Elementare Zahlentheorie

gehalten von Prof. Dr. Weitze-Schmithüsen im SS '20

UNIVERSITÄT
DES
SAARLANDES

Hinweise zu Schreibfehlern an s9fhguen@stud.uni-saarland.de.

Inhaltsverzeichnis

Kapitel I.

Zahlbereiche

1. Natürliche Zahlen

In dieser Vorlesung verfolgen wir einen axiomatischen Ansatz und führen die natürlichen Zahlen über die Peano-Axiome ein. Dazu setzen wir die (naive) Mengentheorie und Logik als bekannt voraus.

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

(P1) Die Menge $\mathbb{N}$ ist nicht leer. Es existiert ein ausgezeichnetes Element $0 \in \mathbb{N}$.

(P2) Zu jedem Element $n \in \mathbb{N}$ existiert ein wohlbestimmtes Element $n^* \in \mathbb{N}$, der sogenannte *Nachfolger von* n.

(P3) Es gibt kein $n \in \mathbb{N}$ mit $n^* = 0$, d. h. 0 hat keinen Vorgänger.

(P4) Für alle $n_1, n_2 \in \mathbb{N}$ gilt: Aus $n_1^* = n_2^*$ folgt $n_1 = n_2$. Das heißt zwei verschiedene natürliche Zahlen können nicht den gleichen Nachfolger haben.

(P5) Falls für eine Teilmenge $M \subseteq \mathbb{N}$ gilt:

(1) $0 \in M$,

(2) Ist $n \in M$, dann ist auch $n^* \in M$,

dann ist bereits $M = \mathbb{N}$.

Das Axiom (P5) heißt auch *Prinzip der vollständigen Induktion.*

Bemerkung I.1.2: In dieser Vorlesung betrachten wir die Null als natürliche Zahl, in anderen Kontexten wird die Null nicht als natürliche Zahl angesehen.

Notation I.1.3: (i) Die Abbildung $\sigma\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n^*$ heißt *Nachfolge-Funktion*. Nach (P4) ist σ injektiv.

(ii) Wir schreiben $1 := 0^*$, $2 := 1^*$, $3 := 2^*$, und so weiter.

Proposition I.1.4 (Einzigartigkeit der Null): *Es sei*

$$\mathbb{N}^* := \{n \in \mathbb{N} \mid \textit{Es gibt } k \in \mathbb{N} \textit{ mit } n = \sigma(k)\}$$

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

Beweis: Setze $M := \mathbb{N}^* \cup \{0\}$. Wir wollen zeigen, dass $M = \mathbb{N}$ und verwenden dazu (P5). Per Definition ist $0 \in M$. Außerdem gilt per Definition von M für jedes Element $n \in M$, dass auch $\sigma(n) \in M$ und wir schließen $M = \mathbb{N}$. □

Im Folgenden kümmern wir uns um die gewohnten Verknüpfungen von natürlichen Zahlen, d. h. Addition, Multiplikation und Potenzen.

Ansatz I.1.5: Die bekannten Verknüpfungen haben die folgenden Eigenschaften:

(S1) Für alle $n \in \mathbb{N}$ setze $n + 0 := n$,

(S2) Für alle $n, m \in \mathbb{N}$ setze $n + \sigma(m) := \sigma(n + m)$,

(M1) Für alle $n \in \mathbb{N}$ setze $n \cdot 0 = 0$,

(M2) Für alle $n, m \in \mathbb{N}$ setze $n \cdot \sigma(m) := n \cdot m + n$,

(P1) Für alle $a \in \mathbb{N}$ setze $a^0 := 1$,

(P2) Für alle $a, m \in \mathbb{N}$ setze $a^{\sigma(m)} := a^m \cdot a$.

Jetzt müssen wir uns davon überzeugen, dass dadurch eindeutige Funktionen $+, \cdot, \hat{}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ festgelegt werden. Zum Glück ist das der Fall, das sehen wir in der nächsten Vorlesung.

Proposition I.1.6 (Rechenregeln): *Für Addition und Multiplikation gelten die folgenden Rechenregeln:*

(i) *Für alle* $n \in \mathbb{N}$ *ist* $n + 1 = \sigma(n)$.

(ii) *Für alle* $k, n, m \in \mathbb{N}$ *ist* $(k + m) + n = k + (m + n)$,

(iii) *Für alle* $m, n \in \mathbb{N}$ *gilt* $m + n = n + m$,

(iv) *Für alle* $k, m, n \in \mathbb{N}$ *gilt* $k \cdot (m + n) = k \cdot m + k \cdot n$,

(v) *Für alle* $n \in \mathbb{N}$ *ist* $n \cdot 1 = n$.

Die Aussagen (ii) *und* (iii) *gelten auch für die Multiplikation.*

Beweis: Wir zeigen exemplarisch die Aussagen (i), (iii) und (v), der Beweis von (ii) und (iv) werden als Übungsaufgabe gestellt werden.

Zu (i): Es ist $n + 1 = n + \sigma(0) = \sigma(n + 0) = \sigma(n)$, wobei wir Rechenregel (i), (S2) und (S1) verwendet haben.

Zu (iii): Im ersten Schritt zeigen wir, dass für alle $n \in \mathbb{N}$ gilt: $n + 0 = 0 + n$. Wir verwenden dazu (P5) und setzen $M := \{n \in \mathbb{N} \mid n + 0 = 0 + n\}$. Zunächst gilt $0 \in M$. Ist jetzt $n \in M$, dann ist wegen (S2), weil n zu M gehört und wegen (S1)

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

Mit (P5) folgern wir jetzt $M = \mathbb{N}$.

Im zweiten Schritt zeigen wir, dass für alle $n \in \mathbb{N}$ gilt dass $n + 1 = 1 + n$. Wir verwenden erneut (P5) und setzen an $M := \{n \in \mathbb{N} \mid n + 1 = 1 + n\}$. Nach dem ersten Schritt gilt $0 \in M$. Sei jetzt $n \in M$. Dann ist

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

wegen (S2), da n ein Element von M ist und wegen Rechenregel (i). Damit ist $M = \mathbb{N}$.

Im dritten Schritt sei $m \in \mathbb{N}$ gegeben. Wir zeigen per Induktion, dass für alle natürlichen Zahlen n gilt, dass $n + m = m + n$. Dazu setzen wir $M_m := \{n \in \mathbb{N} \mid m + n = n + m\}$. Nach dem ersten Schritt gilt $0 \in M_m$. Sei $n \in M_m$ gegeben. Dann haben wir

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

wobei wir der Reihenfolge nach (S2), dass $n \in M_n$, (S2), Rechenregel (i), Rechenregel (ii) und Rechenregel (i) verwendet haben. Das beschließt den Beweis.

Zu (v): Es gilt $n \cdot 1 = n \cdot \sigma(0)$. Wegen (M2) sehen wir ein, dass $n \cdot \sigma(0) = n \cdot 0 + n$ und wegen (M2) ist $n \cdot 0 + n = 0 + n = n$. □

Wir haben im Beweis der Kommutativiät der Addition die Assoziativität der Addition verwendet.

Proposition I.1.7 (Weitere Rechenregeln):

(i) *Für alle* $k, m, n \in \mathbb{N}$ *gilt: Ist* $k + n = m + n$*, dann ist* $k = m$*.*

(ii) *Für alle* $m, n \in \mathbb{N}$ *gilt: Ist* $m + n = 0$*, dann ist* $m = n = 0$*.*

Beweis: (i) Wir setzen $M := \{n \in \mathbb{N} \mid \text{Gilt } k + n = m + n, \text{ dann ist } k = m\}$ und gehen vor wie bisher.

