KAPITEL 5

Zahlbereiche und Grundlagen der Algebra

Dieser Text dient zur Unterstützung der Studierenden bei der Navigation durch die Teile der Kapitel 5 und 6 des Buches "Einführung in das Mathematische Arbeiten" von Schichl und Steinbauer, die in der Vorlesung "Einführung in der Mathematik" im WS 2016/17 von A. Čap und G. Hörmann behandelt werden. Es wird meist auf das Buch verwiesen, das hier als [**EMA**] zitiert wird, in einigen Teilen ist der Text auch eigenständig.

Grundsätzlich ist die Algebra das Teilgebiet der Mathematik, das die Eigenschaften von "Rechenoperationen" (in einem sehr breiten Sinn) studiert. Im Buch [**EMA**] werden erst die grundlegenden Begriffe der Algebra in Kapitel 5 entwickelt, dann werden in Kapitel 6 die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ besprochen. Dabei wird einerseits auf aus der Schule bekannte Eigenschaften verwiesen, andererseits werden die mengentheoretischen Konstruktionen (Großteils als Erweiterungsstoff) diskutiert. Im Fall der reellen und komplexen Zahlen wird in dem Kapitel die Basis für eine exakte Behandlung gelegt, die in der Schule üblicherweise nicht besprochen wird.

Im Bachelorstudium für das Unterrichtsfach "Mathematik" wird die exakte Behandlung der reellen und komplexen Zahlen erst in der Vorlesung über Analysis besprochen, sie gehört daher nicht mehr zum Stoff der "Einführung in die Mathematik". Wir werden über reelle Zahlen nur in Form eines Ausblicks über das Schulwissen hinausgehen. Daher haben wir uns entschlossen, den Aufbau der Vorlesung anders zu gestalten als im Buch [**EMA**] und die exaktere Besprechung der Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ in die Besprechung der algebraischen Grundbegriffe zu integrieren.

5.1. Motivation und Gruppen

Folgt (mit kleinen Auslassungen) den Abschnitten 5.1 und 5.2 von [**EMA**].

5.2. Natürliche und ganze Zahlen

Wie schon besprochen sind wir mit den natürlichen und ganzen Zahlen und den üblichen Operationen der Addition und Multiplikation auf diesen Zahlbereichen von Kindheit an vertraut. Wir kennen auch die schönen Eigenschaften dieser Operationen und "wissen" daher, dass die Addition auf beiden Bereichen assoziativ und kommutativ ist und ein neutrales Element 0 besitzt. Im Fall der ganzen Zahlen ist $(\mathbb{Z}, +)$ sogar eine kommutative Gruppe.

Beim Lesen des Abschnittes über sehr große natürliche Zahlen in der Einleitung von Kapitel 6 von [**EMA**] könnten aber doch Zweifel aufkommen, wie vertraut man mit den Rechenoperationen auf $\mathbb{N}$ tatsächlich ist. Das führt dann direkt zur Frage, "was die natürlichen Zahlen eigentlich sind" und wie man Aussagen über die Rechenoperationen auf $\mathbb{N}$ beweisen kann.

Die mathematisch exakte Behandlung der natürlichen Zahlen beginnt (wie es uns vertraut ist) mit der Idee des *Zählens* daraus wird dann erst die Idee des Rechnens abgeleitet. Formal wird die Idee des Zählens in den Peano–Axiomen formuliert wie in

6.1.1 von [**EMA**] besprochen. Man muss an einer Stelle mit dem Zählen beginnen (und hier ist es wesentlich handlicher bei 0 als bei 1 zu beginnen) und dann wissen "welche Zahl als nächste kommt", was durch die Nachfolgerfunktion S beschrieben wird. Die Axiome (PA3) und (PA4) sind aus der Idee des Zählens ziemlich offensichtliche Forderungen, das Herzstück der Peano Axiome ist das Induktionsprinzip in (PA5). In 6.1.1 von [**EMA**] wird bemerkt, dass diese 5 Axiome die Menge $\mathbb{N}$ und die Nachfolgerfunktion S eindeutig festlegen. Die mengentheoretische Konstruktion selbst ist nicht sehr erhellend, also werden wir sie hier nicht weiter besprechen, sie findet sich im Abschnitt 6.1.1 (Erweiterungsstoff) von [**EMA**].

Um vom Zählen zum Rechnen zu kommen, muss man nur zwei Ideen benutzten. Einerseits soll die Addition von 0 jede Zahl gleich lassen. Andererseits soll $S(n) = n+1$ sein, womit insbesondere $1 = S(0)$ gelten muss. Die erste Eigenschaft kann man direkt als $m + 0 = m$ für alle $m \in \mathbb{N}$ schreiben. Soll die Addition assoziativ sein, dann muss zusätzlich natürlich $m + (n + 1) = (m + n) + 1$ und damit $m + S(n) = S(m + n)$ gelten. Nun kann man aber zeigen, dass diese beiden Eigenschaften die Addition schon eindeutig festlegen und als *rekursive* Definition für die Addition verwendet werden können:

THEOREM A 1. *(1) Es gibt eine eindeutig bestimmte Funktion* $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*, sodass für alle* $m, n \in \mathbb{N}$ *die folgenden beiden Eigenschaften erfüllt sind:*

$$\begin{cases} m + 0 = m \\ m + S(n) = S(m + n) \end{cases}.$$

(2) Die Operation $+$ *aus Teil (1) ist assoziativ und kommutativ und* 0 *ist ein neutrales Element für* $+$*.*

BEWEISSKIZZE. (1) Die Eindeutigkeit der Operation ist leicht zu beweisen. Angenommen, wir haben zwei Operationen $+$ und $\oplus$ auf $\mathbb{N}$, die die entsprechenden Eigenschaften haben. Dann definiert man $M := \{n \in \mathbb{N} : \forall m \in \mathbb{N} : m + n = m \oplus n\} \subset \mathbb{N}$. Dann gilt nach Voraussetzung $m + 0 = m$ und $m \oplus 0 = m$, also $0 \in M$. Sei nun $n \in M$ und $m \in \mathbb{N}$ eine beliebige Zahl. Dann gilt nach Voraussetzung $m + S(n) = S(m + n)$ und $m \oplus S(n) = S(m \oplus n)$. Da $n \in M$ gilt, ist $m + n = m \oplus n$, also folgt $m + S(n) = m \oplus S(n)$ und somit $S(n) \in M$. Nach (PA5) folgt $M = \mathbb{N}$ und damit $m + n = m \oplus n$ für alle $m, n \in \mathbb{N}$.

Die (ziemlich einsichtig erscheinende) Tatsache, dass man durch die beiden Bedingungen tatsächlich eine Funktion $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definieren kann, erfordert etwas mehr mengentheoretische Arbeit. Wir werden uns damit nicht genauer beschäftigen.

