Elementare Zahlentheorie

gehalten von Prof. Dr. Weitze-Schmithüsen im Sommer 23

UNIVERSITÄT
DES
SAARLANDES

Inhaltsverzeichnis

I Zahlbereiche **7**
1 Natürliche Zahlen 7
2 Rekursionen 11
3 Das Prinzip des kleinsten Täters 15
4 Die ganzen Zahlen 17
5 Die rationalen Zahlen 23
6 Dezimalbruchentwicklung rationaler Zahlen 27
7 Die reellen Zahlen 32

II Teilbarkeitslehre **39**
1 Euklidischer Algorithmus 39
2 Der chinesische Restsatz 42
3 Primzahlen 43

Allgemeine Informationen

Dieser Vorlesungsmitschrieb wird von einem Studenten erstellt und es handelt sich um einen nicht autorisierten Aufschrieb. Textsatz ist keine Garantie für Fehlerfreiheit. Wenn Sie Fehler in diesem Aufschrieb finden, schreiben Sie gerne eine E-Mail (zum Beispiel unter Angabe von Nummer des Abschnittes und Fehlerbeschreibung oder mit einem handschriftlich markiertem pdf) an:

s9fhguen@stud.uni-saarland.de

Kapitel I

Zahlbereiche

Ziel dieses Kapitels wird es sein, aus den natürlichen Zahlen die anderen gebräuchlichen Zahlbereiche der ganzen, rationalen und reellen Zahlen zu konstruieren.

1 Natürliche Zahlen

In dieser Vorlesungen wollen wir die natürlichen Zahlen axiomatisch (statt konstruktiv) einführen. Wir werden sehen, dass wir aus diesen Axiomen die gewohnten Rechenregeln folgern können.

Definition I.1.1 (Peano-Axiome): Die Menge $\mathbb{N}$ der natürlichen Zahlen wird durch folgende Axiome definiert:

(P1) Die Menge $\mathbb{N}$ enthält ein ausgezeichnetes Element 0. Insbesondere ist $\mathbb{N}$ nicht die leere Menge.

(P2) „Nachfolger-Axiom“: Zu jedem Element n der Menge $\mathbb{N}$ gibt es ein wohldefiniertes Element n^* aus $\mathbb{N}$. Das Element n^* wird *Nachfolger* genannt.

(P3) „Null hat keinen Vorgänger“: Es gibt kein Element k von $\mathbb{N}$, sodass $0 = k^*$.

(P4) „Injektivität der Nachfolgerfunktion“: Für alle n_1 und n_2 aus $\mathbb{N}$ mit $n_1^* = n_2^*$ gilt $n_1 = n_2$.

(P5) „Prinzip der vollständigen Induktion“: Falls für eine Teilmenge T von $\mathbb{N}$ gilt, dass 0 in T ist und dass für jedes n in T auch n^* zu T gehört, dann ist $T = \mathbb{N}$.

Im Rahmen dieser Vorlesung ist die Null eine natürliche Zahl. Das wird in anderen Kontexten unterschiedlich gehandhabt.

Notation I.1.2: Die Abbildung $\sigma\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n^*$ heißt *Nachfolgefunktion.* Wir schreiben 1 für $\sigma(0)$, 2 für $\sigma(1)$ und so weiter, wie gewohnt.

Proposition I.1.3 (Eindeutigkeit der Null): *Es bezeichne* $\mathbb{N}^*$ *die Menge*

$$\{n \in \mathbb{N} \mid \textit{Es gibt } k \textit{ in } \mathbb{N} \textit{ mit } n = k^*\}.$$

Dann gilt $\mathbb{N} = \{0\} \cup \mathbb{N}^*$. *Insbesondere ist Null das einzige Element von* $\mathbb{N}$, *das kein Nachfolger ist.*

Beweis: Wir wollen die Gleichheit der beiden Mengen per Axiom (P5) zeigen. Wir schreiben $M = \{0\} \cup \mathbb{N}^*$. Zunächst gehört 0 per Definition zu M. Bleibt zu zeigen, dass für n in M auch der Nachfolger n^* zu M gehört. Aber per Definition von $\mathbb{N}^*$ ist n^* ebenfalls ein Element von M. Nach (P5) ist deshalb $M = \mathbb{N}$. □

Nun wollen wir uns den Rechenarten für die natürlichen Zahlen widmen: Der Addition, Multiplikation und den Potenzen.

Ansatz I.1.4: Addition, Multiplikation und Potenzen natürlicher Zahlen erfüllen die folgenden Eigenschaften:

(S1) Für jede natürliche Zahl n ist $n + 0 = n$.

(S2) Für jedes Paar n, m natürlicher Zahlen ist $n + \sigma(m) = \sigma(n + m)$.

(M1) Für jede natürliche Zahl n ist $n \cdot 0 = 0$.

(M2) Für jedes Paar n, m natürlicher Zahlen ist $n \cdot \sigma(m) = n \cdot m + n$.

(Exp1) Für jede natürliche Zahl a ist $a^0 = 1$.

(Exp2) Für jedes Paar a, m natürlicher Zahlen ist $a^{\sigma(m)} = a^m \cdot a$.

(Σ1) Ist M die leere Menge, dann ist $\sum_{a \in M} a = 0$.

(Σ2) Für jede Zahl n aus $\mathbb{N}^*$, natürliche Zahlen $a_1, \ldots, a_n$, $M = \{a_1, \ldots, a_n\}$ und $M' = M - \{a_n\}$ ist $\sum_{a \in M} a = (\sum_{a \in M'} a) + a_n$.

(Π1) Ist M die leere Menge, dann ist $\prod_{a \in M}\ a = 1$.

(Π2) Für jede Zahl n aus $\mathbb{N}^*$, natürliche Zahlen $a_1, \ldots, a_n$, $M = \{a_1, \ldots, a_n\}$ und $M' = M - \{a_n\}$ ist $\prod_{a \in M} a = (\prod_{a \in M'} a)a_n$.

Notation: Für eine natürliche Zahl n und die Teilmenge $M = \{a_1, \ldots, a_n\}$ der natürlichen Zahlen schreiben wir

$$\sum_{i=1}^{n} a_i = \sum_{a \in M} a, \quad \text{und} \quad \prod_{i=1}^{n} a_i = \prod_{a \in M} a.$$

Die Forderungen in Ansatz I.1.4 führen unmittelbar zu einem Problem: Gibt es überhaupt, geschweige denn eindeutige, Funktionen $+, \cdot, .^- \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sowie $\Sigma, \Pi \colon \mathfrak{P}^{\text{fin}}(\mathbb{N}) \to \mathbb{N}$, wobei $\mathfrak{P}^{\text{fin}}(\mathbb{N})$ die Menge der endlichen Teilmengen der natürlichen Zahlen bezeichnet, die die Eigenschaften (S1), (S2), (M1), (M2), (Exp1), (Exp2), (Σ1), (Σ2), (Π1) und (Π2) erfüllen?

Die Antwort auf diese Frage(n) ist „Ja“, was wir mithilfe des Konzepts der Rekursion in der nächsten Vorlesung zeigen werden. Für die heutige Vorlesung und das erste Übungsblatt gehen wir von der Existenz solcher Funktionen aus und zeigen, welche weiteren Eigenschaften daraus folgen. Dabei dürfen nur die oben aufgelisteten Eigenschaften verwendet werden.

Proposition I.1.5 (Rechenregeln): *Für „+“ und „·“ gelten die folgenden Rechenregeln:*

(NF) *Für jede natürliche Zahl n ist $\sigma(n) = n + 1$.*

(A) *Für alle natürlichen Zahlen k, m, n gilt $(k + m) + n = k + (m + n)$.*

(K) *Für alle natürlichen Zahlen m und n gilt $m + n = n + m$.*

(D) *Für alle natürlichen Zahlen k, m, n gilt $k(m + n) = km + kn$.*

(E) *Für jede natürliche Zahl n gilt $n \cdot 1 = n$.*

Analog formuliert man das Assoziativ- und Kommutativgesetz für die Multiplikation.

Beweis: Die Aussagen (A) und (D) sind Übungsaufgaben auf dem ersten Blatt. Exemplarisch zeigen wir (NF) und (K). Die Rechenregel (E) zeigt man mit den gleichen Argumenten.

(NF) Für jede natürliche Zahl n ist $n + 1 = n + \sigma(0) = \sigma(n + 0) = \sigma(n)$. Hierbei haben wir im ersten Schritt die Definition von 1, im zweiten Schritt die Rechenregel (S2) und im dritten Schritt die Rechenregel (S1) verwendet.

(K) Zweckmäßig ist die Verwendung des Peano-Axioms (P5) zum Nachweis des Kommutativgesetzes. Zunächst haben wir zu zeigen, dass für jede natürliche Zahl n gilt, dass $n+0 = 0+n$. Sei $M_0 = \{n \in \mathbb{N} \mid n+0 = 0+n\}$. Per Definition gehört 0 zu M_0. Sei nun n ein Element von N_0. Wir müssen zeigen, dass $\sigma(n)$ zu M_0 gehört. Wir haben

$$0 + \sigma(n) = \sigma(0 + n) = \sigma(n + 0) = \sigma(n) = \sigma(n) + 0,$$

wobei wir bei der ersten Gleichheit (S2), an der zweiten Gleichheit, dass n zu M_0 gehört, bei der dritten Gleichheit (S1) und bei der vierten Gleichheit erneut (S1) verwendet haben. Das Axiom (P5) liefert uns nun die Aussage für Null.

Als nächstes zeigen wir, dass für jede natürliche Zahl n gilt, dass $n+1 = 1+n$. Sei dazu $M_1 = \{n \in \mathbb{N} \mid n+1 = 1+n\}$. Nach dem ersten Schritt gehört 0 zu M_1. Für ein Element n von M_1 erhalten wir

$$1 + \sigma(n) = \sigma(1+n) = \sigma(n+1) = \sigma(\sigma(n)) = \sigma(n) + 1.$$

Hier haben wir zuerst die Definition der Nachfolgefunktion, dann die Zugehörigkeit von n zu M_1, und dann zwei mal erneut die Definition der Nachfolgefunktion verwendet. Aus (P5) folgt nun $M_1 = \mathbb{N}$.

Seien nun m eine natürliche Zahl und $M_m = \{n \in \mathbb{N} \mid m+n = n+m\}$. Nach Schritt 1 gehört 0 zu M_m. Es gehöre n zu M_m. Dann haben wir

$$\begin{aligned} m + \sigma(n) &= \sigma(m+n) \\ &= \sigma(n+m) \\ &= n + \sigma(m) \\ &= n + (m+1) = n + (1+m) = (n+1) + m = \sigma(n) + m. \end{aligned}$$

Dabei haben wir als erstes die Definition von σ verwendet, dann, dass n zu M_m gehört, anschließend die Definition der Nachfolgerfunktion, dann den zweiten Induktionsanfang und dann das Assoziativitätsgesetz in Verbindung mit der Definition der Nachfolgefunktion. Wiederum folgt aus (P5), dass $M_m = \mathbb{N}$ ist und damit, dass die Behauptung gilt. □

Bemerkung I.1.6 (Prinzip der vollständigen Induktion): Aus dem Axiom (P5) leitet sich das folgende Prinzip ab: Sei A eine Aussage über eine Variable n, die Werte in den natülrichen Zahlen annimmt. Falls A erstens für Null gilt (Induktionsanfang), und zweitens aus der Gültigkeit von A für n (Induktionsvoraussetzung) folgt, dass A für $n+1$ gilt, dann gilt A für alle natürlichen Zahlen.

Proposition I.1.7 (Weitere Rechenregeln zur Addition):

(i) *Seien k, m und n natürliche Zahlen mit $k+n = m+n$. Dann gilt $k = m$.*[1]

(ii) *Sind m und n natürliche Zahlen mit $m+n = 0$, dann muss $m = n = 0$ gelten.*

Beweis: (i) Wir zeigen die Rechenregel mithilfe von vollständiger Induktion. Dazu arbeiten wir mit der Menge

$$M = \{n \in \mathbb{N} \mid \text{Für alle naürlichen Zahlen } m, n \text{ gilt: } k+n = m+n \Longrightarrow k = m\}.$$

[1] Diese Rechenregel wird „additive Kürzungsregel“ genannt.

Aus den vorherigen Rechenregeln folgt, dass 0 zu M gehört und mithilfe von (P4), der Injektivität der Nachfolgerfunktion, folgert man, dass die Aussage für alle natürlichen Zahlen gilt.

(ii) Seien m und n natürliche Zahlen, deren Summe 0 ist. Angenommen, n wäre nicht Null. Dann gäbe es nach Proposition I.1.3 eine natürliche Zahl k, sodass $n = \sigma(k)$ und wir hätten

$$0 = m + n = m + \sigma(k) = \sigma(m + k)$$

im Widerspruch zu (P3). Das heißt n muss bereits Null sein. Die Summenregel (S1) zeigt dann, dass $m = 0$ sein muss. □

Proposition I.1.8 (Rechengesetze für Potenzen):

(i) *Für alle natürlichen Zahlen a, m und n gilt $a^m a^n = a^{m+n}$.*

(ii) *Für alle natürlichen Zahlen a, m und n gilt $(a^m)^n = a^{mn}$.*

Beweis: Wir zeigen exemplarisch (i), (ii) zeigt man genau so. Natürlich beweisen wir die Aussage mithilfe von vollständiger Induktion über n. Seien a und m natürliche Zahlen. Für $n = 0$ haben wir $a^m a^0 = a^m \cdot 1 = a^m = a^{m+0}$, wobei wir der Reihe nach (Exp1), (E) und (S1) verwendet haben.

Die Aussage gelte für die natürliche Zahl n, d. h. für alle natürlichen Zahlen a und m ist $a^m a^n = a^{m+n}$. Wir zeigen, dass daraus die Gültigkeit für $n + 1$ folgt. Es gilt

$$a^m a^{\sigma(n)} = a^m(a^m \cdot a) = (a^m a^n)a = (a^{m+n})a = a^{\sigma(m+n)} = a^{m+\sigma(n)},$$

wobei wir (Exp2), die Assoziativität der Multiplikation natürlicher Zahlen, unsere Induktionsvoraussetzung, (Exp2) und (S2) verwendet haben. □

2 Rekursionen

Das Ziel für diesen Abschnitt soll die Einführung rekursiver Funktionsdefinitionen sein.

Beispiel I.2.1 (zur Motivation): (i) Sei $f\colon \mathbb{N} \to \mathbb{N}$ die Funktion, die durch $f(0) = 1$ und $f(n + 1) = f(n)(n + 1)$ definiert ist. Diese Funktion wird oft „Fakultät“ genannt.

(ii) Sei $g\colon \mathbb{N} \to \mathbb{N}$ diejenige Funktion, die definiert ist durch $g(0) = 1$ und $g(n+1) = g(n) + (n+1)$. Diese Funktion zählt Punkte mit ganzzahligen Koordinaten in einem gleichschenkligen Dreieck mit Schenkellänge n. Die zugehörigen Funktionswerte werden auch Dreieckszahlen genannt.

Definition I.2.2 (Binäre Relation): Seien M und N zwei Mengen. Eine Teilmenge R von $M \times N = \{(m,n) \mid m \in M, n \in N\}$ heißt *binäre Relation*.

Definition I.2.3 (Eigenschaften von Relationen): Seien M eine nichtleere Menge und R eine Relation auf M, d. h. R sei eine Teilmenge von $M \times M$.

(i) Falls für jedes Element m von M das Paar (m,m) zu R gehört, dann heißt R *reflexiv*.

(ii) Falls für jedes Element (m,n) von R auch (n,m) zu R gehört, dann heißt R *symmetrisch*.

(iii) Falls für jedes Element (m,n) von R, für das (n,m) ebenfalls zu R gehört schon $m = n$ gilt, dann heißt R *antisymmetrisch*.

(iv) Falls für alle Elemente (m,n) und (n,k) von R auch (m,k) zu R gehört, dann heißt R *transitiv*.

