Vorkurs für
Studierende der Mathematik
Winersemester 2023/24

Prof. Dr. Annette Huber-Klawitter

Fassung vom 8. Oktober 2023

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Ernst-Zermelo-Str. 1
79104 Freiburg

0761-203-5560
annette.huber@math.uni-freiburg.de

Inhaltsverzeichnis

Vorwort

Dieser Vorkurs soll eine Brücke sein zwischen dem Mathematikunterricht in der Schule und dem Mathematikstudium.

- Gerade am Anfang sind die Gegenstände fast die gleichen (Ableitungen, Gleichungssysteme), aber der Umgang ist ganz anders. In der Schule steht die Vorstellung von Rechenverfahren und deren Einübung im Vordergrund. Ab jetzt geht es um saubere Beweise, dass die Verfahren leisten was sie sollen.
- Dafür ist es nötig, alle Begriffe vorher sauber einzuführen. Über präzise und zielführende Definitionen nachzudenken, nimmt viel Raum ein. (Ist 1 eine Primzahl?)
- Sie sollen lernen, Beweise selbst zu finden und zu formulieren.
- Im Prinzip wird die Mathematik im Studium von Null auf eingeführt. Lücken aus dem Schulunterricht werden dabei geschlossen. Um die geht es diese Woche nicht.

Statt dessen werden wir exemplarisch einige Gegenstände durchgehen, die Schulstoff sind (oder sein könnten/sollten), mit den Augen der Hochschulmathematik und den Lehrmethoden des Mathematikstudiums: Vorlesung und Übung.

Also los!

Annette Huber-Klawitter

Kapitel 1

Teilbarkeitsregeln

Ist die Zahl 7011 durch 3 teilbar? Wir bilden die Quersumme:

$$7 + 0 + 1 + 1 = 9.$$

Sie ist durch 3 teilbar, also auch 7011. Wir rechnen nach:

$$7011 : 3 = 2337$$

(Wie war das mit der schriftlichen Division?) Unser Ziel ist es jetzt, dieses Kriterium zu formulieren und zu beweisen.

1.1 Stellenwertsysteme

Das Kriterium setzt voraus, dass wir die Zahl im *Dezimalsystem*, also zur Basis 10 angeben. Was bedeutet das?

Notation 1. Wir bezeichnen mit

- $\mathbb{N} = \{1, 2, 3, \dots\}$[1] die Menge der *natürlichen Zahlen*, $\mathbb{N}_0 = \{0, 1, \dots\}$,
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$ die Menge der *ganzen Zahlen*
- $\mathbb{Q} = \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}\}$ die Menge der *rationalen Zahlen*
- $\mathbb{R}$ die Menge der *reellen Zahlen.*

Heute geht es nur um natürliche und ganze Zahlen. Und noch eine Schreibweise:

Notation 2. Sei $n \geq 0$ und $x_0, x_1, \dots, x_n \in \mathbb{R}$. Dann schreiben wir

$$\sum_{i=0}^{n} x_i = x_1 + x_2 + \cdots + x_n.$$

[1] Je nach Quelle ist 0 eine natürliche Zahl oder nicht. In diesm Vorkurs nicht.

Beispiel.

$$\sum_{i=0}^{n} 1 = n + 1 \tag{1.1}$$

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{1.2}$$

(Beweis siehe Übungsaufgabe)

Definition 1.1. Seien $a_0, a_1, \ldots, a_n \in \{0, \ldots, 9\}$. Dann heißt

$$a_n a_{n-1} \ldots a_0$$

Dezimaldarstellung der natürlichen Zahl

$$\sum_{i=0}^{n} a_i 10^i.$$

Beispiel. $n = 3$ und $a_0 = a_1 = 1$, $a_2 = 0$ und $a_3 = 7$ liefert die Dezimaldarstellung von 7011 (ja eben). Die Zahl 7^2 hat die Dezimaldarstellung mit $n = 2$, $a_0 = 9$, $a_1 = 4$, nämlich $7^2 = 49$.

Satz 1.2. *Für jede natürliche Zahl N existieren eindeutige n und $a_0, \ldots, a_n \in \{0, \ldots, 9\}$ mit $a_n \neq 0$, so dass $a_n \ldots a_0$ Dezimaldarstellung von N ist.*

Der Beweis benutzt eine der wichtigsten Tatsachen über natürliche Zahlen:

Lemma 1.3 (Division mit Rest)**.** *Seien $a, b \in \mathbb{N}$. Dann gibt es eindeutige $q, r \in \mathbb{N}_0$, so dass*

$$a = qb + r$$

wobei

$$0 \leq r < b.$$

Dies ist die Division mit Rest aus der Grundschule. Für den (einfachen) Beweis verweisen wir auf das Studium.

Beweis des Satzes. Wir zeigen die Existenz durch die Angabe eines Algorithmus. Wir wenden Division mit Rest an auf $a = N$ und $b = 10$. Sei a_0 der Rest, also

$$N = q10 + a_0.$$

Im nächsten Schritt betrachten wir

$$N_1 = (N - a_0)/10.$$

Dies ist q. Falls $q = 0$, so sind wir fertig. Es ist $n = 0$ und a_0 ist die Dezimaldarstellung. Sonst wenden wir Division mit Rest an auf $a = N_1$ und $b = 10$. Sei a_1 der Rest, also

$$N_1 = q_1 10 + a_1.$$

Ist $q_1 = 0$, so ist $n = 2$ und a_1a_0 die Dezimaldarstellung. Wir wiederholen das Verfahren. Es bricht nach endlich vielen Schritte ab, weil die Zahlen $N, N_1, N_2, \dots$ immer kleiner werden.
Die Methode zeigt auch die Eindeutigkeit: Sei

$$a_n \dots a_0 = b_m \dots b_0$$

(jeweils Dezimaldarstellungen). Dann ist $a_0 = b_0$ der eindeutige Rest von N bei Division durch 10. Es folgt

$$N_1 = a_n \dots a_1 = b_m \dots b_1.$$

Mit demselben Argument folgt iterativ $a_1 = b_1$, $a_2 = b_2$ etc. Es muss dann auch $n = m$ sein, da $a_n, b_m \neq 0$. □

Warum 10? An der Zahl ist nicht Besonderes.