(ii) Seien $m, n \in \mathbb{N}$ mit $m + n = 0$. Angenommen n wäre nicht Null. Dann gäbe es $k \in \mathbb{N}$ mit $\sigma(k) = n$ und wir hätten

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

was (P3) widerspricht. Also muss $n = 0$ sein. Wegen der Kommutativtität der Addition erhalten wir außerdem $m = 0$. □

Bemerkung I.1.8: Aus (P5) leitet sich das Prinzip der vollständigen Induktion ab, d. h. sei A eine Aussage über eine Variable n. Sind

(i) A gilt für 0 (Induktionsanfang),

(ii) Wenn A für $n \in \mathbb{N}$ gilt (Induktionsvoraussetzung), dann gilt A auch für $\sigma(n)$,

erfüllt, dann gilt A für alle natürlichen Zahlen.

Lemma I.1.9 (Potenzen):

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

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

Beweis: Wir zeigen exemplarisch (i). Wie zuvor zeigen wir die Behauptung per Induktion nach n. Für $n = 0$ und natürliche Zahlen a und m haben wir

$$a^m \cdot a^0 = a^m \cdot 1 = a^m = a^{m+0},$$

wegen Regel (P1) aus Ansatz I.1.5, Rechenregel (v) und (S1), wie gewünscht.

Es gelte die Aussage jetzt für eine natürliche Zahl n. Für den Induktionsschluss wollen wir zeigen, dass für alle $a, m \in \mathbb{N}$ gilt, dass $a^m \cdot a^{\sigma(n)} = a^{m+\sigma(n)}$. Es ist

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

wobei wir Regel (P2) aus Ansatz I.1.5, die Assoziativität der Multiplikation, erneut (P2) und (S2) benutzt haben. Damit ist alles gezeigt. □

2. Rekursion

Für den Rest dieses Abschnitts seien M und N Mengen.

Definition I.2.1: Eine Teilmenge $R \subseteq M \times N$ heißt *binäre Relation* oder kurz *Relation zwischen M und N*. Die Menge

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

heißt *Definitionsmenge*.

Definition I.2.2 (Eigenschaften von Relationen): Es seien M eine nichtleere Menge und $R \subseteq M \times M$ eine Relation.

(i) R heißt *reflexiv*, falls für alle x in M auch $(x, x) \in R$,

(ii) R heißt *symmetrisch*, falls für alle $x, y \in M$ mit $(x, y) \in R$ auch $(y, x) \in R$,

(iii) R heißt *antisymmetrisch*, falls für alle $x, y \in M$ gilt: Sind (x, y) und (y, x) in R, dann ist $x = y$.

(iv) R heißt *transitiv*, falls für alle $x, y, z \in M$ mit (x, y) und (y, z) in M auch $(x, z) \in R$ gilt.

Definition I.2.3 (Spezielle Relationen): Seien M eine Menge und $R \subseteq M \times M$ eine Relation.

(i) Ist R reflexiv, symmetrisch und transitiv, so heißt R eine *Äquivalenzrelation*,

(ii) Ist R reflexiv, antisymmetrisch und transitiv, so heißt R eine *partielle Ordnungsrelation* oder kurz *Ordnung*.

Definition I.2.4 (Funktion): Seien M und N Mengen und $R \subseteq M \times N$ eine Relation. Die Menge

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

heißt der *Definitionsbereich von R*. R heißt eine *Funktion*, falls für alle $x \in M$ und alle $y, z \in N$ gilt: „Ist $(x, y) \in R$ und $(x, z) \in R$, dann ist $y = z$“. Also heißt R Funktion genau dann, wenn es für jedes $x \in D(R)$ genau ein $y \in N$ mit $(x, y) \in R$ gibt. In diesem Fall schreiben wir $y =: R(x)$ und $R\colon D(R) \to N$.

Beispiel I.2.5: Seien $M = N = \mathbb{N}$.

(i) Sei $R = \{(x, y) \mid x \leq y\}$. Dann ist $D(R) = \mathbb{N}$ und R ist keine Funktion.

(ii) Sei $R = \{(x, y) \mid x = 2y\}$. Dann ist $D(R) = 2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$ und R ist eine Funktion $R\colon 2\mathbb{N} \to \mathbb{N}$.

Im Folgenden wollen wir uns davon überzeugen, dass Funktionen auf den natürlichen Zahlen rekursiv definiert werden können. Zur Plausibilisierung zwei Beispiele:

(i) Seien $M = N = \mathbb{N}$. Dann wird durch $f(0) = 1$, $f(n+1) = (n+1) \cdot f(n)$ die wohlbekannte Fakultätsfunktion erklärt.

(ii) Seien $M = \mathbb{N}$ und $N = \{r, b, s\}$. Betrachte

$$g_1\colon N \longrightarrow N, \qquad g_1(r) = b, \quad g_1(b) = r \quad \text{und} \quad g_1(s) = s,$$
$$g_2\colon N \longrightarrow N, \qquad g_2(r) = r, \quad g_2(b) = s \quad \text{und} \quad g_2(s) = b.$$

Dann definiert

$$f(0) := s, \qquad f(n+1) := \begin{cases} g_1(f(n)), & \text{falls } n \text{ ungerade,} \\ g_2(f(n)), & \text{falls } n \text{ gerade,} \end{cases}$$

eine Funktion $f\colon M \to N$.

Die Situation im Folgenden wird sein: Gegeben sind $x \in M$ und für alle natürlichen Zahlen n Funktionen $g_n\colon M \to M$. Wir suchen eine (hoffentlich eindeutige) Funktion $f\colon \mathbb{N} \to M$ mit $f(0) = x$ und $f(n+1) = g_n(f(n))$.

Satz I.2.6 (über die Rekursion): *Sei $x \in M$. Weiter sei für jede natürliche Zahl n eine Funktion $g_n\colon M \to M$ gegeben. Dann gibt es genau eine Funktion $f\colon \mathbb{N} \to M$ mit $f(0) = x$ und $f(n+1) = g_n(f(n))$.*

Beweis: Als ersten Schritt zeigen wir die Eindeutigkeit von f. Seien dazu $f, f'\colon \mathbb{N} \to M$ gegeben, die $f(0) = x = f'(0)$ und $f(n+1) = g_n(f(n))$ beziehungsweise $f'(n+1) = g_n(f'(n))$ erfüllen. Sei $K = \{n \in \mathbb{N} \mid f(n) = f'(n)\}$. Nach Voraussetzung gilt $0 \in K$. Ist jetzt $n \in K$ gegeben, dann haben wir

$$f(\sigma(n)) = g_n(f(n)) = g_n(f'(n)) = f'(\sigma(n)),$$

d. h. $\sigma(n) \in K$. Damit gilt schon $K = \mathbb{N}$.

