrow \mathbb{Q}$$

$$n \mapsto \varphi_k(n) \text{ falls } n \in B_k.$$

Die Abbildung φ ist eine Bijektion, da \mathbb{N} die disjunkte Vereinigung der B_k und \mathbb{Q} die disjunkte Vereinigung der A_k ist. □

Dieser Beweis zeigt allgemeiner, dass jede Menge, die eine abzählbare Vereinigung endlicher Mengen ist, selber abzählbar ist. Man könnte diese Aussage zum Beispiel für Aufgabe 5 auf Serie 1 verwenden.

Frage. Ist jede unendliche Menge abzählbar?

Georg Cantor hat ca. 1870 als erste Person die Antwort “nein” auf diese Frage festgehalten. Wir konstruieren nun nach seiner Idee eine Menge, die nicht abzählbar ist. Dazu betrachten wir die *Potenzmenge* $P(M)$ einer Menge M , definiert als die “Menge aller Teilmengen von M ”. Ein wenig formaler,

$$P(M) = \{A \mid A \subset M\}.$$

Beispiel. Sei $M = \{0, 1\}$. Dann ist

$$P(M) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Hier bedeutet \emptyset die *leere Menge*.

Bemerkung. Falls die Menge M selbst n Elemente hat, dann hat ihre Potenzmenge 2^n Elemente. Um das zu beweisen, bilden wir jede Teilmenge A von M auf die Funktion

$$f_A: M \rightarrow \{0, 1\}$$

$$x \mapsto \begin{cases} 0, & \text{falls } x \notin A, \\ 1, & \text{falls } x \in A, \end{cases}$$

ab. Diese Abbildung $A \mapsto f_A$ ist eine Bijektion zwischen $P(M)$ und der Menge von Funktionen $f: M \rightarrow \{0, 1\}$, und es gibt 2^n solche Funktionen.

Proposition 2 (Cantor). *Sei M eine beliebige Menge. Dann existiert keine surjektive Abbildung $\varphi: M \rightarrow P(M)$. Insbesondere existiert keine Bijektion $\varphi: M \rightarrow P(M)$.*

Korollar. *Die Potenzmenge $P(\mathbb{N})$ ist nicht abzählbar.*

Beweis der Proposition. Wir führen einen klassischen Widerspruchsbeweis. Wir nehmen an, es gäbe doch eine solche Surjektion $\varphi: M \rightarrow P(M)$. Betrachte nun die Teilmenge A von M aller x , die nicht in $\varphi(x)$ enthalten sind. In Symbolen,

$$A = \{x \in M \mid x \notin \varphi(x)\}.$$

Die Forderung $x \notin \varphi(x)$ macht Sinn, da $\varphi(x)$ selbst eine Teilmenge von M ist. Da φ surjektiv ist, muss ein $a \in M$ existieren mit $\varphi(a) = A$. Wir fragen nun, ob $a \in A$ ist oder nicht. Wäre $a \in A$, so müsste nach Definition von A gelten, dass $a \notin \varphi(a)$. Aber das widerspricht der Definition von $\varphi(a) = A$. Wäre jedoch $a \notin A$, dann wäre die Bedingung $a \notin \varphi(a)$ erfüllt, also $a \in A$. Aber da $A = \varphi(a)$, widerspricht auch dies der Definition von A . Somit führen beide Möglichkeiten zu einem Widerspruch. Dies bedeutet, dass unsere ursprüngliche Annahme, dass eine Surjektion $\varphi: M \rightarrow P(M)$ existiert, verworfen werden muss: Es kann keine solche Abbildung geben. \square

Einschub: Beweismethoden

Ein *Beweis* ist eine “Deduktion einer Aussage aus bereits bewiesenen Aussagen oder Grundaxiomen”. Wichtig ist hier, dass die Deduktion logisch korrekt erfolgt. Folgende Beweismethoden sind typisch.

- Geometrische Beweise, zum Beispiel mit Hilfe von Euklids Axiomen. Das erste Theorem der Vorlesung haben wir so bewiesen.
- Beweise mithilfe von logischen Schlussfolgerungen, zum Beispiel Widerspruchsbeweise. Proposition 2 haben wir so bewiesen.
- Kombinatorische Beweise, zum Beispiel Beweise mit vollständiger Induktion.

Wir führen nun ein Beispiel eines Beweises durch vollständige Induktion.

Definition. Die n -te *Catalanzahl* C_n ist die Anzahl korrekte Klammerungen mit $2n$ Klammern (n linke und n rechte Klammern).