(2) Das ist eine Folge von nicht besonders schwierigen, aber mühsamen Induktionsbeweisen. Als einfaches Beispiel zeigen wir, dass für alle $n \in \mathbb{N}$ die Gleichung $0 + n = n$ gilt, was zusammen mit der ersten Eigenschaft in (1) zeigt, dass 0 ein neutrales Element für die Addition ist. Dazu sei $M := \{n \in \mathbb{N} : 0 + n = n\}$. Nun gilt aber nach Definition (wegen der "rechten" Null) $0 + 0 = 0$, also $0 \in M$. Ist $n \in M$, dann betrachten wir $0 + S(n)$. Nach Definition ist das $S(0 + n)$ und, weil $n \in M$ gilt, ist $S(0 + n) = S(n)$. Damit haben wir aber $0 + S(n) = S(n)$ und somit $S(n) \in M$ gezeigt. Damit folgt $M = \mathbb{N}$ aus (PA5) und somit die Behauptung. Ähnlich (nur etwas mühsamer) verifiziert man dann, dass $+$ kommutativ und assoziativ ist, für Interessierte findet sich das in Proposition 6.1.15 im Erweiterungsstoff von [**EMA**]. □

Eine wichtige Eigenschaft der Addition, die nicht aus den bisher verifizierten Eigenschaften folgt, ist die sogenannte *Kürzungsregel*:

LEMMA A 2. *Seien* $m, n, k \in \mathbb{N}$*, sodass* $m + k = n + k$ *gilt. Dann ist* $m = n$*.*

BEWEIS. Sei $M := \{k \in \mathbb{N} : \forall m, n \in \mathbb{N} : m+k = n+k \implies m = n\} \subset \mathbb{N}$. Für $k = 0$ gilt natürlich $m + 0 = m$ und $n + 0 = n$, also folgt aus $m + 0 = n + 0$ sofort $m = n$ und damit $0 \in M$. Sei andererseits $k \in M$ und sind $m, n \in \mathbb{N}$ so, dass $m + S(k) = n + S(k)$ gilt. Dann ist nach Definition $m + S(k) = S(m + k)$ und $n + S(k) = S(n + k)$, also folgt $S(m + k) = S(n + k)$. Aber nach (PA4) impliziert das $m + k = n + k$, was wegen $k \in M$ wiederum $m = n$ impliziert. Damit gilt $S(k) \in M$, also $M = \mathbb{N}$ nach (PA5). □

Wir sind mit diesen einfachen algebraischen Operationen so gut vertraut, dass uns solche Resultate vollkommen selbstverständlich erscheinen. Um zu sehen, dass sie nicht so selbstverständlich sind, muss man nur beachten, dass sie für die Multiplikation auf den Zahlbereichen *nicht* erfüllt ist. Selbst in $\mathbb{R}$ folgt aus $ac = bc$ nur dann $a = b$, wenn $c \neq 0$ ist.

Hat man die Addition auf $\mathbb{N}$ definiert, dann kann man auch die "übliche" Ordnungsrelation $\leq$ auf $\mathbb{N}$ leicht definieren:

DEFINITION A 3. Definiere eine Relation $\leq$ für $m, n \in \mathbb{N}$ durch

$$m \leq n \iff \exists a \in \mathbb{N} : m + a = n.$$

PROPOSITION A 4. *Die Relation $\leq$ definiert eine Totalordnung auf $\mathbb{N}$, die mit der Addition in dem Sinne verträglich ist, dass für $m, n, k \in \mathbb{N}$ aus $m \leq n$ immer $m + k \leq n + k$ folgt.*

BEWEIS. Wir zeigen zunächst, dass $\leq$ eine Ordnungsrelation im Sinne von Definition 4.2.24 von [**EMA**] ist. Für jedes $n \in \mathbb{N}$ ist $n = n + 0$, also $n \leq n$, also ist die Relation $\leq$ reflexiv. Ist $m \leq n$ und $n \leq p$, dann gibt es Elemente $a, b \in \mathbb{N}$, sodass $m + a = n$ und $n + b = p$ gelten. Dann ist aber $a + b \in \mathbb{N}$ und $m + (a + b) = (m + a) + b = n + b = p$, also $m \leq p$. Damit ist die Relation $\leq$ transitiv.

Überraschenderweise ist die Antisymmetrie der Relation $\leq$ etwas schwieriger zu beweisen. Wenn $m \leq n$ und $n \leq m$ gelten, dann gibt es nach Definition Elemente $a, b \in \mathbb{N}$ sodass $m + a = n$ und $n + b = m$ gelten. Dann ist aber $m + (a + b) = m = m + 0$ und nach der Kürzungsregel folgt $a + b = 0$. (An dieser Stelle ist für die uns bekannten natürlichen Zahlen klar, dass das nur für $a = b = 0$ gelten kann, aber wir müssen das erst formal beweisen.) Dazu bemerken wir zunächst, dass es kein Element $c \in \mathbb{N}$ geben kann, sodass $b = S(c)$ ist. Wäre das nämlich der Fall, dann wäre $0 = a+b = a+S(c) = S(a+c)$, ein Widerspruch zu (PA3). Betrachten wir aber nun

$$M := \{0\} \cup \{n \in \mathbb{N} : \exists m \in \mathbb{N} : n = S(m)\} \subset \mathbb{N}.$$

Dann gilt natürlich $0 \in M$ und für $n \in M$ liegt $S(n)$ auf jeden Fall in M. Damit ist aber $M = \mathbb{N}$, also ist 0 das einzige Element von $\mathbb{N}$, das nicht als $S(m)$ für ein $m \in \mathbb{N}$ geschrieben werden kann. Damit folgt tatsächlich $b = 0$ und damit schon $m = n+b = n$.

Um zu zeigen, dass $\leq$ eine Totalordnung ist, fixieren wir ein beliebiges Element $m \in \mathbb{N}$ und setzten $M := \{n \in \mathbb{N} : m \leq n\} \cup \{n \in \mathbb{N} : n \leq m\}$. Wegen $m = 0 + m$ ist $0 \leq m$, also $0 \in M$. Ist $n \in M$, dann gilt entweder $m \leq n$, oder $n \leq m$. Im ersten Fall gibt es nach Definition ein Element $a \in \mathbb{N}$, sodass $n = m + a$ ist. Dann ist aber $S(n) = S(m + a) = m + S(a)$. Damit ist $m \leq S(n)$, also $S(n) \in M$. Im zweiten Fall gibt es ein Element $a \in \mathbb{N}$ sodass $n + a = m$ gilt. Ist $a = 0$, dann ist $n = m$, also $S(n) = m + 1$, also $m \leq S(n)$. Ist $a \neq 0$, dann wissen wir aus dem letzten Beweisschritt, dass es ein Element $b \in \mathbb{N}$ mit $a = S(b)$ gibt. Dann ist aber $m = n + a = n + S(b) = S(n + b) = S(n) + b$, also $S(n) \leq m$. In beiden Fällen ist $S(n) \in M$, also folgt wieder $M = \mathbb{N}$ und damit die Behauptung aus (PA5).

Die Verträglichkeit mit der Addition ist einfach zu beweisen: Ist $m \leq n$, dann gibt es ein Element $a \in \mathbb{N}$ mit $m + a = n$. Damit ist aber $(m + k) + a = (m + a) + k = n + k$, also $m + k \leq n + k$. □

Man kann die Ordnungsrelation auf $\mathbb{N}$ benutzen um eine Umformulierung des Induktionsprinzips anzugeben, die in vielen Anwendungen sehr nützlich ist. Diese Eigenschaft wird als *Wohlordnungseigenschaft* bezeichnet und sagt, dass jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes Element besitzt.

