Anhang A

Konstruktion der reellen Zahlen

Wir werden die etwas längliche, und über weite Strecken auch ziemlich langweilige, Konstruktion hier nur skizzieren. Eine systematische Darstellung findet sich beispielsweise in: Hans-Dieter Ebbinghaus et al. *Zahlen* aus der Reihe "Grundwissen Mathematik", 3. Auflage, Springer (1992) [ISBN 3-540-55654-0].

A.1 Die natürlichen Zahlen und das Prinzip der vollständigen Induktion

Auch Selbstverständlichkeiten wie "Zwei-Mal-Zwei-Gleich-Vier" sind in der Mathematik grundsätzlich beweisbedürftig,[1] und da erhebt sich natürlich erst mal die

[1] Dedekind im Vorwort zu seiner Abhandlung *Was sind und was sollen die Zahlen* (1893): "Was beweisbar ist, soll in der Wissenschft nicht ohne Beweis geglaubt werden".

Frage, was “Zwei” eigentlich genau ist ...

Definition der natürlichen Zahlen Die natürlichen Zahlen bilden eine Menge $\mathbb{N}$, in der ein Element $1 \in \mathbb{N}$ ausgezeichnet ist und auf der eine *Nachfolgerfunktion*[2] $S : \mathbb{N} \to \mathbb{N}$ definiert ist, so dass folgende *Axiome* erfüllt sind:

(1) S ist injektiv

(2) $1 \notin S(\mathbb{N})$

(3) Wenn eine Teilmenge $M \subset \mathbb{N}$ die 1 enthält und durch S in sich abgebildet wird, dann ist $M = \mathbb{N}$.

Statt “n ist Element von $\mathbb{N}$” sagt man auch “n ist eine natürliche Zahl”, oder einfach nur “die (natürliche) Zahl n”.

Die Definition klingt trocken erfüllt aber ihren Zweck. Die Abbildung S beschreibt den Vorgang des Zählens, wobei das erste Axiom dafür sorgt, dass man beim Zählen nicht mehrmals auf die gleiche Zahl stoßen kann, und das zweite Axiom dafür sorgt, dass man auch anfangen kann zu zählen. Nehmen wir also mal das ausgezeichnete Elemet (die ausgezeichnete Zahl) 1, bilden mit S ab, und bezeichnen das Bild mit dem Symbol “2”, sind wegen Axiom (2) sicher, dass damit nicht das Element 1 bezeichnet wird, und halten fest

$$2 := S(1)\,. \tag{A.1}$$

Von nun an ist 2 eine Element von $\mathbb{N}$, also eine Zahl, nicht länger lediglich ein Symbol, insbesondere $2 \neq 1$. Dann bilden wir 2 mit S ab, bezeichnen das Bild mit

[2] engl. “successor” Nachfolger

dem Symbol "3", sind wegen Axiom (1) sicher, dass damit weder 1 noch 2 gemeint sein können, und schauen auf

$$3 := S(2) \text{ bzw. } 3 = S(S(1)), \tag{A.2}$$

dann auf

$$4 := S(3) \text{ bzw. } 4 = S(S(S(1))), \tag{A.3}$$

und so weiter.

So könnte man beliebig lange weitermachen und käme doch nie ans Ziel – alle natürlichen Zahlen (d.h. die Menge $\mathbb{N}$) sauber definiert zu haben. Für das Zählen der Sternlein am Himmelszelt wäre das keine Kalamität – deren Anzahl ist zwar groß aber endlich. Um mit natürlichen Zahlen zu Rechnen, oder gar Aussagen alle natürlichen Zahlen betreffend zu beweisen, reicht einfaches Zählen aber nicht aus. Da hilft nun das dritte Axiom.

Das dritte Axiom ist eine mengentheoretische Formulierung für das *Prinzip der vollständigen Induktion*:

> Wenn die Zahl 1 die Eigenschaft E hat (Induktionsanfang), und für jede Zahl n, welche die Eigenschaft E hat, auch der Nachfolger $S(n)$ die Eigenschaft E hat (Induktionsschluss), dann haben alle natürlichen Zahlen diese Eigenschaft.

Wenn für die Zahl 1 die Aussage $E(1)$ zutrifft (Induktionsanfang), und für jedes n, für welches $E(n)$ zutrifft, auch $E(S(n))$ zutrifft (Induktionsschluss), dann trifft $E(n)$ für alle n zu.

Die Äquivalenz zum dritten Axiom ergibt sich, wenn die Eigenschaft E durch die Teilmenge M derjenigen Zahlen ersetzt wird, die die Eigenschaft E haben, $M = \{n|E(n) \text{ gilt}\}$.

Das Prinzip der vollständigen Induktion wird gerne für Beweise herangezogen, aber auch Rechenoperationen, wie etwa die *Addition*, lassen sich damit kurz und griffig definieren:

$$m+1 := S(m) \tag{A.4}$$
$$m+S(n) := S(m+n) \tag{A.5}$$

Die Definition ist offensichtlich *induktiv* in Bezug auf n. Induktionsanfang (die Defintion für $n=1$) ist mit Gl. (A.4) gegeben; der Induktionsschluss von n nach $S(n)$ ist mit Gl. (A.5) vollzogen.