Definition 1.4. Sei $b \in \mathbb{N}$, $b \geq 2$. Seien $a_0, a_1, \dots, a_n \in \{0, \dots, b-1\}$. Dann heißt

$$a_n a_{n-1} \dots a_{0b}$$

Darstellung der natürlichen Zahl

$$\sum_{i=0}^{n} a_i b^i$$

zur Basis b.

Satz 1.5. *Sei $b \in \mathbb{N}$. Für jede natürliche Zahl N existieren eindeutige n und $a_0, \dots, a_n \in \{0, \dots, b-1\}$ mit $a_n \neq 0$, so dass $a_n \dots a_{0b}$ Darstellung von N zur Basis b ist.*

Der Beweis ist derselbe wir für $b = 10$. Der Beweis enthält auch das Verfahren zur Bestimmung der Entwicklung.

Beispiel. $N = 9$ hat die Entwicklung 1001_2, da

$$1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 = 9.$$

Bemerkung. Die Basis $b = 2$ wird von Computern benutzt. Der Bequemlichkeit halber benutzt man in der Informatik oft $b = 16$. Von historischem Interesse ist auch $b = 60$ (Uhr, Winkel) oder das Verwandte $b = 12$.

Wir erreichen unse erstes Zwischenziel:

Definition 1.6. Sei $b \in \mathbb{N}$ und $a_n \dots a_{0b}$ Darstellung einer natürlichen Zahl N zur Basis b. Dann heißt

$$Q(N) = a_0 + \cdots + a_n$$

Quersumme von N zur Basis b.

Für $b = 10$ sprechen wir einfach von der *Quersumme.*

Theorem 1.7. *Eine natürliche Zahl N ist genau dann durch 3 (bzw. 9) teilbar, wenn ihre Quersumme durch 3 (bzw. 9) teilbar ist.*

1.2 Rechnen mit Restklassen

Definition 1.8. Sei $b \in \mathbb{N}$. Für $x, y \in \mathbb{Z}$ schreiben wir

$$x \equiv y \mod b$$

(lies: x kongruent zu y modulo b), wenn x und y den selben Rest bei Division durch b haben. Wir schreiben

$$\overline{x} = \{y \in \mathbb{Z} | x \equiv y \mod b\},$$

die *Restklasse von x modulo b.*

Beispiel. Für $b = 2$ besteht die Restklasse $\overline{0}$ aus den geraden Zahlen und die Restklasse $\overline{1}$ aus den ungeraden.

Mit Restklassen kann man rechnen!

Lemma 1.9. *Sei $b \in \mathbb{N}$, $x, y, x', y' \in \mathbb{Z}$. Es ist $x \equiv y \mod b$ genau dann, wenn b die Differenz $x - y$ teilt. Wenn $x \equiv x' \mod b$ und $y \equiv y' \mod b$, dann gilt*

$$x + y \equiv x' + y' \mod b, \quad xy \equiv x'y' \mod b.$$

Beispiel. Die Summe von zwei geraden Zahlen ist stets gerade.

Beweis: Sei

$$x = qb + r, \ y = tb + s$$

für $q, t \in \mathbb{Z}$, $0 \leq r, s < b$ Es folgt also

$$x - y = (q - t)b + (r - s)$$

Die Zahl b teilt genau dann die linke Seite, wenn sie auch $r - s$ teilt. Wegen der Beschränkung für die Reste r, s folgt

$$-b < r - s < b.$$

Die Differenz istgenau dann durch b teilbar, wenn $r = s$.
Sei weiter

$$x' = q'b + r, \ y' = t'b + s.$$

Dann ist

$$(x + y) - (x' + y') = (q - q' + t - t')b + 0,$$

also sind die Summen kongruent. Genauso gilt

$$\begin{aligned}(xy) - (x'y') &= (qb + r)(tb + s) - (q'b + r)(t'b + s) \\ &= b(qtb + rt + qs - q't'b - r't' - q's') + rs - rs.\end{aligned}$$

Wieder ist die Differenz durch b teilbar, also sind die Produkte kongruent. □

1.3 Teilbarkeitskriterien

Beweis des Theorems. Wir rechnen mit Resten modulo 3. Es ist $10 \equiv 1 \mod 3$. Sei $N = a_n \dots a_0$ die Dezimaldarstellung, also

$$N = \sum_{i=0}^{n} a_i 10^i.$$

Da Restklassenbildung mit Summe umd Multiplikation vertauscht, folgt

$$N = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i 1^i = Q(N) \mod 3.$$

Die Teilbarkeitsregel für $b = 9$ folgt genauso, da $10 \equiv 1 \mod 9$. $\square$

Kapitel 2

Binomialkoeffizienten

Aus der Schule wohlbekannt ist die *1. binomische Formel*

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Wir studieren heute allgemeiner $(a+b)^n$ für $n \in \mathbb{N}$. Wir rechnen erstmal ein paar kleine Beispiele aus.