Beispiele.

- $C_1 = 1$, die einzige Korrekte Klammerung ist $()$.
- $C_2 = 2$, die Klammerungen $()()$ und $(())$ sind beide korrekt.
- $C_3 = 5$.

Behauptung. Die n -te *Catalanzahl* C_n erfüllt $C_n \geq 2^{n-1}$.

Beweis durch vollständige Induktion. Für die *Induktionsverankerung* testen wir die Aussage für $n = 1$: Tatsächlich ist $C_1 \geq 2^0$.

Die *Induktionsannahme* ist nun, dass die Aussage für ein festes $n \in \mathbb{N}$ stimmt.

Im *Induktionsschritt* leiten wir nun die Aussage für $n + 1$ aus der Induktionsannahme (für n) her. Hier heisst das, dass wir $C_{n+1} \geq 2^n$ aus $C_n \geq 2^{n-1}$ herleiten wollen. Sei dazu K eine korrekte n -Klammerung, das heisst eine korrekte Klammerung mit n linken und n rechten Klammern. Dann sind sowohl (K) als auch $()K$ korrekte $(n + 1)$ -Klammerungen. Weiter gilt, dass diese beiden Klammerungen verschieden sind: Die erste der beiden Klammerungen beginnt mit zwei geöffneten Klammern, wobei die zweite mit einer geöffneten und einer geschlossenen Klammer beginnt. Weiter gilt, dass für verschiedene korrekte n -Klammerungen K_1 und K_2 auch $()K_1, (K_1), ()K_2, (K_2)$ verschieden sind (wieso?). Wir können also aus jeder korrekten n -Klammerung zwei korrekte $(n + 1)$ -Klammerungen konstruieren. Somit folgt, dass

$$C_{n+1} \geq 2C_n \geq 2 \cdot 2^{n-1} = 2^n.$$

Dies zeigt die Aussage für $n + 1$. □

In Serie 1 sehen wir, dass sogar $C_n \geq 3^n$ gilt, jedenfalls für $n \geq 17$. Um dies zu zeigen reicht es aber nicht, zu bemerken, dass neben (K) und $()K$ auch $K()$ eine korrekte Klammerung ist. Diese könnte nämlich mit $()K$ übereinstimmen. Hierzu brauchen wir die Formel in folgender Bemerkung.

Bemerkung. Es gilt

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1} \binom{2n}{n}.$$

Die zweite Gleichheit ist eine einfache Rechnung. Wir rechtfertigen die erste Gleichheit. Der erste der Binomialkoeffizienten zählt alle n -Klammerungen (auch inkorrekte). Der zweite Binomialkoeffizient zählt die Anzahl inkorrektur Klammerungen. Man kann sich dies folgendermassen skizzenhaft überlegen. Eine inkorrekte Klammerung hat eine erste Position, wo eine rechte Klammer zuviel ist. Drehe alle Klammern hinter dieser Position um. Die Klammerung die wir so erhalten, hat $n+1$ rechte Klammern. Weiter kann man diesen Prozess rückgängig machen: Jede Klammerung mit $n+1$ rechten Klammern liefert eine inkorrekte Klammerung mit n rechten Klammern. Also sind die schlechten n -Klammerungen in Bijektion mit der Anzahl Klammerungen mit $n+1$ rechten (und $n-1$ linken) Klammern.

3 Gruppen und Körper

Definition. Eine *Gruppe* ist eine Menge G mit einer *Verknüpfung* $\circ: G \times G \rightarrow G$, welche folgende Eigenschaften erfüllt.

- (i) Es existiert ein Element $e \in G$, so dass für alle $g \in G$ gilt, dass $g \circ e = e \circ g = g$.
- (ii) Für alle $g \in G$ existiert ein $h \in G$ mit $g \circ h = h \circ g = e$.
- (iii) Für alle $a, b, c \in G$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

Notation.

- (i) Das Element e bezeichnen wir als das *neutrale Element*.
- (ii) Wir schreiben häufig g^{-1} für h und nennen g^{-1} das zu g *inverse Element*.
- (iii) Das Gesetz $(a \circ b) \circ c = a \circ (b \circ c)$ nennt man das *Assoziativgesetz*.

Beispiele.