Definition I.2.4 (Spezielle Relationen): Seien M eine nichtleere Menge und R eine Relation auf M.

(i) Falls R reflexiv, symmetrisch und transitiv ist, dann heißt R eine *Äquivalenzrelation*.

(ii) Falls R reflexiv, antisymmetrisch und transitiv ist, dann heißt R eine *Ordnungsrelation* oder *partielle Ordnung*.

Definition I.2.5 (Funktion): Seien M und N nichtleere Mengen und es sei $R \subseteq M \times N$ eine Relation. Die Menge

$$D(R) = \{x \in M \mid \text{Es gibt } y \text{ in } N \text{ mit } (x,y) \in M\}$$

heißt *Definitionsbereich der Relation* R und wird mit $D(R)$ bezeichnet.

Falls für jedes x in M und alle y_1 und y_2 in N mit (x,y_1) in R und (x,y_2) in R bereits gilt, dass $y_1 = y_2$, dann heißt R *Funktion auf* $D(R)$. Das ist äquivalent zur Forderung, dass es zu jedem x in $D(R)$ genau ein y in N gebe, sodass (x,y) zu R gehört.

Wir schreiben $R(x) = y$, falls (x,y) zu R gehört, und wir notieren die Funktion R als $R\colon D(R) \to N$.

Satz 1 (über die Rekursion): *Seien x_0 in M und $\{g_n \colon M \to M \mid n \in \mathbb{N}\}$ eine Familie von Funktionen auf $D(g_n) = M$. Dann gibt es genau eine Funktion $f \colon \mathbb{N} \to M$ mit $f(0) = x_0$ und $f(n+1) = g_n(f(n))$.*

Beispiel I.2.6: Aus Satz 1 folgt: In Beispiel I.2.1 erhalten wir wohldefinierte Funktionen durch die angegebene Rekursionsvorschrift.

(i) Wähle $x_0 = 0$ und $g_n \colon x \mapsto x(n+1)$.

(ii) Wähle $x_0 = 1$ und $g_n \colon x \mapsto x + (n+1)$.

Beispiel I.2.7 (Addition und Multiplikation): (i) Es gibt eine eindeutige Funktion $+ \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass für jedes n in $\mathbb{N}$ gilt, dass $+(n, 0) = n$, und sodass für alle natürlichen Zahlen n und m gilt: $+(n, \sigma(m)) = \sigma(+(n, m))$.

(ii) Es gibt eine eindeutige Funktion $\cdot \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass einerseits für jede natürliche Zahl n gilt, dass $\cdot(n, 0) = 0$ und sodass für alle natürlichen Zahlen n und m gilt: $\cdot(n, \sigma(m)) = +(\cdot(n, m), m)$.

Im Folgenden schreiben wir wieder $n + m$ für $+(n, m)$ und $n \cdot m$ für $\cdot(n, m)$; wie gewohnt.

Beweis (Satz 1): Wir zeigen die Behauptung in Schritten. Der erste Schritt wird die Eindeutigkeit, d. h. es gibt höchstens eine Funktion $f \colon \mathbb{N} \to M$, sodass $f(0) = x_0$ und $f(n+1) = g_n(f(n))$. Seien dazu $f_1, f_2 \colon \mathbb{N} \to M$ Funktionen mit dieser Eigenschaft. Wir setzen $A = \{n \in \mathbb{N} \mid f_1(n) = f_2(n)\}$, um einen Induktionsbeweis vorzubereiten. Per Voraussetzung haben wir $f_1(0) = x_0 = f_2(0)$, sodass 0 zu A gehört. Die natürliche Zahl n gehöre zu A. Dann haben wir

$$f_1(\sigma(n)) = g_n(f_1(n)) = g_n(f_2(n)) = f_2(n),$$

wobei die erste Gleichheit per Voraussetzung gilt, die zweite Gleichheit per der Wohldefiniertheit von g_n und Zugehörigkeit von n zu A, und die dritte Gleichung wieder per Voraussetzung. Die Menge A ist deshalb die Menge der natürlichen Zahlen und die Abbildungen f_1, f_2 stimmen überein.

Der zweite Schritt ist die Existenz, d. h., es gibt überhaupt eine Funktion mit den gewünschten Eigenschaften. Dazu formulieren wir die Bedingungen, die die Funktion erfüllen soll, für ihren Graphen und konstruieren über die möglichen Graphen unsere Funktion.

Nach unserer Definition ist eine solche Funktion eine Teilmenge R von $\mathbb{N} \times M$ mit $D(R) = \mathbb{N}$ mit der Eigenschaft, dass für Tupel (n, x) und (n, y) in R schon $x = y$ folgt.

Erfüllt f die gewünschten Bedingungen, so muss für R in $\mathbb{N} \times M$ gelten, dass einerseits $(0, x_0)$ in R liegt, und dass andererseits für (n, x) in R gilt: $(\sigma(n), g_n(x)) \in R$. Es sei

$$\mathfrak{R} = \{R \subseteq \mathbb{N}\times M \mid (0, x_0) \in R, \forall\, n \in \mathbb{N} : ((n, x) \in R) \Longrightarrow ((\sigma(n), g_n(x)) \in R)\}.$$

das System all dieser Teilmengen von $\mathbb{N} \times M$, die die Bedingungen erfüllen, die unsere Funktion erfüllen muss. Wir setzen

$$R_0 = \bigcap_{R\in\mathfrak{R}} R = \{(n, x) \in \mathbb{N} \times M \mid \forall\, R \in \mathfrak{R} : (n, x) \in R\}.$$

Zunächst gehört R_0 zu $\mathfrak{R}$, denn jedes R in $\mathfrak{R}$ enthält $(0, x_0)$ (und so auch R_0) und für ein Tupel (n, x) in R_0 liegt (n, x) in jedem R aus $\mathfrak{R}$, d. h. in jedem R in $\mathfrak{R}$ ist $(\sigma(n), g_n(x))$ enthalten, und damit gehört $(\sigma(n), g_n(x))$ auch zu R_0.

Es bleibt zu zeigen, dass R_0 eine Funktion ist. Zuerst zeigen wir, dass $D(R_0) = \mathbb{N}$ ist. Sei $B = D(R_0)$. Per Konstruktion gehört 0 zu B, weil $(0, x_0)$ zu R_0 gehört.

Sei nun n ein Element von $D(R)$. Dann gibt es ein x in M, sodass (n, x) in R_0 liegt. Weil R_0 ein Element von $\mathfrak{R}$ ist, liegt $(\sigma(n), g_n(x))$ in R_0, sodass auch $\sigma(n)$ zu B gehört. Per vollständiger Induktion folgt $B = \mathbb{N}$.

Schließlich zeigen wir, dass jedes Element von B nur ein Bild bekommt. Das zeigen wir durch vollständige Induktion. Sei dazu

$$C = \{n \in \mathbb{N} \mid \forall\, x, x' \in M : ((n, x) \in R_0 \wedge (n, x') \in R_0) \Longrightarrow (x = x')\}.$$

Angenommen, in R_0 gäbe es ein Tupel $(0, x_0')$, sodass x_0' ungleich x_0 ist. Sei $R_0' = R_0 - \{(0, x_0')\}$. Da $(0, x_0)$ zu R_0 gehört, und da per Voraussetzung $(0, x_0') \neq (0, x_0)$ gilt, liegt $(0, x_0)$ in R_0'. Wir haben für jede natürliche Zahl n und jedes Element x von M: Gehört (n, x) zu R_0', dann erst recht zu R_0. In R_0 liegt dann auch $(\sigma(n), g_n(x))$, und da 0 kein Nachfolger ist, gehört $(\sigma(n), g_n(x))$ auch zu R_0'. Das heißt, dass auch R_0' zu $\mathfrak{R}$ gehört. Das widerspricht aber der Minimalität von R_0, es kann also kein solches Tupel $(0, x_0') \neq (0, x_0)$ in R_0 geben.

Sei nun n ein Element von C. Wir haben bereits gezeigt, dass $D(R_0)$ die ganzen natürlichen Zahlen sind, d. h. zu n gibt es ein x in M mit (n, x) in R_0. Per Rekursionsvorschrift gehört auch $(\sigma_n, g_n(x))$ zu R_0. Angenommen, $\sigma(n)$ würde nicht zu C gehören. Das hieße es gäbe y in $M - \{g_n(x)\}$, sodass $(\sigma(n), y)$ in R_0 liegt. Wir setzen $R_0' = R_0 - \{(\sigma(n), y)\}$ und rechnen wir im vorherigen Schritt nach, dass R_0' die Rekursionsvorschrift erfüllt. Da wir $(0, x_0)$ nicht entfernt haben, ist $(0, x_0)$ weiterhin ein Element von R_0'. Sei (k, x) ein Element von R_0'. Dann gehört auch $(\sigma(k), g_k(x))$ zu R_0', denn sonst wäre ja

$(\sigma(k), g_k(x)) = (\sigma(n), y)$, was bedeuten würde, dass $k = n$ und $g_n(x) = y$, was wir ausgeschlossen haben. Wir hätten wieder einen Widerspruch zur Minimalität von R_0, d. h. $\sigma(n)$ gehört zu C, die Induktion war erfolgreich und R_0 ist tatsächlich eine Funktion. □

Proposition I.2.8 (Addition und Multiplikation): *Es gibt eine eindeutige Funktion* $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*, sodass für alle natürlichen Zahlen* n *und* m *gilt:*

$$+(n, 0) = n, \qquad +(n, \sigma(m)) = \sigma(+(n, m)).$$

Genau so gibt es eine eindeutige Multiplikation $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*.*

Beweis: Für jede natürliche Zahl n definieren wir eine Funktion „Addition mit n“. Seien n also n eine natürliche Zahl und $x_0 = n$. Der Satz über die Rekursion liefert für die Familie $(g_n\colon \mathbb{N} \to \mathbb{N} \mid n \in \mathbb{N}) = (\sigma\colon \mathbb{N} \to \mathbb{N} \mid n \in \mathbb{N})$ eine Funktion $f_n\colon \mathbb{N} \to \mathbb{N}$ mit $f_n(0) = n$ und $f_n(\sigma(m)) = \sigma(f_n(m))$ wie gewünscht. Nun definieren wir die Funktion $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch $+(n, m) = f_n(m)$. Diese Funktion leistet das Gewünschte.

Auf die gleiche Weise wurde auf dem dritten Übungsblatt bereits gezeigt, dass es eine eindeutige Funktion $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ mit den Eigenschaften $\cdot(n, 0) = 0$, $\cdot(n, \sigma(m)) = \cdot(n, m) + n$ gibt. □

Im Folgenden schreiben wir wieder, wie gewohnt, „$n + m$“ anstelle von „$+(n, m)$“. Genau so für Multiplikation.

3 Das Prinzip des kleinsten Täters

In diesem Abschnitt möchten wir eine Ordnung auf den natürliche Zahlen einführen, und dann das Prinzip des kleinsten Täters formulieren.

Definition I.3.1 (Ordnung): Seien n und m natürliche Zahlen.

(i) Gibt es eine natürliche Zahl k gibt, sodass $m = n + k$, dann schreiben wir „$n \leq m$“.

(ii) Ist $m \leq n$, dann schreiben wir auch $n \geq m$ dafür.

(iii) Ist $n \leq m$ und $n \neq m$, dann schreiben wir $n < m$.

(iv) Für $n < m$ schreiben wir auch $m > n$.

Bemerkung I.3.2 (zu den Ordnungen): Die Relationen „$\leq$“ beziehungsweise „$\geq$“ sind *totale Ordnungsrelationen*, d. h. sie sind reflexiv, antisymmetrisch, transitiv und es gilt beispielsweise für „*leq*“: Sind n und m natürliche Zahlen, dann ist $n \leq m$ oder $m \leq n$. Achtung: Die Relationen „$<$“ und „$>$“ sind keine Ordnungsrelationen.

Proposition I.3.3 (Kürzbarkeit bei Ungleichungen): *Seien k, n und m natürliche Zahlen. Dann gilt:*

(i) *Genau dann ist $k + n \leq m + n$, wenn $k \leq m$ gilt;*

(ii) *Genau dann ist $kn \leq mn$, wenn $k \leq m$ ist.*

Bemerkung I.3.4: Für eine natürliche Zahl n definieren wir die Ordnungsmenge $\mathbb{N}_{\leq n} = \{m \in \mathbb{N} \mid m \leq n\}$, entsprechend für „$<$“. Es folgen ein paar Eigenschaften dieser Ordnungsmengen:

(i) $\mathbb{N}_{\leq 0} = \{0\}$, $\mathbb{N}_{\geq 0} = \mathbb{N}$,

(ii) $\mathbb{N}_{\leq n} = \mathbb{N}_{<n+1}$.

Beweis: Die Aussagen zeigt man sehr ähnlich, wir zeigen deshalb exemplarisch den Beweis für (i).

„$\Longleftarrow$“: Seien k und m natürliche Zahlen mit $k \leq m$. Per Definition gibt es eine natürliche Zahl ℓ, sodass $m = k+\ell$. Deshalb ist $m+n = k+\ell+n = k+n+\ell$. Per Definition von „$\leq$“ ist also $k + n \leq m + n$.

„$\Longrightarrow$“: Seien k, n und m natürliche Zahlen, sodass $k + n \leq m + n$. Dann gibt es eine natürliche Zahl ℓ, sodass $m + n = k + n + \ell = k + \ell + n$. Nach der additiven Kürzungsregel Proposition I.1.7 gilt deshalb $m = k + \ell$, was gerade heißt, dass $k \leq m$ ist. □

Satz 2 (Das Prinzip des kleinsten Täters): *Die natürlichen Zahlen bilden mit der oben definierten Ordnung eine wohlgeordnete Menge, d. h. „$\leq$“ ist eine Totalordnung und jede nichtleere Teilmenge M besitzt ein kleines Element.*[2]

Beispiel I.3.5: Nach Bemerkung I.3.4 ist 0 das kleinste Element unter den natürlichen Zahlen.

[2]Das Element m_0 der nichtleeren Menge M natürlicher Zahlen ist ein kleinstes Element, falls für jedes m in M gilt: $m_0 \leq m$.

Beweis (von Satz 2): Mithilfe vollständiger Induktion zeigen wir die folgende Aussage: „Sei M eine nichtleere Teilmenge der natürlichen Zahlen. Hat M jede natürliche Zahl n nichtleeren Schnitt mit $N_{\leq n}$, dann enthält M ein kleinstes Element."

Für $n = 0$ haben wir $\varnothing \neq M \cap \mathbb{N}_{\leq 0} = M \cap \{0\} \subseteq \{0\}$, sodass 0 zu M gehören muss. Da $0 \leq m$ für jede natürliche Zahl m gilt, gilt das insbesondere für die Elemente von M und 0 ist ein kleinstes Element von M.

Die Aussage gelte für die natürliche Zahl n. Sei also M eine nichtleere Teilmenge der natürlichen Zahlen, sodass $M \cap \mathbb{N}_{\leq n+1}$ nichtleer ist. Ist $n+1$ ein kleinstes Element von M, dann gilt die Behauptung. Sonst muss es ein m in M geben, sodass $m < n + 1$. Nach Bemerkung I.3.4 ist dann $m \leq n$, d. h. m liegt in $M \cap \mathbb{N}_{\leq n}$. Per Induktionsvoraussetzung hat M dann ein kleinstes Element.□

Bemerkung I.3.6: Satz 2 ist wichtig und fundamental. Aus ihm folgt beispielsweise, dass jede natürliche Zahl eine Primfaktorzerlegung hat.

Man kann sogar zeigen, dass Satz 2 äquivalent zum Axiom (P5) ist.

Satz 3 (Schubfachprinzip): *Seien n und m natürliche Zahlen mit $m > n$ und sei $f\colon \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$ eine Abbildung. Dann ist f nicht injektiv, d. h. es gibt a und b aus $\mathbb{N}_{\leq m}$, sodass $f(a) = f(b)$.*

Diese Aussage haben Sie als Übungsaufgabe auf dem dritten Übungsblatt gezeigt.