Als zweiten Schritt zeigen wir die Existenz von f. Dazu betrachten wir alle Relationen, die die angegebenen Wert enthalten und wollen zeigen, dass die kleinste solche eine Funktion ist. Setze also

$$\mathfrak{R} := \{R \subseteq \mathbb{N} \times M \mid (0, x) \in R \text{ und } „foralln \in \mathbb{N} : (n, y) \in R \Rightarrow (n, y) \in R“\}$$

und definiere $R_0 := \bigcap_{R\in\mathfrak{R}} R := \{(n,y) \in \mathbb{N}\times M \mid \forall\, R \in \mathfrak{R} : (n,y) \in R\}$. Wir wollen zeigen, dass auch R_0 zu $\mathfrak{R}$ gehört. Zunächst ist $(0,x) \in R_0$, denn $(0,x)$ ist Element jeder Relation $R \in \mathfrak{R}$. Ist jetzt $(n,y) \in R_0$, dann ist (n,y) auch Element jeder Relation $R \in \mathfrak{R}$. Wegen der Definition von $\mathfrak{R}$ heißt das, dass auch $(\sigma(n), g_n(y))$ ein Element jeder Relation $R \in \mathfrak{R}_0$ ist, d. h. $(\sigma(n), g_n(y))$ gehört zu R_0.

Bleibt zu zeigen, dass $D(R_0) = \mathbb{N}$ und dass für alle Tupel $(n,y) = (n,y') \in R_0$ gilt, dass $y = y'$. Beides zeigen wir per Induktion. Setze dazu zunächst $K := D(R_0)$. Es gehört 0 zu K, denn $(0,x) \in R_0$. Ist jetzt $n \in K$, dann gibt es $y \in M$, sodass $(n,y) \in R_0$. Damit ist auch $(\sigma(n), g_n(y))$ in R_0, d. h. $\sigma(n)$ gehört zu K.

Setze nun $K := \{n \in \mathbb{N} \mid (n,y) \in R_0 \wedge (n,y') \in R_0 \Rightarrow y = y'\}$. Angenommen es gäbe $y \in M$ mit $x \neq y$ und $(0,y) \in R_0$. Dann wäre auch $R_0' := R_0 - \{(0,y)\}$ eine Relation mit den vorgegebenen Eigenschaften, die bezüglich Inklusion kleiner wäre als R_0 – ein Widerspruch zur Definition von R_0. Damit gehört $(0,x)$ zu K.

Sei jetzt $n \in K$. Dann gibt es genau ein $y \in M$ mit $(n,y) \in R_0$ und per Definition wäre auch $(\sigma(n), g_n(y)) \in R_0$. Angenommen es gäbe $z \neq g_n(y)$, sodass $(\sigma(n), z)$ zu R_0 gehörte. Dann wäre wieder $R_0' := R_0 - \{(\sigma(n), z)\}$ eine Relation in $\mathfrak{R}$, die bezüglich Inklusion kleiner wäre als R_0. Damit folgern wir $K = \mathbb{N}$ und erhalten dass $f = R_0$ die eindeutige Funktion mit den gewünschten Eigenschaften ist. □

Beispiel I.2.7: (i) Nach Satz I.2.6 können wir per $f(0) = 0$, $f(1) = 1$, $f(n+2) = f(n+1) + f(n)$ eine eindeutige Funktion $f\colon \mathbb{N} \to \mathbb{N}$ definieren. Dieses f heißt die *Fibonacci-Folge*.

(ii) Per $s(0) = 1$, $S(n+1) = S(n) + q^{n+1}$ wird eine eindeutige Funktion $S\colon \mathbb{N} \to \mathbb{N}$ definiert.

Proposition I.2.8 (Addition und Multiplikation):

(i) *Es gibt eine Funktion* $+\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ *mit den Eigenschaften*

$$\forall\, n \in \mathbb{N} : +(n,0) = n, \qquad \forall\, m,n \in \mathbb{N} : +(m,\sigma(n)) = \sigma(+(m,n)).$$

(ii) *Es gibt eine Funktion* $\cdot\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ *mit den Eigenschaften*

$$\forall\, n \in \mathbb{N} : \cdot(n,0) = 0, \qquad \forall\, n,m \in \mathbb{N} : \cdot(n,\sigma(n)) = +(\cdot(n,m), n).$$

Beweis: Wir zeigen exemplarisch (i). Für die natürliche Zahl m erhalten wir mit Satz I.2.6 die Funktion $f_m\colon \mathbb{N} \to \mathbb{N}$ wie folgt: Wähle $x = m$ und $g_n := \sigma$.

Dann ist $f_m(0) = m$ und $f_m(\sigma(n)) = \sigma(f_m(n))$. Nun können wir „+“ definieren als

$$+ \colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \qquad (m, n) \longmapsto f_m(n).$$

Diese Funktion „+“ hat die gewünschten Eigenschaften. □

3. Das Prinzip des kleinsten Täters

Definition I.3.1 (Anordnung auf $\mathbb{N}$): Für natürliche Zahlen m und n definieren wir $m \leq n$, falls es eine natürliche Zahl k mit $n = m + k$ gibt.

Proposition I.3.2 („$\leq$“ als Ordnungsrelation): *Die Menge*

$$R := \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m \leq n\}$$

ist eine totale Ordnungsrelation*, d. h. R ist eine Ordnungsrelation und für alle $m, n \in \mathbb{N}$ gilt $m \leq n$ oder $n \leq m$.*

Der Beweis der Proposition wird Ihre Aufgabe auf einem Übungsblatt werden.

Proposition I.3.3 („Kürzbarkeit“ bei Ungleichungen):

(i) *Für alle $k, m, n \in \mathbb{N}$ gilt $k + n \leq m + n$ genau dann, wenn $k \leq m$,*

(ii) *Für alle $k, m, n \in \mathbb{N}$ gilt $km \leq kn$ genau dann, wenn $m \leq n$*

Beweis: Wir zeigen exemplarisch (i), (ii) zeigt man analog.

„$\Rightarrow$“: Seien $k, n, m \in \mathbb{N}$ mit $k + n \leq m + n$. Per Definition gibt es eine natürliche Zahl ℓ, sodass $m + n = k + n + \ell$, d. h. wegen der Kommutativtität der Addition haben wir $m + n = k + \ell + n$. Wegen Proposition I.1.7 (i) haben wir $m = k + \ell$, also ist $k \leq m$.

„$\Leftarrow$“: Seien k und m natürliche Zahlen mit $k \leq n$. Per Definition gibt es $\ell \in \mathbb{N}$ mit $m = k + \ell$, d. h. $m + n = k + \ell + n$. Mit der Assoziativität und Kommutativität der Addition ist also $m + n = k + n + \ell$, d. h. $k + n \leq m + n$.□

Definition I.3.4: Seien m und n natürliche Zahlen. Wir definieren $m \geq n$, falls $n \leq m$; $m < n$, falls $m \leq n$ und $m \neq n$ sowie $m > n$, falls $n \leq m$ und $m \neq n$.

Definition I.3.5 (Ordnungsmengen): Sei n eine natürliche Zahl. Wir setzen

$$\mathbb{N}_{\geq n} := \{k \in \mathbb{N} \mid k \geq n\}, \quad \mathbb{N}_{\leq n} := \{k \in \mathbb{N} \mid k \leq n\}$$

und definieren analog die Mengen $\mathbb{N}_{<n}$ und $\mathbb{N}_{>n}$.

Bemerkung I.3.6: Seien n und m natürliche Zahlen. Die Zahl m ist genau dann echt größer als n, wenn m nicht kleinergleich n ist. Somit haben wir die Zerlegungen $\mathbb{N} = \mathbb{N}_{\leq n} \cup \mathbb{N}_{>n}$ und $\mathbb{N} = \mathbb{N}_{\geq n} \cup \mathbb{N}_{<n}$. Einige offensichtliche Regeln für „$\leq$“ sind:

(i) Jede natürliche Zahl ist größergleich Null.

(ii) Jede natürliche Zahl die kleinergleich Null ist, ist gleich Null.