THEOREM A 5. *Sei $A \subset \mathbb{N}$ eine nichtleere Teilmenge. Dann gibt es ein Element $n_0 \in A$ sodass $\forall m \in A : n_0 \leq m$.*

BEWEIS. Sei $A \subset \mathbb{N}$ eine Teilmenge, die kein kleinstes Element besitzt und sei $M := \{n \in \mathbb{N} : \forall k \leq n : k \notin A\}$. Dann gilt natürlich $0 \notin A$ (sonst wäre es offensichtlich das kleinste Element), also $0 \in M$. Nehmen wir nun an, dass $n \in M$ gilt und betrachten $S(n)$. Ist $k < S(n)$, dann gibt es eine Zahl $a > 0$ sodass $k + a = S(n)$ ist, und aus dem Beweis von Proposition A 4 wissen wir, dass $a = S(b)$ für ein $b \in \mathbb{N}$ gilt. Dann ist aber $S(n) = k + S(b) = S(k + b)$, also $n = k + b$ nach (PA4). Damit ist $k \leq n$, also $k \notin A$ nach Voraussetzung. Damit kann aber auch $S(n)$ nicht in A liegen, weil es sonst das kleinste Element wäre. Also gilt $S(n) \in M$, also $M = \mathbb{N}$ nach (PA5). Da $n \leq n$ für alle $n \in \mathbb{N}$ gilt, folgt insbesondere $n \notin A$ für alle $n \in \mathbb{N}$, also $A = \emptyset$. □

Der Übergang zu $\mathbb{Z}$. Im Beweis von Proposition A 4 haben wir explizit gesehen, dass $(\mathbb{N}, +)$ sehr weit entfernt davon ist, eine Gruppe zu sein. Wir haben nämlich gezeigt, dass $m + n = 0$ nur für $m = n = 0$ möglich ist. Trotzdem kann man versuchen, zu den Elementen von $\mathbb{N}$ additiv inverse Elemente für alle $n \neq 0$ hinzuzufügen. Dabei erweist es sich als einfacher, mit Paaren von natürlichen Zahlen zu arbeiten, wobei das Paar (m, n) die ganze Zahl $m - n$ repräsentieren soll. Da viele Wahlen von Paaren die gleiche Differenz liefern, muss man die jeweiligen Paare für äquivalent erklären.

DEFINITION A 6. Wir definieren eine Relation auf der Menge $\mathbb{N} \times \mathbb{N}$ aller geordneten Paare von natürlichen Zahlen durch

$$(m_1, n_1) \sim (m_2, n_2) : \Longleftrightarrow \; m_1 + n_2 = m_2 + n_1.$$

LEMMA A 7. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

BEWEIS. Die Reflexivität und Symmetrie der Relation sind offensichtlich. Nehmen wir also an, dass $(m_1, n_1) \sim (m_2, n_2)$ und $(m_2, n_2) \sim (m_3, n_3)$. Dann gilt $m_1 + n_2 = m_2 + n_1$ und $m_2 + n_3 = m_3 + n_2$. Addiert man diese beiden Gleichungen, dann erhält man (nach Umordnen der Summen) $m_1 + n_3 + (m_2 + n_2) = m_3 + n_1 + (m_2 + n_2)$. Nach der Kürzungsregel aus Lemma A 2 folgt $m_1 + n_3 = m_3 + n_1$, also $(m_1, n_1) \sim (m_3, n_3)$ und damit die Transitivität. □

Damit können wir nun $\mathbb{Z}$ als die Mengen aller Äquivalenzklassen definieren, also $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$ setzen. Wir schreiben $[(m, n)]$ für die Äquivalenzklasse von (m, n). Nun können wir versuchen eine Addition auf $\mathbb{Z}$ zu definieren, die wir vorerst mit $\oplus$ bezeichnen um sie von der Addition in $\mathbb{N}$ zu unterscheiden. Betrachtet man die obige Motivation, dann sollte man $[(m, n)] \oplus [(k, \ell)]$ als $[(m + k, n + \ell)]$ definieren. Hier tritt das übliche Problem auf, dass man überprüfen muss, das diese Abbildung wohldefiniert ist.

THEOREM A 8. *(1) Die Vorschrift*

$$[(m, n)] \oplus [(k, \ell)] := [(m + k, n + \ell)]$$

liefert eine wohldefinierte Operation $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*, sodass* $(\mathbb{Z}, \oplus)$ *eine kommutative Gruppe ist.*

(2) Die Abbildung $f : \mathbb{N} \to \mathbb{Z}$*, die durch* $f(n) := [(n, 0)]$ *definiert ist, ist injektiv und erfüllt* $f(n + m) = f(n) \oplus f(m)$ *für alle* $n, m \in \mathbb{N}$*.*

Beweis. (1) Für die Wohldefiniertheit müssen wir zeigen, dass aus $(m_1, n_1) \sim (m_2, n_2)$ und $(k_1, \ell_1) \sim (k_2, \ell_2)$ immer $(m_1 + k_1, n_1 + \ell_1) \sim (m_2 + k_2, n_2 + \ell_2)$ folgt. Die Voraussetzung sagt aber $m_1 + n_2 = m_2 + n_1$ und $k_1 + \ell_2 = k_2 + \ell_1$. Addiert man diese Gleichungen, dann folgt (nach Umordnen) $(m_1 + k_1) + (n_2 + \ell_2) = (m_2 + k_2) + (n_1 + \ell_1)$ und damit die Behauptung.

Die Eigenschaften von $\oplus$ sind nun leicht zu verifizieren: Offensichtlich ist $[(0, 0)]$ ein neutrales Element für $\oplus$. Außerdem gilt nach Definition

$$[(m, n)] \oplus [(n, m)] = [(m + n, m + n)].$$

Nach Definition von $\sim$ ist aber $(m+n, m+n) \sim (0, 0)$, also besitzt jedes Element von $\mathbb{Z}$ ein additiv inverses Element. Die Kommutativität und Assoziativität von $\oplus$ folgen direkt aus den entsprechenden Eigenschaften von $+$, also ist der Beweis von (1) vollständig.

(2) Ist $f(n) = f(m)$, dann gilt $(n, 0) \sim (m, 0)$, also $n + 0 = m + 0$ und damit $n = m$. Somit ist f injektiv und nach Definition gilt für $n, m \in \mathbb{N}$ natürlich $f(n) \oplus f(m) = [(n, 0)] \oplus [(m, 0)] = [(n + m, 0)] = f(n + m)$. □

In Anbetracht von Teil (2) kann man $\mathbb{N}$ einfach als Teilmenge von $\mathbb{Z}$ betrachten. Man schreibt einfach n statt $[(n, 0)]$ (und damit insbesondere 0 statt $[(0, 0)]$) und bezeichnet die Addition auf $\mathbb{Z}$ wieder mit $+$. Dann gilt natürlich $n + [(0, n)] = 0$, also schreibt man $-n$ für $[(0, n)]$. Nun ist leicht zu sehen, dass jedes Element $\neq 0$ von $\mathbb{Z}$ entweder von der Form k oder von der Form $-k$ für ein $k \in \mathbb{N}$ ist. Betrachten wir nämlich $[(m, n)] \in \mathbb{Z} \setminus \{0\}$, dann ist $m \neq n$. Nach Proposition A 4 gilt entweder $m \leq n$ oder $n \leq m$. Im ersten Fall ist $n = m + a$ für ein Element $a \in \mathbb{N}$ (und $a \neq 0$ wegen $m \neq n$). Das bedeutet aber gerade, dass $(m, n) \sim (0, a)$ also $[(m, n)] = -a$ gilt. Im zweiten Fall ist $m = n + a$, was analog $(m, n) \sim (a, 0)$, also $[(m, n)] = a$ impliziert. Man erhält also genau das "übliche" Bild von $\mathbb{Z}$.