Beispiel. $n = 3$:

$$\begin{aligned}(a+b)^3 = (a+b)^2(a+b) = (a^2+2ab+b^2)(a+b) &= a^3+2a^2b+ab^2+a^2b+2ab^2+b^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3\end{aligned}$$

$n = 4$:

$$\begin{aligned}(a+b)^4 &= (a+b)^3(a+b) = (a^3+3a^2b+3ab^2+b^3)(a+b) \\ &= a^4 + 3a^3b + +2a^2b^2 + ab^3 + a^3b + 3a^2b^2 + 2ab^3 + b^4 \\ &= a^3 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\end{aligned}$$

Man erkennt ein Muster.

Satz 2.1. *Sei $n \in \mathbb{N}$. Dann gilt für alle $a, b \in \mathbb{R}$*

$$(a+b)^n = \sum_{i=0}^{n} c_i(n) a^{n-i} b^i$$

für natürliche Zahlen $c_i(n)$ unabhängig von a und b. Es gilt

(i) $c_0(n) = c_n(n) = 1$,

(ii) $c_i(n) = c_{i-1}(n-1) + c_i(n-1)$ *für* $n > 1$, $0 < i < n$.

Definition 2.2. Die Koeffizienten $c_i(n)$ aus dem Satz heißen *Binomialkoeffizienten*

$$\binom{n}{i} := c_i(n).$$

(Lies: n über i, englisch: n choose i)

Den Beweis wollen wir mit vollständiger Induktion führen, daher eine schnelle Erinnerung/Einführung.

Beweisprinzip der vollständigen Induktion 2.3. *Gegeben sei eine Aussage $P(n)$ für jedes $n \in \mathbb{N}$. Wenn $P(1)$ gilt und für $m \geq 1$ aus $P(m)$ die Aussage $P(m+1)$ folgt, dann gelten alle Aussagen $P(n)$.*

Es handelt sich hier nicht um einen beweisbaren Satz, sondern um ein *Axiom* der natürlichen Zahlen. Dies wird im Studium noch genauer diskutiert.

Beweis des Satzes. Induktionsanfang $m = 1$: Die Behauptung ist trivial.
Induktionsvoraussetzung: Die Behauptung gelte für ein $m \geq 1$, also

$$(a+b)^m = \sum_{i=0}^{m} c_i(m) a^{m-i} b^i$$

für natürliche Zahlen $c_i(m)$ unabhängig von a und b. Hierbei ist $c_0(m) = c_m(m) = 1$.
Induktionsschluss: Wir betrachten die Behauptung für $m+1$. Es ist

$$
\begin{aligned}
(a+b)^{m+1} &= (a+b)^m(a+b) && (2.1)\\
&= \left(\sum_{i=0}^{m} c_i(m) a^{m-i} b^i\right)(a+b) \quad \text{Induktionsvoraussetzung} && (2.2)\\
&= \left(\sum_{i=0}^{m} c_i(m) a^{m-i} b^i\right) a + \left(\sum_{i=0} c_i(m) a^{m-i} b^i\right) b \quad \text{Klammer auflösen} && (2.3)\\
&= \sum_{i=0}^{m} c_i(m) a^{m+1-i} b^i + \sum_{i=0}^{m} c_i(m) a^{m-i} b^{i+1} && (2.4)\\
&= \sum_{i=0}^{m} c_i(m) a^{m+1-i} b^i + \sum_{j=1}^{m+1} c_{j-1}(m) a^{m-j+1} b^j \quad \text{Indexverschiebung} && (2.5)\\
&= c_0(m) a^{m+1} + \sum_{i=1}^{m} a^{m+1-i} b^i + \sum_{i=1}^{m} c_{i-1}(m) a^{m+1-i} b^i + c_m(m) b^{m+1} && (2.6)\\
&= a^{m+1} + \sum_{i=1}^{m} (c_{i-1}(m) + c_i(m)) a^{m+1-i} b^i + b^{m+1} && (2.7)
\end{aligned}
$$

Dies ist von der gewünschten Form, einschließlich der Formeln für die Koeffizienten. □

2.1 Eigenschaften

Der Satz enthält Rekursionformeln für alle Binomialkoeffienten. Diese legen alle Binomialkoeffizienten eindeutig fest. Am bequemsten wird dies mit dem *Pascalschen Dreieck* visualisiert:

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

Hierbei beginnen wir links und rechts mit einer 1 und ergänzen an den anderen Stellen jeweils die Summe der beiden Zahlen, die darüber stehen.

Korollar 2.4. *(i) Für all $n \geq 0$, $n \geq k \geq 0$ gilt*

$$\binom{n}{k} = \binom{n}{n-k}.$$

(ii) Für alle $n > 0$ gilt

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

(iii) Es ist

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Beweis: Die Symmetrie sieht man im Dreieck gut. Sie gilt, weil

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

Beim letzten Gleichheitszeichen wird die Summation über k durch die über $n-k$ ersetzt. Die Behauptung folgt durch Vergleich der Koeffizienten. Die zweite Behauptung wird leicht mit Induktion bewiesen. Für die zweite Behauptung berechnen wir

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

□

2.2 Kombinatorik

Kombinatorik ist die Lehre des Zählens von Dingen. Zum Aufwärmen: Gegeben n verschiedene Objekte, z.B. die Zahlen $1, 2, \dots, n$. Wieviele Möglichkeiten gibt es, sie anzuordnen? Für die erste Stelle gibt es n Möglichkeiten. Für die zweite $n-1$ (da ja ein Objekt weggenommen wurde), für die dritte $n-2$ (wieder eins weniger), etc. Insgesamt also

$$n(n-1)\dots 1 =: n!$$

(lies: n Fakultät, englisch n factorial).
Jetzt unser Fall:

$$(a+b)^n = (a+b)(a+b)\dots(a+b) \quad n \text{ Faktoren}$$

Beim Ausmultiplizieren wählen wir in jedem Faktor a oder b. Wir erhalten 2^n Summanden, die jeweils Produkte von n Faktoren a oder b sind. Der Summand $a^{n-k}b^k$ (für $0 \leq 0 \leq n$) entsteht jedes Mal, wenn wir k-mal b gewählt haben. Wie oft passiert das?