(iii) Für alle natürlichen Zahlen m, n gilt: Ist $m < n + 1$, dann ist $m \leq n$.

(iv) Sind n, m und k natürliche Zahlen, dann gilt: Ist $n > m$ und $m > k$, dann ist $n > k$.

Satz I.3.7 (Prinzip des kleinsten Täters): *Die natürlichen Zahlen sind, zusammen mit der oben definierten Ordnung, eine Wohlordnung. Das heißt, dass jede nicht-leere Teilmenge M von $\mathbb{N}$ ein kleinstes Element besitzt, in Zeichen: „$\exists\, m_0 \in M : \forall\, n \in M : m_0 \leq n$“.*

Beispiel I.3.8 (Null als kleinste natürliche Zahl): Null ist die kleinste natürliche Zahl, d. h. für alle natürlichen Zahlen n gilt $0 \leq n$. Das folgt aus Bemerkung I.3.6.

Beweis: Per vollständiger Induktion nach n zeigen wir die folgende Aussage: Ist M eine Teilmenge von $\mathbb{N}$ und gibt es $m \in \mathbb{N}$, sodass $m \leq n$ und $m \in M$, dann hat M ein kleinstes Element.

Für den Induktionsanfang sei $n = 0$. Dann gehört Null zu M und nach Bemerkung I.3.6 ist Null das kleinste Element von M.

Für den Induktionsschritt gelte die Aussage für eine natürliche Zahl n. Wir zeigen, dass die Aussage dann auch für $n + 1$ gilt. Sei also $M \subseteq \mathbb{N}$ und es gebe $m \in \mathbb{N}$, sodass $m \leq n + 1$ und $m \in M$.

Ist $n + 1$ kleinstes Element von M, dann sind wir fertig. Ist $n + 1$ nicht das kleinste Element von M, dann gibt es ein $m \in M$, sodass $m < n + 1$. Nach Induktionsvoraussetung hat M jetzt ein kleinestes Element. □

Satz I.3.9 (Schubfachprinzip): *Seien n und m natürliche Zahlen mit $m > n$ und $f \colon \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$. Dann ist f nicht injektiv, d. h. es gibt verschiedene a und b in $\mathbb{N}_{\leq m}$ mit $f(a) = f(b)$.*

Beweis: Wir zeigen die Behauptung via Induktion nach n.

Ist $n = 0$, dann ist $\mathbb{N}_{\leq n} = \mathbb{N}_{\leq 0} = \{0\}$. Nach Bemerkung Bemerkung I.3.6 sind 0 und 1 enthalten in $\mathbb{N}_{\leq 1}$, wir haben also $0 = f(0) = 1$ und f ist nicht injektiv.

Unsere Induktionsvoraussetzung ist, dass für alle natürlichen Zahlen m, die größer sind als n, jede Abbildung $f\colon \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$ nicht injektiv ist. Seien jetzt $m > n+1$ und $f\colon \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n+1}$ eine Abbildung. Wir zeigen, dass f nicht injektiv ist.

Da m größer ist als $n+1$, ist m jedenfalls nicht Null, das heißt wir finden $m' \in \mathbb{N}$, sodass $m = m' + 1$.

Gibt es $a \in \mathbb{N}_{\leq m'}$, das $f(a) = f(m)$ leistet, dann gilt die Behauptung und wir sind fertig.

Gilt für $a \in \mathbb{N}_{\leq m'}$, dass $f(a) \neq f(m)$, dann definieren wir

$$g\colon \mathbb{N}_{\leq n-1} - \{f(m)\} \longrightarrow \mathbb{N}_{\leq n}, \qquad i \longmapsto \begin{cases} i, & \text{falls } i < n+1, \\ f(m), & \text{falls } i = n+1. \end{cases}$$

Wir bemerken, dass der zweite Fall in der Definition von g für $f(m) = n+1$ nicht eintritt.

Da für $a \leq m'$ gilt, dass $f(a) \neq f(m)$, ist $g \circ f|_{\mathbb{N}_{\leq m'}}\colon \mathbb{N}_{m'} \to \mathbb{N}_{\leq n}$ mit $m' > n$. Das folgt aus Proposition I.3.3. Nach Induktionsvoraussetzung gibt es verschiedene a und b in $\mathbb{N}_{m'}$, sodass $g(f(a)) = g(f(b))$. Da g injektiv ist, folgt daraus $f(a) = f(b)$. □

Bemerkung I.3.10 (Interpretation des Schubfachprinzips): Aus Satz I.3.9 über das Schubfachprinzip folgt: Sind n und m positive natürliche Zahlen mit $n > m$ und verteilt man n Objekte auf m Mengen, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Bemerkung I.3.11: (i) Das Prinzip des kleinsten Täters ist äquivalent zum Axiom (P5).

(ii) Sind m und n natürliche Zahlen und ist $m \geq n$, dann existiert per Definition eine natürliche Zahl k, sodass $m = n + k$. In diesem Fall können wir $m - n := k$ als Differenz von m und n definieren. Das geht aber nicht für beliebige natürliche Zahlen m und n. Wir wollen im Folgenden die natürlichen Zahlen so erweitern, dass Gleichungen der Form $m = n + x$ immer eine Lösung haben. Dazu betrachten wir die Relation R auf $\mathbb{N} \times \mathbb{N}$, die erklärt ist durch

$$(a, b)R(a', b') \Leftrightarrow a + b' = b + a'.$$

4. Die ganzen Zahlen

Im Folgenden schreiben wir statt R oft $\sim$ für eine Äquivalenzrelation und statt aRb, was ja für $(a, b) \in R$ steht, schreiben wir einfach $a \sim b$. Ist $R \subseteq A \times A$, dann sprechen wir von einer Äquivalenzrelation auf A.

Definition I.4.1 (Äquivalenzklassen): Sei $\sim$ eine Äquivalenzrelation auf einer Menge A.

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

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

(iii) Seien a und a' Elemente von A. Gilt $a' \in [a]$, dann heißt a' *Repräsentant der Restklasse von a.*

Erinnerung I.4.2: Seien A eine Menge und $\sim$ eine Äquivalenzrelation auf A. Dann ist A die disjunkte Vereinigung seiner Äquivalenzklassen, d. h. es gilt

(i) Jedes Element von A gehört zu einer Äquivalenzklasse,

(ii) Sind a, b Elemente von A und ist $[a] \neq [b]$, dann ist sogar $[a] \cap [b] = \varnothing$.

Beispiel I.4.3: Auf den natürlichen Zahlen erklärt

$$a \sim b \iff \text{Es gibt } k \in \mathbb{N} \text{ mit } a = b + 3k \text{ oder } b = a + 3k\}$$

eine Äquivalenzrelation (überzeugen Sie sich davon). Es sind

$$[0] = \{0, 3, 6, 9, 12, \dots\}, \quad [1] = \{1, 4, 7, 10, 13, \dots\}, \quad [2] = \{2, 5, 8, 11, 14, \dots\}$$

und das sind auch die einzigen Äquivalenzklassen; d. h. $\mathbb{N}/\sim = \{[0], [1], [2]\}$.

Sind a und b natürliche Zahlen, dann hat die Gleichung $x + b = a$ im Allgemeinen keine Lösung in den natürlichen Zahlen. Diesem Problem wollen wir begegnen, indem wir x als Lösung von $x + b = a$ mithilfe der Daten $(a, b) \in \mathbb{N} \times \mathbb{N}$ beschreiben.