Die Ordnungsrelation lässt sich auch relativ einfach auf $\mathbb{Z}$ erweitern. Denkt man wieder an die Motivation, dass $[(m, n)]$ die Differenz $m - n$ symbolisieren soll, dann sieht man leicht, dass man die "richtige" Definition der Ordnung folgendermaßen erhält. Man definiert $(m_1, n_1) \leq (m_2, n_2)$ genau dann, wenn $m_1 + n_2 \leq m_2 + n_1$ in $\mathbb{N}$ gilt. Dann folgt aus Proposition A 4 sofort, dass diese Relation reflexiv und transitiv ist. Außerdem gilt sowohl $(m_1, n_1) \leq (m_2, n_2)$ als auch $(m_2, n_2) \leq (m_1, n_1)$ genau dann, wenn $(m_1, n_1) \sim (m_2, n_2)$ gilt. Daraus schließt man leicht, dass die Relation

$$[(m_1, n_1)] \leq [(m_2, n_2)] : \Longleftrightarrow \; m_1 + n_2 \leq m_2 + n_1$$

wohldefiniert ist und eine Ordnungsrelation definiert. Aus Proposition A 4 folgt dann auch, dass man eine Totalordnung auf $\mathbb{Z}$ erhält, die mit der Addition analog zu dieser Proposition verträglich ist. Offensichtlich stimmt diese Ordnung auf $\mathbb{N} \subset \mathbb{Z}$ mit der Ordnung aus Definition A 3 überein. Für $m, n \in \mathbb{N}$ mit $m \leq n$ folgt dann natürlich $[(0, n)] \leq [(0, m)]$, also $-n \leq -m$ und insbesondere $-n \leq 0$ für alle $n \in \mathbb{N}$.

Die Multiplikation. Die Konstruktion von $\mathbb{Z}$ war ganz durch die Eigenschaften der Addition bestimmt. Wie wir alle schon lange wissen, kann man natürliche Zahlen aber nicht nur addieren, sondern auch multiplizieren und die Multiplikation dann auf die ganzen Zahlen erweitern. Man lernt die Multiplikation als Kind als iterierte Addition kennen, also $m \cdot 1 = m$, $m \cdot 2 = m + m$, $m \cdot 3 = m + m + m$, und so weiter. Daraus sehen

wir aber sofort, wie wir, analog zur Addition in Satz A 1, die Multiplikation rekursiv definieren können. Es sollte nämlich $m \cdot S(n) = (m \cdot n) + m$ gelten. Benutzt man nun noch $1 = S(0)$ dann liefert diese Regel nur dann den "richtigen"Wert für $n = 0$, wenn wir $m \cdot 0 = 0$ definieren. Analog zu Satz A 1 beweist man dann das folgende Resultat:

THEOREM A 9. *(1) Es gibt eine eindeutig bestimmte Operation $\cdot$ auf $\mathbb{N}$, sodass für alle $m, n \in \mathbb{N}$ die folgenden beiden Eigenschaften erfüllt sind:*

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot S(n) = (m \cdot n) + m \end{cases}.$$

(2) Die Operation $\cdot$ aus Teil (1) ist assoziativ und kommutativ und 1 ist ein neutrales Element für $\cdot$. Außerdem gilt für alle $k, m, n \in \mathbb{N}$ das Distributivgesetz

$$k \cdot (m + n) = (k \cdot m) + (k \cdot n).$$

Zusätzlich zu den "schönen" Eigenschaften der beiden Operationen $+$ und $\cdot$ hat man also das Distributivgesetz, das die Verträglichkeit der beiden Operationen miteinander regelt. Man beachte aber, dass diese Verträglichkeit die beiden Operationen verschieden behandelt. Definiert man $f : \mathbb{N} \to \mathbb{N}$ als die Funktion $f(n) := k \cdot n$, dann sagt das Distributivgesetz genau, dass $f(m + n) = f(m) + f(n)$, also f ein Homomorphismus $(\mathbb{N}, +) \to (\mathbb{N}, +)$ ist. Es gibt keine analoge Regel in der "umgekehrten Richtung". Dies motiviert auch die übliche Konvention "Punktrechnung geht vor Strichrechnung", in der man das Distributivgesetz einfach als $k \cdot (m + n) = k \cdot m + k \cdot n$ schreibt.

Das Distributivgesetz liefert auch die Information, wie man die Multiplikation auf $\mathbb{Z}$ ausdehnen könnte. Soll das Distributivgesetz weiterhin gelten, dann muss für $m, n \in \mathbb{N}$ natürlich $0 = m \cdot 0 = m \cdot (n + (-n)) = (m \cdot n) + (m \cdot (-n))$ gelten. Also muss $m \cdot (-n)$ gleich dem additiv inversen Element $-(m \cdot n)$ sein. Dann kann man aber die gleiche Rechnung nochmals mit $-m$ statt m durchführen, und sieht, dass $(-m) \cdot (-n) = m \cdot n$ gelten muss. "Minus mal minus ist plus" ist also eine unvermeidliche Konsequenz des Distributivgesetzes.

Aus diesen Überlegungen kann man auch sofort ableiten, wie man die Fortsetzung der Multiplikation auf $\mathbb{Z}$ formal durchführen sollte. Es sollte ja

$$(m_1 - n_1) \cdot (m_2 - n_2) = ((m_1 m_2 + n_1 n_2) - (m_1 n_2 + n_1 m_2))$$

gelten. Tatsächlich zeigt man analog zu Satz A 8:

THEOREM A 10. *(1) Die Vorschrift*

$$[(m, n)] \odot [(k, \ell)] := [(m \cdot k + n \cdot \ell, m \cdot \ell + n \cdot k)]$$

liefert eine wohldefinierte Operation $\odot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, die assoziativ und kommutativ ist und $[(1, 0)]$ als neutrales Element besitzt.

(2) Die Abbildung $f : \mathbb{N} \to \mathbb{Z}$, $f(n) := [(n, 0)]$ aus Satz A 8 erfüllt $f(m \cdot n) = f(m) \odot f(n)$ für alle $m, n \in \mathbb{N}$.