Lemma 2.5. *Sei $n \in \mathbb{N}$, $0 \leq k \leq n$. Dann gilt*

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

Beweis: Die Multiplizität ist genau der Koeffizient aus der binomischen Formel, also $\binom{n}{k}$. Andererseits zählen wir ab.
Wir wählen k-mal aus n Faktoren. Das erste Mal haben wir n Möglichkeiten, beim zweiten Mal $n-1$, etc. bis zum k-ten Mal $n-k+1$ Möglichkeiten. Am Ende steht eine Liste von k Faktoren. Für unsere Zählaufgabe kommt es aber

auf die Reihenfolge der Liste nicht an. Es gibt $k!$ Möglichkeiten, die Liste zu sortieren. Die Anzahl der Summanden ist also

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

□

Insbesondere ergibt der Ausdruck immer eine natürliche Zahl. Alle Faktoren des Nenners kürzen sich gegen Faktoren des Zählers.

2.3 Der kleine Satz von Fermat

Eine Primzahl ist eine natürliche Zahl $p \geq 2$, die nur durch 1 und p teilbar ist, also $p = 2, 3, 5, \dots$.

Satz 2.6. *Sei p Primzahl. Dann ist $\binom{p}{k}$ für $0 < k < p$ durch p teilbar, also*

$$\binom{p}{k} \equiv 0 \mod p.$$

Beweis: Wir betrachten den Bruch $\frac{p!}{k!(p-k)!}$. Die Primzahl p teilt den Zähler. Für $k < p$ teilt sie nicht $k!$ und für $p - k < p$ (also $0 < k$) teilt sie nicht $(p-k)!$. Sie wird nicht weggekürzt, also ist der Quotient durch p teilbar. □

Bemerkung. Wir verwenden hier Eigenschaften von Primzahlen, die im Studium bewiesen werden.

Korollar 2.7 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl. Für jede ganze Zahl gilt*

$$a^p \equiv a \mod p.$$

Beweis: Für ganze Zahlen a, b gilt wegen des letzten Satzes

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

Es folgt

$$\begin{aligned}
&1^p = 1, \\
&2^p = (1+1)^p \equiv 1^p + 1^p = 2, \\
&3^p = (2+1)^p \equiv 2^p + 1^p = 2 + 1 = 3, \\
&\quad \dots
\end{aligned}$$

□

Bemerkung. Dieser Sachverhalt wird für *Primzahltests* verwendet. Es ist

$$2^9 = 8^3 \equiv (-1)^3 = -1 \mod 9$$

also ist 9 keine Primzahl. Achtung: Es gibt Zahlen, die den Test für alle a bestehen, aber trotzdem keine Primzahlen sind.

Bemerkung. Das RSA-Verfahren zum Verschlüsseln von Nachrichten beruht auf dem kleinen Satz von Fermat. Man rechnet modulo N, wobei N ein Produkt von zwei großen Primzahlen ist.

Kapitel 3

Dezimalbrüche und reelle Zahlen

In der ersten Vorlesung haben wir natürliche Zahlen als Dezimalzahlen dargestellt. Dasselbe funktioniert auch mit negativen Exponenten:

Definition 3.1. Seien $n < m$ ganze Zahlen, $a_n, a_{n+1}, \ldots, a_m \in \{0, \ldots, 9\}$ Dann heißt

$$\sum_{i=n}^{m} a_i 10^i$$

(endlicher) Dezimalbruch.

Für $n < 0$ können wir die Summe umschreiben zu

$$\frac{\sum_{i=n}^{m} a_i 10^{i+|n|}}{10^{|n|}},$$

also als einen Bruch, dessen Nenner eine Potenz von 10 ist.

Bemerkung. Nicht jede rationale Zahl lässt sich als Dezimalbruch schreiben!

Beweis: Angenommen, $\frac{1}{3}$ ist ein Dezimalbruch, also

$$\frac{1}{3} = \frac{a}{10^i}$$

für eine natürliche Zahl a und $i \geq 0$. Dann folgt

$$10^i = 3a.$$

Modulo 3 folgt

$$0 \equiv 10^i \equiv 1^i = 1 \mod 3.$$

Dies ist falsch, also kann 3 nicht als Dezimalbruch geschrieben werden. □

Bemerkung. Dies war unser erstes Beispiel für einen *indirekten Beweis*. Eine Aussage gilt, weil ihre Umkehrung falsch ist.

Aus der Schule wissen wir den Ausweg: Wir müssen auch unendliche Dezimalbrücke zulassen. Zur Vereinfachung der Notation arbeiten wir nur mit Zahlen im Intervall $[0, 1]$, also ohne Vorkommazahlen und ohne Vorzeichen.