Bemerkung I.3.7 (Interpretation des Schubfachprinzips): Aus Satz 3 folgt insbesondere: Sind n und m natürliche Zahlen mit $m > n$ und verteilt man m Objekte auf n Schubfächer, dann gibt es mindestens ein Schubfach, in dem mehr als ein Objekt liegt.

4 Die ganzen Zahlen

Sind m und n natürliche Zahlen mit $m \geq n$, dann gibt es eine natürliche Zahl k, sodass $m = n + k$. In diesem Fall können wir auch $m - n$ für k schreiben. Das funktioniert aber nicht, wenn $m < n$.

Diesen Defekt wollen wir beheben und die natürlichen Zahlen so zu einer Menge $\mathbb{Z}$ erweitern, dass in $\mathbb{Z}$ eine Gleichung der Form $m = n + x$ für m und n aus $\mathbb{Z}$ immer eine Lösung x in $\mathbb{Z}$ hat.

Um das zu erreichen, beschreiben wir den Lösungskandidaten k als Paar (m, n) der an der obigen Gleichung beteiligten natürlichen Zahlen. Allerdings gibt es mehrere Gleichungen dieser Art, die dieselbe Lösung k haben. Diese

sollten wir zusammenfassen. Für zwei derartige Gleichungen $m = n + k$ und $m' = n' + k$ haben wir $m + n' = n + k + n' = n + m'$. Das wird der Startpunkt für unsere Bemühungen, die Gleichungen mit derselben Lösung zu einem neuen Objekt zusammenzufassen: Wir betrachten die Äquivalenzrelation

$$(m, n) \sim (m', n') \Longleftrightarrow m + n' = n + m'$$

auf $\mathbb{N} \times \mathbb{N}$. (Achtung, noch haben wir nicht gezeigt, dass es sich um eine Äquivalenzrelation handelt.)

Nebenbei wird diese Konstruktion auch diejenigen Gleichungen zusammenfassen, die zwar die gleiche Lösung haben müssten, die wir in den natürlichen Zahlen aber nicht lösen können. Für diese Sammlungen von Gleichungen führen wir dann im Wesentlichen neue Namen ein.

Erinnerung I.4.1 (Äquivalenzklassen): Seien A eine Menge und „$\sim$“ eine Äquivalenzrelation auf A.

(i) Für ein a aus A heißt die Menge $[a] = \{b \in A \mid a \sim b\}$ die *Äquivalenzklasse von a*.

(ii) Die Menge $A/\sim = \{[a] \mid a \in A\}$ heißt *Menge der Äquialenzklassen*.

(iii) Seien a und a' Elemente von A. Wenn a' zu $[a]$ gehört, dann heißt a' *Repräsentant von* $[a]$.

Erinnerung I.4.2 (Partition von A in seine Äquivalenzklassen): Seien A eine Menge und „$\sim$“ eine Äquivalenzklasse auf A. Dann liegt jedes Element von A in genau einer Äquivalenzklasse, d. h. A ist die disjunkte Vereinigung der Äquivalenzklassen bezüglich „$\sim$“.

Erinnerung I.4.3: Seien A die Menge der natürlichen Zahlen und k eine natürliche Zahl. Dann erklärt „$a \sim b$ genau dann, wenn es eine natürliche Zahl ℓ gibt, sodass $b = a + \ell k$“ eine Äquivalenzrelation auf A. Die Äquivalenzklasse $[a]$ heißt *Kongruenzklasse von a modulo k*. Die Menge der Äquivalenzklassen $\mathbb{N}/\sim$ ist

$$\mathbb{N}/\sim = \{[0], [1], [2], \ldots, [n-1]\}.$$

Für $k = 1$ ist beispielsweise $[0] = \mathbb{N}$ und $\mathbb{N}/\sim = \{[0]\}$. Für $k = 2$ ist $[0]$ die Menge der geraden- und $[1]$ die Menge der ungeraden Zahlen. Die natürlichen Zahlen lassen sich schreiben als $\mathbb{N} = [0] \cup [1]$ und $\mathbb{N}/\sim = \{[0], [1]\}$.

Proposition I.4.4 (Äquivalenzrelation für $\mathbb{Z}$): *Sei $A = \mathbb{N} \times \mathbb{N}$. Die durch*

$$(a_1, b_1) \sim (a_2, b_2) \Longleftrightarrow a_1 + b_2 = a_2 + b_1$$

erklärte Relation ist eine Äquivalenzrelation auf A.

Beweis: Zur Reflexivität: Sei (a, b) ein Tupel natürlicher Zahlen. Dann ist $a + b = b + a$, sodass $(a, b) \sim (a, b)$ und die Relation ist reflexiv.

Zur Symmetrie: Seien (a_1, b_1) und (a_2, b_2) Tupel natürlicher Zahlen mit $(a_1, b_1) \sim (a_2, b_2)$. Das bedeutet

$$a_1 + b_2 = a_2 + b_1 \iff a_2 + b_1 = a_1 + b_2,$$

also gilt auch $(a_2, b_2) \sim (a_1, b_1)$.

Zur Transitivität: Seien (a_1, b_1), (a_2, b_2) und (a_3, b_3) Tupel natürlicher Zahlen und es gelte $(a_1, b_1) \sim (a_2, b_2)$ sowie $(a_2, b_2) \sim (a_3, b_3)$. Per Definition sind also $a_1 + b_2 = a_2 + b_1$ sowie $a_2 + b_3 = a_3 + b_2$. Addieren wir jeweils rechte und linke Seiten, so erhalten wir $a_1 + b_2 + a_2 + b_3 = b_1 + a_2 + b_2 + a_3$. Mit der additiven Kürzungsregel folgt $a_1 + b_3 = b_1 + a_3$ und so $(a_1, b_1) \sim (a_3, b_3)$. □

Definition I.4.5 (Die ganzen Zahlen): Die Menge $\mathbb{N} \times \mathbb{N}/\sim$ der Äquivalenzklassen bezüglich der oben eingeführten Äquivalenzrelation „$\sim$“ nennen wir die *Menge der ganzen Zahlen* und bezeichnen sie mit dem Symbol $\mathbb{Z}$.

Bemerkung I.4.6 (Einbettung der natürlichen Zahlen): Wir haben die natürliche Abbildung $\iota\colon \mathbb{N} \to \mathbb{Z}$, $n \mapsto [(n, 0)]$. Diese Abbildung ist injektiv, wie sie auf dem Übungsblatt zeigen werden. Man spricht von einer *Einbettung*, weil sie eine Kopie der natürlichen Zahlen innerhalb der ganzen Zahlen etabliert, die sich genau so verhält wie die Menge der natürlichen Zahlen selbst.

Für die natürliche Zahl n definieren wir $-n = [(0, n)]$ und erhalten so die disjunkte Zerlegung

$$\mathbb{Z} = \mathbb{N} \cup \{-k \mid k \in \mathbb{N}_{\geq 1}\} = \{[(k, 0)] \mid k \in \mathbb{N}\} \cup \{[(0, k)] \mid k \in \mathbb{N}_{\geq 1}\}$$

der ganzen Zahlen in die bekannten natürlichen Zahlen und die „neuen Zahlen“, die wir hinzugefügt haben.

Im Folgenden möchten wir Addition und Multiplikation auf den ganzen Zahlen definieren. Die ganze Zahl $[(a_1, b_1)]$ interpretieren wir als $a_1 - b_1$; genau so für $[(a_2, b_2)]$. Addieren wir diese ganzen Zahlen, dann möchten wir gerne haben, dass $[(a_1 + a_2, b_1 + b_2)]$ das Ergebnis ist – denn dieses interpretieren wir als $(a_1 + a_2) - (b_1 + b_2)$.

Für das Produkt von $[(a_1, b_1)]$ und $[(a_2, b_2)]$ erwarten wir wegen der symbolischen Rechnung $(a_1 - b_1)(a_2 - b_2) = (a_1a_2 + b_1b_2) - (a_1b_2 + a_2b_1)$ das Ergebnis $[(a_1a_2 + b_1b_2, a_1b_2 + a_2b_1)]$.

Genau so wollen wir die Verknüpfungen nun definieren und überlegen uns anschließend, dass diese Festsetzungen sich überall so verhalten, wie wir das erwarten.

Proposition I.4.7: *Die folgenden Abbildungen sind wohldefiniert und hängen nicht von den gewählten Repräsentanten ab:*

$$+\colon \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}, \qquad ([(a_1,b_1)],[(a_2,b_2)])\longmapsto[(a_1+a_2,b_1+b_2)],$$
$$\cdot\colon \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}, \qquad ([(a_1,b_1)],[(a_2,b_2)])\longmapsto[(a_1a_2+b_1b_2,a_1b_2+a_2b_1)].$$

Beweis: Wir betrachten exemplarisch die Addition, die Multiplikation wird auf einem Übungsblatt näher untersucht. Seien dazu (a_1,b_1), (a_1',b_1'), (a_2,b_2) und (a_2',b_2') Paare natürlicher Zahlen, sodass (a_1,b_1) und (a_1',b_1') sowie (a_2,b_2) und (a_2',b_2') in Relation stehen. Unser Ziel ist es zu zeigen, dass $(a_1,b_1)+(a_2,b_2)$ und $(a_1',b_1')+(a_2',b_2')$ in Relation stehen. Per Definition ist das genau dann der Fall ist, wenn

$$a_1'+a_2'+b_1+b_2 \ = a_1+a_2+b_1'+b_2'.$$

Es gilt nach Voraussetzung, dass $a_1+b_1'=a_1'+b_1$ und $a_2+b_2'=a_2'+b_2$. Addieren wir beide Gleichungen, dann erhalten wir genau die gewünschte Gleichung. □

Proposition I.4.8 (Strukturelle Eigenschaften der Verknüpfungen):

(i) *Die Verknüpfungen „$+$“ und „$\cdot$“ auf den ganzen Zahlen sind assoziativ und kommutativ.*

(ii) *Es gelten die Distributivgesetze, d. h. für alle ganzen Zahlen z_1,z_2,z_3 gilt $(z_1+z_2)z_3=z_1z_3+z_2z_3$.*

(iii) $0=[(0,0)]$ *ist neutrales Element für die Addition, d. h. für jede ganze Zahl z ist $0+z=z=z+0$.*

(iv) $1=[(1,0)]$ *ist neutrales Element der Multiplikation, d. h. für jede ganze Zahl z gilt $1\cdot z=z=z\cdot 1$.*

(v) *Die Menge der ganzen Zahlen ist „nullteilerfrei“, d. h. sind z_1,z_2 ganze Zahlen und ist $z_1z_2=0$, dann ist $z_1=0$ oder $z_2=0$.*

(vi) *Für jede ganze Zahl z ist $0\cdot z=0$.*

Beweis: Wir zeigen exemplarisch die zweite Aussage. Seien dazu $z_1 \ =[(a_1,b_1)]$, $z_2=[(a_2,b_2)]$ und $z_3=[(a_3,b_3)]$. Wir haben

$$\begin{aligned}(z_1+z_2)z_3 &= [(a_1+a_2,b_1+b_2)][(a_3,b_3)]\\ &= [((a_1+a_2)a_3+(b_1\ +b_2)b_3,(a_1+a_2)b_3+(b_1+b_2)a_3)]\end{aligned}$$

und da wir bereits wissen, dass Multiplikation natürlicher Zahlen distributiv ist, erhalten wir

$$\begin{aligned}(z_1+z_2)z_3 &= [(a_1a_3+a_2a_3+b_1b_3+b_2b_3,a_1b_3+a_2b_3+b_1a_3+b_2a_3)]\\ &= [(a_1,b_1)][(a_3,b_3)]+[(a_2,b_2)][(a_3,b_3)]=z_1z_3+z_2z_3.\end{aligned}$$ □

Im Folgenden verwenden wir die Konvention „Punkt vor Strich“, um Klammern zu sparen.

Proposition I.4.9: *Für ganze Zahlen z_1 und z_2 hat die Gleichung $x + z_1 = z_2$ stets genau eine Lösung in den ganzen Zahlen. Das heißt für alle ganzen Zahlen z_1 und z_2 gibt es genau eine ganze Zahl x, sodass $x + z_1 = z_2$.*

Beweis: Seien $z_1 = [(a_1, b_1)]$, $z_2 = [(a_2, b_2)]$ und $x = [(a_3, b_3)]$ ganze Zahlen. Dann gilt

$$\begin{aligned} x + z_1 = z_2 &\iff [(a_3 + a_1, b_3 + b_1)] = [(a_2, b_2)] \\ &\iff a_3 + a_1 + b_2 = b_3 + b_1 + a_2 \\ &\iff [(a_3, b_3)] = [(b_1 + a_2, a_1 + b_2)] \\ &\iff x = [(b_1 + a_2, a_1 \ + b_2)]. \end{aligned}$$

Definition I.4.10 (Differenz): Für ganze Zahlen $z_1 = [(a_1, b_1)]$ und $z_2 = [(a_2, b_2)]$ schreiben wir

$$z_1 - z_2 = [(a_1 \ + b_2, b_1 + a_2)]$$

und nennen $z_1 - z_2$ die *Differenz von z_1 und z_2*.

Die Differenz $z_1 - z_2$ ist die eindeutig bestimmte ganze Zahl, die die Gleichung $x + z_1 = z_2$ löst. Insbesondere für $z = [(a, b)]$ gilt $z - z = [(a+b, a+b)] = [(0, 0)]$.

Proposition I.4.11 (Additive Inverse):

(i) *Für jede ganze Zahl z_1 gibt es genau eine ganze Zahl z_2, sodass $z_1 + z_2 = 0$, d. h. jede ganze Zahl hat ein additives Inverses. In dieser Situation schreiben wir $-z_1 = z_2$. Insbesondere gilt $0 - z_1 \ = -z_1$.*

(ii) *Für alle ganzen Zahlen z_1 und z_2 gilt $z_2 - z_1 = z_2 + (-z_1)$.*

(iii) *Für jede ganze Zahl z ist $(-1)z = -z$.*

Beweis: (i) Folgt direkt aus Proposition I.4.9.

(ii) Wir verwenden, dass $z_1 + (-z_1) = 0 = (-z_1) + z_1$. Da $z_2 - z_1$ die eindeutige Lösung der Gleichung $z_1 \ + x = z_2$ ist, genügt es zu überprüfen, dass $z_2 \ + (-z_1)$ ebenfalls Lösung der Gleichung ist. Es gilt $z_1 + z_2 + (-z_1) = 0 + z_2 = z_2$.

(iii) Wegen $z = 1 \cdot z$ erhalten wir nach dem Distributivgesetz, dass

$$z + (-1)z = 1 \cdot z + (-1)z = (1 + (-1))z = 0 \cdot z = 0.$$

Das zeigt, dass $(-1)z$ ebenfalls ein additives Inverses von z ist. Man überlegt sich leicht, dass Inverse eindeutig sind. □

Insgesamt haben wir mit den Aussagen Proposition I.4.8 und I.4.11 gezeigt: Erstens ist $(\mathbb{Z}, +)$ eine Gruppe, d. h. „+“ ist assoziativ, besitzt ein neutrales Element und jedes Element besitzt ein Inverses. Außerdem ist die Gruppe abelsch, d. h. die Verknüpfung „+“ ist zusätzlich kommutativ.

Zweitens ist $(\mathbb{Z}, +, \cdot)$ ein (unitärer) Ring, d. h. $(\mathbb{Z}, +)$ ist eine abelsche Gruppe, $(\mathbb{Z}, \cdot)$ ist ein Monoid, was bedeutet, dass „$\cdot$“ ist assoziativ und es gibt ein neutrales Element, und es gelten die Distributivgesetze.