- Die Menge $G = \{e\}$ mit der Operation $e \circ e = e$ ist eine Gruppe (sie heisst *triviale Gruppe*).
- Die Menge $\{e, a\}$ mit Verknüpfungstabelle zu finden in Tabelle I.1 bildet eine Gruppe.
- Die Menge $\{e, a, b\}$ mit Verknüpfungstabelle zu finden in Tabelle I.2 bildet eine Gruppe. Hier kann man a als ebene Drehung um 0 mit Winkel $2\pi/3$ interpretieren. Ähnlich ist b eine Drehung mit Winkel $4\pi/3$.

	e	a
e	e	a
a	a	e

Tabelle I.1: Verknüpfungstabelle von $\{e, a\}$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabelle I.2: Verknüpfungstabelle von $\{e, a, b\}$

- $(\mathbb{Z}, +)$ ist eine Gruppe.
- (\mathbb{Z}, \cdot) ist keine Gruppe. Zum Beispiel hat die Zahl $2 \in \mathbb{Z}$ kein inverses Element.
- $(\mathbb{Q}, +)$ ist eine Gruppe.
- (\mathbb{Q}, \cdot) ist keine Gruppe. Zum Beispiel hat $0 \in \mathbb{Q}$ kein inverses Element.

Proposition 3. *In jeder Gruppe G hat die Gleichung $a \circ x = c$ eine eindeutige Lösung $x \in G$. Hier sind a, c vorgegeben.*

Beweis. Wir zeigen Existenz und Eindeutigkeit separat. Wir wissen nach Axiom (ii), dass $b \in G$ existiert mit $b \circ a = e$. Multiplikation mit b von links auf beiden Seiten liefert $b \circ (a \circ x) = b \circ c$. Axiom (iii) sagt, dass die linke Seite

$$(b \circ a) \circ x = e \circ x = x$$

ist. Also ist $x = b \circ c = a^{-1} \circ c$ eine Lösung. Um Eindeutigkeit zu zeigen seien $x_1, x_2 \in G$ mit

$$a \circ x_1 = c = a \circ x_2.$$

Linksmultiplikation wie oben mit b liefert

$$b \circ (a \circ x_1) = b \circ (a \circ x_2).$$

Wir erhalten

$$(b \circ a) \circ x_1 = (b \circ a) \circ x_2.$$

Sobald wir uns erinnern, dass $b \circ a = e$, schliessen wir, dass $x_1 = x_2$. □

Spezialfälle.

- (1) Falls $a \circ x = a$ gilt, so ist $x = e$. Dies liefert Eindeutigkeit des neutralen Elements.
- (2) Falls $a \circ x = e$ gilt, so ist $x = a^{-1}$. Dies liefert Eindeutigkeit des inversen Elements.

Körper

Definition. Eine Menge K mit zwei Verknüpfungen $+, \cdot : K \times K \rightarrow K$ heisst *Körper*, falls

- (i) $(K, +)$ ist eine kommutative Gruppe mit neutralem Element $0 \in K$,
- (ii) $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element $1 \in K \setminus \{0\}$ (das heisst $1 \neq 0$),
- (iii) für alle $x, y, z \in K$ gilt das Distributivgesetz $x \cdot (y + z) = x \cdot y + x \cdot z$.

Wir halten uns hier an die Konvention, dass die Multiplikation stärker bindet als die Addition. Konkret haben wir oben

$$x \cdot y + x \cdot z = (x \cdot y) + (x \cdot z).$$

Dass (G, \circ) eine kommutative Gruppe ist, bedeutet, dass für alle $g, h \in G$ gilt, dass $g \circ h = h \circ g$.

Beispiele.

- (1) $K = \mathbb{Q}$ mit der üblichen Addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und üblichen Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

bildet einen Körper mit neutralen Elementen $0/1$ (für $+$) und $1/1$ (für \cdot). Die Rechengesetze (Assoziativität, Kommutativität und Distributivität) übertragen sich von den entsprechenden Gesetzen für die Menge der ganzen Zahlen \mathbb{Z} mit der üblichen Addition und Multiplikation. Diese wiederum wurden von Dedekind erstmals formal definiert (“was sind und sollen Zahlen”). Wir führen das in dieser Vorlesung nicht weiter aus.

- (2) $K = \{0, 1\}$ mit Verknüpfungstabellen wie in Tabelle I.3 ist ein Körper (der kleinste).

+	0	1	·	0	1
0	0	1	0	0	0
1	1	0	1	0	1

Tabelle I.3: Verknüpfungstabellen von $\{0, 1\}$

- (3) $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da nur ± 1 multiplikative Inverse haben.