Die Gültigkeit von "Zwei plus Zwei ist Vier" ist jetzt zwar schnell bewiesen,

$$2+2 \overset{A.1}{=} S(1)+S(1) \tag{A.6}$$
$$\overset{A.5}{=} S(S(1)+1) \tag{A.7}$$
$$\overset{A.4}{=} S(S(S(1))) \tag{A.8}$$
$$\overset{A.3}{=} 4 \tag{A.9}$$

aber man kann sich vorstellen, dass ein Paar allgemeine Rechenregeln, wie das *Assoziativgesetz* und das *Kommutativgesetz*

$$(m+n)+k = m+(n+k) \tag{A.10}$$
$$m+n = n+m \tag{A.11}$$

das Addieren erleichtern. Solche Regeln sind allerdings immer erst mal beweisbedürftig bevor man sie in der freien Wildbahn benutzt. Das Assoziativgesetzt beweist man am besten mittels vollständiger Induktion nach k. Sei also $E(k)$ die Aussage "$(m+n)+k = m+(k+n)$". Wir wollen zeigen, dass $E(k)$ für alle natürlichen Zahlen k gilt, behaupten also $M := \{k|E(k) \text{ gilt}\} = \mathbb{N}$. Für k ist die Aussage $E(1)$,

ausführlich "$(m+n)+1 = m+(n+1)$", identisch "$S(m+n) = m+S(n)$", und diese Aussage ist angesichts Gl. (A.5) wahr, somit $E(1)$ legitimer Induktionsanfang. Die Aussage $E(k+1)$ wird durch folgende Rechnung bewiesen, wobei an der Stelle $*$ die Aussage $E(k)$ als Induktionsvoraussetzung benutzt wird:

$$\begin{aligned}
(m+n)+k+1 &\overset{A.4}{=} (m+n)+S(k) && \text{(A.12)}\\
&\overset{A.5}{=} S((m+n)+k) && \text{(A.13)}\\
&\overset{*}{=} S(m+(n+k)) && \text{(A.14)}\\
&\overset{A.5}{=} m+S(n+k) && \text{(A.15)}\\
&\overset{A.4}{=} m+(n+k+1)\,. && \text{(A.16)}
\end{aligned}$$

Der Induktionsschluss "von k nach $k+1$" ist somit vollzogen, und das Assoziativgesetz (A.10) ist als legitime Rechenregel etabliert. Den Beweis des Kommutativgesetzes sparen wir uns. Er verläuft ähnlich wie beim Assoziativgesetz, nur dass man hier mit doppelter Induktion bzgl. n und m arbeitet.

Die Multiplikation kann, in Analogie zur Addition, auch induktiv definiert werden

$$\begin{aligned}
m\cdot 1 &:= m\,, && \text{(A.17)}\\
m\cdot S(n) &:= (m\cdot n)+m\,. && \text{(A.18)}
\end{aligned}$$

Wenn man sicher ist, dass man auch richtig verstanden wird, kann man den Malpunkt auch unter den Tisch fallen lassen. Für "a mal b" schreibt man dann einfach ab, statt $a\cdot b$. Wir behalten den Malpunkt aber erst mal bei ....

Als kleine Anwendung beweisen wir dass Zwei mal Zwei auch tatsächlich gleich Vier,

$$\begin{aligned} 2 \cdot 2 &\overset{A.1}{=} 2 \cdot S(1) && \text{(A.19)} \\ &\overset{A.18}{=} (2 \cdot 1) + 2 && \text{(A.20)} \\ &\overset{A.17}{=} 2 + 2 && \text{(A.21)} \\ &\overset{A.9}{=} 4\,, && \text{(A.22)} \end{aligned}$$

greifen bei größeren Rechnereien aber gerne auf das *Assoziativgesetz und Kommtativgesetz der Multiplikation* zurück,

$$\begin{aligned} (m \cdot n) \cdot k &= m \cdot (n \cdot k)\,, && \text{(A.23)} \\ m \cdot n &= n \cdot m\,, && \text{(A.24)} \end{aligned}$$

und benutzen, wenn Plus- und Malrechnung kombiniert werden, das *Distributivgesetz der Arithmetik*

$$(m + n) \cdot k = m \cdot k + n \cdot k\,. \qquad \text{(A.25)}$$

Stillscheigend nehmen wir mal an, dass Sie die Regeln beweisen bevor Sie sie benutzen ...

Stößt man beim Abzählen bei m anfangend nach $k \in \mathbb{N}$ Schritten auf ein n, sagt man m sei kleiner als n. Mathematisch *definiert* man die Relation "kleiner" mittels Addition,

$$m < n \text{ genau dann wenn es ein } k \in \mathbb{N} \text{ gibt, mit } k + m = n. \qquad \text{(A.26)}$$

Die Zahl k nennt man dann auch die *Differenz* der beiden Zahlen, notiert $k = n - m$. Dabei ist zu beachten, dass die so eingeführte *Subtraktion* zwar als Umkehrung der Addition erscheint, dass sie aber im Bereich der natürlichen Zahlen nicht uneingeschränkt ausführbar ist. Sie ist eben nicht für alle Paare (m, n) definiert ist, sondern nur für solche mit $m < n$.

Statt "m ist kleiner als n" kann man natürlich auch sagen "n ist größer als m", notiert $n > m$. Und will man offen lassen ob m kleiner oder gleich n schreibt man $m \leq n$, entprechend $n \geq m$ für die Variante "n ist größer oder gleich m".

Die hier eingeführte Beziehung $\leq$ erfüllt die Kriterien einer *Ordnungsrelation*: sie ist 1. *reflexiv*, denn $n \leq n$, 2. *antisymmetrisch*, denn wenn $n \leq m$ und $m \leq n$, dann gilt $m = n$, und 3. *transitiv*, denn wenn $n \leq m$ und $m \leq l$, dann gilt $n \leq l$. Die Ordnung ist *total*, auch genannt *linear*, denn für alle $m, n \in \mathbb{N}$ ist $n < m$ oder $m \leq n$. Und sie ist *monoton* bzgl. Addition und Multiplikation: Für alle $l, m, n \in \mathbb{N}$ folgt aus $n \leq m$, dass auch $n + l \leq m + l$ und $n \cdot l \leq m \cdot l$.