Natürlich schreibt man dann für das Produkt von $a, b \in \mathbb{Z}$ wieder $a \cdot b$ (oder überhaupt nur ab). Schließlich kann man noch leicht verifizieren, dass die Ordnungsrelation $\leq$ auf $\mathbb{Z}$ mit der Multiplikation verträglich ist, in dem Sinne, dass für $a, b \in \mathbb{Z}$ mit $a > 0$ und $b > 0$ auch $ab > 0$ gilt. Auf $\mathbb{Z}$ ist aber das Analogon der Wohlordnungseigenschaft aus Satz A 5 nicht erfüllt, insbesondere hat $\mathbb{Z}$ selbst kein kleinstes Element. Es gilt aber immer noch, dass nach unten beschränkte Teilmengen von $\mathbb{Z}$ ein kleinstes Element besitzen.

5.3. Ringe, Teilbarkeit und Primfaktorzerlegung

Analog zum allgemeinen Begriff der Gruppe gibt es den Begriff des Ringes für Mengen mit zwei Operationen. Motiviert durch das Beispiel der Zahlbereiche bezeichnet man die beiden Operationen als *Addition* und *Multiplikation* und verwendet die übliche Konvention "*Punkt– vor Strichrechnung*" um nicht zu viele Klammern schreiben zu müssen. Wie wir schon in den Beispielen von $\mathbb{N}$ und $\mathbb{Z}$ gesehen haben, sind die beiden Operationen nicht gleichberechtigt. Insbesondere verlangt man immer, dass die Addition die Struktur einer kommutativen Gruppe definiert, während man an die Multiplikation im Allgemeinen viel schwächere Anforderungen stellt.

Wir folgen zunächst (mit einigen Auslassungen) den Abschnitten 5.3.1 bis 5.3.38 von [**EMA**].

Als nächstes geben wir einen alternativen Beweis für das Primzahlkriterium aus Proposition 5.3.46 von [**EMA**] (ohne die Eindeutigkeit der Primfaktorzerlegung zu benutzen). Daraus leiten wir den Fundamentalsatz der Arithmetik (Theorem 5.3.45 von [**EMA**]) ab. Man bemerke, dass wir Spezialfälle des Primzahlkriteriums schon bewiesen haben: Da das Produkt zweier ungerader Zahlen ungerade ist, sehen wir, dass die Primzahl 2 ein Produkt genau dann teilt, wenn sie einen der Faktoren teilt.

PROPOSITION A 11. *Eine Zahl $p \in \mathbb{N}$ mit $p > 1$ ist genau dann eine Primzahl, wenn für beliebige Zahlen $k, \ell \in \mathbb{Z}$ aus $p|k\ell$ immer $p|k$ oder $p|\ell$ folgt.*

BEWEIS. Ist p nicht prim, dann ist $p = rs$ für $r, s \in \mathbb{N}$ mit $r, s < p$. Dann gilt natürlich $p|rs$ aber p kann weder r noch s teilen.

Die andere Implikation beweisen wir indirekt. Wir nehmen also an, dass es Primzahlen gibt, für die das angegebene Kriterium nicht gilt. Sei p die kleinste dieser Primzahlen. Dann gibt es also Zahlen k und ℓ sodass p weder k noch ℓ teilt, aber $p|k\ell$ gilt. Wir können uns auf $k, \ell \in \mathbb{N}$ einschränken und wir betrachten jenen Fall, für den das Produkt $k\ell$ so klein wie möglich ist.

Dann muss zunächst $k, \ell < p$ gelten. Wir können nämlich k und ℓ mit Rest durch p dividieren und erhalten $k = ap + u$, $\ell = bp + v$ mit $0 < u, v < p$. Dann ist aber $k\ell = abp^2 + avp + ubp + uv$, also $uv = k\ell - (abp + av + bu)p$. Wären a oder b ungleich 0, dann wäre $uv < k\ell$ und $p|uv$, aber natürlich kann p weder u noch v teilen und das wäre ein Widerspruch zur Minimalität von $k\ell$.

Schreiben wir also $k\ell = pm$ für $m \in \mathbb{N}$, dann muss $1 < m < p$ gelten. Aus Lemma 2.1.4 von [**EMA**] wissen wir bereits, dass man m als Produkt von Primzahlen schreiben kann. Ist p' eine dieser Primzahlen, dann gilt natürlich $p'|k\ell$ und wegen $p' < p$ muss die Primzahl p' einen der beiden Faktoren teilen. Ist etwa $k = p'k'$ und $m = p'm'$, dann folgt aus $k\ell = pm$ natürlich $p'k'\ell = p'pm'$, also $k'\ell = pm'$. Damit gilt aber $p|k'\ell$ und $k'\ell < k\ell$, also muss wegen der Minimalität von $k\ell$ entweder $p|k'$ (und damit $p|k$) oder $p|\ell$ gelten, was wiederum einen Widerspruch darstellt. □

Mit Induktion nach der Anzahl der Faktoren beweist man dann sofort: Ist p eine Primzahl und sind $k_1, \ldots, k_n \in \mathbb{Z}$ sodass $p|(k_1 \cdots k_n)$ gilt, dann gibt es mindestens ein i, sodass $p|k_i$ gilt. Mit diesem Kriterium wird der Beweis des Fundamentalsatzes der Arithmetik ziemlich einfach:

THEOREM A 12. *Sei $m > 1$ eine ganze Zahl. Dann kann man m als Produkt von Primzahlen schreiben, wobei die Darstellung eindeutig ist, wenn man die Primzahlen der Größe nach ordnet.*

BEWEIS. Die Existenz der Primfaktorzerlegung wurde bereits in Lemma 2.1.4 von [**EMA**] bewiesen. Zur Eindeutigkeit betrachten wir für $n \geq 1$ folgende Aussage: Sind $p_1, \ldots, p_n$ und $q_1, \ldots, q_k$ mit $k \geq n$ Primzahlen, sodass $p_1 \cdots p_n = q_1 \cdots q_k$ gilt, dann ist $k = n$ und die p_i unterscheiden sich von den q_j höchstens in der Reihenfolge. Wir beweisen diese Aussage durch Induktion nach n.

Für den Induktionsanfang ist $n = 1$, also haben wir Primzahlen p und $q_1, \ldots, q_k$ gegeben, sodass $p = q_1 \cdots q_k$ gilt. Dann ist q_1 ein Teiler von p und als Primzahl ist $q_1 > 1$, also $q_1 = p$ und damit auch $k = 1$.