Nun bleibt die Ordnung „$\leq$“ auf die Menge der ganzen Zahlen fortzusetzen. Seien $[(a_1, b_1)]$ und $[(a_2, b_2)]$ ganze Zahlen. Diese interpretieren wir als $a_1 - b_1$ respektive $a_2 - b_2$ und für $a_1 - b_1 \leq a_2 - b_2$ wie gewohnt müssen wir haben, dass $a_1 + b_2 \leq a_2 + b_1$. Genau so wollen wir eine Relation auf $\mathbb{Z}$ definieren.

Definition I.4.12 (Ordnung für ganze Zahlen): Auf der Menge der ganzen Zahlen $\mathbb{Z}$ definieren wir durch

$$[(a_1, b_1)] \leq [(a_2, b_2)] \Longleftrightarrow a_1 + b_2 \leq a_2 + b_1$$

eine Relation „$\leq$“.

Diese Festsetzung ist unabhängig von den gewählten Vertretern und erklärt eine Ordnungsrelation auf $\mathbb{Z}$. Wie schon für die natürlichen Zahlen verwenden wir die Symbole „$\geq$“, „$<$“ und „$>$“.

Proposition I.4.13 (Eigenschaften der Ordnung):

(i) *Die Ordnungsrelation „$\leq$“ auf $\mathbb{Z}$ setzt die Ordnung auf $\mathbb{N}$ fort, d. h. für natürliche Zahlen n_1 und n_2 gilt $n_1 \leq n_2$ genau dann, wenn $\iota(n_1) \leq \iota(n_2)$.*

(ii) *Für ganze Zahlen z_1 und z_2 gilt $z_1 \leq z_2$ genau dann, wenn $z_2 - z_1 \geq 0$.*

(iii) *Für ganze Zahlen z_1, z_2, z_3 gilt $z_1 \leq z_2$ genau dann, wenn $z_1 + z_2 \leq z_2 + z_3$.*

(iv) *Für ganze Zahlen z_1, z_2 und eine von Null verschiedene natürliche Zahl n gilt $z_1 \leq z_2$ genau dann, wenn $nz_1 \leq nz_2$.*

(v) *Für ganze Zahlen z_1, z_2 und z_3, wobei $-z_3$ in $\mathbb{N}_{\geq 1}$ liegt, gilt $z_1 \leq z_2$ genau dann, wenn $z_3 z_2 \geq z_3 z_1$.*

(vi) *Für ganze Zahlen z_1 und z_2 gilt: Sind $z_1, z_2 \geq 0$, dann ist $z_1 z_2 \geq 0$; sind $z_1, z_2 \leq 0$, dann ist $z_1 z_2 \geq 0$; ist $z_1 \geq 0$ und $z_2 \leq 0$, dann ist $z_1 z_2 \leq 0$.*

(vii) *Für jede natürliche Zahl n gilt $[(n, 0)] \geq 0$ und $[(0, n)] \leq 0$.*

(viii) *Die Relation „$\leq$“ ist eine totale Ordnungsrelation auf den ganzen Zahlen.*

Die Aussagen sind durch direktes Nachrechnen zu zeigen und werden teilweise auf Blatt 7 als Übungsaufgaben nachzurechnen sein.

5 Die rationalen Zahlen

Bis jetzt haben wir die natürlichen Zahlen rigoros über die Peano-Axiome eingeführt und anschließend Addition, Multiplikation und Ordnung studiert. Dabei sind wir auf das Problem gestoßen, dass wir Gleichungen der Bauart $b + x = a$ mit natürlichen Zahlen a und b nicht in den natürlichen Zahlen lösen können, wenn a kleiner als b ist.

Dem Ansatz folgend, jeder solchen Gleichung eine Lösung zu verschaffen, haben wir die ganzen Zahlen konstruiert: Zwei Gleichungen $b + x = a$ und $b' + x = a'$ haben genau dann die gleiche Lösung (wenn es eine gibt), falls $a + b' = a + b'$ ist. Deshalb haben wir $\mathbb{Z}$ definiert als $\mathbb{N} \times \mathbb{N}/\sim$, wobei $(a, b) \sim (a', b')$, wenn $a + b' = a' + b$. In den ganzen Zahlen können wir Gleichungen der Form $b + x = a$ immer eindeutig lösen – sogar für ganze Zahlen a und b.

Im Anschluss haben wir auf den ganzen Zahlen wieder Addition, Multiplikation und Ordnung eingeführt und untersucht.

In den ganzen Zahlen gibt es nun einen neuen Typ Gleichung, der üblicherweise keine Lösung besitzt: Sind a und b ganze Zahlen, $b \neq 0$, dann können wir meistens keine ganzzahlige Lösung von $bx = a$ angeben.

Genau dann haben die Gleichungen $bx = a$ und $b'x = a'$, $b, b' \neq 0$, dieselbe Lösung, wenn $ab' = a'b$. Im Folgenden konstruieren wir mithilfe der zugehörigen Äquivalenzrelation die Menge der rationalen Zahlen $\mathbb{Q}$.

Bemerkung I.5.1: Die Gleichung $2x = 1$ hat keine Lösung x in der Menge der ganzen Zahlen $\mathbb{Z}$.

Beweis: Für $x = 0$ erhielten wir $1 = 2x = 2 \cdot 0 = 0$, das heißt $x = 0$ ist keine Lösung der Gleichung.

Angenommen, es gäbe eine ganze Zahl x, die die angegebene Gleichung löst. Wir wissen bereits, dass x von Null verschieden sein müsste. Wegen Bemerkung I.4.6 und Proposition I.4.13(vii) müsste $x > 0$ oder $x < 0$ sein.

Für $x < 0$ erhielten wir $1 = 2x < 2 \cdot 0 = 0$ wegen Proposition I.4.13(i) und I.4.8(vi), was Proposition I.4.13(vii) widerspräche.

Wir dürfen also $x > 0$ annehmen. Aus Proposition I.4.13(vii) wissen wir deshalb, dass x eine von Null verschiedene natürliche Zahl sein müsste. Es gäbe deshalb nach Proposition I.1.3 eine natürliche Zahl y, sodass $x = \sigma(y) = y + 1$. Insbesondere wäre $y + 1 > 0$, was nach Bemerkung I.3.4 (ii) äquivalent zu $y \geq 0$ ist. Das bedeutet: $x = y + 1$ wäre mindestens 1. Wir erhielten also

$$1 = 2x \geq 2 \cdot 1 = 2 = 1 + 1,$$

nach Proposition I.4.13(iv) und der Definition von 2, sodass $1 = 2$ folgen müsste. □

Bemerkung I.5.2: Seien a, a', b, b' ganze Zahlen und seien b, b' von Null verschieden.

(i) Die Gleichung $bx = a$ hat höchstens eine Lösung.

(ii) Angenommen, $bx = a$ besitzt eine Lösung. Genau dann hat $b'x = a'$ dieselbe Lösung, wenn $ab' = a'b$ gilt.

Beweis: (i) Angenommen, wir hätten ganze Zahlen x_0, x_1, die unsere Gleichung lösen; d. h. $bx_0 = a = bx_1$. Dann hätten wir $0 = a - a = bx_0 - bx_1 = b(x_0 - x_1)$ nach Proposition I.4.8 und der Definition von „$-$“. Wegen $b \neq 0$ müsste nach der Nullteilerfreiheit von $\mathbb{Z}$ gelten, dass $x_0 - x_1 = 0$ (Proposition I.4.8), also $x_0 = x_1$ per Definition von „$-$“.

(ii) „$\Longrightarrow$“: Angenommen, die Lösung x_0 wäre von Null verschieden. Dann wäre $bx_0 = a$ und $b'x_0 = a'$, weshalb $bx_0a' = aa' = b'x_0a$ gälte. Daraus könnten wir mithilfe von Proposition 4.8(v) folgern, dass $ba' = b'a$.

Für $x_0 = 0$ wäre $a = bx_0 = b \cdot 0 = 0$ und analog $a' = 0$. Es würde also $ab' = 0 = a'b$ folgen, wie gewünscht.

„$\Longleftarrow$“: Angenommen, es gälte $ab' = a'b$ sowie $bx_0 = a$.

Für $a \neq 0$ hätten wir $b'x_0a = bx_0a' = aa' = a'a$, sodass $b'x_0 = a'$ nach Proposition I.4.8 (v) folgen würde.

Für $a = 0$ hätten wir $a'b = 0$, sodass nach Proposition I.4.8(v) $a' = 0$ folgen würde. Wiederum aus Proposition I.4.8 (v) würde aus $bx_0 = a = 0$ folgen, dass $x_0 = 0$ und $b'x_0 = b'0 = 0 = a'$. □

Proposition I.5.3 (Die Quotientenrelation): *Die auf* $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ *durch*

$$(a_1, b_1) \sim (a_2, b_2) \Longleftrightarrow a_1b_2 = a_2b_1$$

erklärte Relation ist eine Äquivalenzrelation.

Man zeigt diese Aussage wie üblich. Beim Nachweis der Transitivität muss man jedoch Fälle unterscheiden um zu verhindern, dass „Nenner“ Null werden. Seien (a_1, b_1), (a_2, b_2) und (a_3, b_3) Tupel mit $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$. Das bedeutet $a_1b_2 = a_2b_1$ und $a_2b_3 = a_3b_2$, d. h. $a_1b_2a_2b_3 = b_1a_2b_2a_3$.

Ist $a_2b_2 \neq 0$, dann folgt aus Proposition I.4.8(v), dass $a_1b_3 = a_3b_1$, also $(a_1, b_1) \sim (a_3, b_3)$.

Ist $a_2b_2 = 0$, dann ist $a_2 = 0$ wegen Proposition I.4.8(v). Damit wären $a_1b_2 = a_2b_1 = 0$ und $a_3b_2 = a_2b_3 = 0$. Wiederum aus Proposition I.4.8(v) folgt $a_1 = 0 = a_3$, sodass $a_1b_3 = a_3b_1$ und $(a_1, b_1) \sim (a_3, b_3)$.

Wir halten fest, dass insbesondere gilt: Sind a_1, b_1, z ganze Zahlen, sodass b_1 und z von Null verschieden sind, dann ist $(a_1z, b_1z) \sim (a_1, b_1)$.

Definition I.5.4 (Die rationalen Zahlen): Wir nennen die Menge der Äquivalenzklassen $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ der Relation aus I.5.3 die *Menge der rationalen Zahlen* $\mathbb{Q}$.

In diese Sprache übersetzt liest sich die Bemerkung von oben wie folgt: Für a_1, b_1, z aus $\mathbb{Z}$, $b_1, z \neq 0$, gilt $[(a_1, b_1)] = [(a_1 z, b_1 z)]$.

Wir fassen die Menge der ganzen Zahlen $\mathbb{Z}$ via der injektiven Abbildung

$$\mathbb{Z} \hookrightarrow \mathbb{Q}, \qquad a \longmapsto [(a, 1)]$$

als Teilmenge der Menge der rationalen Zahlen auf.

Proposition I.5.5:

(i) *Die Verknüpfungen* $+, \cdot \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$*, die durch*

$$[(a_1, b_1)] + [(a_2, b_2)] = [(a_1 b_2 + a_2 b_1, b_1 b_2)],$$
$$[(a_1, b_1)] \cdot [(a_2, b_2)] = [(a_1 a_2, b_1 b_2)]$$

definiert werden, sind wohldefiniert, d. h. unabhängig von den gewählten Repräsentanten.

(ii) *Die Verknüpfungen „$+$“ und „$\cdot$“ sind kommutativ und assoziativ. Es gelten die Distributivitätsgesetze.*

(iii) *Für jedes x in $\mathbb{Q}$ gilt $x + 0 = x$ und $x \cdot 1 = x$. Hierbei ist $0 = [(0, 1)]$ und $1 = [(1, 1)]$.*

(iv) *Für jedes x in $\mathbb{Q}$ gibt es genau ein y in $\mathbb{Q}$ mit $x + y = 0$. Für jedes x in $\mathbb{Q} - \{0\}$ gibt es genau ein y in $\mathbb{Q}$ mit $xy = 1$.*

Man zeigt alle diese Aussagen einfach durch Nachrechnen. Für Teil (iv) möchten wir trotzdem die Inversen festhalten. Dazu schreiben wir $x = [(a_1, b_1)]$ für ganze Zahlen a_1, b_1 mit $b_1 \neq 0$. Dann gilt für $y = [(-a_1, b_1)]$, dass $x + y = 0$. Ist $x \neq 0$, dann ist auch $a_1 \neq 0$ und für $y = [(b_1, a_1)]$ gilt $xy = 1$.

Notation I.5.6: Für eine rationale Zahl $x = [(a_1, b_1)]$ bezeichnen wir mit $-x = [(-a_1, b_1)]$ das eindeutige additive Inverse, und falls x von Null verschieden ist, dann bezeichnen wir mit $1/x = [(b_1, a_1)]$ das multiplikative Inverse.

Korollar I.5.7: *Seien a und b rationale Zahlen, $b \neq 0$. Dann hat die Gleichung $bx = a$ eine eindeutige Lösung, nämlich $(1/b) \cdot a$.*

Beweis: Es gilt $b \cdot (1/b) \cdot a = 1 \cdot a = a$. □

Notation I.5.8 (Bruchschreibweise): Für ganze Zahlen a und b, $b \neq 0$, schreiben wir im Folgenden $a/b = [(a, b)]$.

Sind x und y rationale Zahlen, $y \neq 0$, dann schreiben wir im Folgenden $x/y = x \cdot (1/y)$.

Für rationale Zahlen x und y schreiben wir $x - y$ für $x + (-1)y$.

Wir halten fest, dass die Schreibweisen a/b und $x/y = x \cdot (1/y)$ von oben miteinander verträglich sind. Sind nämlich a und b ganze Zahlen mit $b \neq 0$, dann ist $1/[(b, 1)] = [(1, b)]$, sodass

$$\frac{[(a,1)]}{[(b,1)]} = [(a,1)] \cdot [(1,b)] = [(a,b)] = \frac{a}{b}.$$

Bemerkung I.5.9 (Rechengesetze): Mit der Notation aus I.5.8 erhalten wir vertraute Rechengesetze. Für rationale Zahlen w, x, y, z und $a,\ z, w, a \neq 0$, gilt:

(i) Für $v = x/z$ ist $-v = -x/z$ und $1/v = z/x$.

(ii) $x/z \cdot y/w = xy/zw$,

(iii) $x/z + y/w = (xw + yz)/zw$,

(iv) $(xa)/(za) = x/z$,

(v) $-x = 0 - x = (-1)x$.

Definition I.5.10 (Ordnung auf den rationalen Zahlen): Seien $x = x_1/x_2$ und $y = y_1/y_2$ rationale Zahlen, d. h. x_i, y_i sind ganze Zahlen und x_2, y_2 sind von Null verschieden.

(i) Durch $0 \leq x$ genau dann, wenn $0 \leq x_1, x_2$ oder $x_1, x_2 \leq 0$ und $x \leq y$ genau dann, wenn $0 \leq x - y$ wird eine Ordnungsrelation auf $\mathbb{Q}$ erklärt. Analog zu Definition I.3.1 erklärt man „$\leq$“, „$>$“, „$<$“.

(ii) Die Abbildung

$$|\colon|\colon \mathbb{Q} \longrightarrow \mathbb{Q}_{\geq 0} = \{x \in \mathbb{Q} \mid x \geq 0\}, \qquad |x| = \begin{cases} x, & \text{falls } x > 0, \\ 0, & \text{falls } x = 0, \\ -x, & \text{falls } x < 0 \end{cases}$$

heißt *Betrag* oder *Betragsfunktion*.

(iii) Die durch $d(x, y) = |x - y|$ definierte Funktion $d\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_{\geq 0}$ heißt *Abstandsfunktion*.

