Stichpunkte zu „Zahlen und Zahlbereiche“

Teil der Ringvorlesung

Schulmathematik nach dem ersten Studienjahr wiederentdecken

Karlsruhe, WS 2014/15, PD Dr. Stefan Kühnlein

1. Sitzung

1.1 Test auf Teilbarkeit einer natürlichen Zahl durch 3 bzw. 9 durch Betrachtung ihrer Quersumme; Beweis, dass n bei Division durch 3 bzw. 9 denselben Rest lässt wie die Quersumme von n.

Denn: Beispiel: Die Rechnung

$$\begin{aligned} 1478 &= 1 \cdot 1000 + 4 \cdot 100 + 7 \cdot 10 + 8 \cdot 1 \\ &= 1 \cdot (999 + 1) + 4 \cdot (99 + 1) + 7 \cdot (9 + 1) + 8 \cdot 1 \\ &= (1 \cdot 999 + 4 \cdot 99 + 7 \cdot 9) + 1 + 4 + 7 + 8 \\ &= 9 \cdot (1 \cdot 111 + 4 \cdot 11 + 7 \cdot 11) + \text{Quersumme von } 1478 \end{aligned}$$

zeigt, dass $1478 -$ Quersumme von 1478 durch 9 und damit auch durch 3 teilbar ist, was für dieses Beispiel die Behauptung belegt.

Allgemein geht das ganz ähnlich: Wenn $n = \sum_{i=0}^{k} a_i 10^i$ die Dezimaldarstellung der Zahl n ist, dann ist

$$n = \sum_{i=0}^{k} a_i (10^i - 1 + 1) = \sum_{i=0}^{k} a_i (10^i - 1) + \sum_{i=0}^{k} a_i.$$

Der erste Summand ist durch 9 (und damit auch durch 3) teilbar, der zweite ist die Quersumme.

Dabei nutzen wir aus, dass eine ganze Zahl n genau dann durch eine ganze Zahl d teilbar ist, wenn dies für $n - d$ oder allgemeiner für $n - md$ für ein $m \in \mathbb{Z}$ gilt.

Klar: d teilt n sagt: $\exists a \in \mathbb{Z} : n = ad$, und das impliziert $n + md = (a + m)d$, also teilt d auch $n + md$. Die Rückrichtung geht genauso.

1.2 Test auf Teilbarkeit einer natürlichen Zahl durch 2 oder 5; Beweis, dass n bei Division durch 2 bzw. 5 denselben Rest lässt wie seine Einerstelle.

Das geht ähnlich wie der Beweis in 1.1, nur noch einfacher: Sei $n = \sum_{i=0}^{k} a_i 10^i$. Dann ist a_0 die Einerstelle, und es gilt

$$n - a_0 = \sum_{i=1}^{k} a_i 10^i = 10 \cdot \sum_{i=1}^{k} a_i 10^{i-1},$$

also ist $n - a_0$ durch 10 teilbar und damit

$$n = a_0 + \text{etwas durch 10 teilbares.}$$

Damit unterscheiden sich n und a_0 additiv nur um etwas durch 2 bzw. 5 teilbares, was die behauptete Teilbarkeitsregel nach sich zieht.

1.3 Erinnerung an die Restklassenringe $\mathbb{Z}/d\mathbb{Z}$.

Es ist

$$\mathbb{Z}/d\mathbb{Z} = \{[n] \mid n \in \mathbb{Z}\},$$

wobei $[n] = [m] \Leftrightarrow d$ teilt $n - m$. Die Zahlen m, n liefern also genau dann dieselben Elemente in $\mathbb{Z}/d\mathbb{Z}$, wenn sie bei Division durch d denselben Rest lassen; daher auch der Name *Restklassenring*.

Addition und Multiplikation werden durch

$$[m] + [n] := [m + n], \quad [m] \cdot [n] := [m \cdot n]$$

festgelegt, und es gelten die Axiome für einen kommutativen Ring mit Eins.

Im **Spezialfall** $d = 2$ folgen die bekannten Regeln *gerade mal gerade ist gerade, ungerade mal ungerade ist ungerade* und so fort. Denn es gibt ja genau die beiden Restklassen der geraden und der ungeraden Zahlen.

1.4 Neue Sichtweise auf die Beweise aus 1.1 durch Verwendung der Restklassenringe $\mathbb{Z}/d\mathbb{Z}$, wobei $d \in \{2, 3, 5, 9\}$:

Es ist aufgrund der Rechenregeln in $\mathbb{Z}/d\mathbb{Z}$

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

Im Fall $d = 3$ oder 9 ist $[10] = [1]$ und damit $[n] = [\sum_{i=0}^{k} a_i]$.

Im Fall $d = 2$ oder 5 ist $[10] = [0]$ und damit $[n] = [a_0]$.

1.5 Übertragung auf andere Fälle, Loslösung vom Zehnersystem.