Ausblick (Algebra). Sei $p \in \mathbb{N}$ prim. Dann ist die Menge

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$$

mit “Addieren und Multiplizieren modulo p ” ein Körper.

4 Konstruktion der reellen Zahlen

Ziel. Wir konstruieren eine Zahlenmenge \mathbb{R} , die Menge der reellen Zahlen, mit folgender Eigenschaft: Jede stetige Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$, welche negative und positive Werte annimmt, hat eine Nullstelle in \mathbb{R} . Insbesondere soll jede Funktion der Form $f(x) = x^2 - a$ mit $a > 0$ eine Nullstelle in \mathbb{R} haben. Folglich hat in \mathbb{R} jede positive Zahl $a > 0$ eine Quadratwurzel.

Wir konstruieren die reellen Zahlen nach Dedekind, ca. 1872.

Definition. Eine Teilmenge $D \subset \mathbb{Q}$ heisst *Dedekindscher Schnitt*, oder kurz *Schnitt*, falls

- (1) $D \neq \emptyset, D \neq \mathbb{Q}$,
- (2) für alle $x, y \in \mathbb{Q}$ mit $x \in D$ und $x \leq y$ gilt $y \in D$,
- (3) D hat kein kleinstes Element.

Intuitiv ist ein Schnitt eine “rechte Hälfte” von \mathbb{Q} , wobei die Grenze zwischen den Hälften nicht unbedingt bei 0 ist, und sie auch nicht als Element der rechten Hälfte gilt. Siehe auch Abbildung I.2.



Abbildung I.2: Ein Dedekindscher Schnitt

Beispiel. Sei $x = p/q \in \mathbb{Q}$. Setze $D_x = \{y \in \mathbb{Q} \mid y > x\} \subset \mathbb{Q}$. Dann ist D_x ein Schnitt. Wir nennen D_x einen *rationalen Schnitt*, da diese später die rationalen Zahlen in \mathbb{R} werden.

Bemerkung. Seien $D, D' \subset \mathbb{Q}$ zwei Schnitte mit $D \neq D'$. Dann existiert $x \in \mathbb{Q}$ mit entweder $x \in D$ und $x \notin D'$, oder $x \notin D$ und $x \in D'$. Im ersten Fall gilt $D' \subset D$, und im zweiten Fall gilt $D \subset D'$.

Frage. Sei $D \subset \mathbb{Q}$ ein Schnitt. Existiert eine Zahl $x \in \mathbb{Q}$ mit $D = D_x$? (Hier ist D_x die Menge aus dem Beispiel oben.)

Wie erwartet ist die Antwort nein, siehe Proposition 4 unten.

Definition. Die Menge \mathbb{R} der *reellen Zahlen* ist definiert als die Menge aller Dedekindscher Schnitte $D \subset \mathbb{Q}$.

Beispiele.

- Sei $p/q \in \mathbb{Q}$. Dann ist

$$D_{p/q} = \{x \in \mathbb{Q} \mid x > p/q\}$$

ein rationaler Schnitt. So erhalten wir eine “Einbettung” $\mathbb{Q} \rightarrow \mathbb{R}$.

- Nicht alle Schnitte sind rational. Zum Beispiel ist

$$D_{\sqrt{2}} = \{x \in \mathbb{Q} \mid x^2 > 2 \text{ oder } x < 0\}$$

kein rationaler Schnitt.

Proposition 4 (Cantor). *Die Menge \mathbb{R} ist überabzählbar, das heisst unendlich aber nicht abzählbar.*

Korollar. *Es gibt irrationale Schnitte, das heisst Schnitte $D \subset \mathbb{Q}$, welche nicht vom Typ D_x für $x \in \mathbb{Q}$ sind.*

Beweis. Die Menge \mathbb{Q} ist abzählbar (siehe Proposition 1). □

Beweis von Proposition 4. Wir erinnern uns an Proposition 2 und ihr Korollar, die sagten, dass die Potenzmenge $P(\mathbb{N})$ überabzählbar ist. Wir konstruieren nun eine injektive Abbildung $\psi: P(\mathbb{N}) \rightarrow \mathbb{R}$. Daraus folgt dann, dass \mathbb{R} überabzählbar ist.