Analog zur Subtraktion wird die Division als Umkehrung der Multiplikation eingeführt: Lässt sich eine natürtliche Zahl n als das Produkt zweier natürlicher Zahlen m, l schreiben, also $n = m \cdot l$, notiert man diesen Umstand auch gerne in der Form $n \div l = m$ bzw. $n \div m = l$. Die Zahl m (und die Zahl l) heißt dann *Divisor* von n. Wie bei der Subtraktion gilt es hier zu beachten, die Division nicht für alle Paare (m, n) erkärt ist.

Eine Zahl, die die Zahl 2 als Divisor hat heißt *gerade*, ansonsten heißt sie *ungerade*. Die Abbildung mit $n \mapsto 2n$ ist eine Bijektion von $\mathbb{N}$ auf die Menge der geraden Zahlen. Es gibt demnach "genauso viele" gerade Zahlen wie es natürliche Zahlen gibt, und das obwohl die geraden Zahlen eine echte Teilmenge der Menge aller natürlichen Zahlen. Tja – so ist das halt mit den unendlichen Mengen ...

Hat eine Zahl p nur sich selbst und die Zahl 1 als Divisor, dann handelt es sich um eine sog. *Primzahl*. Eine Primzahl ist immer ungerade. Eine Ausnahme ist die Zahl 2 – the oddest of all prime numbers.

Jede natürliche Zahl n lässt sich als Produkt von Primzahlen schreiben, $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, wobei eine Primzahl durchaus mehrmals vorkommen kann. Beispiel: $12 = 2 \cdot 2 \cdot 3$. Die Primzahl 1 schreibt man dabei meist nicht hin. Die Primzahlzerlegung

einer gegebenen Zahl wird umso schwieriger, je größer die Zahl. Man kennt bis heute keinen effektiven Algorithmus, der einem eine solche Zerlegung liefern würde. Diese Tatsache spielt für die Verschlüsselung im sog. *public key encryption* eine prominente Rolle.

Neben dem Typ "Primzahl" gibt es weitere Typen, die in der Arithmetik der natürlichen Zahlen eine prominente Rolle spielen. "Vollkommen", beispielsweise, ist eine Zahl, wenn sie gleich der Summe aller ihrer Divisoren ist, die Zahl selber ausgenommen. Die Zahl 6, beispielsweise, hat als Divisoren die Zahlen $1, 2, 3$, und wie man sich leicht überzeugt, ist 6 vollkommen da $6 = 1 + 2 + 3$. Vollkommene Zahlen sind selten, und es ist eine ungelöste Frage ob es unendlich viele vollkommene Zahlen gibt und ob diese immer gerade sein müssen.

DIe Gleichung $a^2 + b^2 = c^2$ hat Lösungen in ganzen Zahlen, beispielsweise $(a, b, c) = (3, 4, 5)$. Solche Zahlentripel heißen *Pythagoräische* Tripel, und solcher Tripel gibt es unendlich viele wie schon in Euklids Geometrie bewiesen. Im Gegensatz dazu hat die Gleichung $a^n + b^n = c^n$ hat für jedes gegebene $n \geq 3$ keine Lösung in den natürlichen Zahlen. Das ist der Inhalt des *letzten Fermatschen Satzes*, der bis ins Jahr 1995 allerdings noch *Fermatsche Vermutung* hieß, weil er erst im Jahr 1995 durch Andrew Wiles bewiesen wurde.

Zum Abschluss nun noch eine Vermutung, die einfach zu formulieren ist, deren Beweis (oder Widerlegung) bislang aber nicht gelungen. In heutiger Formulierung

Goldbachsche Vermutung Jede gerade Zahl größer 4 lässt sich als Summe zweier Primzahlen schreiben.

Ok. Fangen wir mal an: $6 = 5 + 1$, $8 = 5 + 3 = 7 + 1$, $10 = 7 + 3 = 5 + 5$, $12 = 11 + 1 = 7 + 5$. Sieht aus, als ob Goldbach recht hat. Aber ein Beweis ist das natürlich nicht. Hätten Sie einen?

A.2 Die ganzen Zahlen

Die gesamte Arithmetik der natürlichen Zahlen – das ist das Rechnen mit "Plus" und "Mal" – läßt sich mit Hilfe der Axiome (1)–(3) und Definitionen von Addition und Multiplikation rekonstruieren. Im Abgleich mit dem was man so in der Schule vielleicht schon mal gesehen hat fällt allerdings auf, dass "Null" noch nie erwähnt wurde, und auch dass bislang weder von "minus" noch von "negativen Zahlen" , weden von "durch" noch von "Brüchen" die Rede war, geschweige denn von Monstern wie $\sqrt{2}$ oder π.

Dem Selbstverständnis von Mathematik entsprechend, sollten diese neuen Dinge – in ihrer Gesamtheit genannt die *reellen Zahlen* – möglichst unter ausschließlichem Rückgriff auf die alten Dinge eingeführt werden, d.h. durch Definitionen oder ähnliches, aber eben ohne neue Axiome oder Postulate. Man nennt dieses Vorgehen *konstruktiv*, weil es eben diese neuen (=ganze, rationale, reelle) Zahlen schafft, und nicht etwa postuliert. Das konstruktive Vorgehen hat seinen Charme, aber es dauert ziemlich lang, bevor sie von -1 reden dürfen oder gar damit rechnen.