Bei **Division durch 11** lässt $n = \sum_{i=0}^{k} a_i 10^i$ denselben Rest wie seine alternierende Quersumme $\sum_{i=0}^{k} (-1)^i a_i$, denn in $\mathbb{Z}/11\mathbb{Z}$ ist $[10] = [-1]$ und damit

$$[n] = \sum_{i=0}^{k} [a_i][10]^i = [\sum_{i=0}^{k} (-1)^i a_i].$$

Beispiel: 1478 lässt bei Division durch 11 denselben Rest wie

$$8 - 7 + 4 - 1 = 4.$$

Tatsächlich ist

$$1478 - 4 = 1474 = 134 \cdot 11.$$

Alternativ kann man die Teilbarkeit durch 11 auch durch die Quersumme im 100-System testen. Beispielsweise ist hier die Quersumme von $1478 = 14 \cdot 100 + 78$ gerade

$$14 + 78 = 92$$

und lässt bei Division durch 11 natürlich auch Rest 4.

Bei **Division durch 37** lässt n denselben Rest wie seine Quersumme im Tausendersystem, denn $1000 = 27 \cdot 37 + 1$ lässt bei Division durch 37 Rest 1.

Beispiel: $14783 = 14 \cdot 1000 + 783$ hat hier Quersumme

$$14 + 783 = 797 = 777 + 20 = 21 \cdot 37 + 20.$$

Tatsächlich ist

$$14783 - 20 = 14763 = 399 \cdot 37.$$

Analog lässt sich im System zur Basis g die Teilbarkeit durch (einen Teiler von) $g - 1$ stets durch die Quesumme dieser Zahl testen. Denn wenn d dieser Teiler ist und $n = \sum_{i=0}^{k} a_i g^i$, dann ist in $\mathbb{Z}/d\mathbb{Z}$

$$[n] = \sum_{i=0}^{k} [a_i][g]^i = [\sum_{i=0}^{k} a_i],$$

den $[g] = [1]$.

Die Teilbarkeitsregeln spiegeln also in erster Linie unsere Art der Zahldarstellung wider, und keine „absoluten“ Eigenschaften der Zahlen.

1.6 Übertragung auf andere Ringe, insbesondere: Polynomdivision, Abspaltung von Nullstellen.

Nur ganz kurz, mehr dazu gibt es in der Übung: Für eine Zahl c ist $X - c$ im Polynomring ein Teiler von $X^i - c^i$ für alle natürlichen Zahlen i, wie man etwa an den Partialsummen der geometrischen Reihe sieht. Es folgt für eine Polynom

$$f = \sum_{i=0}^{k} a_i X^i = \sum_{i=0}^{k} a_i (X^i - c^i) + \sum_{i=0}^{k} a_i c^i,$$

dass $X - c$ genau dann ein Teiler ist von f, wenn es ein Teiler ist von $f(c) = \sum_{i=0}^{k} a_i c^i$. Da dies letzte eine Zahl ist, kann das nur sein, wenn diese Zahl 0 ist, also: f ist durch $X - c$ teilbar genau dann, wenn $f(c) = 0$.

2. Sitzung

2.1 Dezimaldarstellung: Jede rationale Zahl lässt sich als Dezimalzahl entwickeln. Die Dezimalzahl von $-q$ ist das negative der Dezimalzahl von q, also genügt es, eine Dezimalentwicklung von $q = \frac{z}{n}$ anzugeben, wenn z, n natürliche Zahlen sind. Dazu teilen wir zunächst z durch n mit Rest: $z = a_0 n + r$, $0 \leq r < n$. Wir brauchen noch die Dezimalentwicklung von r/n und wählen dazu zunächst ein $a_1 \in \{0, \ldots, 9\}$ mit

$$a_1 \cdot 10^{-1} \leq \frac{r}{n} < (a_1 + 1) \cdot 10^{-1}.$$

Wenn wir bereits $a_1, \ldots, a_k$ gewählt haben mit

$$\sum_{i=0}^{k} a_i 10^{-i} \leq \frac{r}{n} < \big(\sum_{i=0}^{k} a_i 10^{-i}\big) + 10^{-k},$$

so gibt es ein $a_{k+1} \in \{0, \ldots, 9\}$ derart, dass

$$\sum_{i=0}^{k+1} a_i 10^{-i} \leq \frac{r}{n} < \big(\sum_{i=0}^{k} a_i 10^{-i}\big) + 10^{-k-1},$$

und wir definieren auf diese Art eine Folge (a_i), sodass für alle k gilt:

$$|\frac{r}{n} - \sum_{i=0}^{k+1} a_i 10^{-i}| < 10^{-k}.$$

Die Folge der endlichen Dezimalzahlen konvergiert also gegen $\frac{r}{n}$.

Auf ähnliche Art sieht man, dass jede reelle Zahl eine Dezimalentwicklung zulässt (Intervallschachtelung!).

Beobachtung: Es gibt reelle Zahlen, die nicht rational sind.

Zum Beispiel die Quadratwurzel aus 2 ist nicht rational. Wäre nämlich

$$\sqrt{2} = \frac{z}{n},$$

so dürften wir annehmen, dass nicht sowohl Zähler als auch Nenner gerade sind.

Es gilt aber

$$2n^2 = z^2,$$

was zeigt, dass z^2 gerade ist, und mit dem Spezialfall aus 1.3 folgt, dass z gerade ist. Wir schreiben $z = 2y$ und sehen

$$2n^2 = 4y^2, \quad \text{also} \quad n^2 = 2y^2,$$

was erzwingt, dass n gerade ist. Also sind – entgegen unserer erlaubten Annahme – z und n beide gerade, wenn $\sqrt{2} = \frac{z}{n}$. Dies zeigt, dass $\sqrt{2}$ eben nicht rational sein kann.