Nehmen wir als Induktionsvoraussetzung an, dass die obige Aussage für je n Primzahlen p_i gilt und betrachten wir Primzahlen $p_1, \ldots, p_{n+1}$ und $q_1, \ldots, q_\ell$ mit $\ell \geq n + 1$, sodass $p_1 \cdots p_{n+1} = q_1 \cdots q_\ell$ gilt. Dann teilt die Primzahl p_{n+1} das Produkt $q_1 \cdots q_\ell$, also gibt es ein i, sodass $p_{n+1} | q_i$ und damit $p_{n+1} = q_i$ gilt. Damit können wir aus $p_1 \cdots p_{n+1} = q_1 \cdots q_\ell$ sofort

$$p_1 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell$$

folgern. Wendet man darauf die Induktionsvoraussetzung an, so folgt die Behauptung sofort. □

Mit Hilfe des Primzahlkriteriums können wir leicht unser Resultat über die Irrationalität von $\sqrt{2}$ aus Theorem 3.2.7 von [**EMA**] verallgemeinern:

THEOREM A 13. *Sei k eine positive ganze Zahl. Dann ist $\sqrt{k}$ entweder ebenfalls eine ganze Zahl oder irrational.*

BEWEIS. Betrachten wir eine rationale Zahl $r = \frac{a}{b}$ sodass $r^2 = k$ gilt. Dabei dürfen wir annehmen, dass $a, b > 0$ gilt und der Bruch gekürzt ist, also a und b keinen gemeinsamen Teiler haben. Dann bedeutet $r^2 = k$ natürlich $a^2 = kb^2$. Nehmen wir nun indirekt an, dass $b > 1$ gilt. Dann gibt es eine Primzahl p, die b teilt. Damit teilt p aber auch b^2 und weil k ganz ist, auch die ganze Zahl $kb^2 = a^2 = a \cdot a$. Nach dem Primzahlkriterium (Proposition A 11) muss p die Zahl a teilen, ein Widerspruch zur Teilerfremdheit von a und b. Damit ist $b = 1$ und $k = a^2$. □

Ab hier folgen wir wieder (mit einigen Auslassungen) den Abschnitten 5.3.47 bis 5.3.57 von [**EMA**].

5.4. Rationale und Reelle Zahlen; Körper

Die Körper stellen die letzte Station auf unserer (kurzen) Reise durch die algebraischen Strukturen dar. Körper sind ein Spezialfall von kommutativen Ringen mit Einselement. Schon aus der Schule sind die Beispiele $\mathbb{Q}$, $\mathbb{R}$, die wir im Verlauf des Kapitels noch genauer studieren werden, und wahrscheinlich auch $\mathbb{C}$ bekannt. Wir werden aber sehen, dass es auch endliche Körper gibt.

DEFINITION A 14. Ein *Körper* $(K, +, \cdot)$ ist ein kommutativer Ring mit Einselement, sodass jedes Element $a \in K \setminus \{0\}$ ein multiplikativ inverses Element besitzt.

Wie in Abschnitt 5.2 von [**EMA**] sieht man leicht, dass das multiplikativ inverse Element zu a eindeutig bestimmt ist. Daher schreibt man es wieder als a^{-1}, also gilt $a \cdot a^{-1} = 1$.

Aus Beispiel 5.3.9 wissen wir schon, dass die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ mit den üblichen Operation von Addition und Multiplikation kommutative

Ringe mit Einselement sind. Aus der Schule ist schon bekannt, dass in diesen Zahlbereichen jedes Element ungleich Null ein multiplikativ Inverses besitzt, also sind $\mathbb{Q}$ und $\mathbb{R}$ Körper.

Als nächstes beweisen wir Proposition 5.4.8 von [**EMA**]:

PROPOSITION A 15. *Ist $(K, +, \cdot)$ ein Körper und sind $a, b \in K$, dann gelten die folgenden Rechenregeln:*

(i) *Für $a, b \neq 0$ gilt $(ab)^{-1} = a^{-1}b^{-1}$.*
(ii) *Für $a \neq 0$ gilt $(-a)^{-1} = -a^{-1}$.*
(iii) *Ist $ab = 0$, dann gilt $a = 0$ oder $b = 0$.*
(iv) *Für $a \neq 0$ hat die Gleichung $ax = b$ die eindeutige Lösung $x = a^{-1}b$.*

BEWEIS. (i) Wir rechnen einfach

$$(ab)(a^{-1}b^{-1}) = aba^{-1}b^{-1} = aa^{-1}bb^{-1} = 1 \cdot 1 = 1,$$

wobei wir Assoziativität und Kommutativität der Multiplikation benutzt haben. Damit ist $a^{-1}b^{-1}$ ein multiplikativ inverses Element zu ab also gleich $(ab)^{-1}$.

(ii) Nach Proposition 5.3.16 gilt $(-a^{-1}) \cdot (-a) = a^{-1} \cdot a = 1$. Damit ist aber $-a^{-1}$ multiplikativ invers zu $-a$, also gleich $(-a)^{-1}$.

(iii) Angenommen es gilt $ab = 0$ und $a \neq 0$. Dann gibt es ein multiplikativ inverses Element a^{-1} und multipliziert man damit die Gleichung $ab = 0$, dann erhält man $a^{-1}ab = a^{-1} \cdot 0$. Nun ist aber $a^{-1}ab = 1 \cdot b = b$ und $a^{-1} \cdot 0 = 0$ nach Proposition 5.3.16.

(iv) Natürlich gilt $aa^{-1}b = 1 \cdot b = b$, also ist $x = a^{-1}b$ eine Lösung von $ax = b$. Umgekehrt kann man die Gleichung $ax = b$ auf beiden Seiten mit a^{-1} multiplizieren und erhält $a^{-1}ax = a^{-1}b$ und die linke Seite liefert x. □

Aus Teil (iii) dieser Proposition folgt, dass Körper nullteilerfrei sind (siehe Definition 5.3.37). Anderseits zeigt das auch, dass man die Multiplikation als Abbildung

$$(K \setminus \{0\}) \times (K \setminus \{0\}) \to K \setminus \{0\}$$

und damit als Operation auf $K \setminus \{0\}$ betrachten kann. Nach Definition ist diese Operation assoziativ und kommutativ, besitzt ein neutrales Element und zu jedem Element (von $K \setminus \{0\}$!) ein inverses Element. Also ist $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe. Somit haben die beiden Rechenoperationen in einem Körper fast gleich schöne Eigenschaften. Der Unterschied liegt in der asymmetrischen Form des Distributivgesetzes, das auch die ausgezeichnete Rolle von 0 bedingt.

Mit diesem Resultat können wir auch unser Verständnis der Restklassenringe vervollständigen, indem wir Theorem 5.4.10 von [**EMA**] beweisen.

THEOREM A 16. *Für eine natürliche Zahl n betrachten wir den kommutativen Ring $(\mathbb{Z}_n, +, \cdot)$ mit Einselement. Dann ist $\mathbb{Z}_n$ genau dann ein Körper, wenn n eine Primzahl ist.*

BEWEIS. Ist n keine Primzahl, dann finden wir Zahlen $r, s \in \mathbb{N}$ mit $r, s < n$, sodass $n = rs$ gilt. Dann kann n natürlich weder r noch s teilen, also sind $\bar{r}, \bar{s} \in \mathbb{Z}_n$ beide ungleich $0 = \bar{0}$. Andererseits ist $\bar{r} \cdot \bar{s} = \overline{rs} = \bar{n} = \bar{0}$. Damit hat $\mathbb{Z}_n$ Nullteiler und kann daher nach Teil (iii) von Proposition A 15 kein Körper sein.