Proposition I.5.11: *Es gelten die analogen Eigenschaften von „$\leq$“ aus Proposition I.4.13:*

(i) *„$\leq$“ setzt die Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$ fort.*[3]

(ii) *„$\leq$“ ist eine Totalordnung.*

(iii) *Für rationale Zahlen x, y gilt $x \leq y$ genau dann, wenn für alle rationalen Zahlen z gilt, dass $x + z \leq y + z$.*

(iv) *Für rationale Zahlen x, y gilt $x \leq y$ genau dann, wenn für alle positiven rationalen Zahlen z gilt, dass $xz \leq yz$.*

(v) *Für rationale Zahlen x, y gilt $x \leq y$ genau dann, wenn für alle negativen rationalen Zahlen z gilt, dass $xz \geq yz$.*

(vi) *Für rationale Zahlen x, y gilt: Sind x, y nichtnegativ, dann auch xy; sind x, y nichtpositiv, dann auch xy, und sind x nichtnegativ, y nichtpositiv, dann ist xy nichtpositiv.*

(vii) *Wir haben die disjunkte Zerlegung $\mathbb{Q} = \mathbb{Q}_{<0} \cup \{0\} \cup \mathbb{Q}_{>0}$.*

All diese Eigenschaften zeigt man durch direktes Nachrechnen mit Methoden, wie wir sie bereits gesehen haben.

6 Dezimalbruchentwicklung rationaler Zahlen

Satz 4 (Division mit Rest): *Seien a und b ganze Zahlen, b von Null verschieden. Dann gibt es ganze Zahlen q und r, sodass $0 \leq r < |b|$, sodass $a = qb + r$. Die Teilnehmer q und r sind dabei eindeutig.*

Sind a und b natürliche Zahlen, dann ist auch q eine natürliche Zahl.

Beweis: Zuerst zeigen wir die Existenz der Zahlen q und r. Dazu definieren wir eine Funktion $r\colon \mathbb{Z} \to \mathbb{Z}$, $q \mapsto a - qb$. Per Definition ist $r(0) = a$. Die Menge $M(a, b) = \{r(q) \mid q \in \mathbb{Z}, qb \leq a\} \subseteq \mathbb{N}$ ist deshalb eine nichtleere Teilmenge der natürlichen Zahlen und wir können das Prinzip des kleinsten Täters verwenden, um ein kleinstes Element $r_0 = r(q_0)$ in $M(a, b)$ zu erhalten. Wir haben also $r_0 = a - q_0 b$, also $a = q_0 b + r_0$. Es bleibt zu zeigen, dass $0 \leq r_0 < |b|$. Wegen $q_0 b \leq a$ folgt zunächst $0 \leq r_0 = a - q_0 b$.

Angenommen, r_0 wäre mindestens $|b|$. Dann wäre $r_1 = r_0 - |b| \geq 0$ und $r_0 - r_1 = |b| > 0$, sodass $0 \leq r_1 < r_0$. Außerdem gilt

$$r_1 = r_0 - |b| = \begin{cases} a - (q_0 + 1)b = r(q + 1), & \text{falls } b > 0, \\ a - (q_0 - 1)b = r(q - 1), & \text{falls } b < 0, \end{cases}$$

[3] Hierbei fassen wir $\mathbb{Z}$ vermöge $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $x \mapsto x/1$ als Teilmenge von $\mathbb{Q}$ auf.

was der Wahl von r_0 widerspräche.

Als zweites zeigen wir die Eindeutigkeit der Teilnehmer q und r. Angenommen, wir hätten Gleichungen $a = q_1 b + r_1$ und $a = q_2 b + r_2$ mit ganzen Zahlen q_i, r_i, sodass $0 \leq r_1, r_2 < |b|$.

Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $r_2 \geq r_1$. Da wir zeigen wollen, dass r_1 und r_2 gleich sind, nehmen wir an, r_2 wäre echt größer als r_1. Dann wäre $0 < r_2 - r_1 = (q_1 - q_2)b$, weshalb $q_1 \neq q_2$ folgen muss.

Die von Null verschiedene natürliche Zahl $|q_1 - q_2|$ ist mindestens 1, woraus folgt: $r_2 - r_1 = |r_2 - r_1| = |q_1 - q_2||b| \geq |b|$. Wegen $r_2 - r_1 \leq r_2 < |b|$ kann das nicht sein. □

Proposition I.6.1 (Dezimalbruchzerlegung natürlicher Zahlen): *Für jede natürliche Zahl n gibt es eine natürliche Zahl ℓ und $a_1, \ldots, a_\ell$ aus $\{0, 1, \ldots, 0\}$, sodass $n = \sum_{i=0}^{\ell} a_i 10^i$.*

Beweis: Für die natürliche Zahl ℓ definieren wir die Menge

$$M_\ell = \{n \in \mathbb{N} \mid 10^\ell \leq n < 10^{\ell+1}\}.$$

Dann zerfällt $\mathbb{N}_{\geq 1}$ in die disjunkte Vereinigung $\mathbb{N}_{\geq 1} = \dot{\bigcup}_{\ell \in \mathbb{N}} M_\ell$. Für 0 tut $0 = 0 \cdot 10^0$ das Gewünschte.

Wir zeigen nun durch vollständige Induktion über ℓ, dass die Behauptung für jede n aus M_ℓ gilt.

Für $\ell = 0$ ist $M_0 = \{n \in \mathbb{N} \mid 0 \leq n < 10^1 = 10\} = \{n \in \mathbb{N} \mid 0 \leq n \leq 9\}$ und $\ell = 0$, $a_0 = n$ liefert die Darstellung $n = n \cdot 1 = a_0 10^0$ wie gewünscht.

Die Aussage gelte für die natürliche Zahl ℓ und n sei eine natürliche Zahl in $M_{\ell+1}$. Dann gilt $10^{\ell+1} \leq n < 10^{\ell+2}$. Nach Satz 4 können wir mit Rest durch $10^{\ell+1}$ teilen, d. h. es gibt natürliche Zahlen q und r, sodass $n = q \cdot 10^{\ell+1} + r$ und $0 \leq r < 10^{\ell+1}$. Wäre $q \geq 10$, dann hätten wir $n = q10^{\ell+1} + r \geq 10^{\ell+2} + r \geq 10^{\ell+2}$, was nicht mehr in $M_{\ell+1}$ läge. Es muss also q in $\{0, \ldots, 9\}$ liegen. Das heißt wir setzen $a_{\ell+1} = q$ und wenden die Induktionsvoraussetzung auf r in $\bigcup_{j=0}^{\ell} M_\ell$ an, um Zahlen $a_0, \ldots, a_\ell$ in $\{0, \ldots, 9\}$ zu erhalten, sodass $r = \sum_{i=0}^{\ell} a_i 10^i$. Damit ist

$$n = a_{\ell+1} 10^{\ell+1} + \sum_{i=0}^{\ell} a_i 10^i = \sum_{i=0}^{\ell+1} a_i 10^i.$$

□

Bemerkung I.6.2: Verlangt man in Proposition I.6.1 für $n \neq 0$, dass $a_\ell \neq 0$ und für $n = 0$, dass $\ell = 0$ und $a_0 = 0$, dann sind ℓ und $a_0, \ldots, a_\ell$ für n eindeutig bestimmt. Das liegt daran, dass die Vereinigung $\dot{\bigcup}_{\ell \in \mathbb{N}} M_\ell$ disjunkt ist.

Im Folgenden möchten wir untersuchen, wie wir einen Bruch $x = x_1/x_0$ mit $0 \leq x < 1$ schreiben können als $x = a_{-1}\frac{1}{10} + a_{-2}\frac{1}{10^2} + \cdots$.

Beispiel I.6.3 (Dezimaldarstellung für zwei Brüche): (i) Sei $x = \frac{3}{25}$. Im ersten Schritt schreiben wir $x = \frac{3}{25} = a_{-1}\frac{1}{10} + r_{-1}$ mit $0 \leq r_{-1} < \frac{1}{10}$. Diese Gleichung ist äquivalent zu $3 \cdot 10^{-1} = a_{-1}25 + \tilde{r}_{-1}$ mit $\tilde{r}_{-1} = 25 \cdot 10 \cdot r_{-1}$, und damit $0 \leq \tilde{r}_{-1} < 25$.

Aus Satz 4 folgt $30 = 1 \cdot 25 + 5$, d. h. $a_{-1} = 1$, $\tilde{r}_{-1} = 5$ und $r_{-1} = \frac{5}{25 \cdot 10^1}$. Zusammenfassend haben wir im ersten Schritt erhalten, dass

$$\frac{3}{25} = 1 \cdot \frac{1}{10} + \frac{5}{25 \cdot 10^1}.$$

Im zweiten Schritt zerlegen wir r_{-1} weiter und erhalten

$$r_{-1} = \frac{5}{25 \cdot 10} = a_{-2} \cdot \frac{1}{10^2} + r_{-2},$$

wobei $0 \leq r_{-2} < \frac{1}{10^2}$. Genau wie zuvor erkennen wir, dass diese Gleichung äquivalent ist zu

$$5 \cdot 10 = a_{-2} \cdot 25 + \tilde{r}_{-2}$$

für $\tilde{r}_{-2} = r_{-2} \cdot 25 \cdot 10^2$ und $0 \leq \tilde{r}_{-2} < 25$. Division mit Rest zeigt $50 = 2 \cdot 25 + 0$, sodass $a_{-2} = 2$, $\tilde{r}_{-2} = 0$ und $r_{-2} = 0$. Insgesamt folgt

$$x = \frac{3}{25} = 1\frac{1}{10} + 2\frac{1}{10^2},$$

was wir als $x = 0.12$ schreiben.

(ii) Sei $x = \frac{5}{11}$. Im ersten Schritt schreiben wir $\frac{5}{11} = a_{-1}\frac{1}{10} + r_{-1}$ mit $0 \leq r_{-1} < \frac{1}{10}$. Ausräumen der Nenner führt auf die Gleichung $5 \cdot 10 = a_{-1}11 + \tilde{r}_1$, was auf die Lösung $a_{-1} = 4$ und $\tilde{r}_{-1} = 6$ führt, sodass $r_{-1} = \frac{6}{10 \cdot 11}$.

Im zweiten Schritt schreiben wir $r_{-1} = \frac{6}{10 \cdot 11} = a_{-2}\frac{1}{10^2} + r_{-2}$ für ein $0 \leq r_{-2} < \frac{1}{10^2}$. Das führt auf die ganzzahlige Gleichung $6 \cdot 10 = a_{-2}11 + \tilde{r}_{-2}$, die von $a_{-2} = 5$ und $\tilde{r}_{-2} = 5$ gelöst wird. Damit ist $r_{-2} = \frac{5}{11 \cdot 10^2}$.

Im dritten Schritt schreiben wir $r_{-2} = \frac{5}{11 \cdot 10^2} = a_{-3}\frac{1}{10^3} + r_{-3}$ für $0 \leq r_{-3} < \frac{1}{10^3}$. Das führt auf die ganzzahlige Gleichung $5 \cdot 10 = a_{-3}11 + \tilde{r}_3$. Diese hat die Lösung $a_{-3} = 4$, $\tilde{r}_3 = 6$, sodass schließlich $r_{-3} = \frac{6}{10^3 \cdot 10}$. Im dritten Schritt haben wir dabei dieselbe Gleichung wie in Schritt 1 gelöst, sodass die Folge der a_{-i}, $i \in \mathbb{N}$, ab hier periodisch wird.

Proposition I.6.4: *Sei $x = x_1/x_2$ eine rationale Zahl für natürliche Zahlen x_1, x_2, $x_2 \neq 0$, sodass $0 \leq x < 1$. Dann gibt es eine Folge $(a_i)_{i \in \mathbb{Z}_{<0}}$, sodass die a_i in $\{0, \ldots, 9\}$ liegen, und für jede natürliche Zahl ℓ ein $0 \leq r_{-\ell} < \frac{1}{10^\ell}$, sodass gilt: $x = \sum_{j=1}^{\ell} a_{-j}\frac{1}{10^j} + r_{-\ell}$.*

Ist j eine natürliche Zahl, dann schreiben wir im Folgenden $10^{-j} = \frac{1}{10^j}$.

Bemerkung I.6.5: (i) Aus Beispiel I.6.3 beziehungsweise Proposition I.6.4 ergibt sich folgende Rechenvorschrift für die Berechnung der Ziffern a_{-j} der Dezimaldarstellung des Bruchs $0 \leq x = p/q < 1$: Wir schreiben $R_0 = p$ und für $i \geq 1$ sind die Zahlen a_{-i} sowie R_{-i} sind eindeutig bestimmt durch die Gleichung

$$10R_{-(i-1)} = a_{-i}q + R_{-i},$$

wobei $R_{-i} \in \{0, \ldots, q-1\}$.

(ii) Die Folge (a_{-i}) wird *periodisch* (ab einer bestimmten Stelle), d. h. es gibt positive natürliche Zahlen N und k, sodass $a_{-i} = a_{-(i+k)}$ für alle $i \geq N$ gilt. Das muss immer so sein, da R_{-i} nur endlich viele Werte annehmen kann und da wir die Rekursionsvorschrift haben.

Mithilfe von Proposition I.6.4 möchten wir im Folgenden die Dezimalbruchzerlegung definieren und die Konvergenz der unendlichen Summe $\sum_{j=1}^{\infty} a_{-j}10^{-j}$ zeigen.

Wir erinnern uns daran, dass $(\mathbb{Q}, \leq)$ eine totalgeordnete Menge ist, auf der wir die Betragsfunktion $|\cdot|$ definiert haben. Mithilfe des Betrages haben wir durch $d(q_1, q_2) = |q_1 - q_2|$ einen Abstandsbegriff auf den rationalen Zahlen definiert.

Bemerkung I.6.6: (i) Für jede rationale Zahl x und jede positive rationale Zahl a gilt $|x| < a$ genau dann, wenn $-a < x < a$.

(ii) Für jede rationale Zahl x gilt $-|x| \leq x \leq |x|$.

Man zeigt die erste Aussage per Fallunterscheidung nach $x \geq 0$ und $x < 0$. Die zweite Aussage ist eine direkte Konsequenz von (i).

Proposition I.6.7 (Betrag als Norm): *Die Betragsfunktion $|\cdot|$ auf den rationalen Zahlen hat folgende Eigenschaften:*

(i) *Für jede rationale Zahl x ist $|x| \geq 0$. Genau dann ist $|x| = 0$, wenn $x = 0$ ist.*

(ii) *Für alle rationalen Zahlen x und y ist $|xy| = |x||y|$.*

(iii) *Für alle rationalen Zahlen x, y und z gilt $|x + y| \leq |x| + |y|$.*

Eigenschaft (i) wird positive Definitheit*, Eigenschaft (ii)* Homogenität *und Eigenschaft (iii)* Dreiecksungleichung *genannt.*

Diese Aussage lässt sich durch direktes Nachrechnen zeigen.

Proposition I.6.8 (Metrik auf den rationalen Zahlen): *Die via* $d(x,y) = |x - y|$ *erklärte Funktion* $d\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_{\geq 0}$ *hat folgende Eigenschaften:*

(i) *Für alle rationalen Zahlen* x *und* y *ist* $d(x,y) \geq 0$ *und* $d(x,y) = 0$ *genau dann, wenn* $x = y$.

(ii) *Für alle rationalen Zahlen* x *und* y *ist* $d(x,y) = d(y,x)$.

(iii) *Für alle rationalen Zahlen* x, y *und* z *ist* $d(x,z) \leq d(x,y) + d(y,z)$.

Dass das stimmt folgt aus der Definition der Funktion d und Proposition I.6.7. Aussage (iii) zeigt man so:

$$d(x,z) = |x - z| = |x - y + y - z| \leq |x - y| + |y - z| = d(x,y) + d(y,z).$$

Eine Norm lässt sich durch die Eigenschaften aus Proposition I.6.7 allgemeiner für Vektorräume über den Körpern $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ definieren.

Eine Metrik lässt sich mit den Eigenschaften aus Proposition I.6.8 allgemeiner auf beliebigen Mengen definieren.