Zunächst hätte man gerne zu jeder natürlichen Zahl n auch eine negative Zahl $-n$, eine Zahl Null, die die Summe $n + (-n)$ bezeichnet, und ein paar Regeln, die einem das Rechnen mit all diesen Zahlen erlaubt.

Auch wenn an dieser Stelle noch kein uneingeschränkter Begriff der Subtraktion zur Verfügung steht – aus ihrer Schulzeit wissen sie sehr wohl, dass sich jede *ganze Zahl* p als Differenz zweier natürlicher Zahlen darstellen lässt, soll heißen gibt es $m, n \in \mathbb{N}$ mit $p = m - n$. Daher liegt es nahe, die ganze Zahl $m - n$ (ob nun positiv oder negativ) durch das geordnetes Paar (m, n) zu beschreiben. Dabei gilt es allerdings zu beachten, dass auch andere Paare (k, l) dieselbe ganze Zahl $m-n = k-l$ beschreiben können, nämlich genau dann, wenn $m + l = k + n$.

Inspiriert von diesen Hinweisen definiert man auf $N \times N$ die Relation

$$(m,n) \sim (k,l) \text{ genau dann, wenn } m+l = n+k\,, \tag{A.27}$$

und überzeugt sich zunächst, dass es sich bei $\sim$ um eine Äquivalenzrelation handelt. Die durch (m,n) repräsentierte Äquivalenzklasse $\{(x,y)|(x,y) \sim (m,n)\}$ wird mit $[m-n]$ bezeichnet, wobei das "Minus" hier lediglich ein Symbol, keine Rechenvorschrift. Wegen $\{(x,y)|(x,y) \sim (m,n)\} = \{(x,y)|(x,y) \sim (m+p,n+p)\}$ für jedes $p \in \mathbb{N}$ gilt

$$[m-n] = [(m+p)-(n+p)] \tag{A.28}$$

wobei hier Gleichheit (von Mengen bzw. Äquivalenzklassen) ausgedrückt wird, und nicht $\sim$-Äquivalenz (von Zahlenpaaren).

Angesichts der Kürzungsrgel (A.28) kann es nun nicht schaden, wenn sie so tun, als handele es sich bei $[m-n]$ tatsächlich um eine Differenz, obwohl sie offiziell bislang nur Differenzen für $m > n$ bilden können. Sie würden dann beispielsweise erhalten $[4-2] = [2]$, oder $[2-4] = [-2]$, und sich garnicht wundern wenn nun die Menge der ganzen Zahlen $\mathbb{Z}$ als die Menge der Mengen $\sim$-äquivalenter Paare natürlicher Zahlen eingeführt wird. Im Notationsjargon der Mathematik ist das die Faktormenge

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim\,, \tag{A.29}$$

bzw. etwas ausführlicher, weil explizit

$$\mathbb{Z} = \{[1-1],[2-1],[1-2],[3-1],[1-3],[4-1],[1-4],\ldots\}\,. \tag{A.30}$$

Bei der Erzeugung dieser Liste aus der Defintion (A.29) ist man gut beraten die *Kürzungsregel* (A.28) zu berücksichtigen, um Mehrfachnennungen ein-und-derselben ganzen Zahl zu vermeiden.

In $\mathbb{Z}$ gibt es ein ausgezeichnetes Element,

$$0 := \{(x,x)|x \in \mathbb{N}\} \tag{A.31}$$

in Worten "Null". Die Null ist also eine Menge – man lernt nie aus .... Angesichts der Kürzungsregel (A.28) gilt übrigens $0 = [n - n]$ für beliebige natürliche Zahl n, insbesondere $0 = [1 - 1]$.

Um in $\mathbb{Z}$ zu rechnen müssen jetzt entsprechende Operationen (Addition, Multiplikation, Subtraktion) definiert werden. Auch hier soll aussschließlich auf den bereits eingeführten Operationen aufgebaut werden, ohne irgendwelche zusätzlichen Postulate einzuführen.

Frisch ans Werk. Die fraglichen Operationen werden komponentenweise verabredet,

$$[m - n] +_{\mathbb{Z}} [k - l] := [(m + k) - (n + l)] , \tag{A.32}$$

$$[m - n] \cdot_{\mathbb{Z}} [k - l] := [(m \cdot k + n \cdot l) - (m \cdot l + n \cdot k)] , \tag{A.33}$$

$$[m - n] -_{\mathbb{Z}} [k - l] := [(m + l) - (n + k)] , \tag{A.34}$$

wobei wir hier sicherheitshalber die neuen Operatoren mit einem Subskript gekennzeichnet haben um sie von den bereits definierten Operatoren $+, \cdot$ zu unterscheiden (letztere Verknüpfen natürliche Zahlen, erstere verknüpfen Äquivalenzklassen von Paaren natürlicher Zahlen).

Die Definitionen sind unabhängig von der Wahl der repräsentierenden Paare, d.h. sie verknüpfen die Klassen und nicht nur deren Repräsentanten. Für die Addition, beispielsweise, bedeutet das, dass wenn $[m' - n'] = [m - n]$ und $[k' - l'] = [k - l]$, dann ist $[(m' + k') - (n' + l')] = [(m + k) - (n + l)]$. Diese Festellung erlaubt es, das Subskript in (A.32)–(A.34) wieder fallenzulassen, da sich die Addition in $\mathbb{Z}$ genauso verhält wie die Addition in $\mathbb{N}$. Insbesondere sind die Assoziativgesetze, Kommutativgesetze und das Distributivgesetz auch in $\mathbb{Z}$ gültige Rechenregeln (was man in einem ordentlichen Matheskript beweisen sollte).