Nehmen wir umgekehrt an, dass n eine Primzahl ist und dass $\bar{r}, \bar{s} \in \mathbb{Z}_n$ die Gleichung $\bar{r} \cdot \bar{s} = 0$ erfüllen. Dann ist $\bar{0} = \overline{rs}$, also teilt n das Produkt rs. Nach Proposition A 11 muss n einen der Faktoren teilen und das bedeutet gerade, dass $\bar{r} = \bar{0}$ oder $\bar{s} = \bar{0}$ gelten muss. Betrachten wir nun ein fixes Element $0 \neq \bar{k} \in \mathbb{Z}_n$ und die Funktion $f : \mathbb{Z}_n \to \mathbb{Z}_n$, die gegeben ist durch $f(\bar{r}) = \bar{k} \cdot \bar{r}$. Ist $f(\bar{r}_1) = f(\bar{r}_2)$, also $\bar{k} \cdot \bar{r}_1 = \bar{k} \cdot \bar{r}_2$, dann erhalten

wir $0 = \bar{k} \cdot \bar{r}_1 - \bar{k} \cdot \bar{r}_2 = \bar{k} \cdot (\bar{r}_1 - \bar{r}_2)$. Da $\bar{k} \neq \bar{0}$ ist, ist das nur für $0 = \bar{r}_1 - \bar{r}_2$ und damit $\bar{r}_1 = \bar{r}_2$ möglich. Somit ist die Funktion f injektiv und weil $\mathbb{Z}_n$ endlich ist, muss f auch surjektiv sein. Also gibt es ein Element $\bar{\ell} \in \mathbb{Z}_n$, sodass $\bar{1} = f(\bar{\ell}) = \bar{k} \cdot \bar{\ell}$ gilt. Damit besitzt jedes Element $\bar{k} \in \mathbb{Z}_n \setminus \{0\}$ ein multiplikativ inverses Element. □

Nachdem wir jetzt endliche Körper kennen gelernt haben, wollen wir uns noch, analog zu den Abschnitten über $\mathbb{N}$ und $\mathbb{Z}$, genauer mit der Konstruktion der rationalen Zahlen $\mathbb{Q}$ beschäftigen. Die Idee ist ganz ähnlich wie bei der Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$, wobei hier die formale Konstruktion dem Bild aus der Schulmathematik noch näher liegt. Details dazu finden sich in den Abschnitten 6.3.9 bis 6.3.16 von [**EMA**].

Definition A 17. Betrachte die Menge $\{(p, q) : q > 0\} \subset \mathbb{Z} \times \mathbb{Z}$. Darauf definiert man eine Relation durch

$$(p_1, q_1) \sim (p_2, q_2) :\Longleftrightarrow\ p_1 q_2 = p_2 q_1 \text{ in } \mathbb{Z}.$$

Diese Relation ist offensichtlich reflexiv und symmetrisch. Für die Transitivität sieht man zunächst, dass $(p_1, q_1) \sim (0, q_2)$ genau dann gilt, wenn $p_1 = 0$ gilt. Insbesondere folgt aus $(p_1, q_1) \sim (0, q_2)$ und $(0, q_2) \sim (p_3, q_3)$ sofort $p_1 = p_3 = 0$ und damit $(p_1, q_1) \sim (p_3, q_3)$. Nehmen wir also an, dass $(p_1, q_1) \sim (p_2, q_2)$ und $(p_2, q_2) \sim (p_3, q_3)$ gelten, wobei $p_2 \neq 0$ ist. Dann folgt leicht, dass $p_1 q_3 p_2 = p_3 q_1 p_2$ und damit $0 = (p_1 q_3 - p_3 q_1) p_2$ gilt. Da es in $\mathbb{Z}$ keine Nullteiler gibt, folgt $0 = p_1 q_3 - p_3 q_1$ und damit $(p_1, q_1) \sim (p_3, q_3)$. Somit ist $\sim$ eine Äquivalenzrelation und wir schreiben wieder $[(p, q)]$ für die Äquivalenzklasse von (p, q). Diese Klasse soll den Bruch p/q repräsentieren, was auch die Definition der Relation motiviert. Die Menge der Äquivalenzklassen wird mit $\mathbb{Q}$ bezeichnet. Aus dieser Motivation folgt auch, wie die Rechenoperationen auf $\mathbb{Q}$ aussehen "sollten". Genauer zeigt man:

Proposition A 18. *(1) Die Abbildung*

$$((p_1, q_1), (p_2, q_2)) \mapsto (p_1 q_2 + p_2 q_1, q_1 q_2)$$

liefert eine wohldefinierte Addition $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$*, sodass* $(\mathbb{Q}, +)$ *eine kommutative Gruppe ist. Das neutrale Element für die Addition ist* $0 := [(0, 1)]$*, das additiv inverse Element zu* $[(p, q)]$ *ist* $[(-p, q)]$*.*

(2) Die Abbildung $((p_1, q_1), (p_2, q_2)) \mapsto (p_1 p_2, q_1 q_2)$ *induziert eine wohldefinierte Multiplikation* $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$*, sodass* $(\mathbb{Q}, +, \cdot)$ *ein Körper ist. Das neutrale Element für die Multiplikation ist* $[(1, 1)]$ *und für ein Element* $[(p, q)] \neq 0$ *ist* $p \neq 0$ *und das multiplikativ inverse Element ist für* $p > 0$ *durch* $[(q, p)]$ *und für* $p < 0$ *durch* $[(-q, -p)]$ *gegeben.*

(3) Die Abbildung $n \mapsto [(n, 1)]$ *definiert eine injektive Funktion* $\mathbb{Z} \to \mathbb{Q}$ *die sowohl mit der Addition als auch mit der Multiplikation verträglich, also ein Ringhomomorphismus ist.*

Beweis. Das sind durchwegs direkte Verifikationen, siehe die Abschnitte 6.3.9 bis 6.3.14 im Erweiterungsstoff von [**EMA**]. □

Man schreibt dann $\frac{p}{q}$ für die Äquivalenzklasse $[(p, q)]$. Die Äquivalenzrelation bedeutet gerade $\frac{p}{q} = \frac{pr}{qr}$ für alle $r \in \mathbb{N}$ mit $r \neq 0$, also dass man Brüche kürzen kann. Die Operationen erhalten dann die vertraute Form $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}$ und $\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2}$.

Schließlich erweitert man auch noch die Ordnungsrelation auf $\mathbb{Q}$ indem man

$$[(p_1, q_1)] \geq [(p_2, q_2)] \iff p_1 q_2 \geq p_2 q_1$$

setzt, wobei auf der rechten Seite die Ordnungsrelation auf $\mathbb{Z}$ verwendet wird. Man verifiziert direkt, dass $\leq$ eine Totalordnung auf $\mathbb{Q}$ definiert, die $\mathbb{Q}$ zu einem *geordneten*

Körper macht. Das bedeutet, dass für $x, y, z \in \mathbb{Q}$ aus $x \leq y$ auch $x + z \leq y + z$ folgt und dass $x > 0$ und $y > 0$ immer $xy > 0$ impliziert.

Bis zu dieser Stelle waren die Erweiterungen der Zahlbereiche durch "Verbesserungen" der algebraischen Eigenschaften der Rechenoperationen motiviert. Man gelangt von $\mathbb{N}$ zu $\mathbb{Z}$ indem man additiv inverse Element "hinzufügt". Analog gelangt man von $\mathbb{Z}$ zu $\mathbb{Q}$ indem man für alle Elemente $\neq 0$ multiplikativ inverse Elemente "hinzufügt". Damit ist die "beste" algebraische Struktur erreicht. Den weiteren Übergang zu den reellen und komplexen Zahlen werden wir hier nur als Vorgeschmack auf die Vorlesung über Analysis kurz skizzieren.