Stünden uns die ganzen Zahlen schon zur Verfügung, dann wäre $x = a - b$ eine Lösung der Gleichung. Wäre x Lösung einer weiteren Gleichung $x = a' - b'$, dann gälte $a + b' = a' + b$.

Im Folgenden wollen wir uns von der Eindeutigkeit der Lösung x überzeugen. Dazu überlegen wir uns, wann die Gleichungen $x + b = a$ und $x + b' = a'$ dieselbe Lösung haben.

Seien a, a', b, b' und x natürliche Zahlen. Gilt $x + b = a$ und $x + b' = a'$, dann haben wir auch $x + b + a' = x + b' + a$, also nach Proposition I.3.3 $b + a' = a + b'$. Haben also die Gleichungen $x + b = a$ und $x + b' = a'$ dieselbe Lösung, dann gilt schon $a + b' = a' + b$.

Ist andersherum $a + b' = a' + b$ und gilt $x + b = a$, dann haben wir

$$x + b' + a = x + a' + b = a + a',$$

also nach Proposition I.3.3 auch $x + b' = a'$. Das heißt: Ist $a + b' = a' + b$ und hat die Gleichung $x + a = b$ eine Lösung, dann hat auch $x + a' = b'$ eine Lösung; und zwar die gleiche wie $x + b = a$.

Ein zielführender Ansatz ist also, x aus der Gleichung $x+b = a$ mit dem Tupel $(a, b) \in \mathbb{N} \times \mathbb{N}$ zu identifizieren und diejenigen Tupel (a, b) und $(a', b') \in \mathbb{N} \times \mathbb{N}$ nicht zu unterscheiden, für die $a + b' = a' + b$ gilt. Das richtige Werkzeug für diese Einteilung der Tupel in $\mathbb{N} \times \mathbb{N}$ ist eine Äquivalenzrelation.

Proposition I.4.4: *Sei $A = \mathbb{N} \times \mathbb{N}$. Auf A wird durch*

$$(a, b) \sim (a', b') \iff a + b' = b + a'$$

eine Äquivalenzrelation erklärt.

Beweis: Die Relation $\sim$ ist reflexiv, denn für alle $(a, b) \in A$ gilt $a + b = b + a$.

Sind (a_1, b_1) und (a_2, b_2) Elemente von A mit $(a_1, b_1) \sim (a_2, b_2)$, dann folgt $a_1 + b_2 = b_1 + a_2$, d. h. wegen der Kommutativität $a_2 + b_1 = b_2 + a_1$, also $(a_2, b_2) \sim (a_1, b_1)$, d. h. die Relation ist symmetrisch.

Schließlich ist die Relation transitiv, denn für (a_1, b_1), (a_2, b_2) und (a_3, b_3) aus A mit $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$ hätten wir $a_1 + b_2 = b_1 + a_2$ und $a_2 + b_3 = a_3 + b_2$, d. h. es wäre

$$a_1 + b_2 + a_2 + b_3 = b_1 + a_2 + b_2 + a_3,$$

mit Proposition I.3.3 also $a_1 + b_3 = b_1 + a_3$, d. h. $(a_1, b_1) \sim (a_3, b_3)$. □

Definition I.4.5 (ganze Zahlen): Die Menge der Äquivalenzklassen für die Äquivalenzrelation aus Proposition I.4.4 nennen wir die *Menge der ganzen Zahlen* und notieren sie mit $\mathbb{Z}$, d. h. $\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim$.

Die Abbildung $\iota\colon \mathbb{N} \to \mathbb{Z}$, $n \mapsto [(n, 0)]$ ist injektiv. Sind nämlich $(n_1, 0)$, $(n_2, 0)$ Repräsentanten derselben Äquivalenzklasse, dann gilt $n_1 + 0 = n_2 + 0$, also $n_1 = n_2$. Via ι fassen wir $\mathbb{N}$ als Teilmenge von $\mathbb{Z}$ auf.

Notation: Seien n eine natürliche Zahl und k eine positive natürliche Zahl. Wir schreiben $n := [(n, 0)]$ und $-k := [(0, k)]$.

Wir wollen im Folgenden eine Addition und eine Multiplikation auf $\mathbb{Z}$ erklären. Sind $a = [(a_1, a_2)]$ und $b = [(b_1, b_2)]$ Elemente von $\mathbb{Z}$, dann gilt

$$a_1 - a_2 + b_1 - b_2 = a_1 + b_1 - (a_2 + b_2),$$
$$(a_1 - a_2) \cdot (b_1 - b_2) = a_1 b_1 + a_2 b_2 - (a_1 b_2 + a_2 b_1).$$

Beispiel: Wir betrachten $[(4,1)]$ und $[(0,2)]$ aus $\mathbb{Z}$. Einsetzen in die Definitionen für Addition und Multiplikation liefert

$$[(4,1)] + [(0,2)] = [(1,0)] = [(4,3)], \qquad [(4,1)] \cdot [(0,2)] = [(0,6)] = [(2,8)].$$

Lemma I.4.6 (Addition und Multiplikation): *Die folgenden Abbildungen sind wohldefiniert und hängen nicht von den gewählten Vertretern ab:*

$$\begin{aligned} +\colon \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}, \qquad ([(a_1,a_2)],[(b_1,b_2)]) \longmapsto [(a_1+b_1, a_2+b_2)], \\ \cdot\colon \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}, \qquad ([(a_1,a_2)],[(b_1,b_2)]) \longmapsto [(a_1b_1+a_2b_2, a_1b_2+a_2b_1)] \end{aligned}$$

Beweis: Wir zeigen exemplarisch, dass die Addition wohldefiniert ist. Der Beweis für die Multiplikation geht analog.

Seien dazu $(a_1,a_2),(b_1,b_2),(a_1',a_2'),(b_1',b_2') \in A$ mit $(a_1,a_2) \sim (a_1',a_2')$ und $(b_1,b_2) \sim (b_1',b_2')$. Wir müssen zeigen, dass (a_1+b_1, a_2+b_2) in derselben Äquivalenzklasse liegt wie $(a_1'+b_1', a_2'+b_2')$. Wegen der Definition der Relation „$\sim$“ haben wir, dass $a_1'+a_2 = a_2'+a_1$ sowie $b_1'+b_2 = b_2'+b_1$. Damit erhalten wir

$$a_1'+b_1'+a_2+b_2 = a_2'+b_2'+a_1+b_1,$$

d. h. $(a_1'+b_1', a_2'+b_2') \sim (a_1+b_1, a_2+b_2)$, was die Wohldefiniertheit von „$+$“ zeigt. □

Proposition I.4.7 (Strukturelle Eigenschaften von $+$ und $\cdot$): *Die Verknüpfungen „$+$“ und „$\cdot$“ sind beide assoziativ und kommutativ. Für „$+$“ und „$\cdot$“ gelten die Distributivgesetze. Für alle ganzen Zahlen a gilt $a+0 = a = 0+a$, $a \cdot 1 = a = 1 \cdot a$ und $a \cdot 0 = 0 = 0 \cdot a$. Schließlich sind die ganzen Zahlen nullteilerfrei, d. h. es gilt für alle ganzen Zahlen a, b: Ist $a \cdot b = 0$, dann ist schon $a = 0$ oder $b = 0$.*

Beweis: Wir zeigen exemplarisch die Distributivität. Sind dazu $a = [(a_1,a_2)]$, $b = [(b_1,b_2)]$ und $c = [(c_1,c_2)] \in \mathbb{Z}$, dann rechnen wir nach, dass

$$\begin{aligned} (a+b) \cdot c &= [(a_1+b_1, a_2+b_2)] \cdot [(c_1,c_2)] \\ &= [(a_1c_1 + b_1c_1 + a_2c_2 + b_2c_2, a_1c_2 + b_1c_2 + a_2c_1 + b_2c_1)] \\ &= [(a_1c_1 + a_2c_2, a_1c_2 + a_2c_1)] + [(b_1c_1 + b_2c_2, b_1c_2 + b_2c_1)] \\ &= ([(a_1,a_2)] \cdot [(c_1,c_2)]) + ([(b_1,b_2)] \cdot [(c_1,c_2)]) = a \cdot c + b \cdot c, \end{aligned}$$

was wir zeigen wollten. □

Notation I.4.8: Ab jetzt folgen wir der Konvention „Punkt vor Strich“, d. h. wir führen Multiplikation vor Addition aus und sparen uns auf diese Weise Klammern in der Notation.