Wirklich neu sind hier die Subtraktion, die angesichts

$$[m - n] - [k - l] + [k - l] = [(m + k + l) - (m + k + l)] = [m - n] \tag{A.35}$$

mit Fug und Recht als Umkehrung der Addition gilt, und die Existenz eines Neutralelements $[k-k]$ für die Addition,

$$[m-n]+[k-k]=[(m+k)-(n+k)]=[m-n] \tag{A.36}$$

das bereits in (A.31) mit der Zahl 0 identifiziert wurde. Die zu einer Zahl $[m-n]\in\mathbb{Z}$ bezgl. der Addition inverse Zahl ist wegen

$$[m-n]+[n-m]=[(m+n)-(m+n)]=0 \tag{A.37}$$

die Zahl $[n-m]$. Das legt es nahe, die Verwandschaft der beiden Zahlen $[m-n]$ und $[n-m]$ durch ein vorangestelltes Minuszeichen zum Ausdruck zu bringen indem man definiert

$$-[m-n]:=[n-m] \tag{A.38}$$

Die Definition verträgt sich mit den arithmetischen Operatoren in $\mathbb{Z}$. Für die ganze Zahl 0 – und nur für diese Zahl – ergibt sich die Regel

$$-0=0 \tag{A.39}$$

was man vielleicht auch schon mal gesehen hat.

Natürlich notiert niemand im täglichen Leben die ganzen Zahlen in der Form $[m-n]$. Der Anschluss an die tägliche Praxis wird vollzogen, indem man für ein gegebenes $n\in\mathbb{N}$ schreibt

$$+n \quad \text{für die ganze Zahl } [S(n)-1] \text{ und} \tag{A.40}$$
$$-n \quad \text{für die ganze Zahl } [1-S(n)] \tag{A.41}$$

worin S die in Abschnitt definierte Nachfolgerfunktion. Man nennt $[S(n)-1]$ bzw. $[1-S(n)]$ auch eine *Normalform* der Darstellung $[k-l]$ für den Fall $k>l$ bzw.

$l > k$. Das hier auftretende Plus- bzw, Minuszeichen nennt man das *Vorzeichen* der entsprechenden Zahl.

Da man jede Zahl $[m - n]$ auf die Form 0, $[S(k) - 1]$ oder $[1 - S(k)]$ mit wohlbestimmtem $k \in \mathbb{N}$ kürzen kann (die Genannten bilden ein Repräsentantensystem von $\mathbb{Z}$) lässt sich die Menge der ganzen Zahlen schreiben

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \{0, \pm 1, \pm 2, \ldots\} \tag{A.42}$$

was man vielleicht auch schon mal gesehen hat.

Die Anordung in $\mathbb{Z}$ wird wie in $\mathbb{N}$ erklärt,

$$q \leq p \text{ genau dann, wenn } p - q \in \mathbb{N} \cup \{0\}. \tag{A.43}$$

Die Anordnung ist total, denn für alle $q, p \in \mathbb{Z}$ ist $p < q$ oder $q \leq p$. Und sie ist monoton bzgl. Addition, denn ür alle $p, q, r \in \mathbb{Z}$ folgt aus $p \leq q$, dass auch $p + r \leq q + r$.

Die Menge der ganzen Zahlen ist abzählbar. Die Abbildung $\mathbb{Z} \to \mathbb{N}$, erklärt $[1-1] \mapsto 1$, $[S(n) - 1] \mapsto 2n$, $[1 - S(n)] \mapsto 2n + 1$, ist umkehrbar eindeutig. Also ist $\mathbb{Z}$ eine abzählbar-unendliche Menge. Es gibt "genauso viele" ganze Zahlen, wie es natürliche Zahlen gibt ...

A.3 Die rationalen Zahlen

In Anolgie zu den ganzen Zahlen werden auch die rationalen Zahlen als Klassen von Zahlenpaaren eingeführt. Ausgangspunkt ist die Äquivalenzrelation

$$(p, q) \sim (r, s) \text{ genau dann, wenn } p \cdot s = q \cdot r. \tag{A.44}$$

auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Äquivalenzklassen sind die *rationalen Zahlen*, im Alltag auch genannt *Brüche*. Die Menge der rationalen Zahlen, bezeichnet $\mathbb{Q}$, ist demnach gegeben

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim \ . \tag{A.45}$$

Der durch (p, q) repräsentierte Bruch $\{(x, y) | (x, y) \sim (p, q)\} \in \mathbb{Q}$ wird mit $\frac{p}{q}$ bezeichnet. Die Zahl p heißt der *Zähler*, die Zahl q heißt der *Nenner*. Das Äquivalenzkriterium () übersetzt sich in die *Kürzungsregel*

$$\frac{k \cdot p}{k \cdot q} = \frac{p}{q}\,, \tag{A.46}$$

von rechts nach links gelesen genannt *Erweiterungsregel*.

Die Abbildung $\mathbb{Z} \ni p \mapsto \frac{p}{1} \in \mathbb{Q}$ ist injektiv. Man kann also die ganze Zahl p mit der Klasse $\frac{p}{1}$ identifizieren, und schreibt nach vollzogener Identifizierung $\mathbb{Z} \subset \mathbb{Q}$ – gelesen "die ganzen Zahlen sind eine Teilmenge der rationalen Zahlen". Auf diese Art wird die $1 \in \mathbb{Z}$ mit der "Eins" in $\mathbb{Q}$, repräsentiert durch die Brüche $\frac{p}{p}$, identifiziert, und die $0 \in \mathbb{Z}$ wird mit der "Null" in $\mathbb{Q}$, das sind die Brüche $\frac{0}{p}$, identifiziert.