Die Konstruktion von ψ ist folgendermassen. Sei $B \in P(\mathbb{N})$, das heisst $B \subset \mathbb{N}$. Schreibe $B = \{n_0, n_1, n_2, \dots\}$ mit $n_0 < n_1 < n_2 < \dots$. Diese Menge könnte auch endlich sein. Definiere einen Schnitt

$$D_B = \left\{ x \in \mathbb{Q} \mid x > \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^{n_k} \right\}.$$

Es gilt zum Beispiel:

- (1) Sei $B = \emptyset$. Wir halten uns an die Konvention “leere Summe gleich 0”. Es gilt also $D_{\emptyset} = D_0$.
- (2) Sei $B = \mathbb{N}$, das heisst $B = \{0, 1, 2, \dots\}$ (also $n_k = k$). Berechne

$$\begin{aligned} \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^k &= 1 + \frac{1}{3} + \left(\frac{1}{3}\right)^2 + \dots \\ &= \frac{1}{1 - 1/3} \\ &= \frac{3}{2}. \end{aligned}$$

Also ist $D_{\mathbb{N}} = D_{3/2}$.

Sei nun $B = \{n_0, n_1, \dots\} \subset \mathbb{N}$ beliebig. Dann gilt

$$\begin{aligned} 0 &\leq \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^{n_k} \\ &\leq \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^k \\ &= \frac{3}{2}. \end{aligned}$$

Also gilt $D_0 \supset D_B \supset D_{3/2}$. Insbesondere ist $D_B \neq \emptyset$ und $D_B \neq \mathbb{Q}$, das heisst D_B ist wirklich ein Schnitt. Setze nun

$$\psi(B) = D_B \in \mathbb{R}.$$

Wir behaupten nun, dass ψ injektiv ist. Konkreter, seien $B_1, B_2 \in P(\mathbb{N})$ mit $B_1 \neq B_2$. Wir zeigen, dass $D_{B_1} \neq D_{B_2}$. Schreibe dazu

$$\begin{aligned} B_1 &= \{m_0, m_1, m_2, \dots\} \text{ mit } m_0 < m_1 < m_2 < \dots, \\ B_2 &= \{n_0, n_1, n_2, \dots\} \text{ mit } n_0 < n_1 < n_2 < \dots \end{aligned}$$

Sei $\ell \in \mathbb{N}$ minimal mit $m_\ell \neq n_\ell$. So ein ℓ existiert, da $B_1 \neq B_2$. Wir nehmen an, dass $m_\ell < n_\ell$. Beispielsweise, für $B_1 = \{0, 1, 2\}$ und $B_2 = \{0, 1, 3, 4, 5\}$ ist $\ell = 2$, $m_2 = 2$ und $n_2 = 3$. Vergleiche die Summen

$$\begin{aligned} S_1 &= \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^{m_k} \geq \sum_{k=0}^{\ell} \left(\frac{1}{3}\right)^{m_k} = \sum_{k=0}^{\ell-1} \left(\frac{1}{3}\right)^{m_k} + \left(\frac{1}{3}\right)^{m_\ell}, \\ S_2 &= \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^{n_k} = \sum_{k=0}^{\ell-1} \left(\frac{1}{3}\right)^{n_k} + \sum_{k=\ell}^{\infty} \left(\frac{1}{3}\right)^{n_k}. \end{aligned}$$

Setzen wir

$$\begin{aligned} X &= \sum_{k=0}^{\ell-1} \left(\frac{1}{3}\right)^{n_k}, \\ Y &= \sum_{k=\ell}^{\infty} \left(\frac{1}{3}\right)^{n_k}, \end{aligned}$$

so erhalten wir aus $n_\ell > m_\ell$, dass $n_\ell \geq m_\ell + 1$. Also folgt

$$Y \leq \left(\frac{1}{3}\right)^{m_\ell} \cdot \left(\frac{1}{3} + \left(\frac{1}{3}\right)^2 + \dots\right).$$

Es gilt also

$$\begin{aligned} S_1 &\geq X + \left(\frac{1}{3}\right)^{m_\ell}, \\ S_2 &\leq X + \left(\frac{1}{3}\right)^{m_\ell} \cdot \frac{1}{2}. \end{aligned}$$

Setze

$$x = X + \frac{2}{3} \cdot \left(\frac{1}{3}\right)^{m_\ell} \in \mathbb{Q}.$$

Dann ist $x < S_1$, also $x \notin D_{B_1}$, und $x > S_2$, also $x \in D_{B_2}$. Wir schliessen, dass $\psi(B_1) \neq \psi(B_2)$. Also ist ψ injektiv und \mathbb{R} überabzählbar. \square

Frage. Wo kommen all diese Schnitte D_B her?