Auch die beliebten Zahlen e und π sind irrational.

2.2 Untergruppen von $\mathbb{Z}$ und der größte gemeinsame Teiler.

Für $n \in \mathbb{N}_0$ ist $\mathbb{Z} \cdot n = \{kn \mid k \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$.

Behauptung: Für jede Untergrupe $H \subseteq \mathbb{Z}$ gibt es ein $n \in \mathbb{N}_0$ mit $H = \mathbb{Z} \cdot n$.

Denn: Wenn $H = \{0\}$ gilt, nehme ich $n = 0$. Sei also $H \neq \{0\}$. Dann gibt es in H auch positive Zahlen, und ich wähle n als

$$n := \min H \cap \mathbb{N}.$$

Dann gilt $\mathbb{Z} \cdot n \subseteq H$, da mit n auch $n + n, -n, \ldots$ zu H gehören müssen.

Sei nun $h \in H$. Dann gibt es $k \in \mathbb{Z}$ mit

$$kn \leq h < (k+1)n.$$

Es folgt (subtrahiere überall kn)

$$0 \leq h - kn < n.$$

Da h und kn zu H gehören, tut dies auch $h - kn$. Da n das kleinste positive Element in H ist, muss demnach $h - kn = 0$ gelten.

Das zeigt insgesamt $H = \mathbb{Z} \cdot n$.

Folgerung: Wenn a, b natürliche Zahlen sind, dann sei $H = \{ka + lb \mid k, l \in \mathbb{Z}\}$. Das ist eine Untergruppe von $\mathbb{Z}$, und wegen des vorangegangenen sehen wir, dass es ein $g \in H$ gibt mit $H = \mathbb{Z} \cdot g$.

Da insbesondere a und b zu H gehören, ist g ein gemeinsamer Teiler von a und b.

Wenn d irgendein gemeinsamer Teiler von a und b ist, dann teil d jedes Element von H, also auch g. Daher ist g der größte gemeinsame Teiler von a und b.

Fazit: Der größte gemeinsame Teiler g von a und b lässt sich schreiben als

$$g = ka + lb, \quad k, l \in \mathbb{Z} \text{ geeignet.}$$

Er ist der einzige gemeinsame Teiler mit dieser Eigenschaft.

2.3 Genau die rationalen Zahlen sind die reellen Zahlen mit einer (schließlich) periodischen Dezimaldarstellung.

Denn: Ist x eine reelle Zahl mit schließlich periodischer Dezimaldarstellung, dann gibt es eine Zehnerpotenz 10^n, sodass der Nachkommaanteil von $10^n \cdot x$ rein periodisch ist, und wir nennen seine Periodenlänge l. Also ist

$$10^n \cdot x = k + 0, \overline{a_1 a_2 \dots a_l}.$$

Hierbei ist k eine ganze Zahl; es gilt

$$z := 10^l \cdot 0, \overline{a_1 a_2 \dots a_l} - 0, \overline{a_1 a_2 \dots a_l} \in \mathbb{Z},$$

genauer ist $z = \sum_{i=0}^{l-1} 10^i a_{l-i}$.

Es folgt

$$0, \overline{a_1 a_2 \dots a_l} = \frac{z}{10^l - 1} \in \mathbb{Q}$$

und damit auch

$$x = 10^{-n} \cdot (k + \frac{z}{10^l - 1}) \in \mathbb{Q}.$$

Ist umgekehrt $q = \frac{z}{n}$ eine rationale Zahl mit Zähler $z \in \mathbb{Z}$ und Nenner $n \in \mathbb{N}$, so erweitern wir den Bruch erst einmal derart, dass $n = 10^m \cdot d$ gilt mit $m \in \mathbb{N}_0$ und einer zu 10 teilerfremden Zahl d.

Dann ist q genau dann schließlich periodisch, wenn $q' = z/d$ schließlich periodisch ist, denn Multiplikation mit 10^m liefert nur einen Shift der Dezimaldarstellungen.

Da nun 10 und d teilerfremd sind, gibt es eine natürliche Zahl l, sodass d ein Teiler von $10^l - 1$ ist; siehe 2.4. Wir schreiben $10^l - 1 = dt$ und sehen:

$$(10^l - 1)\frac{z}{d} = dt \cdot \frac{z}{d} = zt$$

ist eine ganze Zahl, also haben $\frac{z}{d}$ und $10^l \frac{z}{d}$ denselben Nachkommaanteil, der damit periodisch sein muss (mit Periodenlänge l).

2.4 Die Periode der Dezimaldarstellung von a/b ist ein Teiler der Ordnung von $[10]$ in der Einheitengruppe des Ringes $\mathbb{Z}/d\mathbb{Z}$, wobei $b = 2^m \cdot 5^n \cdot d$, $m, n \in \mathbb{N}_0$, und d teilerfremd zu 10 ist.