Definition I.6.9 (Konvergenz): Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge rationaler Zahlen, d. h. eine Funktion $x\colon \mathbb{N} \to \mathbb{Q}$, die wir mit der Familie ihrer Bilder $(x(n))_{n\in\mathbb{N}}$ identifizieren und wobei wir x_n statt $x(n)$ schreiben.

(i) Gibt es für jede positive rationale Zahl ε einen Index N in $\mathbb{N}$, sodass $|x_n| < \varepsilon$ für jedes $n \geq N$ gilt, dann heißt $(x_n)_{n\in\mathbb{N}}$ eine *Nullfolge*.

(ii) Ist x eine rationale Zahl und ist $(x_n - x)$ eine Nullfolge, dann sagen wir, $(x_n)_{n\in\mathbb{N}}$ *konvergiert gegen* x.

Bemerkung I.6.10: Für die Folge (a_i) aus Proposition I.6.4 zu $x = p/q$ sei $x_n = \sum_{j=1}^{n} a_{-j}10^{-j}$. Dann konvergiert die Folge $(x_n)_{n\in\mathbb{N}}$ gegen x.

Definition I.6.11 (Dezimaldarstellung): Seien $x = p/q$ eine positive rationale Zahl und $(a_\ell, a_{\ell-1}, a_{\ell-2}, \dots) = (a_i)_{i\in\mathbb{Z}_{\leq \ell}}$ eine Folge mit a_j in $\{0, \dots, 9\}$. Für die natürliche Zahl n, setze $x_n = \sum_{j=0}^{n} a_{\ell-j}10^{\ell-j}$. Falls $(x_n)_{n\in\mathbb{N}}$ gegen x konvergiert, dann heißt die Folge $(a_j)_{j\in\mathbb{Z}_{\leq \ell}}$ eine *Dezimaldarstellung* oder *Dezimalbruchzerlegung von* x. In diesem Fall schreiben wir auch $x = a_\ell a_{\ell-1} \dots a_0, a_{-1}a_{-2} \dots$, falls $\ell \geq 0$, beziehungsweise $x = 0,0 \dots 0a_\ell a_{\ell-1} \dots$, falls $\ell < 0$, oder auch als $x = \sum_{j=0}^{\infty} a_{\ell-j}10^{\ell-j}$.

Für eine negative rationale Zahl $x = p/q$ definieren wir die Dezimalbruchentwicklung über $-x$, wir setzen nämlich $x = -a_\ell a_{\ell-1} \dots a_0, a_{-1}a_{-2} \dots$, falls $\ell \geq 0$, beziehungsweise $x = -0,0 \dots 0a_\ell a_{\ell-1} \dots$, wenn diese Koeffizienten zur Dezimalbruchentwicklungen von $-x$ gehören.

Falls es einen Index N aus den ganzen Zahlen gibt, sodass $a_k = 0$ für alle $k \leq N$, dann heißt die Dezimaldarstellung *abbrechend*.

Bemerkung I.6.12: Proposition I.6.4 und Bemerkung I.6.5 zeigen, dass jede rationale Zahl eine Dezimaldarstellung besitzt. Ferner ist diese Dezimaldarstellung periodisch, denn abbrechende Dezimaldarstellungen sind periodisch mit Periode Null.

Im Folgenden wollen wir uns mit der Frage beschäftigen, wie wir den Zahlbereich erweitern müssen, um für nicht-periodische Ziffernfolgen (a_j) einen Grenzwert für $\sum_{j=0}^{\infty} a_{\ell-j}10^{\ell-j}$ zu erhalten.

7 Die reellen Zahlen

Folgen reeller Zahlen sollten konvergieren, wenn sie Cauchyfolgen sind. Für jede Cauchyfolge wollen wir eine Zahl hinzufügen und diese hinzugefügten Zahlen wollen wir identifizieren, wenn die Differenz der zugehörigen Cauchyfolgen Nullfolgen sind.

Erinnerung I.7.1 (Cauchyfolge): Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge rationaler Zahlen.

(i) Gibt es für jede positive rationale Zahl ε einen (von ε abhängigen) Index N, sodass $d(x_n, x_m)$ für alle natürlichen Zahlen $n, m \geq N$ gilt, dann heißt $(x_n)_{n\in\mathbb{N}}$ eine (rationale) *Cauchyfolge*.

(ii) Wir schreiben $C = \{x = (x_n)_{n\in\mathbb{N}}$ ist rationale Cauchyfolge$\}$ für die Menge der rationalen Cauchyfolgen.

(iii) Sind $x = (x_n)_{n\in\mathbb{N}}$ und $y = (y_n)_{n\in\mathbb{N}}$ rationale Cauchyfolgen und λ eine rationale Zahl, dann definieren wir

$$x \pm y = (x_n \pm y_n)_{n\in\mathbb{N}}, \qquad \lambda x = (\lambda x_n)_{n\in\mathbb{N}}, \qquad x \odot y = (x_n y_n)_{n\in\mathbb{N}}$$

und erhalten so neue Cauchyfolgen.

Definition I.7.2: Auf der Menge der rationalen Cauchyfolgen C wird durch

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \Longleftrightarrow x - y = (x_n - y_n)_{n\in\mathbb{N}} \longrightarrow 0$$

eine Äquivalenzrelation erklärt. Wir nennen die Menge der Äquivalenzklassen $C/\!\sim\, = \mathbb{R}$ die *Menge der reellen Zahlen*.

Bemerkung I.7.3: Zusammen mit „+“ und „$\odot$“ wird C zu einem kommutativen Ring mit neutralen Elementen $0 = (0, 0, \dots)$ und $1 = (1, 1, \dots)$.

Ist $(x_n)_{n\in\mathbb{N}}$ eine Nullfolge, dann ist $(x_n)_{n\in\mathbb{N}}$ erst recht eine Cauchyfolge. Das sieht man so: Sei eine positive rationale Zahl ε gegeben. Dann gibt es

einen Index N, sodass $|x_n| < \varepsilon/2$ für alle $n \geq N$ und per Dreiecksungleichung erhalten wir

$$|x_n - x_m\ | = |x_n - x + x - x_m| \leq |x_n - x| + |x_m - x| = \varepsilon/2 + \varepsilon/2 = \varepsilon$$

für alle $m, n \geq N$.

Wir schreiben $N = \{x = (x_n)$ rationale Nullfolge$\}$ für die Teilmenge von C, die aus den rationalen Nullfolgen besteht. Wir halten fest, dass $x \sim y$ gilt genau dann, wenn $x - y$ zu N gehört.

Vorüberlegung I.7.4: Seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und S eine Teilmenge von R. Auf R definieren wir eine Relation durch „$r_1 \sim r_2$ genau dann, wenn $r_1 - r_2$ in S liegt“ und schreiben

$$R/\sim = \{[r]_\sim = \{r' \in R : r' \sim r\} \mid r \in R\}.$$

Unter welchen Umständen ist „$\sim$“ eine Äquivalenzrelation? Und wenn das so ist: Wann definiert die Ringstruktur auf R eine Ringstruktur auf $R/\sim$? Das heißt: Wann sind die repräsentantenweisen Verknüpfungen auf den Äquivalenzklassen wohldefiniert und wann ist $R/\sim$ mit diesen Verknüpfungen selbst ein Ring?

Zunächst dazu, wann die oben erwähnte Definition eine Äquivalenzrelation ist. Die Relation ist reflexiv, d. h. wir haben für alle r aus R dass $r \sim r$ genau dann, wenn 0 zu S gehört.

Soll die Relation symmetrisch sein, dann brauchen wir für alle r_1, r_2 aus R, für die $r_1 - r_2$ in S liegt, dass $r_2 - r_1\ = -(r_2 - r_1$ zu S gehört. Das ist erfüllt, wenn für jedes s aus S auch $-s$ in S liegt.

Wenn wir wollen, dass die Relation transitiv ist, dann brauchen wir für alle r_1, r_2, r_3 in R mit $r_1 \sim r_2$ und $r_2 \sim r_3$, dass $r_1 \sim r_3$. Per Definition der Relation brauchen wir also, dass wenn immer $r_1 - r_2$ und $r_2 - r_3$ in S liegen, auch $r_1 - r_3$ in S liegt. Dieser Wunsch ist erfüllt, wenn S unter „$+$“ abgeschlossen ist.

Zusammenfassend ist die Relation „$\sim$“ eine Äquivalenzrelation genau dann, wenn $(S, +)$ eine Untergruppe von $(R, +)$ ist. Für die nachfolgenden Fragen müssen wir deshalb annehmen, dass $(S, +)$ eine Untergruppe von $(R, +)$ ist.

Als zweites denken wir über die repräsentantenweise Addition nach. Die ist wohldefiniert genau dann, wenn wir für $r_1 \sim r_1'$ und $r_2 \sim r_2'$ haben, dass $r_1 + r_2\ \sim r_1' + r_2'$. Es gilt $r_i \sim r_i'$ genau dann, wenn $r_i - r_i'$ in S liegt. Nun ist $r_1 + r_2 - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2')$, was aber gerade bedeutet, dass $r_1 + r_2\ \sim r_1' + r_2'$. Die repräsentantenweise Addition ist deshalb auf $R/\sim$ immer wohldefiniert.

Wir haben zum Umsortieren verwendet, dass die Addition kommutativ ist. Es gibt auch Gruppen, deren Verknüpfung nicht kommutativ ist, für die man eine

ähnliche Konstruktion durchführen kann. In diesem Fall muss das Analogon zu S eine spezielle Untergruppe sein, damit die repräsentanteweise Verknüpfung wohldefiniert ist.

Als drittes zur repräsentantenweisen Multiplikation. Wir hätten gerne für alle r_i, r_i' aus R mit $r_i \sim r_i'$, dass $r_1 r_2 \sim r_1' r_2'$. Wir schreiben $s_1 = r_1 - r_1'$ und $s_2 = r_2 - r_2'$ für die resultierenden Elemente von S. Damit können wir schreiben

$$r_1 r_2 = (s_1 + r_1')(s_2 + r_2') = r_1' r_2' + r_1' s_2 + r_2' s_1 + s_1 s_2.$$

Wenn für alle r aus R und s aus S gilt, dass rs wieder zu S gehört, dann ist $r_1 r_2 \sim r_1' r_2'$.

Sind die repräsentantenweisen Verknüpfungen wohldefiniert, dann wird $R/\!\sim$ mit diesen immer zu einem Ring, was die letzte Frage beantwortet.

Passend zu diesen Vorüberlegungen geben wir den für unsere Zwecke geeigneten Untergruppen nun einen Namen

Definition I.7.5: Seien $(R, +, \cdot)$ ein kommutativer Ring mit Einselement und S eine Teilmenge. Ist $(S, +)$ eine Untergruppe von $(R, +)$ und ist S abgeschlossen unter Multiplikation mit Elementen von R, d. h. für r aus R und s aus S ist rs in S, dann heißt S ein *Ideal*.

Satz 5 (Quotienten von Ringen): *Seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und S ein Ideal in R. Dann wird die Menge der Äquivalenzklassen $R/\!\sim$ bezüglich der Äquivalenzrelation „$\sim$“ aus Vorüberlegung I.7.4 zusammen mit den repräsentantenweisen Verknüpfungen zu einem Ring mit Eins $(R/\!\sim, +, \cdot)$.*

Bemerkung I.7.6: Die Menge N der rationalen Nullfolgen ist ein Ideal im Ring C der rationalen Cauchyfolgen.

Korollar I.7.7 (Die reellen Zahlen als Ring): $(\mathbb{R}, +, \cdot)$ *ist ein kommutativer Ring mit Eins.*

Definition I.7.8 (Körper): Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Falls jedes Element r aus $R - \{0\}$ multiplikativ invertierbar ist, d. h. dass es r' in R gibt, sodass $rr' = 1$, dann heißt R ein *Körper*.

Proposition I.7.9 (Die reellen Zahlen als Körper): *Der kommutative Ring $\mathbb{R}$ zusammen mit den repräsentantenweisen Verknüpfungen ist ein Körper. Wir fassen $\mathbb{Q}$ vermöge $q \mapsto [(q, q, q, \dots)]$ als Teilmenge von $\mathbb{R}$ auf.*

Diese Aussage wird Ihnen als Übungsaufgabe überlassen.

Beispiel I.7.10 (Einige reelle Zahlen):

(i) $x = [(1; 1.1; 1.101; 1.101\,001; 1.101\,001\,075\,6; \dots)]$.

(ii) $x = [(0.9; 0.99; 0.999; 0.9999, \dots)] = 1$, denn $(0.1, 0.01, 0.001, \dots)$ ist eine Nullfolge.

Definition I.7.11 (Anordnung, Betrag, Metrik, Konvergenz):

(i) Sei $r = [(x_n)_{n\in\mathbb{N}}]$ eine reelle Zahl. Gibt es eine positive rationale Zahl q und einen Index N, sodass $x_n > q$ für alle $n \geq N$, dann schreiben wir $r > 0$. Für reelle Zahlen r und s mit $r - s > 0$ schreiben wir $r > s$. Wie gewohnt definiert man „$\leq$“, „$\geq$“, „$<$“, $\mathbb{R}_{>r}$, „$\mathbb{R}_{\geq r}$“, ...

(ii) Genau wie auf $\mathbb{Q}$ definiert man den Betrag $|\cdot|$ durch

$$|r| = \begin{cases} r, & \text{falls } r \geq 0, \\ -r, & \text{falls } r < 0. \end{cases}$$

(iii) Durch $d(r_1, r_2) = |r_1 - r_2|$ wird auf $\mathbb{R}$ eine Metrik d erklärt.

(iv) Seien $(r_n)_{n\in\mathbb{N}}$ eine Folge reeller Zahlen und r eine reelle Zahl. Falls es für jedes $\varepsilon > 0$ einen Index N gibt, sodass $d(r_n, r) < \varepsilon$ für jedes $n \geq N$, dann *konvergiert* (r_n) *gegen* r. Wir schreiben auch $r_n \to r$.

Proposition I.7.12 (Eigenschaften von Ordnung und Betrag):

(i) *Die gerade definierte Ordnung „$\leq$“ ist eine Totalordnung auf* $\mathbb{R}$.

(ii) *Ist* $r = [(x_n)_{n\in\mathbb{N}}]$, *dann ist* $|r| = [(|x_n|)_{n\in\mathbb{N}}]$.

(iii) *Der Betrag* $|\cdot|$ *ist eine Norm auf* $\mathbb{R}$, *d. h. sie erfüllt die Eigenschaften aus Proposition I.6.7.*

(iv) *Die Abbildung* d *aus der vorherigen Definition ist eine Metrik, d. h. erfüllt die Eigenschaften aus Proposition I.6.8*

(v) *Ist* $r = [(x_n)]$ *eine reelle Zahl, dann konvergiert die Folge* (x_n) *aufgefasst als Folge reeller Zahlen gegen* r.

Satz 6 (Die reellen Zahlen als vollständiger Körper): *Das Paar* $(\mathbb{R}, d)$ *bildet einen* vollständigen Körper, *d. h. jede Cauchyfolge reeller Zahlen konvergiert in* $\mathbb{R}$.

Beweis: Sei $(r_n)_{n\in\mathbb{N}}$ eine Cauchyfolge reeller Zahlen. Wir wollen zeigen, dass es eine reelle Zahl r gibt, sodass $r_n \to r$, d. h. für jedes reelle $\varepsilon > 0$ muss es einen Index N geben, sodass für jedes $n \geq N$ gilt: $|r - r_n| < \varepsilon$. Diese passende reelle Zahl r wollen wir im Folgenden konstruieren.

Jedes Folgenglied r_i ist per Konstruktion eine Äquivalenzklasse einer rationalen Cauchyfolge, d. h. für jedes i ist $r_i = [(x_{i,n})_{n\in\mathbb{N}}]$ für eine geeignete rationale Cauchyfolge $(x_{i,n})_{n\in\mathbb{N}}$.