Die wesentliche "Schwachstelle" von $\mathbb{Q}$ haben wir schon in Theorem 3.2.7 von [**EMA**] (und allgemeiner in Theorem A 13) exemplarisch kennen gelernt, wo wir bewiesen haben, dass es keine rationale Zahl x gibt, die $x^2 = 2$ erfüllt. Nun kann man natürlich rationale Zahlen finden, deren Quadrat beliebig nahe bei 2 liegt, aber die Menge der rationalen Zahlen hat "Löcher". Insbesondere kann sie kein gutes Modell für eine Gerade darstellen. Formaler kann man das auf mehrere Arten formulieren, zum Beispiel über die Eigenschaften der Ordnungsrelation, über Intervallschachtelungen, oder über Folgen. Betrachten wir zum Beispiel die Teilmenge $A := \{x \in \mathbb{Q} : x^2 \leq 2\} \subset \mathbb{Q}$. Diese Teilmenge ist *nach oben beschränkt*. Nehmen wir nämlich Zahlen $y, z \in \mathbb{Q}$ mit $y^2 > 2$ und $z \geq 0$, dann ist $(y+z)^2 = y^2 + 2yz + z^2 \geq y^2 > 2$. Damit muss aber jede Zahl $x \in A$ natürlich $x < y$ erfüllen, also ist y eine *obere Schranke* für A. So sind zum Beispiel 2, 1.5, 1.42, 1.415, 1.4143, 1.41422 immer kleinere (also "bessere") obere Schranken für A.

Man kann aber zeigen, dass es in $\mathbb{Q}$ keine kleinste obere Schranke y_0 für A geben kann, weil eine solche Schranke $(y_0)^2 = 2$ erfüllen müsste. Ähnlich kann man das über die ineinander geschachtelten Intervalle rationaler Zahlen

$$[1, 2] \supset [1.4, 1.5] \supset [1.41, 1.42] \supset [1.414, 1.415] \supset \ldots,$$

beschreiben, deren Länge gegen Null geht und die keinen gemeinsamen (rationalen) Punkt enthalten. Schließlich kann man noch sogenannte Cauchy–Folgen, die keinen Grenzwert besitzen, betrachten.

In den reellen Zahlen $\mathbb{R}$ ist dieser Mangel behoben, diese bilden nicht nur einen geordneten Körper, sondern sind auch noch *vollständig*. Die Vollständigkeit kann man dadurch beschreiben, dass jede nichtleere, nach oben beschränkte Teilmenge von $\mathbb{R}$ eine kleinste obere Schranke besitzt. Äquivalent kann sie auch mit dem Intervallschachtelungsprinzip oder mit der Konvergenz von Cauchy–Folgen beschrieben werden. Mit einer ziemlich aufwändigen Konstruktion kann man im Rahmen der Mengenlehre $\mathbb{R}$ aus $\mathbb{Q}$ konstruieren und beweisen, dass die oben angeführten Eigenschaften $(\mathbb{R}, +, \cdot, \leq)$ eindeutig festlegen. Damit kann man dann, wie in Vorlesungen über Analysis üblich, diese Eigenschaften der reellen Zahlen als axiomatische Basis verwenden.

Die Vollständigkeit von $\mathbb{R}$ erlaubt es, ganz neue Beweismethoden anzuwenden. So kann man zum Beispiel für jede positive reelle Zahl y die Existenz einer reellen Zahl u, für die $u^2 = y$ beweisen, indem man folgendermaßen vorgeht: Man zeigt (leicht), dass die Menge $A := \{x \in \mathbb{R} : x^2 \leq y\}$ nicht leer und nach oben beschränkt ist. Nach der Vollständigkeit besitzt sie somit eine kleinste obere Schranke u_0. Nun kann man einerseits verifizieren, dass eine Zahl u, für die $u^2 < y$ gilt, keine obere Schranke für A sein kann. Andererseits zeigt man, dass es für Zahlen u mit $u^2 > y$ kleinere obere Schranken für A als u gibt, also muss $(u_0)^2 = y$ gelten. Das zeigt, dass trotz der komplizierten Definition, die reellen Zahlen in vieler Hinsicht viel leichter zu handhaben sind, als die rationalen Zahlen.

Die Vollständigkeit sagt auch, dass man $\mathbb{R}$ als gutes Modell für eine Gerade verwenden kann. Das Produkt $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$ ist dann ein Modell für die Ebene und $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$ ein Modell für den dreidimensionalen Raum. Das ist der übliche Ausgangspunkt für Vorlesungen über Geometrie und Vektorrechnung. In diesen Gebieten ist aber, zumindest so lange man nur Objekte wie Geraden und Ebenen betrachtet, der Unterschied zwischen $\mathbb{R}$ und $\mathbb{Q}$ weit weniger bedeutend.

Zum Abschluss erwähnen wir noch kurz die *komplexen Zahlen* $\mathbb{C}$, die ja (zumindest ansatzweise) auch schon aus der Schule bekannt sein sollten. Die Motivation für die Erweiterung von $\mathbb{R}$ zu $\mathbb{C}$ ist, dass es über $\mathbb{R}$ Polynome gibt, die keine Nullstellen besitzen, zum Beispiel $p(x) = x^2 + 1$. Es zeigt sich, dass es genügt, eine Nullstelle für dieses Polynom "zu $\mathbb{R}$ dazu zu geben" um das Problem völlig zu lösen. Formal definiert man $\mathbb{C} := \mathbb{R}^2$ und darauf die Operationen durch

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

Dann rechnet man direkt nach, dass diese Operationen $\mathbb{C}$ zu einem Körper machen, wobei die neutralen Elemente durch $(0, 0)$ und $(1, 0)$ und die inversen Elemente durch

$$-(x, y) = (-x, -y) \qquad \text{und} \qquad (x, y)^{-1} = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right)$$

gegeben sind. Dann kann man $\mathbb{R}$ als die Teilmenge $\{(x, 0) : x \in \mathbb{R}\}$ betrachten und $(x, 0)$ einfach wieder als x schreiben. Betrachtet man dann noch $i := (0, 1)$ dann gilt $i \cdot i = (-1, 0) = -1$ und für $y \in \mathbb{R}$ ist $(0, y) = i \cdot y$. Damit kann man (x, y) als $x + iy$ schreiben und kommt zur üblichen Form der komplexen Zahlen.

Der sogenannte Fundamentalsatz der Algebra zeigt dann, dass über $\mathbb{C}$ tatsächlich jedes Polynom mindestens eine Nullstelle besitzt. Allerdings muss man in diesem Fall einen Preis bezahlen: Im Gegensatz zu $\mathbb{Q}$ und $\mathbb{R}$ gibt es auf $\mathbb{C}$ keine Ordnungsrelation mehr, die in schöner Weise mit den algebraischen Operationen verträglich ist.

Literaturverzeichnis

[EMA] H. Schichl, R. Steinbauer, *Einführung in das mathematische Arbeiten*, 2. Auflage, Springer–Verlag 2012.