Dabei ist die Ordnung von $[10]$ in der Einheitengruppe das kleinste l, für das $[10]^l = [1]$ gilt. Solch ein l gibt es, da wir nur endlich viele Einheiten haben und daher natürliche Zahlen $l < l'$ existieren mit

$$[10]^l = [10]^{l'}.$$

Da $[10]$ invertierbar ist, folgt

$$[1] = [10]^{l'-l}, \text{ wobei } l' - l \in \mathbb{N}.$$

3. Sitzung

3.1 Was ist eigentlich eine natürliche Zahl?

Diese Frage wird von der Mathematik spätestens seit der *Grundlagenkrise* Ende 19. / Anfang 20. Jahrhundert nicht mehr in dieser naiven Form thematisiert. Erschwerend kommt hinzu, dass vielleicht verschiedene Leute auch verschiedene Vorstellungen von Zahlen haben, und es dadurch schwer wird, allgemein gültige Argumente zu etablieren.

Daher beschränkt sich die Mathematik darauf, Eigenschaften der Menge aller natürlichen Zahlen festzulegen, die mit den Erwartungen aus der elementaren Erfahrungswelt konform sind, sodass jeder ihnen zustimmen kann. Diese Eigenschaften formuliert man daher auch möglichst knapp, um nicht zu viele Wünsche anzumelden (das könnte außerdem zu Inkonsistenzen führen) und um nachher gut kontrollierbare Argumentationsmuster an der Hand zu haben, mit denen sich Aussagen verifizieren lassen. Ausgehend von der Erfahrung, dass sich jede natürliche Zahl um 1 vergrößern lässt und dass jede nichtleere Teilmenge von natürlichen Zahlen ein kleinstes Element hat, wünscht man sich von den natürlichen Zahlen folgendes:

Die Peano-Axiome: Die Natürlichen Zahlen sind eine Menge N, zusammen mit einer injektiven Abbildung $S : N \to N$ und einem Element $e \in N$ sodass

- $S(N) = N \setminus \{e\}$.
- Wenn $T \subseteq N$ eine Teilmenge ist, die e enthält und unter S invariant ist (also $S(T) \subseteq T$), dann gilt bereits $T = N$.

Auf jeden Fall ist so eine Menge nicht leer (denn e soll darin liegen) und sogar unendlich, denn es gibt eine injektive Abbildung von N in eine echte Teilmenge. Das könnte man als Definition der Unendlichkeit einer Menge nehmen, nachdem man ein naives Verständnis für diesen Begriff entwickelt hat.

3.2 Gibt es so etwas in der Welt der Mathematik?

Das ist eine ganz grundsätzliche Frage, für deren positive Beantwortung man an sich etwas tiefer in Logik und Mengenlehre einsteigen müsste, denn hier werden die Weichen gestellt, wie Mengen gebastelt werden dürfen. Wir bleiben hier beim naiven Mengenbegriff.

Eine Möglichkeit, ein Modell für eine Menge zu basteln, die die Peanoaxiome erfüllt, ist das folgende: Eine Menge N, deren Elemente alle selbst schon Mengen sind, heißt *induktiv*, wenn $\emptyset \in N$ und mit $m \in N$ auch $m \cup \{m\} \in N$. Es gehört zum Aufbau der Mengenlehre dazu, die Existenz solch einer Menge zu fordern. Der Durchschnitt aller induktiven Mengen ist dann auch eine Menge, und zwar die kleinste induktive Menge. Man kann nachweisen, dass sie mit $e = \emptyset$ und $S(m) := m \cup \{m\}$ die Anforderungen an die natürlichen Zahlen erfüllt.

Letztlich aber verlagert man dabei die Frage nach der Existenz nur auf eine andere Ebene und ersetzt ehrlich gesagt einen Glaubenssatz durch einen anderen.

3.3 Wie argumentiere ich mit den Peanoaxiomen?

Die Peanoaxiome liefern insbesondere die Möglichkeit an die Hand, rekursiv Vorschriften zu machen.

Wir können etwa einsehen, dass zwei verschiedene Tupel (N, e, S) und (M, f, T), die beide die Peanoaxiome erfüllen, gleich gut sind. Das präzisieren wir durch folgende Überlegung:

Wir definieren eine Abbildung $f : N \to M$ mittels

$$\alpha(e) = f \quad \text{und} \quad \alpha(S(n)) = T(\alpha(n)).$$

Die Menge aller $n \in N$, für die α definiert ist, enthält e und mit n auch $S(n)$, ist also ganz N. Außerdem ist α wohldefiniert, da S injektiv ist.

Analog definieren wir $\beta : M \to N$ durch

$$\beta(f) = e \quad \text{und} \quad \beta(T(m)) = S(\beta(m)).$$

Dann gilt

$$\beta(\alpha(e)) = \beta(f) = e$$

und wenn $\beta(\alpha(n)) = n$ gilt, folgt

$$\beta(\alpha(S(n))) = \beta(T(\alpha(n))) = S(\beta(\alpha(n))) = S(n),$$

also gilt für alle $n \in N : \beta(\alpha(n)) = n$.

Analog gilt für alle $m \in M : \alpha(\beta(m)) = m$.

Daher sind α und β zueinander inverse Bijektionen, die die Strukturen (N, e, S) und (M, f, T) sinnvoll ineinander überführen. Wir wählen eine solche Struktur und nennen die Grundmenge $\mathbb{N}$. Ab jetzt ist $(\mathbb{N}, 1, S)$ eine feste Peanostruktur.