Definition 3.2. Sei $a_1, a_2, a_3, \dots$ eine Folge von Elementen von $\{0, 1, \dots, 9\}$. Dann heißt

$$0, a_1 a_2 a_3 \dots$$

unendlicher Dezimalbruch mit den Nachkommastellen $a_1, a_2, \dots$. Er repräsentiert die Zahl

$$a = \sum_{i=1}^{\infty} a_i 10^{-i}.$$

Beispiel.

$$\frac{1}{3} = 0,3333\dots$$

Bemerkung. Es kann passieren, dass zwei Dezimalbrüche dieselbe Zahl repräsentieren, z.B.

$$0,99999 \dots = 1,000\dots$$

Hier gibt es gleich ein Problem. Was soll die unendliche Summe bedeuten? In Analysis 1 werden Werte von solchen *Reihen* als *Grenzwerte* eingeführt. Alternativ:

Definition 3.3. Mit der Notation der letzten Definition ist

$$\sum_{i=1}^{\infty} a_i 10^{-i}$$

die kleinste reelle Zahl a, für die

$$a \geq \sum_{i=1}^{n} a_i 10^{-i} \quad \text{für alle } n \in \mathbb{N}.$$

Wir haben ein Problem gelöst, stoßen aber sofort auf zwei neue:

- Was ist eine reelle Zahl?
- Gibt es a und ist es eindeutig?

3.1 Axiomatische Charakterisierung

Es gibt verschiedene Konstruktionen der reellen Zahlen. Die konkrete Definition ist aber nicht wichtig, sondern ihre Eigenschaften.

Definition 3.4. Die reellen Zahlen $(\mathbb{R}, \leq)$ sind eine Menge mit einer Totalordnung, die die rationalen Zahlen $(\mathbb{Q}, \leq)$ enthält, so dass gilt:

(i) Jede reelle Zahl $x \in \mathbb{R}$ ist eindeutig bestimmt durch die Menge der rationalen Zahlen $\{a \in \mathbb{Q} | a \leq x\}$ ($\mathbb{Q}$ *ist dicht in* $\mathbb{R}$).

(ii) Für jede nach oben beschränkte Menge $A \subset \mathbb{Q}$ gibt es eine kleinste reelle Zahl s mit $a \leq s$ für alle $a \in A$ (*Vollständigkeit*).

Die Zahl s heißt *Supremum von* A. Wir schreiben

$$s = \sup A.$$

Die Antwort auf unsere beiden Fragen ist also *ja*, nach Definition.

Bemerkung. Eine Totalordnung $\leq$ erfüllt:

(i) Wenn $x \leq y$ und $y \leq z$, dann gilt $x \leq z$;

(ii) Wenn $x \leq y$ und $y \leq x$, dann gilt $x = y$;

(iii) $x \leq x$.

Satz 3.5. *Jede reelle Zahl* $0 \leq x < 1$ *hat eine Dezimalbruchentwicklung*

$$0, a_1 a_2 \ldots.$$

Zwei unendliche Dezimalbrüche repräsentieren genau dann dieselbe Zahl

$$0, a_1 a_2 \cdots = 0, b_1 b_2 \ldots$$

$a_i = b_i$ *für alle* $i \in \mathbb{N}$ *oder wenn es* $n > 0$ *gibt, so dass*

$$\begin{cases} a_i = b_i & i < n \\ a_n = b_n + 1 & \\ a_i = 0, b_i = 9 & i > n \end{cases}$$

oder umgekehrt.

Beweis: Wir bestimmen die Nachkommastellen iterativ. Wir starten mit

$$x \in [0, 1) = \{t \in \mathbb{R} \mid 0 \leq t < 1\}.$$

Daher ist $10x \in [0, 10)$. Sei $a_1 = \{0, 1, \ldots, 9\}$ die größte Zahl mit

$$a_1 \leq 10x.$$

Dann gilt $x_1 := 10x - a_1 \in [0, 1)$ und daher

$$x - 0, a_1 < \frac{1}{10}$$

Mit demselben Verfahren bestimmen wir $a_2 \in \{0, \ldots, 9\}$, so dass $x_2 := 10x_1 - a_1 \in [0, 1)$ und daher

$$x - 0, a_1 a_2 < \frac{1}{10^2}.$$

Iterativ entsteht ein unendlicher Dezimalbruch

$$0, a_0 a_1 \ldots,$$

so dass

$$x - 0, a_0 a_1 \ldots a_n < \frac{1}{10^n} \quad \text{für alle } n.$$

Daher ist x die kleine reelle Zahl, die größer gleich allen $0, a_0 \ldots a_n$ ist.
Die Eindeutigkeitsaussge wird als Übungsaufgabe gestellt. □

Bemerkung. Derselbe Satz gilt auch für unendliche Brüche bezüglich jeder anderen Basis $b \geq 2$.

3.2 Rechnen mit reellen Zahlen

Natürlich sind die reellen Zahlen nicht nur eine angeordnete Menge, man kann mit ihnen rechnen.

Definition 3.6. Seien $x, y \in \mathbb{R}$. Dann ist

$$x + y = \sup\{a + b \mid a, b \in \mathbb{Q}, a \leq x, b \leq y\}$$

die kleinste reelle Zahl s, so dass $a + b \leq s$ für alle rationalen Zahlen $a \leq x$ und $b \leq y$.
Seien $x, y \in \mathbb{R}$, $x, y > 0$. Dann ist

$$xy = \{ab \mid a, b \in \mathbb{Q}, a \leq x, b \leq y\}$$

die kleinste reelle Zahl p, so dass $ab \leq p$ für alle rationalen Zahlen $a \leq x$ und $b \leq y$.

Hier ist nun einiges zu verifizieren:

- Sind $x, y \in \mathbb{Q}$, so stimmt die obige Addition/Multiplikation mit der Addition/Multiplikation in $\mathbb{Q}$ überein.
- Es gelten die vertrauten Rechenregeln, z.B. $x + y = y + x$.
- Für jede reelle Zahl x gibt es eine reelle Zahl $-x$, so dass $(-x) + x = 0$.
- Für jede reelle Zahl $x > 0$ gibt es eine reelle Zahl $x^{-1} > 0$, so dass $x^{-1}x = 1$.