Addition und Multiplikation rationaler Zahlen sind definiert,

$$\frac{p}{q} + \frac{r}{s} := \frac{p \cdot s + r \cdot q}{q \cdot s} \tag{A.47}$$

$$\frac{p}{q} \cdot \frac{r}{s} := \frac{p \cdot r}{q \cdot s}\,. \tag{A.48}$$

Diese Definitionen sind unabhängig von der Wahl des Repräsentanten, für ganze Zahlen $\frac{p}{q}$, $\frac{r}{s}$ sind das genau die bisherige Addition und Multiplikation, es gelten die Assoziativ-, Kommtativ- und Distributivgesetze.

Die Erweiterung von $\mathbb{N}$ nach $\mathbb{Z}$ hat die uneingeschränkte Subtraktion ermöglicht. Das wesentlich neue an den rationalen Zahlen ist, dass nun auch die Division uneingeschränkt möglich ist. Angesichts

$$\frac{p}{q} \cdot \frac{q}{p} \equiv \frac{p \cdot q}{q \cdot p} = 1 \,. \tag{A.49}$$

gibt es nämlich zu jeder rationalen Zahl $\frac{p}{q} \neq 0$ eine multiplikativ inverse rationale Zahl $\frac{q}{p}$.

Verabredungsgemeäss notiert man das Inverse von $a \in \mathbb{Q} \setminus \{0\}$ als $\frac{1}{a}$. Kennt man eine Bruchdarstellung von a, also $a = \frac{p}{q}$, ist beim Rumrechnen auch die 1 in der Bruchdarstellung, z.B. $\frac{1}{1}$ zu verwenden,

$$\frac{1}{a} = \frac{\frac{1}{1}}{\frac{p}{q}} = \frac{q}{p} \,. \tag{A.50}$$

Ganzzahlige Potenzen einer rationalen Zahl sind definiert

$$a^0 := 1 \,, \qquad a^n := a \cdot a^{n-1} \,, \qquad a^{-n} := a^{-(n-1)} \cdot \frac{1}{a} \qquad \text{für alle natürliche Zahlen } n = 1, 2, \ldots. \tag{A.51}$$

wobei die negativen Potenzen $a \neq 0$ voraussetzen. Das Rechnen mit Potenzen wird durch folgende Regeln erleichtert,

$$a^r \cdot b^r = (a \cdot b)^r \tag{A.52}$$

$$a^r \cdot a^s = a^{r+s} \tag{A.53}$$

$$(a^r)^s = a^{r \cdot s} \tag{A.54}$$

die man mittels Kommtutativ- und Assoziativgesetz, gegebenenfalls vollständiger Induktion, beweist. Ausgerüstet mit der Potenzschreibweise lässt sich jetzt das a-fache des b-Inversen, $a \cdot \frac{1}{b}$, statt in der vertikal anspruchsvollen Form $\frac{a}{b}$ nun auch in

der Fließtext-freundlichen Form $a \cdot b^{-1}$ notieren,

$$a \cdot \frac{1}{b} \equiv \frac{a}{b} \equiv a \cdot b^{-1} \tag{A.55}$$

Ein Bruch $\frac{p}{q}$ heißt *positiv*, wenn p und q entweder beide positiv oder beide negativ. Ein Bruch heißt *negativ*, wenn $p \cdot q < 0$. Fasst man alle positiven Brüche zu einer Menge $\mathbb{P}$ zusammen, und alle negativen Brüche zu einer Menge $-\mathbb{P}$, kann $\mathbb{Q}$ als disjunkte Vereinigung dargestellt werden

$$\mathbb{Q} = -\mathbb{P} \times \{0\} \times \mathbb{P}\,. \tag{A.56}$$

Das Adjektiv "disjunkt" bedeutet, dass jede rationale Zahl Element genau einer der drei Mengen ist.

Die Menge $\mathbb{P}$ der postivien Brüche ist unter Addition und Multiplikation abgeschlossen, d.h. für $a, b \in \mathbb{P}$ ist auch $a + b \in \mathbb{P}$ und $a \cdot b \in \mathbb{P}$. In Analogie zu () definiert

$$a \leq b \text{ genau dann, wenn } b - a \in \mathbb{P} \cup \{0\} \tag{A.57}$$

eine Anordnung der rationalen Zahlen. Auf der Teilmenge $\mathbb{Z} \subset \mathbb{Q}$ gleicht sie der Anordnung der ganzen Zahlen, Gl. (A.43). Man braucht daher nicht zwei verschiedene Anordnungsbegriffe für die beiden Mengen $\mathbb{Z}$ und $\mathbb{Q}$.

Für beliebige zwei positive rationale Zahlen a, b gibt es immer eine natürliche Zahl n so dass a kleiner als das n-fache von b, also $a < n \cdot b$. Man sagt, die rationalen Zahlen seien *archimedisch* geordnet.

Zum Beweis der archimedischen Ordnung von $\mathbb{Q}$ schreibt man zunächst $a = p/r$ und $b = q/r$ als Brüche natürlicher Zahlen mit einem gemeinsamen Nenner. Die archimedische Ordnung ist dann etabliert, wenn $p < n \cdot q$ bewiesen ist (man teile diese Ungleichung einfach durch r). Der Beweis der letzteren Ungleichung kann für

gegebenes q mittels vollständiger Iduktion bzgl. $p = 1, 2, \ldots$ geführt werden: für $p = 1$ (Induktionsanfang) gibt es in jedem Fall ein n, beispielsweise $n = 2$, denn $1 < 2 \cdot q$ für alle $q \in \mathbb{N}$. Gibt es nun für p eine natürliche Zahl n, so dass $p < n \cdot q$ (Induktionsvoraussetzung), dann gibt es wegen $p + 1 < n \cdot q + 1 \leq (n + 1) \cdot q$ auch für $p + 1$ eine natürliche Zahl $n' = n + 1$, so dass $p + 1 < n' \cdot q$. qed