Weil $(x_{i,n})_{n\in\mathbb{N}}$ eine rationale Cauchyfolgen sind, gibt es für jede positive rationale Zahl q einen Index $N_i(q)$, sodass $|x_{i,n} - x_{i,m}| < q$ für alle $n, m \geq N_i(q)$.

Da $(r_i)_{i\in\mathbb{N}}$ eine reelle Cauchyfolge ist, gibt es für jede positive reelle Zahl ε einen Index $M(\varepsilon)$ mit $|r_i - r_j| < \varepsilon$ für $i, j \geq M(\varepsilon)$.

Das folgende Argument ist ein sogenanntes Diagonalfolgenargument. Wir bilden dazu eine neue Folge $(y_k)_{k\in\mathbb{N}}$ rationaler Zahlen durch $y_k = x_{k,i}N_k(1/n)$. Im Folgenden schreiben wir a_k für $N_k(1/n)$. Per Konstruktion haben wir für alle n, n' aus $\mathbb{N}$ mit $n, n' \geq a_n$, dass $|x_{k,n} - x_{k,n'}| < 1/k$.

Insbesondere gilt für alle $n \geq a_n$, dass $|x_{k,n} - y_k| < 1/k$. Nun gilt es zu zeigen, dass $(y_k)_{k\in\mathbb{N}}$ eine Cauchyfolge ist, die damit eine reelle Zahl definiert, und dass $r_i \to r = [(y_k)_{k\in\mathbb{N}}]$. □

Im Folgenden möchten wir das Kapitel mit Überlegungen zu Dezimalbruchentwicklungen reeller Zahlen abschließen. Wir werden zeigen, dass reelle Zahlen Dezimalbruchentwicklungen besitzen und diese beschreiben.

Lemma I.7.13 (Zerlegungslemma in $\mathbb{R}$): *Für jede reelle Zahl α gibt es eine ganze Zahl z und eine reelle Zahl r mit $0 \leq r < 1$, sodass $\alpha = k + r$.*

Beweis: Zunächst betrachten wir positive reelle Zahlen. Für eine positive reelle Zahl α sei $M = \{k' \in \mathbb{Z} \mid k' > \alpha\}$. Per Wahl von α ist M eine Teilmenge der natürlichen Zahlen, sodass M nach dem Prinzip des kleinsten Täters ein kleinstes Element k' besitzt. Für $k' - 1$ haben wir dann $k - 1 \leq \alpha < k$, sodass $k = k' - 1$ das Gewünschte tut. Für $\alpha < 0$ betrachten wir die positive $-\alpha$ und fahren wie gewohnt fort. □

Definition I.7.14 (Unendliche Reihen): Seien N eine ganze Zahl, $(r_{N+n})_{n\in\mathbb{N}}$ eine Folge reeller Zahlen und α eine reelle Zahl. Falls die Folge der Partialsummen $(s_m)_{m\in\mathbb{N}} = (\sum_{k=N}^{N+m} r_n)_{m\in\mathbb{N}}$ gegen α konvergiert, dann schreiben wir $\sum_{k=N}^{\infty} r_n = \alpha$.

Proposition I.7.15 (Dezimalbruchzerlegung reeller Zahlen): *Jede reelle Zahl α besitzt eine Dezimalbruchzerlegung, d. h. es gibt eine ganze Zahl ℓ und eine*

Folge $(a_j)_{j\in\mathbb{Z}_{\leq\ell}}$*, wobei jedes* a_j *in* $\{0,\ldots,9\}$ *liegt, sodass*

$$\alpha = \sum_{j=-\ell}^{\infty} a_{-j}10^{-j}. \tag{I.1}$$

Gl. (I.1) *heißt* Dezimalbruchzerlegung fü α.

Wir setzen eine rekursive Definition an, d. h. wir definieren je eine Folge $(\alpha_n)_{n\in\mathbb{N}}$ reeller Zahlen, $(k_n)_{n\in\mathbb{N}}$ ganzer Zahlen und $(r_n)_{n\in\mathbb{N}}$ eine Folge reeller Zahlen mit $0 \leq r_n < 1$ für alle n, indem wir festlegen $\alpha_0 = \alpha$ und r_0, k_0 definieren als diejenigen Zahlen, die das Zerlegungslemma Lemma I.7.13 hergibt, d. h. $\alpha_0 = k_0 + r_0$.

Für die natürliche Zahl n seien $\alpha_{n+1} = 10r_n$ und r_{n+1}, k_{n+1} diejenigen Zahlen, die Lemma I.7.13 für α_{n+1} hergibt.

Per vollständiger Induktion zeigt man für alle $n \geq 1$, dass einerseits für $s_n = k_0 + \sum_{j=1}^{n} k_j 10^{-j}$ gilt, dass $|s_n - \alpha| < 10^{-n}$ und andererseits, dass $0 \leq k_n < 10$, sodass k_n sogar aus $\{0, 1, \ldots, 9\}$ kommt.

Aus Proposition I.6.1 erhalten wir Ziffern $a_1, \ldots, a_\ell$, sodass $k_0 = \sum_{i=0}^{\ell} a_i 10^i = \sum_{j=-\ell}^{0} a_{-j}10^{-j}$. Für $j < 0$ definieren wir $a_j = k_{-j}$ und erhalten dann die Behauptung.

Bemerkung I.7.16: Mit vollständiger Induktion, oder mithilfe der geometrischen Reihe, kann man zeigen, dass $1 - \sum_{j=1}^{n} 9 \cdot 10^{-j} = 10^{-n}$.

(i) Nach Satz 6 gibt es für jede Folge $(a_j)_{j\leq\ell}$ wie in Proposition I.7.15 gibt es eine reelle Zahl α, sodass $\alpha = \sum_{j=-\ell}^{\infty} a_{-j}10^{-j}$.

(ii) Für die Folge $(a_j)_{j\leq -1}$ mit $a_j = 9$ für alle $j \leq -1$ gilt

$$1 - s_n = 1 - \sum_{j=1}^{n} a_{-j}10^{-j} = 10^{-n},$$

d. h. s_n konvergiert gegen 1 und es gilt $0,\overline{9} = 1$.

Satz 7 (Überabzählbarkeit von $\mathbb{R}$): *Die Menge der reellen Zahlen* $\mathbb{R}$ *ist überabzählbar, d. h. es gibt keine Folge* $(r_k)_{k\in\mathbb{N}}$ *in* $\mathbb{R}$*, in der jede reelle Zahl vorkommt.*

Beweis: Sei $(r_k)_{k\in\mathbb{N}}$ eine Folge reeller Zahlen mit $0 < r_k < 1$. Dann gibt es eine reelle Zahl α aus $(0, 1)$, sodass $\alpha \neq r_k$ für jedes k. Um das zu zeigen, möchten wir Proposition I.7.15 verwenden. Nach dieser Proposition gibt es nämlich für jedes r_k eine Dezimalbruchzerlegung, also $r_k = \sum_{j=1}^{\infty} a_{-j}^{(k)} 10^{-j}$ mit Ziffern $a_{-j}^{(k)}$ aus $\{0, \ldots, 9\}$. Im Folgenden schreiben wir $a_{k,j}$ statt $a_{-j}^{(k)}$.

Für j in $\mathbb{N}$ setzen wir $b_j = 4$, falls $a_{j,j} = 5$, und $b_j = 5$ sonst. Dadurch erhalten wir eine reelle Zahl $\alpha = \sum_{j=1}^{\infty} b_j 10^{-j}$, aber dieses α taucht per Konstruktion nicht in der Folge auf. □

Kapitel II

Teilbarkeitslehre

1 Euklidischer Algorithmus

In diesem Abschnitt sei $(R, +, \cdot)$ stets ein kommutativer Ring mit Einselement. Das Paradebeispiel für einen solchen Ring ist der Ring der ganzen Zahlen $\mathbb{Z}$ zusammen mit der klassischen Addition und Multiplikation ganzer Zahlen.

Definition II.1.1 (Teiler und Einheiten):

(i) Seien a und b Elemente von R. Gibt es r in R, sodass $b = ra$, dann sagen wir a *teilt* b und schreiben dafür $a \mid b$.

(ii) Sei r ein Element von R. Gibt es s in R, sodass $rs = 1$, dann heißt r eine *Einheit*. Wir schreiben

$$R^\times = \{r \in R \mid \text{Es gibt } s \in R \text{ mit } rs = sr = 1\}$$

und nennen $R^\times$ die *Einheitengruppe von* R.

Beispiel II.1.2: In den ganzen Zahlen wird 6 von $\pm 1, \pm 2, \pm 3$ und ± 6 geteilt. Die Einheitengruppe des Rings der ganzen Zahlen $\mathbb{Z}^\times$ ist die Menge $\{\pm 1\}$.

Definition II.1.3 (Größter gemeinsamer Teiler): Seien a, b und g Elemente des Rings R. Falls $g \mid a$ und $g \mid b$ und falls für jedes g' aus R mit $g' \mid a$ und $g' \mid b$ gilt, dass $g' \mid g$, dann heißt g *größter gemeinsamer Teiler von* a *und* b.

Bemerkung II.1.4 (Wie eindeutig sind größte gemeinsame Teiler?): Sei R ein Integritätsring.

(i) Sind g_1 und g_2 größte gemeinsame Teiler von a und b nach Definition II.1.3, dann folgt $g_1 \mid g_2$ und $g_2 \mid g_1$.

(ii) Zwei von Null verschiedene Elemente r und s von R teilen sich genau dann gegenseitig, wenn es eine Einheit u von R gibt, sodass $r = us$.

(iii) Im Ring der ganzen Zahlen $\mathbb{Z}$ gilt für zwei verschiedene größte gemeinsame Teiler von a und b also $g_2 = -g_1$.

Beweis: Aussage (i) folgt direkt aus der Definition des größten gemeinsamen Teilers. Wenn wir (ii) gezeigt haben, folgt (iii) aus $\mathbb{Z}^\times = \{\pm 1\}$. Wenden wir uns also (ii) zu.

„$\Longrightarrow$“: Gilt $r \mid s$ und $s \mid r$, dann gibt es Elemente u_1 und u_2 von R, sodass $s = u_1 r$ und $r = u_2 s$. Damit ist $r = u_2 s = u_2 u_1 s$, d. h. $(1 - u_1 u_2)r = 0$. Weil R nullteilerfrei ist und r von Null verschieden ist, muss also $1 - u_1 u_2 = 0$ gelten, und so sind u_1 und u_2 Einheiten in R. Für die Einheit u_1 gilt $r = u_1 s$ wie gewünscht.

„$\Longleftarrow$“: Ist u eine Einheit von R, dann gibt es eine Einheit u', sodass $uu' = 1$. Per Voraussetzung ist $r = us$ und $s = uu's = u'r$. □

Im Folgenden möchten wir zeigen, dass es für ganze Zahlen a und b stets einen größten gemeinsamen Teiler gibt. Wir halten fest, dass g im Ring $\mathbb{Z}$ genau dann ein größter gemeinsamer Teiler von a und b ist, wenn g ein größter gemeinsamer Teiler von $|a|$ und $|b|$ ist.

Notation II.1.5: Sind a und b Elemente eines nullteilerfreien Rings R, und ist g ein größter gemeinsamer Teiler von a und b aus R, dann schreiben wir $g = \mathrm{ggT}(a, b)$. Größte gemeinsame Teiler sind bis auf Einheiten eindeutig bestimmt. Ist $\mathrm{ggT}(a, b) = 1$, dann heißen a und b *teilerfremd*.

Sind a und b ganze Zahlen, $b \neq 0$, dann gibt es nach Satz 4 eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < |b|$, sodass $a = qb + r$. Wir schreiben $q = a \operatorname{div} b$ und $r = a \pmod{b}$.

Definition II.1.6 (Euklidischer Algorithmus): Eingabe: Ganze Zahlen bzw. Polynome a und b, $b \neq 0$.

Ausgabe: Ganze Zahlen bzw. Polynome r, s und t mit $\mathrm{ggT}(a, b) = r = sa + tb$.

Zu Beginn, setze

$$r_0 = a, \qquad r_1 = b, \qquad s_0 = 1, \qquad s_1 = 0, \qquad t_0 = 0, \qquad t_1 = 1.$$

Für $i = 1, 2, \ldots$, berechne $q_i = r_{i-1} \operatorname{div} r_i$ und setze

$$r_{i+1} = r_{i-1} - q_i r_i, \qquad s_{i+1} = s_{i-1} - q_i s_i, \qquad t_{i+1} = t_{i-1} - q_i t_i.$$

Wenn $r_{i+1} = 0$ ist, setze $r = r_i$, $s = s_i$ und $t = t_i$. Dieser Algorithmus terminiert.

Satz 8 (Euklidischer Algorithmus): *Der Algorithmus aus Definition II.1.6 terminiert. Es gilt:*

(i) *Im i-ten Schritt ist* $r_i = s_i a + t_i b$.

(ii) *Es gibt ein* i_0, *sodass* $r_{i_0+1} = 0$, *d. h. der Algorithmus terminiert.*

(iii) *Für das* i_0 *aus (ii) gilt* $r_{i_0} = \mathrm{ggT}(a, b)$.

Insbesondere erhält man auf diese Weise eine Linearkombination $\mathrm{ggT}(a, b) = s_{i_0} a + t_{i_0} b$.

Beweis: (i) Wir zeigen die Behauptung durch vollständige Induktion. Für $i = 0$ haben wir $r_0 = a$, $s_0 = 1$ und $t_0 = 0$, sodass $r_0 = s_0 a + t_0 b$. Dies ist äquivalent zu $a = 1a + 0b$, und das ist offensichtlich wahr.

Die Behauptung gelte in allen Schritten bis zum Schritt i. Unter Verwendung der Zusammenhänge

$$r_{i+1} = r_{i-1} - q_i r_i, \qquad s_{i+1} = s_{i-1} - q_i s_i, \qquad t_{i+1} = t_{i-1} - q_i t_i$$

sehen wir

$$\begin{aligned} s_{i+1} a + t_{i+1} b &= (s_{i-1} - q_i s_i) a + (t_{i-1} - q_i t_i) b \\ &= s_{i-1} a + t_{i-1} b - q_i (s_i a + t_i b) = r_{i-1} - q_i r_i = r_{i+1}, \end{aligned}$$

wobei wir im letzten Schritt die Induktionsvoraussetzung verwendet haben.

(ii) Es gilt $r_{i+1} = r_{i-1} \mod r_i$, weshalb $r_{i+1} < r_i$. Deshalb muss der Algorithmus terminieren.

(iii) Sei g ein gemeinsamer Teiler von a und b. Zunächst gilt für jedes $i \leq i_0+1$, dass $g \mid r_i$, da $r_i = s_i a + t_i b$. Insbesondere wird r_{i_0} von g geteilt.

Weiter möchten wir für jedes $i \leq i_0 + 1$ zeigen, dass r_i von r_{i_0} geteilt wird. Das zeigen wir wieder per vollständiger Induktion für r_{i_0+1-k} über k.

Die Aussage stimmt jedenfalls fürs $r_{i_0+1} = 0$. Für r_i stimmt die Aussage auch. Die Aussage gelte für r_{i_0+1-k}. Wir wollen nun zeigen, dass die Aussage auch für $r_{i_0+1-(k+1)} = r_{i_0+1-k-1}$ gilt. Es gilt $r_{i_0-k+1} = r_{i_0-k-1} - q_{i_0-k} r_{i_0-k}$, sodass

$$r_{i_0-k-1} = r_{i_0-k+1} + q_{i_0-k} r_{i_0-k}.$$

Per Induktionsvoraussetzung werden r_{i_0-k} und r_{i_0-k+1} von r_{i_0} geteilt, also auch r_{i_0-k-1}. Insbesondere teilt r_{i_0} auch $r_0 = a$ und $r_1 = b$, sodass g von r_{i_0} geteilt wird. Wegen des bisher gezeigten ist $r_{i_0} = \mathrm{ggT}(a, b)$. □

Korollar II.1.7 (Lemma von Bézout): *Zwei ganze Zahlen a und b, nicht beide Null, haben stets einen größten gemeinsamen Teiler. Ist g ein größter gemeinsamer Teiler von a und b, dann gibt es ganze Zahlen k und ℓ, sodass* $g = ka + \ell b$.