3.4 Definition der Addition

Wir definieren für $n \in \mathbb{N}$ eine Abbildung $(n+) : \mathbb{N} \to \mathbb{N}$ wie folgt:

$$(1+)(x) := S(x)$$

und wenn $(n+)$ schon definiert ist, legen wir $(S(n)+)$ fest durch

$$(S(n)+)(x) := S((n+)x).$$

Da S injektiv ist, ist n eindeutig durch $S(n)$ festgelegt, und die Definition ist legitim.

Wenn M die Menge aller Elemente n von $\mathbb{N}$ ist, für die es die Abbildung $(n+)$ gibt, dann ist $1 \in M$ und $\forall n \in M : S(n) \in M$. Also ist $M = \mathbb{N}$.

Nun schreiben wir kurz $(n+)(x) =: n + x$ und haben dadurch eine Abbildung

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

aus der Wiege gehoben – eine Verknüpfung.

Man kann nun mithilfe der Peanoaxiome nachrechnen, dass diese Verknüpfung kommutativ und assoziativ ist. Wir führen das für das Kommutativgesetz vor.

Dafür zeigen wir, dass die Menge $U := \{n \in \mathbb{N} \mid \forall k \in \mathbb{N} : n + k = k + n\}$ das Element 1 enthält und unter S stabil ist.

$\underline{1 \in U :}$ Die Menge $V := \{k \in \mathbb{N} \mid 1 + k = k + 1\}$ enthält 1, da $1 + 1 = 1 + 1$. Außerdem gilt für $k \in V$:

$$1 + S(k) = S(S(k)) = S(1 + k) = S(k + 1) = S(k) + 1.$$

Hier haben wir im vorletzten Schritt benutzt, dass $k \in V$, und im letzten Schritt die Definition von $S(k) + 1$. Damit liegt mit k auch $S(k)$ in V, und nach den Axiomen ist $V = \mathbb{N}$.

$\underline{n \in U \Rightarrow S(n) \in U :}$ In der Menge $V := \{k \in \mathbb{N} \mid S(n)+k = k+S(n)\}$ liegt wegen der ersten Überlegung sicher 1. Mit $k \in V$ folgt

$$\begin{aligned} S(k) + S(n) &= S(k + S(n)) = S(S(n) + k) \\ &= S(S(n + k)) = S(S(k + n)) \\ &= S(S(k) + n) = S(n + S(k)) \\ &= S(n) + S(k), \end{aligned}$$

wobei wir verschiedentlich $k \in V$ und $n \in U$ benutzt haben.

Das zeigt $S(k) \in V$ und damit $V = \mathbb{N}$ und damit $S(n) \in U$ und damit $U = \mathbb{N}$.

Diese etwas ernüchternde Art der Verifikation zieht sich durch alle Nachweise der Eigenschaften der Addition durch. Diese tut letztlich das, was wir von der Addition erwarten.

3.5 Definition der Multiplikation.

Hat man die Addition an der Hand, kann man für $n \in \mathbb{N}$ eine neue Abbildung $(n\cdot)$ definieren durch

$$(e\cdot)(x) := x, \quad (S(n)\cdot)(x) := ((n\cdot)(x)) + x.$$

Wieder ist das wohldefiniert und legt für jedes $n \in \mathbb{N}$ eine Abbildung $(n\cdot)$ fest. Das liefert eine zweite Verknüpfung

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (n, x) \mapsto n \cdot x := (n\cdot)(x).$$

Diese leistet das, was wir von der Multiplikation erwarten, insbesondere kann man Assoziativität, Kommutativität und das Distributivgesetz nachrechnen.

Hinweis: All diese Verifikationen sind langatmige Routinegeschäfte. Es lohnt sich, sie wenigstens zu überfliegen, etwa in Landaus *Grundlagen der Analysis* oder im Buch *Zahlen* von Ebbinghaus e.a., das ohnehin eine erfreuliche und abwechslungsreiche Lektüre ist.

3.6 Anordnung

Auf $\mathbb{N}$ können wir eine Anordnung definieren durch

$$\forall m, n \in \mathbb{N} : [m < n :\Leftrightarrow \exists k \in \mathbb{N} : m + k = n].$$

Diese erfüllt die Bedingungen

$$\forall m, n, k \in \mathbb{N} : m < n \Leftrightarrow m + k < n + k \Leftrightarrow m \cdot k < n \cdot k.$$

Auch dies kann mittels der Peanoaxiome verifiziert werden.

3.7 Ist das alles?

Nun tut sich die Frage auf, ob man alles über die natürlichen Zahlen mithilfe unserer Axiome beweisen kann. In der Tat ist das nicht so. Der Unvollständigkeitssatz von Gödel sagt, dass für jedes in endlicher Art gegebene System von Logik und Mengenlehre, das reich genug ist, um die Arithmetik von $\mathbb{N}$ in unserem Sinn zu gewinnen, Aussagen existieren, die sich weder beweisen noch widerlegen lassen, wenn alles konsistent ist.

Eine Zeitlang dachte man, die Fermatsche Vermutung sei ein Kandidat hierfür. Seit deren Beweis im Jahr 1994 ist das obsolet;-)

Wir kommen in 4.6 noch einmal auf diesen Sachverhalt zu sprechen, wenn wir die Kontinuumshypothese vorstellen.