Proposition I.4.9: *Für ganze Zahlen a und b hat die Gleichung $a + x = b$ stets genau eine Lösung in $\mathbb{Z}$, d. h. „$\forall\, a, b \in \mathbb{Z}\, \exists!\, x \in \mathbb{Z} : a + x = b$“.*

Beweis: Seien ganze Zahlen $a = [(a_1, a_2)]$, $b = [(b_1, b_2)]$ und $x = [(x_1, x_2)]$ vorgegeben. Dann haben wir die Äquivalenzen

$$\begin{aligned} x + b = a &\iff [(x_1 + b_1, x_2 + b_2)] = [(a_1, a_2)] \\ &\iff x_1 + b_1 + a_2 = x_2 + b_2 + a_1 \\ &\iff [(x_1, x_2)] = [(a_1 + b_2, a_2 + b_1)] \end{aligned}$$

was unsere Behauptung zeigt. □

Definition I.4.10 (Differenz): Für ganze Zahlen $a = [(a_1, a_2)]$ und $b = [(b_1, b_2)]$ heißt

$$b - a := [(a_2 + b_1, a_1 + b_2)]$$

die *Differenz von b und a*.

Sind a und b ganze Zahlen, dann ist $a - b$ das eindeutige Element $x \in \mathbb{Z}$, das $x + b = a$ leistet.

Proposition I.4.11 (Additive Inverse): *Seien a und b ganze Zahlen.*

(i) *Es gibt genau eine ganze Zahl c, die $b + c = 0 = c + b$ leistet. Wir schreiben $-b := c$. Insbesondere gilt $0 - b = -b$.*

(ii) *Für die Differenz $a - b$ gilt $a - b = a + (-b)$.*

(iii) *Es ist $(-1) \cdot a = -a$.*

Beweis: (i) Diese Aussage ist eine direkte Konsequenz von Proposition I.4.9 und Definition I.4.10.

(ii) Unter Verwendung von $b + (-b) = 0 = (-b) + b$ können wir schreiben $a + (-b) + b = a + 0 = a$, mit Definition I.4.10 liefert das die Behauptung.

(iii) Wir rechnen nach, dass

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0,$$

wie gewünscht. □

Sind a_1, a_2, b_1 und b_2 natürliche Zahlen, dann gilt $a_1 - a_2 \leq b_1 - b_2$ genau dann, wenn $a_1 + b_2 \leq a_2 + b_1$. Dies wollen wir uns zunutze machen, um auf den ganzen Zahlen eine Ordnung zu erklären. Wir werden sehen, dass diese Ordnung die bereits bekannte Ordnung auf den natürlichen Zahlen fortsetzt, d. h. die Einschränkung dieser Ordnung auf den ganzen Zahlen auf die Teilmenge $\iota(\mathbb{N})$ reproduziert $(\mathbb{N}, \leq)$.

Definition I.4.12 (Ordnung auf den ganzen Zahlen): Wir definieren die Relation „$\leq$“ auf den ganzen Zahlen wie folgt: Für ganze Zahlen $a = [(a_1, a_2)]$ und $b = [(b_1, b_2)]$ gilt

$$a \leq b \iff a_1 + b_2 \leq a_2 + b_1.$$

Diese Definition ist unabhängig von den gewählten Vertretern und eine Ordnungsrelation. Das werden Sie auf dem folgenden Übungsblatt nachweisen dürfen. Weiter können wir die Symbole „$\geq$“, „$<$“ und „$>$“ wie für die Ordnung auf den natürlichen Zahlen erklären.

Proposition I.4.13 (Eigenschaften der Ordnung):

(i) *„$\leq$“ setzt die Ordnungsrelation „$\leq$“ auf $\mathbb{N}$ fort.*

(ii) *Für ganze Zahlen a, b gilt $a \leq b$ genau dann, wenn $b - a \geq 0$.*

(iii) *Für alle ganzen Zahlen a, b, c gilt $a \leq b$ genau dann, wenn $a + c \leq b + c$.*

(iv) *Für alle ganzen Zahlen a, b und eine natürliche Zahl m gilt: Ist $a \leq b$, dann ist auch $am \leq bm$.*

(v) *Für alle ganzen Zahlen a, b und $m \in \mathbb{Z}$ mit $-m \in \mathbb{N}$ gilt: Ist $a \leq b$, dann ist $am \geq bm$.*

(vi) *Seien a und b ganze Zahlen. Gilt $a, b \geq 0$, dann ist auch $a \cdot b \geq 0$. Ist $a \geq 0$ und $b \leq 0$, dann ist $a \cdot b \leq 0$. Sind $a, b \leq 0$, dann ist $a \cdot b \geq 0$.*

Beweis: (i) Seien $[(a, 0)], [(b, 0)]$ ganze Zahlen. Es gilt $[(a, 0)] \leq [(b, 0)]$ per Definition genau dann, wenn $a + 0 \leq b + 0$. Aber das gilt nach Proposition I.3.3 genau dann, wenn $a \leq b$.

(ii) Seien $a = [(a_1, a_2)]$ und $b = [(b_1, b_2)]$ ganze Zahlen. Unter Verwendung von Definition I.4.10 und Definition I.4.12 erkennen wir die Äquivalenzen

$$\begin{aligned} b - a \geq 0 &\iff [(b_1 + a_2, b_2 + a_1)] \geq 0 \\ &\iff b_2 + a_1 \leq b_1 + a_2 \iff [(a_1, a_2)] \leq [(b_1, b_2)]. \end{aligned}$$

(iii) Wegen (ii) ist $a \leq b$ genau dann, wenn $b - a = b + c - (c + a) \geq 0$. Wieder wegen (ii) ist das äquivalent zu $b + c \geq a + c$.

Die Beweise für die restlichen Aussagen bleiben Ihnen als Übungsaufgaben überlassen. □

5. Die rationalen Zahlen

Durch die Konstruktion der ganzen Zahlen haben wir uns eindeutige Lösungen für Gleichungen der Bauart $a + x = b$ verschafft, wobei a, b ganze Zahlen sind. Gleichungen der Bauart $a \cdot x = b$ für ganze Zahlen a, b können wir in den ganzen Zahlen aber (meist) nicht lösen. Wieder wollen wir diesem Problem mit Zahlbereichserweiterung begegnen, das heißt der Gleichung $b \cdot x = a$ ordnen wir wieder das Tupel (a, b) zu. Wir hätten gerne, dass zwei Tupel zu dem Bruch zugeordnet werden, „in den sie gekürzt werden können“, das heißt wir sollten die Relation „$\sim$“ auf $\mathbb{Z} \times (\mathbb{Z} - \{0\})$, die durch

$$(a, b) \sim (a', b') :\Longleftrightarrow a \cdot b' = a' \cdot b$$

erklärt wird, betrachten.