Dafür fehlt uns natürlich die Geduld und vielleicht auch die Technik. Aber hier ein Beispiel:

Beweis: Sei $x > 0$. Wir finden eine monoton steigende Folge

$$a_1 \leq a_2 \leq \cdots \leq x,$$

so dass jeweils

$$a_n + \frac{1}{n} \geq x$$

(denn sonst wäre $a + \frac{1}{n} < x$ für alle $a \in \mathbb{Q}$ mit $a_{n-1} \leq a \leq x$, ein Widerspruch). Es folgt dann auch

$$a_m + \frac{1}{m} \geq a_n \tag{3.1}$$

für alle n, m. Wir setzen

$$b_n = -a_n - \frac{1}{n}$$

und definieren

$$y = \sup\{b_n | n \in \mathbb{N}\}.$$

Wir wollen zeigen, dass $x + y = 0$. Es gilt

$$x + y \geq a_n + b_n = -\frac{1}{n} \quad \text{für alle } n,$$

also $x + y \geq 0$. Für die umgekehrte Ungleichung brauchen wir:

Behauptung. *Es ist $b_n + \frac{1}{n} \geq y$ für alle $n \in \mathbb{N}$.*

Wir fixieren n. Es genügt zu zeigen, dass

$$b_n + \frac{1}{n} \geq b_m \quad \text{für alle } m.$$

Wegen Gleichung (3.1) gilt

$$-a_m - \frac{1}{m} \leq -a_n.$$

Anders ausgedrückt

$$b_m \leq b_n + \frac{1}{n},$$

wie zu zeigen war.
Für jedes n gilt nun

$$x + y \leq a_n + \frac{1}{n} + b_n + \frac{1}{n} = a_n + \frac{1}{n} - a_n = \frac{1}{n}.$$

Das ist nur möglich, wenn $x + y \leq 0$.
Da $x + y \leq 0$ und $x + y \geq 0$, muss $x + y = 0$ gelten. □

In dem Beweis wurde immer nur mit *rationalen* Zahlen gerechnet, wo wir die übliche Regenregeln voraussetzen.

3.3 Konstruktion

Uns fehlt bisher eine Konstruktion der reellen Zahlen, anders formuliert: Ein Beweis für die Existenz von $(\mathbb{R}, \leq)$ wie in Definition 3.4.

Definition 3.7. Eine *reelle Zahl* ist eine nicht-leere Teilmenge $A \subsetneq \mathbb{Q}$ mit der Eigenschaft: Wenn $a \in A$, $b \in \mathbb{Q}$ mit $b < a$, dann ist $b \in A$. Sei $\mathbb{R}$ die Menge dieser reellen Zahlen. Für reelle Zahlen A, B setzen wir $A \leq B$ genau dann, wenn A eine Teilmenge von B ist.
Eine rationale Zahl a definiert die reelle Zahl $\mathbb{R}(a) = \{b \in \mathbb{Q} | b \leq a\}$.

Ist $A \subset \mathbb{Q}$ eine beschränkte Teilmenge, so finden wir ihr Supremum:

$$\sup A = \bigcup_{a \in A} \mathbb{R}(a).$$

Bemerkung. Das ist eine Variante der Konstruktion von $\mathbb{R}$ via *Dedekindschen Schnitten*.

Kapitel 4

Exponentialfunktion

Wir arbeiten stets mit reellen Zahlen. In diesem Kapitel soll es um die Funktion

$$\exp_a : x \mapsto a^x$$

für $a > 0$ gehen. Zum Aufwärmen betrachten wir zunächst die Wurzelfunktion.

4.1 Potenz- und Wurzelfunktionen

Sei $n \in \mathbb{N}$. Die Funktion $f : x \mapsto x^n$ ist auf $\mathbb{R}$ definiert.

Satz 4.1. *Sei $x_0 \geq 0$. Dann gibt es eine eindeutige positive reelle Zahl $\sqrt[n]{x_0}$, so dass*

$$\sqrt[n]{x_0} = x_0.$$

Die Konstruktion ist leicht anzugeben:

$$W = \{a \in \mathbb{Q} | a \geq 0, a^n \leq x_0\}, \quad w = \sup W.$$

Zu zeigen ist $w^n = x_0$. Der Beweis beruht auf der Stetigkeit von f, die wiederum wegen Differenzierbarkeit gilt. Diese Begriffe und ihre Eigenschaften werden in Analysis 1 eingeführt. Man kann aber auch explizit rechnen.

Lemma 4.2. *Die Funktion f ist streng monoton wachsend auf $\mathbb{R}_{>0}$, d.h. Wenn $x < x'$ positive reelle Zahlen sind, so folgt $x^n < x'^n$.*

Beweis: Sei $x' = x + h$ mit $h > 0$. Nach der binomischen Formel ist

$$x'^n = (x+h)^n = x^n + \sum_{i=1}^{n} \binom{n}{i} x^{n-i} h^i > x^n$$

denn alle Summanden sind positiv. □

Lemma 4.3. *Für alle $x > 0$ gibt es $C(x) > 0$, so dass für alle $0 < |h| < 1$ gilt*

$$|f(x+h) - f(x)| \leq |h|C(x).$$

Beweis: Wir benutzen wieder die binomische Formel:

$$\begin{aligned}
|f(x+h) - f(x)| &= \left| \sum_{i=1}^{n} \binom{n}{i} x^{n-i} h^i \right| \\
&\leq \sum_{i=1}^{n} \binom{n}{i} x^{n-i} |h|^i \quad \text{Dreiecksungleichung} \\
&= |h| \sum_{i=1}^{n} \binom{n}{i} x^{n-i} |h|^{i-1} \quad \text{Ausklammern} \\
&\leq |h| \sum_{i=1}^{n} \binom{n}{i} x^{n-i} \quad |h| < 1 \\
&\leq |h| \sum_{i=0}^{n} \binom{n}{i} x^{n-i} \quad x > 0 \\
&= |h|(x+1)^n
\end{aligned}$$