4. Sitzung

4.1 Die ganzen Zahlen

In den natürlichen Zahlen $\mathbb{N}$ können wir nun Gleichungen aufstellen, insbesondere solche der Form $b + x = a$, wobei $a, b \in \mathbb{N}$ fest vorgegeben sind und eine Lösung x gesucht wird. Diese finden wir (nach Definition von $<$ aus 3.6) genau dann in $\mathbb{N}$, wenn $b < a$.

Um nun in jedem Fall eine Lösung zu haben – wo auch immer! – wäre es wünschenswert, $\mathbb{N}$ als Teilmenge einer kommutativen Gruppe $(A, +)$ zu finden, wobei die Addition in A für alle natürlichen Zahlen in A dasselbe liefern soll wie die Addition aus $\mathbb{N}$. Wenn ich so eine Gruppe hätte, dann wäre natürlich $a - b$ (gerechnet in A) eine Lösung unserer obigen Gleichung – und zwar die einzige in A.

Nehmen wir also kurzfristig an, wir hätte eine solche Gruppe $(A, +)$. Dann liegt darin die Teilmenge

$$U := \{a - b \mid a, b \in \mathbb{N}\},$$

und man rechnet leicht nach, dass U eine Untergruppe von A ist, die immer noch $\mathbb{N}$ enthält. Und natürlich gilt

$$a - b = c - d \Leftrightarrow b + c = d + a,$$

denn wir sind in der Gruppe A und können links vom Äquivalenzpfeil auf beiden Seiten $b + d$ addieren.

Die rechte Seite hier ist jedoch allein aufgrund der Arithmetik in $\mathbb{N}$, die wir schon zur Verfügung haben, erklärt, und wir können die Menge U durch ein künstliches Konstrukt ersetzen. Dazu setzen wir

$$Z := \{(a, b) \mid a, b \in \mathbb{N}\}/\sim,$$

als Menge von Äquivalenzklassen in $\mathbb{N}^2$ bezüglich der Relation

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

Das ist der Ausgangspunkt der Aufgabe 2 auf Übungsblatt 3: Man kann auf Z vermöge $[(a,b)]_\sim + [(c,d)]_\sim := [(a+c, b+d)]_\sim$ die Struktur einer kommutativen Gruppe einführen, findet $\mathbb{N}$ mittels der injektiven Abbildung $n \mapsto [(n+1,1)]_\sim$ als Teilmenge in Z wieder, und die Addition auf dieser Teilmenge ist die alte Addition auf $\mathbb{N}$. Das Nullelement (neutrales Element der Addition) ist die Klasse von $(1,1)$. Wir notieren es als 0.

Wir nennen die so erhaltene Gruppe $\mathbb{Z}$ und finden darauf sogar eine Ringstruktur mittels

$$[(a,b)]_\sim \cdot [(c,d)]_\sim := [(ac+bd, ad+bc)]_\sim.$$

Das Einselement ist die Klasse von $(1+1,1)$, wir schreiben dafür wieder kurz 1.

4.2 Nun haben wir den Ring $\mathbb{Z}$ und können sofort wieder Gleichungen hinschreiben, die sich nicht lösen lassen: $3x = 5$ hat keine Lösung $x \in \mathbb{Z}$.

Um dieses Defizit beheben zu können wäre es nett, $\mathbb{Z}$ als Teilmenge in einem Körper K zu entdecken, dessen Addition und Multiplikation die auf $\mathbb{Z}$ fortsetzt. Dann könnten wir die Gleichung $ax + b = c$ mit $a, b, c \in \mathbb{Z}$, $a \neq 0$ immer durch $x = a^{-1}(c-b) \in K$ lösen. Was diese Lösung für die wie auch immer motivierte Gleichung bedeutet, wie sie im jeweiligen Kontext zu interpretieren ist, ist dadurch natürlich nicht allgemeingültig zu sagen.

Das ist ein allgemeines Vorgehen, das sich in vielen mathematischen Situationen wiederfindet: Man verschafft sich erst einen allgemeinen Rahmen, in dem sich eine Klasse von Problemen lösen lässt, und muss dann von Fall zu Fall entscheiden, ob die Lösung sich geeignet interpretieren lässt. Diese allgemeineren Konzepte entwickeln dann eine Eigendynamik und werden nach und nach als legitime Familienmitglieder mit eigener Existenzberechtigung akzeptiert.

Wie in 4.1 nehmen wir nun an, wir hätten so einen Körper K, um einen Ansatz für eine Konstruktion zu entwickeln. In K fände sich dann auch die Teilmenge

$$L := \{zn^{-1} \mid z \in \mathbb{Z}, n \in \mathbb{N}\},$$

und man rechnet leicht nach, dass dies ein Teilkörper von K ist. Vielleicht ist es gut, sich die Abgeschlossenheit bezüglich der Addition zu überlegen:

$$z \cdot n^{-1} + y \cdot m^{-1} = zm(nm)^{-1} + yn(nm)^{-1} = (zm+yn)(nm)^{-1}.$$

Dabei haben wir beim zweiten Gleichheitszeichen ausgenutzt, dass in K das Distributivgesetz gilt, und beim ersten Gleichheitszeichen haben wir uns in die Position gebracht, das ausnutzen zu können (nämlich durch Erweitern).