2 Der chinesische Restsatz

Im Folgenden schreiben wir $\overline{a}$ oder $[a]$ für die Restklasse der ganzen Zahl a in $\mathbb{Z}/m\mathbb{Z}$.

Proposition II.2.1: *Seien a eine ganze Zahle und m eine positive natürliche Zahl. Genau dann ist $\overline{a}$ ein Element von $(\mathbb{Z}/m\mathbb{Z})^\times$, wenn $\mathrm{ggT}(a,m)=1$. Wir haben also die Charakterisierung*

$$\mathbb{Z}/m\mathbb{Z}^\times = \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} \mid \mathrm{ggT}(a,m)=1\}.$$

Beweis: Die Inklusion „$\supseteq$“ folgt aus dem Lemma von Bézout (Korollar II.1.7). Für „$\subseteq$“ sei $g=\mathrm{ggT}(a,b)$. Ist $\overline{a}$ invertierbar in $\mathbb{Z}/m\mathbb{Z}$, dann gibt es ganze Zahlen k und ℓ, sodass $1=ka+\ell m$, das heißt g muss 1 teilen. Damit ist $g \in \{\pm 1\}$. □

Bemerkung II.2.2: Mit dem Euklidischen Algorithmus kann die Inverse von $\overline{a}$ aus $\mathbb{Z}/m\mathbb{Z}^\times$ direkt bestimmt werden.

Proposition II.2.3: *Seien $m_1,\ldots,m_r$ paarweise teilerfremde positive natürliche Zahlen und $a_1,\ldots,a_r$ ganze Zahlen. Dann gibt es eine ganze Zahl x, sodass*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned} \tag{II.1}$$

Beweis: Sei $M=m_1\cdots m_r$ und für $1\le i\le r$ bezeichne $M_i=M/m_i$. Wir halten fest, dass die so definierten Zahlen m_i und M_i teilerfremd sind (siehe auch das folgende Lemma). Deswegen finden wir eine ganze Zahl K_i, sodass $M_iK_i \equiv 1 \pmod{m_i}$. Für $1\le i\le r$ setzen wir $A_i=M_iK_i$, weshalb $A_i\equiv 1 \pmod{m_i}$. Die ganze Zahl $x=\sum_{i=1}^r a_iA_i$ leistet das Gewünschte, denn für $i\neq j$ wird M_i von m_j geteilt, sodass $M_i\equiv 0 \pmod{m_j}$ und $x\equiv a_jA_j\equiv a_j \pmod{m_j}$. □

Lemma II.2.4 (Rechentricks für teilerfremde Zahlen):

(i) *Seien a, b ganze Zahlen und m eine weitere positive natürliche Zahl, sodass $\mathrm{ggT}(a,m)=1=\mathrm{ggT}(b,m)$. Dann ist $\mathrm{ggT}(ab,m)=1$.*

(ii) *Seien m_1, m_2 ganze Zahlen mit $\mathrm{ggT}(m_1,m_2)=1$ und a eine ganze Zahl. Wird a von m_1 und m_2 geteilt, dann auch von m_1m_2.*

Beweis: (i) Nach Proposition II.2.1 sind $\overline{a}$ und $\overline{b}$ Einheiten in $\mathbb{Z}/m\mathbb{Z}$, also auch ihr Produkt nach Aufgabe 1 von Blatt 12. Aus Proposition II.2.1 folgt dann die Behauptung.

(ii) Ohne Einschränkung dürfen wir annehmen, dass m_1 und m_2 positiv sind. Im Folgenden rechnen wir modulo m_2, d. h. $\overline{a}$ bezeichnet die Restklasse von a in $\mathbb{Z}/m_2\mathbb{Z}$. Wieder nach Proposition II.2.1 ist $\overline{m}_1$ eine Einheit in $\mathbb{Z}/m_2\mathbb{Z}$. Es gibt also eine ganze Zahl m_1', sodass $\overline{m}_1\overline{m}_1' = \overline{1}$. Weil a von m_1 geteilt wird, gibt es eine ganze Zahl k, sodass $a = km_1$, weshalb

$$\overline{m}_1'\overline{a} = \overline{m}_1'\overline{k}\overline{m}_1 = \overline{1}\overline{k} = \overline{k}.$$

Andererseits ist $\overline{a} = 0$, weil a nach Voraussetzung von m_2 geteilt wird. Deshalb muss $\overline{k} = \overline{0}$ sein, oder mit anderen Worten: k wird von m_2 geteilt. Damit wird $a = km_1$ von m_1m_2 geteilt. □

Proposition II.2.5 (Simultane Kongruenzen II): *In der Situation von Proposition II.2.3 gilt: Ist $M = m_1 \cdots m_r$ und ist x_0 eine Lösung des simultanen Kongruenzproblems* (II.1)*, dann ist $\mathbb{L} = \{x_0 + kM \mid k \in \mathbb{Z}\}$ die Menge aller Lösungen des simultanen Kongruenzproblems.*

Satz 9 (Simultane Kongruenzen): *Seien $m_1, \ldots, m_r$ paarweise teilerfremde positive natürliche Zahlen und $M = m_1 \cdots m_r$. Die Abbildung*

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}, \qquad [a]_M \longmapsto ([a]_{m_1}, \ldots, [a]_{m_r})$$

ist bijektiv.

Beweis: Die Wohldefiniertheit und die Injektivität dieser Abbildung folgt aus Proposition II.2.5 und die Surjektivität ist gerade Proposition II.2.3. □

3 Primzahlen

Beispiel II.3.1: Die natürliche Zahl 18 hat einige Teiler. Wir haben mehrere Möglichkeiten, die Zahl zu faktorisieren, beispielsweise $18 = 2 \cdot 9 = 2 \cdot 3 \cdot 3$, oder $18 = 3 \cdot 6 = 3 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 3$. Zerlegen wir die Zahl aber so weit, bis jeder Faktor in dieser Darstellung eine Primzahl ist, dann erhalten wir – bis auf Reihenfolge – immer dasselbe Ergebnis.

Definition II.3.2 (Primzahl): Sei $n > 1$ eine natürliche Zahl. Lässt sich n nicht als Produkt zweier echt kleinerer natürlicher Zahlen schreiben, dann heißt n *Primzahl* bzw. *irreduzibel*. Die Menge der Primzahlen notieren wir mit $\mathbb{P}$, d. h. $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$.

Im Folgenden möchten wir einerseits zeigen, dass es unendlich viele Primzahlen gibt, und andererseits, dass die Primfaktorzerlegung einer natürlichen Zahl im Wesentlichen eindeutig ist. Dass jede natürliche Zahl eine Primfaktorzerlegung besitzt, haben Sie bereits auf einem Übungsblatt mithilfe des Prinzips des kleinsten Täters gezeigt.

Satz 10 (Euklid): *Es gibt unendlich viele Primzahlen.*

Proposition II.3.3 (Alternative Primalitätsbedingung): *Sei $n > 1$ eine natürliche Zahl. Genau dann ist n eine Primzahl, wenn für alle natürlichen Zahlen a und b, für die ab von n geteilt wird, schon a oder b von n geteilt wird.*

Beweis: „$\Longleftarrow$“: Angenommen, es gäbe zwei natürliche Zahlen a und b mit $a, b < n$ und $n = ab$. Insbesondere wird dann ab von n geteilt, sodass a oder b von n geteilt werden. Aber das bedeutet $n \leq a$ beziehungsweise $n \leq b$; Widerspruch!

„$\Longrightarrow$“: Wird a oder b von n geteilt, dann wird immer ab von n geteilt. Wir müssen also für ab, das von n geteilt wird, zeigen, dass a oder b von n geteilt wird.

Sei n eine Primzahl im Sinne von Definition II.3.2 und es seien a und b natürliche Zahlen, sodass $n \mid ab$. Das bedeutet es gibt eine natürliche Zahl k, sodass $ab = kn$.

Angenommen, $\mathrm{ggT}(a, n) = 1$. Dann gibt nach dem Lemma von Bézout ganze Zahlen r und s, sodass $1 = ra + sn$. Wegen $b = bra + bsn = abr + bsn = knr + bsn$ ist dann b ein Vielfaches von n, d. h. $n \mid b$.

Ist $g = \mathrm{ggT}(a, n) > 1$, dann wird n von g geteilt. Weil aber n prim ist, ist $g = n$, und weil auch a von g geteilt wird, ist $g = \mathrm{ggT}(g, n)$. □

Satz 11 (Fundamentalsatz der Arithmetik): *Jede natürliche Zahl $n \geq 1$ lässt sich als Produkt*

$$n = \prod_{i=1}^{k} p_i^{\nu_i} \tag{II.2}$$

von Primzahlen $p_1, \dots, p_k$ schreiben. Mit $k = 0$ ist das obige Produkt leer und damit die natürliche Zahl 1 abgedeckt. Die Produktdarstellung (II.2) *ist eindeutig bis auf die Reihenfolge der Primfaktoren. Man nennt* (II.2) *die* Primfaktorzerlegung von n.

Beweis: Die Existenz der Primfaktorzerlegung wurde auf Übungsblatt 5 mithilfe des Prinzips des kleinsten Täters gezeigt. Bleibt also die Eindeutigkeit der Zerlegung zu zeigen. Seien dazu $n = \prod_{i=1}^{s} p_i = \prod_{j=1}^{t} q_j$ zwei Primfaktorzerlegungen von n, d. h. $p_1, \ldots, p_s, q_1, \ldots, q_t \in \mathbb{P}$. Wir zeigen die Behauptung per vollständiger Induktion nach $k = \min\{s, t\}$.

Ist $k = 0$, dann ist $n = 1$ und es muss $s = t = 0$ gelten. Ist $k = 1$, dann ist n selbst eine Primzahl, die keine echten Teiler hat. Es müssen deshalb $s = t = 1$ sein und die Behauptung gilt.

Die Aussage gelte für die natürliche Zahl k. Ohne Einschränkung dürfen wir annehmen, dass $s = k + 1 \leq t$. Wir zeigen, dass es einen Index j in $\{1, \ldots, t\}$ gibt, sodass $p_1 = q_j$.

Wäre das nicht der Fall, dann hätten wir wegen $q_1 \cdots q_t = p_1(p_2 \cdots p_s$, dass q_1 oder $q_2 \cdots q_t$ von p_1 geteilt. Per Annahme müsste $q_2 \cdots q_t$ von p_1 geteilt werden. Weil wir angenommen haben, dass keines der q_j von p_1 geteilt wird, müsste $q_3 \cdots q_t$ geteilt werden, und so weiter, bis wir bei $p_1 = q_t$ angelangen. Ein Widerspruch.

Die Annahme war also falsch, und wir dürfen ohne Einschränkung annehmen, dass $p_1 = q_1$ und so folgt, dass $p_2 \cdots p_s = q_2 \cdots q_t$. Nach Induktionsvoraussetzung ist $s - 1 = t - 1$ und durch Umordnung der Faktoren können wir erreichen, dass $p_i = q_i$ für $2 \leq i \leq s$. □

Beweis (von Satz 10): Angenommen, es gäbe nur endlich viele Primzahlen, sagen wir $p_1, \ldots, p_k$ für eine natürliche Zahl k. Die natürliche $N = p_1 \cdots p_k + 1$ wäre durch keine Primzahlen $p_1, \ldots, p_k$ teilbar, aber hätte nach Satz 11 selbst eine Primfaktorzerlegung. Die zugehörigen Primfaktoren müssten in der Menge $\{p_1, \ldots, p_k\}$ enthalten sein. Sei p_i ein Primteiler von N, d. h. $N \equiv 0 \mod p_i$. Andererseits wäre aber auch $N \equiv p_1 \cdots p_k + 1 \equiv 1 \pmod{p_i}$, was nicht sein kann. □

Satz 12 (von Euler): *Für eine natürliche Zahl n sei $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$. Die dadurch definierte Funktion heißt* Eulersche φ-Funktion*. Ist a eine ganze Zahl, für die $\mathrm{ggT}(a, n) = 1$, dann ist $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Das Argument für Aufgabe 2(v) auf Blatt 12 geht auch in dieser Situation durch.

Proposition II.3.4 (Berechnung von φ):

(i) *Ist p eine Primzahl, dann ist $\varphi(p) = p - 1$.*

(ii) *Ist p eine Primzahl und ist e eine positive natürliche Zahl, dann ist $\varphi(p^e) = p^e - p^{e-1}$.*

(iii) *Sind n und m teilerfremde natürliche Zahlen, dann ist $\varphi(nm) = \varphi(n)\varphi(m)$.*

Bemerkung II.3.5 (RSA-Verfahren[1]): Die zugrundeliegende Idee beim RSA-Verfahren ist „Verschlüsselung ohne Schlüsselaustausch“.

Alice möchte Bob eine Nachricht schicken. Der Spion Mr. X will die Nachricht abfangen. Alice und Bob können sich jedoch nicht treffen, um einen Geheimcode abzusprechen. Beide kommen zu folgender Lösung ihres Problems:

(1) Bob wählt einen öffentlichen Schlüssel e (den jeder kennt) und einen privaten Schlüssel f (den nur er kennt).

(2) Alice hat einen Text T. Alice verschlüsselt Bobs öffentlichen Schlüssel T und erhält einen codierten Text C, mit dem Mr. X nichts anfangen kann. Diesen schickt sie an Bob.

(3) Bob entschlüsselt C mit seinem privaten Schlüssel f und erhält T zurück.

Wie soll das gehen?

Verfahren zur Erstellung der Schlüssel

(i) Bob wählt zwei große Primzahlen p und q aus und berechnet $m = pq$. Es ist $\varphi(m) = (p-1)(q-1)$.

(ii) Für den öffentlichen Schlüssel wählt Bob eine natürliche Zahl e die teilerfremd zu $\varphi(m)$ ist und veröffentlicht das Tupel (e, m).

(iii) Für die Wahl des privaten Schlüssels f bestimmt Bob mithilfe des euklidischen Algorithmus natürliche Zahlen f und g mit $1 = fe - g\varphi(m)$ und verwendet (f, m) als privaten Schlüssel.[2]

Anwendung des Verfahrens Ohne Einschränkung ist der Text gegeben als Zahl x mit $x < p, q$ (zerlege den Text falls nötig).

(i) Zur Codierung berechnet Alice $z = x^e \pmod m$ und schickt z an Bob. Mr. X kann mit z nichts anfangen.[3]

[1] Nach Rivert, Shamir und Adleman am MIT aus dem Jahre 1977.

[2] Es ist tatsächlich möglich, f und g positiv zu wählen.

[3] Die Sicherheit des Verfahrens steht und fällt mit der Fähigkeit des Spions Mr. X, die Zahl m zu faktorisieren. Es ist ein schwieriges Problem, Primfaktorzerlegungen auszurechnen und offensichtlich nimmt die Schwierigkeit der Bestimmung der Faktorisierung zu, wenn die Primzahlen p und q größer werden. Hat Mr. X jedoch ausreichend Rechenleistung zur Verfügung, so kann er m in endlicher Zeit faktorisieren und so die Verschlüsselung knacken.

(ii) Zur Dekodierung berechnet Bob

$$z^f \equiv (x^e)^f \equiv x^{ef} \equiv x^{1+g\varphi(m)} \equiv x \cdot x^{g\varphi(m)} \equiv x \pmod{m}.$$

Dabei sind eingegangen, dass $\mathrm{ggT}(x, m) = 1$ wegen $x < p, q$ und dass es wegen $x < m = pq$ genügt, den Rest von x modulo m zu kennen.

Im Ergebnis hat Bob den Text x erhalten.