Archimedisch geordnet sind auch die ganzen Zahlen, aber es gibt eine wichtigen Unterschied zwischen den ganzen und den rationalen Zahlen: ihre *Dichtigkeit*. Für beliebige zwei rationale Zahlen a, b läßt sich immer ein c angeben mit $a < c < b$, beispielsweise das aritmetische Mittel $c = \frac{1}{2} \cdot (a + b)$.[3] Wem die Zahlengerade vor Augen ist, der sieht, dass man zwischen zwei beliebigen Punkten die zwei rationale Zahlen verkörpern, immer noch einen Punkt angeben kann, der auch eine rationale Zahl verkörpert. Die beiden Punkte mögen dabei noch so eng aneinanderliegen – es gibt immer noch einen Punkt dazwischen.

Es scheint daher, als ob es viel viel mehr rationale Zahlen gäbe als es ganze Zahlen gibt. Das ist aber nicht der Fall: auch die Menge der rationalen Zahlen ist abzählbar, wie Georg Cantor mit seinem berühmten Diagonalverfahren gezeigt hat. Man sagt, die Menge der rationalen Zahlen hat die gleiche *Mächtigkeit* wie die Menge der ganzen Zahlen (und die hat die gleiche Mächtigkeit wie die Menge der natürlichen Zahlen).

[3] Bei den ganzen Zahlen geht das nicht: es gibt keine ganze Zahl p mit $17 < p < 18$.

A.4 Der Dedekind'scher Schnitt und die reellen Zahlen

Die Länge der Diagonalen im Einheitsquadrat – also "Wurzel-Zwei" – ist zwar keine rationale Zahl, lässt sich aber mit Hilfe eines Zirkels auf der Zahlengeraden abtragen. Auch der Umfang eines Einheitskreises ist keine rationale Zahl, lässt sich aber durch Abrollen auf der Zahlengerade fassen. Die Zahlengerade umfasst demnach nicht nur die bereits bekannten rationalen Zahlen, sondern eben auch Konstrukte wie $\sqrt{2}$ oder die Kreiszahl π. Abrollen von Kreisen lässt sich aber nur schwerlich verallgemeinern – wie soll man also einen beliebig herausgegriffenen Punkt auf der Zahlengerade begrifflich fassen wenn man zunächst nur die rationalen Zahlen zur Verfügung hat? Richard Dedekinds verblüffend einfache Antwort: indem man die Zahlengerade durchschneidet und den fraglichen Punkt mit der Schnittkante identifiziert wo die beiden Teile – jeweils aufgefasst als Mengen rationaler Zahlen – aneinanderstoßen ...[4]

Definition: Ein Paar $(\underline{X}, \overline{X})$ von Teilmengen von $\mathbb{Q}$ heißt ein *Dedekind'scher Schnitt über* $\mathbb{Q}$, wenn gilt:

(S1) Jede rationale Zahl gehört einer der beiden Mengen $\underline{X}$, $\overline{X}$ an

(S2) Keine der beiden Mengen ist leer

(S3) Für $r \in \underline{X}$, $s \in \overline{X}$ gilt $r < s$.

(S4) Die Menge $\overline{X}$ hat kein kleinstes Element.

$\underline{X}$ heißt die *Unter-*, $\overline{X}$ die *Oberklasse* des Schnittes.

[4] R. Dedekind *Stetigkeit und irrationale Zahlen*, Braunschweig 1872, S. 10; zitiert nach: Ebbinghaus et al *Zahlen*, S. 23

Jeder Dedekind'sche Schnitt heißt eine *reelle Zahl*. Die Menge aller reellen Zahlen wird mit $\mathbb{R}$ bezeichnet. Reelle Zahlen sind also geordnete Paare von geordneten Mengen (die rationalen Zahlen sind wohlgeordnet – schon vergessen?). Man wundert sich ja über gar nichts mehr ...

Ein Schnitt heißt *rational*, wenn die Unterklasse ein größtes Element aufweist. Betrachte etwa für r rational die Menge

$$\overline{X}_r := \{s \in \mathbb{Q} \mid r < s\} \tag{A.58}$$

und ihr Komplement $\mathbb{Q} \setminus \overline{X}_r =: \underline{X}_r$. Eigenschaften (S1)–(S4) sind hier leicht nachzuweisen[5] – das Paar $(\underline{X}_r, \overline{X}_r)$ ist ein Dedekind'scher Schnitt. Und da $\underline{X}_r$ ein maximales Element aufweist – für alle $q \in \underline{X}_r$ gilt nämlich $q \leq r$ – ist $(\underline{X}_r, \overline{X}_r)$ ein rationaler Schnitt.

Ein wichtiger rationaler Schnitt ist der *Nullschnitt*, die Obermenge $\overline{X}_0 = \{s \in \mathbb{Q} \mid 0 < s\}$ offensichtlich die Menge aller positiven rationalen Zahlen. Auch nicht zu verachten der *Einsschnitt*, die Obermenge $\overline{X}_1 = \{s \in \mathbb{Q} \mid 1 < s\}$ offensichtlich die Menge aller rationalen Zahlen größer 1.

Die Abbildung $\mathbb{Q} \ni r \mapsto (\underline{X}_r, \overline{X}_r) \in \mathbb{R}$ ist injektiv. Man kann demnach die rationale Zahl r mit dem geordneten Paar $(\underline{X}_r, \overline{X}_r)$ identifizieren, und schreibt nach vollzogener Identifizierung $\mathbb{Q} \subset \mathbb{R}$, gelesen "die rationalen Zahlen sind Teilmenge der reellen Zahlen" bzw. "die rationalen Zahlen sind in die reellen Zahlen eigebettet". Wie man sich bettet so liegt man ...