Ein entscheidendes Werkzeug im Folgenden wird die *Kürzungsregel* sein: Ist $x \neq 0$ und gilt $a \cdot x = a' \cdot x$, dann ist schon $a = a'$. Das folgt aus der Nullteilerfreiheit von $\mathbb{Z}$ (siehe Proposition I.4.7), ist nämlich $a \cdot x = a' \cdot x$, dann ist $(a - a') \cdot x = 0$, woraus wir wegen $x \neq 0$ folgern können, dass $a = a'$.

Bemerkung I.5.1: Seien a, a' ganze Zahlen und b, b' von Null verschiedene natürliche Zahlen.

(i) Die Gleichung $b \cdot x = a$ hat höchstens eine Lösung,

(ii) Die Gleichungen $b \cdot x = a$ und $b' \cdot x = a$ haben genau dann die gleiche Lösung x_0, wenn $a \cdot b' = a' \cdot b$.

Beweis: (i) Angenommen wir hätten $b \cdot x = a$ und $b \cdot x' = a$. Dann ist $b \cdot (x - x') = b \cdot x - b \cdot x' = a - a = 0$. Nach Proposition I.4.7 muss dann $x - x' = 0$ gelten, d. h. $x = x'$.

(ii) „$\Rightarrow$“: Zunächst gelte $x_0 \neq 0$. Gilt $b \cdot x = a$ sowie $b' \cdot x = a'$, dann haben wir $b \cdot x \cdot a' = a \cdot b' \cdot x$, d. h. mit Proposition I.4.7 folgt $ab' = ba'$. Ist $x_0 = 0$, dann ist $a = a' = 0$ und die Behauptung folgt.

„$\Leftarrow$“: Wir wissen: Gilt $a \cdot b' = a' \cdot b$ und ist $a = 0$, dann ist wegen $a = a'$ schon $a' = 0$, da die ganzen Zahlen nach Proposition I.4.7 nullteilerfrei sind.

Sei jetzt $x_0 \in \mathbb{Z}$ mit $b \cdot x_0 = a$. Ist $a \neq 0$, dann haben wir

$$b' \cdot x_0 \cdot a = a' \cdot b \cdot x_0 = a' \cdot a,$$

weil a nicht Null ist, können wir also mit der Kürzungsregel folgern, dass $b' \cdot x_0 = a'$.

Ist $a = 0$, dann gibt unsere Vorüberlegung, dass auch $a' = 0$ ist. Außerdem ist $b \cdot x_0 = 0$, weil aber b nach Voraussetzung nicht Null ist, muss $x_0 = 0$ sein und wir haben $b' \cdot x_0 = 0 = a'$. □

Proposition I.5.2 (Die Quotientenrelation): *Die Relation „$\sim$“ auf der Menge* $S := \mathbb{Z} \times (\mathbb{Z} - \{0\})$ *gegeben durch*

$$(x_1, x_2) \sim (y_1, y_2) : \Longleftrightarrow x_1 y_2 = x_2 y_1$$

ist eine Äquivalenzrelation.

Beweis: Der Beweis funktioniert fast genau wie für Proposition I.4.4. Die Reflexivität und Symmetrie sieht man durch direktes Einsetzen. Nun zur Transitivität der Relation: Seien (a_1, b_1), (a_2, b_2) und (a_3, b_3) in $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ mit $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$. Dann haben wir $a_1 \cdot b_2 = b_1 \cdot a_2$ und $a_2 \cdot b_3 = a_3 \cdot b_2$, also

$$a_1 \cdot b_2 \cdot a_2 \cdot b_3 = b_1 \cdot a_2 \cdot b_2 \cdot a_3.$$

Ist $a_2 \neq 0$, dann können wir mit der Kürzungsregel $a_1 \cdot b_3 = a_3 \cdot b_1$ folgern. Ist $a_2 = 0$, dann liefert die Nullteilerfreiheit von $\mathbb{Z}$ (Proposition I.4.7) angewendet auf auf die ersten beiden Gleichungen, dass dann auch a_1 und a_3 Null sein müssen, d. h. $a_1 \cdot b_3 = b_1 \cdot a_3$. □

Definition I.5.3 (der rationalen Zahlen): Die Menge $\mathbb{Q} := S/\sim$ der Äquivalenzklassen von $\sim$ heißt *Menge der rationalen Zahlen.*

Proposition I.5.4 (Der Körper der rationalen Zahlen): (i) *Die Verknüpfungen „$+$“ und „$\cdot$“ auf* $\mathbb{Q}$ *definiert durch*

$$[(x_1, x_2)] + [(y_1, y_2)] := [(x_1 y_2 + x_2 y_1, x_2 y_2)],$$
$$[(x_1, x_2)] \cdot [(y_1, y_2)] := [(x_1 y_1, x_2 y_2)]$$

sind wohldefiniert und unabhängig von den gewählten Vertretern.

(ii) *Die Verknüpfungen „$+$“, „$\cdot$“ sind kommutativ, assoziativ und es gelten die Distributivgesetze.*

(iii) *Für alle rationalen Zahlen* x *gilt* $1 \cdot x = x = x \cdot 1$ *sowie* $x + 0 = x = 0 + x$.

(iv) *Für jede rationale Zahl* x *gibt es eine rationale Zahl* y, *sodass*

$$x + y = 0 = y + x.$$

Ist x *verschieden von Null, dann gibt es* $y \in \mathbb{Q}$ *mit* $x \cdot y = 1 = y \cdot x$.

Beide y *sind eindeutig bestimmt und werden mit* $-x$ *beziehungsweise* $1/x$ *bezeichnet.*

Beweis: Die Beweise von (i) und (ii) gehen ähnlich wie die Beweise von Lemma I.4.6 und Proposition I.4.7.

Zu (iii): Für $x = [(x_1, x_2)]$, $0 = [(0,1)]$ und $1 = [(1,1)]$ können wir einfach nachrechnen, dass

$$0 + x = x + 0 = [(x_1, x_2)] + [(0,1)] = [(x_1 \cdot 1 + x_2 \cdot 0, x_2 \cdot 1)] = [(x_1, x_2)] = x,$$

sowie

$$1 \cdot x = x \cdot 1 = [(x_1, x_2)] \cdot [(1,1)] = [(x_1 \cdot 1, x_2 \cdot 1)] = [(x_1, x_2)] = x.$$

Zu (iv): Seien $x = [(x_1, x_2)]$ und $y = [(y_1, y_2)]$. Dann gilt

$$\begin{aligned} x + y = y + x = 0 &\iff [(x_1y_2 + x_2y_1, x_2y_2)] = [(0,1)] \\ &\iff (x_1y_2 + x_2y_1) \cdot 1 = x_2y_2 \cdot 0 \\ &\iff x_1y_2 + x_2y_1 = 0 \\ &\iff -x_1y_2 = x_2y_1 \iff [(y_1, y_2)] = [(-x_1, x_2)], \end{aligned}$$

das heißt es gibt so ein y und es ist eindeutig bestimmt – nämlich $y = [(-x_1, x_2)]$. Weiter berechnen wir

$$\begin{aligned} x \cdot y = 1 = y \cdot x &\iff [(x_1, x_2)] \cdot [(y_1, y_2)] = [(1,1)] \\ &\iff [(x_1y_1, x_2y_2)] = [(1,1)] \\ &\iff x_1y_1 \cdot 1 = x_2y_2 \cdot 1 \iff [(y_1, y_2)] = [(x_2, x_1)] \end{aligned}$$

was den Beweis beschließt. □

Korollar I.5.5 (Additive und multiplikative Inverse): *Aus dem Beweis von Proposition I.5.4 folgt, dass für $x = [(x_1, x_2)] \in \mathbb{Q}$ gilt:*

$$-x = [(-x_1, x_2)], \qquad x^{-1} = [(x_2, x_1)].$$

Korollar I.5.6: *Seien a und b rationale Zahlen, a verschieden von Null. Dann hat $a \cdot x = b$ eine eindeutige Lösung, nämlich $x = 1/a \cdot b$.*