Analog zu 4.1 überlegt man sich auch hier, dass

$$zn^{-1} = ym^{-1} \Leftrightarrow mz = ny.$$

Da rechter Hand wieder nur die Arithmetik in $\mathbb{Z}$ benutzt wird, kann man sich einen Ersatz für L basteln, ohne <u>vorauszusetzen</u>, dass ein Körper K, wie wir ihn gewünscht hatten, existiert.

4.3 Die Konstruktion von $\mathbb{Q}$.

Wir definieren die Menge Q als die Menge der Äquivalenzklassen in $\mathbb{Z}\times\mathbb{N}$ bezüglich der Äquivalenzrelation

$$(z,n) \sim (y,m) \Leftrightarrow mz = ny.$$

Die Äquivalenzklasse von (z,n) schreiben wir suggestiv als $\frac{z}{n}$.

Wir definieren jetzt Addition und Multiplikation solcher Elemente mittels der folgenden Formeln, die sich aus der Situation in 4.2 motivieren lassen:

$$\frac{z}{n} + \frac{y}{m} = \frac{mz+yn}{mn}, \quad \frac{z}{n} \cdot \frac{y}{m} = \frac{zy}{mn}.$$

Man muss jetzt nachweisen, dass dies jeweils wohldefiniert ist und diese Verknüpfungen auf Q die Struktur eines Körpers festlegen. Wir machen exemplarisch die Wohldefiniertheit und die Assoziativität von $+$:

Wohldefiniertheit: Wenn $\frac{z}{n} = \frac{\tilde{z}}{\tilde{n}}$ und $\frac{y}{m} = \frac{\tilde{y}}{\tilde{m}}$, dann gelten die folgenden Äquivalenzen:

$$\begin{aligned} & \tfrac{zm+yn}{mn} && = \tfrac{\tilde{z}\tilde{m}+\tilde{y}\tilde{n}}{\tilde{m}\tilde{n}} \\ \Leftrightarrow \quad & \tilde{m}\tilde{n}\cdot(zm+yn) && = mn\cdot(\tilde{z}\tilde{m}+\tilde{y}\tilde{n}) \\ \Leftrightarrow \quad & m\tilde{m}z\tilde{n}+n\tilde{n}y\tilde{m} && = m\tilde{m}\tilde{z}n+n\tilde{n}\tilde{y}m \end{aligned}$$

In der letzten Gleichung stimmen jeweils der erste Summand links mit dem ersten Summanden rechts und der zweite Summand links mit dem zweiten Summanden rechts überein, da wir $z\tilde{n} = \tilde{z}n$ und $y\tilde{m} = \tilde{y}m$ vorausgesetzt haben. Folglich stimmt auch die erste Gleichung, was die Wohldefiniertheit von $+$ zeigt.

Assoziativität: Wenn $\frac{z}{n}, \frac{y}{m}, \frac{x}{k} \in Q$ drei Elemente sind, dann ist

$$(\frac{z}{n}+\frac{y}{m})+\frac{x}{k} = \frac{zm+yn}{mn}+\frac{x}{k} = \frac{zkm+ykn+xmn}{mnk} = \frac{z}{n}+\frac{yk+xm}{km} = \frac{z}{n}+(\frac{y}{m}+\frac{x}{k})$$

wie insgeheim erhofft.

Auf diese Weise rechnet man alle Regeln nach, die die Verknüpfungen auf einem Körper zu erfüllen haben, und sieht, dass $(Q,+,\cdot)$ ein Körper ist. Wir bezeichnen ihn in Zukunft mit $\mathbb{Q}$.

Der injektive Ringhomomorphismus

$$\mathbb{Z} \ni z \mapsto \frac{z}{1} \in \mathbb{Q}$$

lässt es zu, $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ aufzufassen.

4.4 Reelle Zahlen

Auch hier wollen wir nur skizzieren, wie man argumentiert. Wir haben auf $\mathbb{Q}$ eine Anordnung mithilfe der Vorschrift

$$\frac{z}{n} < \frac{y}{k} \Leftrightarrow yn - zk \in \mathbb{N}.$$

Diese benutzen wir, um eine Betragsfunktion einzuführen:

$$|q| = \begin{cases} q, & \text{falls } q > 0, \\ 0, & \text{falls } q = 0, \\ -q, & \text{falls } 0 > q. \end{cases}$$

Nun sagen wir, dass eine Folge (q_i) rationaler Zahlen gegen eine rationale Zahl r konvergiert, wenn

$$\forall k \in \mathbb{N} : \exists N \in \mathbb{N} : \forall i \geq N : |q_i - r| < \frac{1}{k}.$$

Dies impliziert (wenn wir k durch $2k$ ersetzen), dass

$$\forall k \in \mathbb{N} : \exists N \in \mathbb{N} : \forall i, j \geq N : |q_i - q_j| < \frac{1}{k}.$$

Durch diese Bedingung wird definiert, wann eine Folge Cauchy-Folge (oder auch Fundamentalfolge) genannt wird.

Offensichtlich konvergiert nicht jede Fundamentalfolge in $\mathbb{Q}$ gegen eine rationale Zahl, da sonst etwa $\sqrt{2}$ rational wäre.

Wenn man wirklich daran interessiert ist, die Konvergenz aller Cauchy-Folgen sicher zu stellen, dann sollte man einen Körper suchen, der $\mathbb{Q}$ umfasst, angeordnet ist (wobei die Anordnung die von $\mathbb{Q}$ fortsetzen soll) und vollständig bezüglich dieser Anordnung.