Es muss irrationale Schnitte D_B geben (sonst wären es abzählbar viele). Insbesondere muss es Teilmengen $B \subset \mathbb{N}$ geben, so dass die entsprechende Summe

$$x = \sum_{k=0}^{\infty} \left(\frac{1}{3}\right)^{n_k}$$

keine rationale Zahl ist. Die Menge all dieser Summen heisst *Cantormenge*.

Eine Ordnung auf den reellen Zahlen

Seien $D, D' \in \mathbb{R}$ mit $D \neq D'$. Dann gilt entweder $D \subset D'$ oder $D' \subset D$ (siehe oben).

Definition. Wir schreiben $D < D'$ falls $D' \subset D$ und $D' \neq D$.

Bemerkung. Falls $D < D'$ (das heisst $D' \subset D$ und $D' \neq D$), dann existiert $y \in \mathbb{Q}$ mit $y \in D$ und $y \notin D'$. Da D kein kleinstes Element enthält, existiert $x \in \mathbb{Q}$ mit $x < y$ und $x \in D$. Dann gilt $D' \subset D_x \subset D$, und all diese Inklusionen sind strikt. Die erste Inklusion ist strikt, da $x < y$. Das war nötig, da $D' = D_y$ gelten könnte. Wir haben also eine rationale Zahl $x \in \mathbb{Q}$ gefunden mit $D < D_x < D'$. Wir haben somit gezeigt, dass zwischen zwei verschiedenen reellen Zahlen immer eine rationale Zahl liegt. Dies ist überraschend, da die Menge \mathbb{Q} abzählbar ist, aber nicht die Menge \mathbb{R} .

Kronecker hat aus diesem Grund Dedekinds Arbeit nicht akzeptiert, und Poincaré hat es sogar als Teufelswerk bezeichnet. Aus diesem Skeptizismus ist unter anderem der Konstruktivismus in der Logik entstanden. Dieser hat jedoch nicht mehr viele Vertreter.

Addition auf den reellen Zahlen

Definition. Seien $D, D' \in \mathbb{R}$ Dedekindsche Schnitte. Wir Definieren die *Summe* von D und D' als

$$D + D' = \{z \in \mathbb{Q} \mid \text{es existieren } x \in D \text{ und } y \in D' \text{ mit } z = x + y\}.$$

Man kann leicht überprüfen, dass $D + D'$ ein Schnitt ist.

Lemma 1. \mathbb{R} mit Addition ist eine kommutative Gruppe mit neutralem Element

$$D_0 = \{x \in \mathbb{Q} \mid x > 0\}$$

Beweis.

- Kommutativität und Assoziativität übertragen sich von der Addition auf \mathbb{Q} .
- D_0 ist das neutrale Element. Zu prüfen ist für alle $D \in \mathbb{R}$, dass $D + D_0 = D$. Wir zeigen beide Inklusionen.
 - (a) Die Inklusion $D + D_0 \subset D$ folgt direkt aus der Definition: Wenn wir eine positive Zahl (ein Element von D_0) zu einem $x \in D$ addieren, erhalten wir eine grössere rationale Zahl als x , die dementsprechend auch in D ist.

- (b) Die umgekehrte Inklusion $D + D_0 \supset D$ zeigen wir wie folgt. Sei $y \in D$. Dann existiert $x \in D$ mit $x < y$, da x nicht das kleinste Element von D ist. Dann gilt $y = x + (y - x) \in D + D_0$, da $x \in D$ und $0 < y - x \in D_0$.

Aus (a) und (b) folgt $D = D + D_0$, also ist D_0 das neutrale Element von \mathbb{R} .

- Die inversen Elemente müssen wir erst noch konstruieren. Das ist der womöglich schwierigste Schritt in diesem Beweis. Wir definieren

$$-D = -(\mathbb{Q} \setminus D) + D_0,$$

Das ist scheinbar die einfachste Art, dies aufzuschreiben. Für ein wenig Intuition dahinter, siehe Abbildung I.3. Hier ist zu beachten, dass das Minus auf der linken Seite anders zu interpretieren ist, als das Minus auf der rechten Seite. Wir behaupten nun, dass $D + (-D) = D_0$. Berechne dazu

$$D + (-D) = D + (-(\mathbb{Q} \setminus D)) + D_0.$$

Seien $x \in D$, $y \in -(\mathbb{Q} \setminus D)$, und $z \in D_0$. Dann gilt:

- (i) $z > 0$,
- (ii) $-y \in \mathbb{Q} \setminus D$, also $y \notin D$. Das heisst $-y < x$, also $x + y > 0$.