□

Beweis des Satzes. Aus Monotonie folgt sofort die Eindeutigkeit.
Sei wie oben

$$w = \sup W, \quad W = \{a \in \mathbb{Q} | a > 0, a^n \leq x_0\}.$$

Sei $0 < \varepsilon < 1$. Es gibt $a \in W$ mit $a + \varepsilon > w \geq a$. Aus dem zweiten Lemma folgt (mit $x = w$, $h = a - w$ und daher $|h| < \varepsilon$)

$$w^n - a^n = |a^n - w^n| \leq |a - w|C(w)$$

und daher

$$w^n \leq a^n + |a - w|C(w) \leq x_0 + \varepsilon C(w). \tag{4.1}$$

Diese Ungleichung gilt für alle $\varepsilon > 0$, also folgt

$$w^n \leq x_0.$$

Angenommen, $w^n > x_0$. Sei $\varepsilon = (w^n - x_0)/C(w)$. In der Ungleichung (4.1) gilt dann

$$x_0 < w^n \overset{(4.1)}{\leq} a^n + \varepsilon C(w) = a^n + \frac{w^n - x_0}{C(w)} C(w) = a^n.$$

Dies ist ein Widerspruch zur Wahl von $a \in W$. Also muss $w^n \geq x_0$ gelten. Aus beiden Abschätzungen zusammen folgt $w^n = x_0$. □

4.2 Die Exponentialfunktion

Sei $a > 0$. Für $x = \frac{m}{n} \in \mathbb{Q}$ mit $n > 0$ setzen wir

$$a^x = \sqrt[n]{a}^m.$$

Es gelten die *Potenzgesetze* für $a, b \in \mathbb{R}_{>0}$, $x, y \in \mathbb{Q}$.

(i) $a^x > 0$,

(ii) $a^x b^x = (ab)^x$,

(iii) $a^{x+y} = a^x a^y$,

(iv) $(a^x)^y = a^{xy}$.

Definition 4.4. Sei $a > 0$, $x \in \mathbb{R}$. Wir definieren

$$a^x = \sup\{a^y \mid y \in \mathbb{Q}_{>0}, y \leq x\}.$$

Die Funktion $\exp_a : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto a^x$ heißt *Exponentialfunktion zur Basis a.*

Satz 4.5. *Die Potenzgesetze gelten auch für $x, y \in \mathbb{R}$, insbesondere gilt die* Funktionalgleichung

$$\exp_a(x + y) = \exp_a(x) \exp_a(y).$$

Beweis: Ausgelassen. □

4.3 Die Logarithmusfunktion

Sei in diesem Abschnitt $a > 1$ (der Fall $a < 1$ geht analog).

Lemma 4.6. *Die Funktion* $\exp_a$ *ist streng monoton steigend, also* $\exp_a(x) < \exp_a(y)$ *für $x < y$, und nimmt alle Werte in $\mathbb{R}_{>0}$ an.*

Beweis: Sei $y > x$. Dann ist

$$\exp_a(y) = \exp_a(x) \exp_a(y - x).$$

Es genügt also zu zeigen, dass $\exp_a(h) > 1$ für $h > 0$. Nach Definition reicht es, die Aussage für $h = \frac{m}{n} \in \mathbb{Q}$ zu überprüfen, also $n, m \in \mathbb{N}$. Mit $a > 1$ ist auch $a^m > 1^m$ und $\sqrt[n]{a^m} > 1$.

Die Potenzen von a sind nach oben unbeschränkt, ihre Kehrwerte nähern sich dann beliebig nah an 0 an. Um zu zeigen, dass jeder Wert dazwischen angenommen wird, muss man ähnlich wir für die Existenz der Wurzelfunktion vorgehen. Dies übersteigt unsere Möglichkeiten und wird daher heute ausgelassen. □

Definition 4.7. Sei $a > 1$. Die eindeutige positive reelle Zahl y mit $a^y = x$ heißt *Logarithmus* $\log_a(x)$ *von x zur Basis a.*

Aus der Funktionalgleichung für die Exponentialfunktion folgt

$$\log_a(x) + \log_a(y) = \log_a(xy).$$

Die Logarithmusfunktion

$$\log_a : \mathbb{R}_{>0} \to \mathbb{R}$$

ist ebenfalls streng monoton und nimmt alle Werte an.

Korollar 4.8. *Seien $a, b > 0$. Dann gilt*

$$\exp_b(x) = \exp_a(\log_a(b)x), \quad \log_b(y) = \frac{\log_a(y)}{\log_a(b)}.$$

Beweis:

$$a^{\log_a(b)x} = (a^{\log_a(b)})^x = b^x$$

mit den Potenzgesetzen und der Definition des Logarithmus. Die zweite Formel folgt durch Anwenden von $\exp_b$

$$\exp_b\left(\frac{\log_a(y)}{\log_a(b)}\right) = \exp_a\left(\log_a(b)\frac{\log_a(y)}{\log_a(b)}\right) = \exp_a(\log_a(y)) = y$$

und der Definition von $\log_b(y)$. □

4.4 Die Ableitung

Aus der Schule kennen Sie den Begriff der Ableitung bereits, aber vielleicht nicht die präzise Definition. Dann müssen Sie auf Analysis 1 warten.
Für $x \in \mathbb{R}$ ist

$$\exp_a'(x) = \lim_{h\to 0} \frac{a^{x+h} - a^x}{h} = \exp_a(x) \lim_{h\to 0} \frac{a^h - 1}{h}.$$

Lemma 4.9. *Der Grenzwert*

$$\lim_{h\to 0} \frac{a^h - 1}{h}$$

existiert.