Es gibt nicht nur rationale Schnitte. Betrachte etwa (das Subskript ist hier rein symbolisch zu verstehen)

$$\overline{X}_{\sqrt{2}} := \{s \in \mathbb{Q} \mid 2 < s^2\} \tag{A.59}$$

[5] Zum Nachweis von (S4) nehme man an, a sei das kleinste Element von $\overline{X}_r$; dann wäre doch $b := (a - r)/2$ rational mit $r < b < a$, also b Element von $\overline{X}_r$, kleiner als a im Widerspruch zur Annahme.

und ihr Komplement $\mathbb{Q} \setminus \overline{X}_{\sqrt{2}} =: \underline{X}_{\sqrt{2}}$. Auch hier sind die Eigenschaften (S1)–(S4) leicht nachgewiesen. Die Menge $\underline{X}_{\sqrt{2}}$ hat aber nun kein größtes Element, d.h. $(\underline{X}_{\sqrt{2}}, \overline{X}_{\sqrt{2}})$ ist zwar ein Schnitt, aber kein rationaler Schnitt.

Für zwei reelle Zahlen $x = (\underline{X}, \overline{X})$ und $y = (\underline{Y}, \overline{Y})$ wird die Ordnungsrelation $x < y$ mengentheoretisch durch die Inklusion der Obermengen $\overline{Y} \subset \overline{X}$ definiert. Beweise für die Reflexivität, Transitivität und Antisymmetrie sind für diese Relation leicht erbracht. Die Ordnung ist total bzw. linear: für zwei beliebige Zahlen $x, y \in \mathbb{R}$ gilt entweder $x < y$ oder $y \leq x$. Die Ordnung ist Archimedisch: für je zwei positive reelle Zahlen x, y gibt es immer eine natürliche Zahl n so dass $y < n \cdot x$ (es gibt keine "unendlich kleinen" reellen Zahlen genausoweinig, wie es keine unendlich kleinen rationalen Zahlen gibt). Und die Ordnung ist *vollständig*: jede nicht leere, nach unten beschränkte Teilmenge $M \subset \mathbb{R}$ hat ein Infimum in $\mathbb{R}$ (ohne Beweis).

Das Rechnen mit reellen Zahlen wird nun im Rahmen der Mengenlehre auf das bereits bekannte Rechnen mit rationalen Zahlen zurückgeführt. Da ein Schnitt entweder durch die Angabe der Obermenge oder Angabe der Untermenge bereits vollständig charakterisiert ist, lassen sich die Rechenregeln unter Bezug auf eine der beiden Mengen formulieren. Ober- und Untermenge irgendeiner reellen Zahl a notieren wir $\mathcal{O}(a)$ und $\mathcal{U}(a)$. Für die reelle Zahl $x = (\underline{X}, \overline{X})$ also $\mathcal{U}(x) = \underline{X}$, $\mathcal{O}(x) = \overline{X}$. Man beachte, dass es sich bei $\mathcal{O}(\cdot)$ und $\mathcal{U}(\cdot)$ in jedem Fall ausschließlich um Teilmengen der rationalen Zahlen handelt.

Addition: Für zwei Zahlen $x = (\underline{X}, \overline{X})$ und $y = (\underline{Y}, \overline{Y})$ aus $\mathbb{R}$ wird die Summe $x+y$ über die Menge $\mathcal{O}(x+y) := \{a+b \mid a \in \overline{X}, b \in \overline{Y}\}$ definiert. Diese Menge und ihr rationales Komplement genügen den Schnittaxiomen (S1)–(S4), d.h. mit x und y in $\mathbb{R}$ ist auch $x+y$ in $\mathbb{R}$. Kommutativität und Assoziativität der Addition (in $\mathbb{R}$) sind einfache Konsequenzen der Kommutativität und Assoziativität von $+$ in $\mathbb{Q}$.

Subtraktion Die Differenz $x - y$ wird mit Hilfe des Additiv-Inversen von y, bezeichnet $-y$, als Addition rekonstruiert, $x - y := x + (-y)$. Die Obermenge von $-y$ wird dabei aus der Untermenge von y gewonnen, $\mathcal{O}(-y) := \{-r \mid r \in \underline{Y}, r \neq \max(\underline{Y})\}$ (um (S4) zu genügen muss $-\max(\underline{Y})$ ausgeschlossen werden).

Multiplikation wird für positive Zahlen in naheliegender Weise definiert, $\mathcal{O}(x \cdot y) := \{r \cdot s \mid r \in \overline{X}, s \in \overline{Y}\}$. Ist eine der beiden Zahlen negativ, sagen wir $y < 0$, wird das Produkt über Angabe der Untermenge formuliert, $\mathcal{U}(x \cdot y) := \{r \cdot s \mid r \in \overline{X}\,, s \in \underline{Y}\}$.

Division wird auf die Multiplikation mit dem Multiplikativ-Inversen zurückgeführt, $x \div y = x \cdot y^{-1}$. Die Obermenge von y^{-1} wird über die Untermenge von y definiert, $\mathcal{O}(y^{-1}) := \{r^{-1} \mid r \in \underline{Y}\,, r > 0\,, r \neq \max(\underline{Y})\}$, wobei die zusätzliche Bedingung $r > 0$ die Positivität von y^{-1} garantiert.

Mächtigkeit des Kontinuums.

 ©Martin Wilkens