Wenn es so einen Körper K gibt, dann liegt darin auch die Menge L aller Grenzwerte rationaler Cauchy-Folgen. Diese ist wieder – wie man nachrechnet – ein Körper, und wir haben eine surjektive Abbildung

$$\lambda : \mathcal{C} \to L, (q_i) \mapsto \lim_{i \to \infty} q_i \in L.$$

Dabei ist $\mathcal{C}$ der Ring der rationalen Cauchy-Folgen. Die Abbildung λ ist ein Ringhomomorphismus (das Argument kennen Sie aus der Analysis-I-Vorlesung) und der Homomorphiesatz sagt uns, dass

$$L \equiv \mathcal{C}/\mathrm{Kern}(\lambda).$$

Es ist aber klar, dass $\mathrm{Kern}(\lambda) =: \mathcal{N}$ die Menge der Nullfolgen in $\mathcal{C}$ ist, und die können wir wieder ohne Kenntnis von L definieren.

Wir benutzen das, um zu definieren, dass

$$\mathbb{R} := \mathcal{C}/\mathcal{N},$$

und man kann (mit etwas Geduld) nachrechnen, dass sich Multiplikation und Addition von Cauchy-Folgen benutzen lassen, um auf $\mathbb{R}$ Verknüpfungen festzulegen, die ihn zu einem Körper machen. Tatsächlich lässt sich dieser Körper wieder anordnen und enthält $\mathbb{Q}$ durch den injektiven Ringhomomorphismus

$$\mathbb{Q} \ni q \mapsto [(q, q, q, q, q, \dots)] \in \mathbb{R}.$$

Und $\mathbb{R}$ ist auch vollständig (was nachzuweisen etwas technisch ist).

Die Dezimalentwicklung einer reellen Zahl im Sinne unserer zweiten Sitzung ist eine spezielle Cauchy-Folge, die unsere reelle Zahl vertritt. Es muss aber nicht die beste Darstellung einer reellen Zahl sein.

4.5 Cantors Diagonalverfahren

Die Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ haben alle gleich viele Elemente in dem Sinn, dass es zwischen je zweien von ihnen eine bijektive Abbildung gibt.

Eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{Z}$ etwa kann man angeben, indem man die ganzen Zahlen in eine Reihe bringt:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}.$$

Eine Bijektion wäre also zum Beispiel die Abbildung

$$\mathbb{N} \ni n \mapsto \begin{cases} -\frac{n-1}{2}, & \text{falls } n \text{ ungerade,} \\ \frac{n}{2}, & \text{falls } n \text{ gerade.} \end{cases}$$

Es war eine grundlegende Neuerkenntnis im Rahmen der Entwicklung der Mengenlehre gegen Ende des 19. Jahrhunderts durch Georg Cantor, dass es Mengen gibt, die eine größere Elementzahl haben als $\mathbb{N}$ in dem Sinn, dass es keine surjektive Abbildung von $\mathbb{N}$ dorthin gibt. Ein Beispiel für solch eine Menge ist etwa das Einheitsintervall $I = [0, 1] \subset \mathbb{R}$.

Wenn nämlich $f : \mathbb{N} \to I$ eine Abbildung ist, dann schreiben wir $f(n)$ in seiner Dezimalbruchentwicklung, die nicht auf Periode 9 enden soll (sonst ersetzen wir sie durch eine andere, die auf Periode 0 endet):

$$f(n) = 0, a_{n,1}a_{n,2}a_{n,3}\dots$$

Nun definieren wir eine Zahl

$$\beta := 0, b_1b_2b_3\dots$$

durch ihre Dezimalentwicklung, wobei

$$b_i = \begin{cases} 1, & \text{falls } a_{ii} \neq 1, \\ 0, & \text{falls } a_{ii} = 1. \end{cases}$$

Dann hat β eine andere Dezimalentwicklung als jede der Zahlen $f(i)$, da die i-te Dezimalstelle eine andere ist. Da wir im Vorfeld Zweideutigkeiten bei der Dezimalentwickung ausgeräumt hatten (die Sache mit Periode 9), gilt also $b \neq f(i)$ für alle i, und damit ist f nicht surjektiv, da ja b nicht im Bild liegt.

4.6* Die Kontinuumshypothese (Nicht in der Vorlesung gemacht, nicht klausurrelevant)

Man kann sich nun fragen, inwieweit es in $\mathbb{R}$ unendliche Teilmengen gibt, die weder eine Bijektion mit $\mathbb{R}$ noch eine mit $\mathbb{N}$ zulassen. Diese Frage – oder vielmehr eine hypothetische Antwort darauf – ist Gegenstand der Kontinuumshypothese. Sie sagt in ihrer ursprünglichen Form, dass es keine solche Menge gibt.

Seit den Arbeiten von Paul Cohen in den 1960er Jahren weiß man, dass die Antwort auf diese Frage sich nicht aus den üblichen Axiomen der Mengenlehre ergibt, und sogar, dass beide Optionen sich diesen Axiomen hinzufügen lassen, ohne einen Widerspruch zu erzeugen.

In diesem Sinne hat man ein erstes Beispiel für Gödels Unvollständigkeitssatz, den wir in 3.7 kurz erwähnt hatten.