Wir schliessen, dass $x + y + z > 0$, also $x + y + z \in D_0$. Das zeigt die Inklusion $D + (-D) \subset D_0$. Sei umgekehrt $p/q \in D_0$, das heisst $p/q > 0$. Wähle $y \in \mathbb{Q}$ mit $0 < y < p/q$, zum Beispiel $y = p/2q$. Es existiert $x \in D$, so dass $x - y \notin D$: Sei hierzu $x' \in D$ beliebig, und sei $n \in \mathbb{N}$ maximal so dass $x' - ny \in D$. Dann erfüllt $x = x' - ny$ diese Eigenschaft. Aus $x - y \notin D$ folgt, dass $x - y \in \mathbb{Q} \setminus D$. Dann ist aber $y - x \in -(\mathbb{Q} \setminus D)$. Also ist $p/q = x + (y - x) + (p/q - y)$, wobei $x \in D$, $y - x \in -(\mathbb{Q} \setminus D)$, und $p/q - y \in D_0$. Also liegt p/q in $D + (-D) = D + (-(\mathbb{Q} \setminus D)) + D_0$, also $D + (-D) \supset D_0$. Wir haben beide Inklusionen gezeigt, und somit erhalten wir $D + (-D) = D_0$. \square



Abbildung I.3: Additive Inverse

Multiplikation auf den reellen Zahlen

Dieser Abschnitt verläuft völlig analog zum letzten, aber wir müssen mit den Vorzeichen vorsichtig sein.

Definition. Seien $D, D' \in \mathbb{R}$. Wir nehmen an, dass $D, D' \geq 0$, das heisst $D, D' \subset D_0$. Dann definieren wir das *Produkt* von D und D' als

$$D \cdot D' = \{z \in \mathbb{Q} \mid \text{es existieren } x \in D, y \in D' \text{ mit } z = x \cdot y\}.$$

Falls $D < 0$ und $D' \geq 0$, dann definieren wir

$$D \cdot D' = -(-D) \cdot D',$$

falls $D \geq 0$ und $D < 0$, definieren wir ähnlich

$$D \cdot D' = D \cdot -(-D'),$$

und falls $D < 0$ und $D' < 0$ definieren wir

$$D \cdot D' = (-D) \cdot (-D').$$

In dieser Definition bezeichnet “ $-D$ ” das in obigem Abschnitt definierte additive Inverse von D (und nicht die gespiegelte Menge).

Lemma 2. Die Menge $\mathbb{R} \setminus \{D_0\}$ mit Multiplikation ist eine kommutative Gruppe mit neutralem Element

$$D_1 = \{x \in \mathbb{Q} \mid x > 1\}.$$

Beweis.

- Die Kommutativität und Assoziativität der Multiplikation übertragen sich von \mathbb{Q} auf \mathbb{R} .
- Wir müssen zeigen, dass D_1 tatsächlich das neutrale Element von \mathbb{R} ist. Sei $D \in \mathbb{R}$. Zu prüfen ist, dass $D \cdot D_1 = D$. Wir prüfen dies für $D > 0$. Die anderen Fälle sind nicht schwieriger, da müssen wir einfach an den entsprechenden Stellen ein Minussymbol hinschreiben. Wir zeigen wieder beide Inklusionen.

(a) Die Inklusion $D \cdot D_1 \subset D$ ist klar nach Definition.

(b) Sei umgekehrt $y \in D$. Wähle $x \in D$ mit $x < y$ und $x > 0$. Dann ist

$$y = x \cdot \frac{y}{x} \in D \cdot D_1$$

da $y/x > 1$.

Also ist $D \cdot D_1 = D$.

- Sei $D \in \mathbb{R}$ mit $D \neq D_0$. Wir konstruieren D^{-1} , das multiplikative Inverse von D . Wir nehmen auch hier der Einfachheit halber $D > 0$ an, auch hier, um uns nicht zu viele Gedanken über das Platzieren der Minussymbole zu machen. Setze

$$D^{-1} = (D_0 \setminus D)^{-1} \cdot D_1.$$

Auch hier bedeutet das Symbol $^{-1}$ links etwas anderes als rechts. Für Intuition dazu betrachte Abbildung I.4. Wir testen wieder beide Inklusionen.