Beweis: Wir müssen die Fälle $h > 0$ und $h < 0$ unterscheiden. Für $h > 0$ ist die Funktion

$$f : h \mapsto \frac{a^h - 1}{h}$$

streng monoton steigend (nicht offensichtlich, siehe Anhang). Die Funktion ist durch 0 nach unten beschränkt. Der Grenzwert ist das Infimum, also die größte reelle Zahl, die kleiner gleich allen Werten ist.

Es ist
$$\frac{a^{-h}-1}{-h} = a^{-h}\frac{a^h-1}{h}.$$
Auch hier existiert also der Grenzwert für $h \to 0$ und stimmt mit dem Grenzwert im positiven Fall überein. □

Definition 4.10. Wir setzen
$$l(a) = \lim_{h\to 0}\frac{a^h-1}{h}.$$
Es gilt also
$$\exp_a' = l(a)\exp_a.$$

Lemma 4.11. *Für alle $a, b > 1$ ist*
$$l(b) = \log_a(b)l(a).$$
Die Funktion $l(x)$ nimmt alle Werte in $\mathbb{R}_{>0}$ an.

Beweis: Wir differenzieren $\exp_b(x) = \exp_a(\log_a(b)x)$ mit der Kettenregel
$$\begin{aligned} l(b)\exp_b(x) = \exp_b'(x) = \exp_a(\log_a(b)x) &= \log_a(b)\exp_a'(\log_a(b)x) \\ &= \log_a(b)l(a)\exp_a(\log_a(b)x) = \log_a(b)l(a)\exp_b(x). \end{aligned}$$
Wir fixieren a und variieren b. Da $\log_a(b)$ alle Werte zwischen in $\mathbb{R}_{>0}$ annimmt, folgt dies auch für das Vielfache $l(b)$. □

Definition 4.12. Die *Eulersche Zahl* e ist die eindeutige positive reelle Zahl mit $l(\mathrm{e}) = 1$. Wir schreiben $\exp(x)$ für $\exp_{\mathrm{e}}$ (*Exponentialfunktion*) und $\log(x) = \log_{\mathrm{e}}(x)$ (*natürlicher Logarithmus*).

Korollar 4.13. *Es ist $l(x) = \log(x)$, $\exp'(x) = \exp(x)$, $\log'(x) = \frac{1}{x}$.*

Beweis: Die erste Aussage wiederholt die Formel des Lemmas für $a = \mathrm{e}$. Die zweite ist die Ableitungsformel mit $l(\mathrm{e}) = 1$. Die Formel für die Ableitung des Logarithmus folgt mit der Kettenregel aus $\exp(\log(x)) = x$:
$$1 = \exp(\log(x))' = \log'(x)\exp'(\log(x)) = \log'(x)\exp(\log(x)) = \log'(x)x.$$
□

In der Analysis 1 werden Sie die Formel
$$\mathrm{e} = \sum_{i=0}^{\infty}\frac{1}{i!} = 1 + \frac{1}{2} + \dots$$
kennenlernen, die aber sehr langsam ihrem Wert
$$\mathrm{e} = 2,71828\dots$$
entgegenstrebt.

Anhang A

Ein Grenzwert für $\exp$

Wir skizzieren die Herleitung, warum $\frac{a^x-1}{x}$ monoton wächst. Die Schritte müssen jeweils mit Sätzen über Grenzwerte rechtfertigt werden, die erst im Rahmen der Vorlesung hergeleitet werden.

1. Schritt: Die Folge

$$a_n = \left(1 + \frac{1}{n}\right)^n$$

ist streng monoton steigend und durch 3 nach oben beschränkt. Wir nennen das Supremum e.

2. Schritt: Für jedes x

$$\lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^{\frac{n}{x}} = \mathrm{e}$$

und daher

$$\lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n = \mathrm{e}^x.$$

3. Schritt: Es ist

$$\frac{\mathrm{e}^x - 1}{x} = \lim_{n\to\infty} x^{-1} \left(\sum_{i=0}^{n} \binom{n}{i} \frac{x^i}{n^i} - 1 \right) = \lim_{n\to\infty} \sum_{i=1}^{n} \binom{n}{i} \frac{x^{i-1}}{n^i}$$

Für $x > 0$ ist jeder Summand monoton wachsend, daher auch die Summe und dann auch der Grenzwert. Dies löst das Frage für $a = \mathrm{e}$. Insbesondere ist $x \mapsto \mathrm{e}^x$ differenzierbar.

4. Schritt: Nach Kettenregel ist a^x für alle a differenzierbar.

5. Schritt Wir berechnen $l(\mathrm{e})$:

$$\begin{aligned} l(\mathrm{e}) &= \lim_{x\to 0} \lim_{n\to\infty} \sum_{i=1}^{n} \binom{n}{i} \frac{x^{i-1}}{n^i} \\ &= \lim_{n\to\infty} \lim_{x\to 0} \sum_{i=1}^{n} \binom{n}{i} \frac{x^{i-1}}{n^i} \\ &= \lim_{n\to\infty} n \frac{1}{n} \\ &= 1. \end{aligned}$$

Die Definition von e im ersten Schritt stimmt mit der aus Kapitel 4 überein. Achtung: Das Vertauschen von Grenzwerten ist *nicht* harmlos. Auf Stackexchange (Frage 671281) findet man eine Herleitung, die den nötigen Grenzwertsatz umgeht.