- (a) Für $x \in D$, $y \in (D_0 \setminus D)^{-1}$, und $z \in D_1$ ist $x \cdot y \cdot z > 1$. Wir schliessen, dass $D \cdot D^{-1} \subset D_1$.
- (b) Sei $p/q \in D_1$, das heisst $p/q > 1$. Wähle $y \in \mathbb{Q}$ mit $1 < y < p/q$, zum Beispiel

$$y = \frac{p+q}{2q}.$$

Wähle $x \in D$ mit $x/y \notin D$. Dann gilt:

$$\frac{p}{q} = x \cdot \frac{y}{x} \in D \cdot (D_0 \setminus D)^{-1} \cdot D_1.$$

Da $x/y \notin D$ ist $x/y \in D_0 \setminus D$, also $y/x \in (D_0 \setminus D)^{-1}$. Wir erhalten die umgekehrte Inklusion $D \cdot D^{-1} \supset D_1$.

Setzen wir (a) und (b) zusammen, erhalten wir $D \cdot D^{-1} = D_1$. □

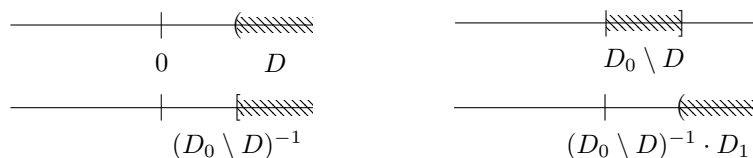


Abbildung I.4: Multiplikative Inverse

Übung. Überprüfe, dass $D_{\sqrt{2}} \cdot D_{\sqrt{2}} = D_2$.

Bemerkung (Zur Notation). Ab jetzt schreiben wir p/q anstatt $D_{p/q}$, auch wenn wir p/q als reelle Zahl (also als Schnitt) meinen. Ebenso schreiben wir $\sqrt{2}$ statt $D_{\sqrt{2}}$. Ausserdem benutzen wir Variablen x, y, z, \dots für reelle Zahlen. Das ist ein bisschen gefährlich, da wir immer noch Axiome zu überprüfen haben, bis wir unser Ziel zu Beginn des Abschnitts erreichen. Das sollte jedoch nicht allzu viele Missverständnisse bereiten.

Eine Ordnung auf den reellen Zahlen (Reprise)

Definition. Seien $D, D' \in \mathbb{R}$. Wir schreiben $D \leq D'$ falls $D \supset D'$ und $D < D'$ falls $D \supset D'$ und $D \neq D'$.

Definition. Ein *geordneter Körper* ist ein Körper $(K, +, \cdot)$ zusammen mit einer binären Relation \leq , welche folgende Eigenschaften hat.

- (i) Für alle $x, y \in K$ gilt $x \leq y$ oder $y \leq x$, und $x = y$ genau dann, wenn $x \leq y$ und $y \leq x$.
- (ii) Für alle $x, y, z \in K$ gilt, dass immer wenn $x \leq y$ und $y \leq z$, dann auch $x \leq z$. Diese Eigenschaft nennt man *Transitivität*.
- (iii) Für alle $x, y, z \in K$ gilt, dass immer wenn $x \leq y$, dann auch $x + z \leq y + z$.

(iv) Für alle $x, y, z \in K$ gilt, dass immer wenn $x \leq y$ und $0 \leq z$, dann auch $xz \leq yz$.

Bei den Eigenschaften (iii) und (iv) spricht man von additiver, beziehungsweise multiplikativer *Monotonie*.

Beispiel. Die Menge der rationalen Zahlen \mathbb{Q} mit der üblichen Addition, Multiplikation und Ordnung, ist ein geordneter Körper. Mit der “üblichen Ordnung” ist die Relation

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc$$

falls $b, d > 0$, gemeint. Wie die Ordnung auf \mathbb{Z} zu verstehen ist, überlassen wir den Mengentheoretikern und fassen das als intuitiv genug auf.

Theorem 1. *Die Menge der reellen Zahlen \mathbb{R} mit der oben definierten Addition, Multiplikation und Ordnung, ist ein geordneter Körper.*

Beweis.

- Nach Lemma 1 und 2 sind $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ kommutative Gruppen.
- Das Distributivgesetz überträgt sich von \mathbb{Q} auf \mathbb{R} .
- Die Ordnungsaxiome (i) bis (iv) sind leicht zu überprüfen. □