Beweis: Ist $b \neq 0$, dann gilt $b \cdot x = a$ genau dann, wenn $1/b \cdot b \cdot x = 1/b \cdot a$, aber das ist äquivalent zu $x = 1/b \cdot a$. Hieraus folgen sowohl Existenz als auch Eindeutigkeit der Lösung. □

Für jede rationale Zahl $x = [(x_1, x_2)]$ gilt $x \cdot 0 = [(x_1, x_2)] \cdot [(0,1)] = [(0, x_2)] = 0$.

Notation I.5.7: Sind x und y ganze Zahlen, y verschieden von Null, dann schreiben wir ab jetzt $x/y := [(x, y)]$.

Für rationale Zahlen x und y, wobei y von Null verschieden ist, schreiben wir ab jetzt $x/y := 1/y \cdot x$. Diese Schreibweisen sind verträglich miteinander, denn

$$\frac{1}{[(y,1)]} \cdot [(x,1)] = [(1,y)] \cdot [(x,1)] = [(x,y)].$$

Für $x, y \in \mathbb{Q}$ schreiben wir $x - y$ für $x + (-y)$.

Bemerkung I.5.8 (Rechengesetze für $\mathbb{Q}$): Mit der Notation aus Notation I.5.7 gelten die folgenden Rechengesetze für rationale Zahlen x, y, z, w, a, wobei z, w und a verschieden von Null sind:

(i) Ist $v := x/z$, dann ist $-v = (-x)/z$ und $1/v = z/x$,

(ii) Für die Brüche x/z und y/w sind

$$\frac{x}{z} \cdot \frac{y}{w} = \frac{x \cdot y}{z \cdot w}, \qquad \frac{x}{z} + \frac{y}{w} = \frac{x \cdot w + y \cdot z}{z \cdot w}, \qquad \frac{x \cdot a}{z \cdot a} = \frac{x}{z}.$$

Beweis: Alle Behauptungen lassen sich durch einfaches Nachrechnen zeigen. Wir zeigen exemplarisch, dass $x/z \cdot y/w = (x \cdot y)/(z \cdot w)$. Schreibe dazu $z = [(z_1, z_2)]$ und $w = [(w_1, w_2)]$. Dann ist

$$\begin{aligned}\frac{x}{z} \cdot \frac{y}{w} = \frac{1}{z} \cdot x \cdot \frac{1}{w} \cdot y &= [(z_2, z_1)] \cdot x \cdot [(w_2, w_1)] \cdot y \\ &= [(z_2 \cdot w_2, z_1 \cdot w_1)] \cdot x \cdot y = \frac{x \cdot y}{[(z_1 w_1, z_2 w_2)]} = \frac{x \cdot y}{z \cdot w}. \quad \square\end{aligned}$$

Definition I.5.9 (Ordnung auf $\mathbb{Q}$): Seien $x = x_1/x_2$ und $y = y_1/y_2$, wobei $x_1, y_1 \in \mathbb{Z}$ und $x_2, y_2 \in \mathbb{N} - \{0\}$.

(i) Auf $\mathbb{Q}$ definieren wir die Relation „$\leq$“ durch

$$0 \leq x :\Longleftrightarrow 0 \leq x_1 \quad \text{in } \mathbb{Z}, \qquad y \leq x :\Longleftrightarrow 0 \leq x - y.$$

(ii) Definiere die Abbildung $|\cdot| \colon \mathbb{Q} \to \mathbb{Q}_{\geq 0} = \{x \in \mathbb{Q} \mid x \geq 0\}$ durch

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

(iii) Definiere die Abbildung $d\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_{\geq 0}$ durch $d(x, y) := |x - y|$.

Genau wie in Definition I.3.4 erklären wir die Symbole „$\geq$“, „$<$“ und „$>$“.

Bemerkung I.5.10 (Eigenschaften der Ordnung auf $\mathbb{Q}$): Es gelten die Analoga der Eigenschaften aus Proposition I.4.13, das heißt:

(i) Die Relation „$\leq$“ ist eine totale Ordnungsrelation,

(ii) Die Relation „$\leq$“ setzt die Ordnung „$\leq$“ auf $\mathbb{Z}$ fort auf $\mathbb{Q}$,

(iii) Für alle $a, b \in \mathbb{Q}$ gilt $a \leq b$ genau dann, wenn $b - a \geq 0$,

(iv) Für alle $a, b, c \in \mathbb{Q}$ gilt $a \leq b$ genau dann, wenn $a + c \leq b + c$,

(v) Für alle $a, b \in \mathbb{Q}$ und $c \in \mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ gilt $a \leq b$ genau dann, wenn $c \cdot a \leq c \cdot b$.

(vi) Für alle $a, b \in \mathbb{Q}$ und $c \in \mathbb{Q}_{<0} := \{x \in \mathbb{Q} \mid x < 0\}$ gilt $a \leq b$ genau dann, wenn $a \cdot c \geq b \cdot c$.

(vii) Für alle $a, b \in \mathbb{Q}$ gilt: Sind $a, b \geq 0$, dann ist auch $a \cdot b \geq 0$; sind $a, b \leq 0$, dann ist $a \cdot b \geq 0$ und ist $a \leq 0$ und $b \geq 0$ oder $a \geq 0$ und $b \leq 0$, dann ist $a \cdot b \leq 0$.

Beweis: (i) Man leitet die Reflexivität, Antisymmetrie, Transitivität und Totalität direkt aus den Eigenschaften der Ordnung auf den ganzen Zahlen ab.

(ii) Für alle $a, b \in \mathbb{Z}$ gilt $[(a, 1)] \leq [(b, 1)]$ per Definition genau dann, wenn $[(0, 1)] \leq [(b - a, 1)]$. Das ist wiederum per Definition genau dann der Fall, wenn $0 \leq b - a$, was äquivalent zu $a \leq b$ ist.

(iii) Das folgt aus der Definition.
Aussagen (iii), (iv) und (vi) beleiben Ihnen als Übungsaufgaben überlassen.

(vi) Es ist $x = [(x_1, x_2)] \in \mathbb{Q}_{<0}$ genau dann, wenn $x_1 < 0$. Das ist äquivalent dazu, dass $-x_1 > 0$, was genau dann der Fall ist, wenn $-x = [(-x_1, x_2)] > 0$ gilt. Damit können wir schreiben

$$\begin{aligned}
a \leq b &\iff a \cdot (-c) \leq b \cdot (-c) && \text{[Aussage (v)]} \\
&\iff -ac \leq -bc \\
&\iff 0 \leq -bc + ac = ac - bc && \text{(Definition)} \\
&\iff bc \leq ac && \text{(Definition)} \\
&\iff ac \geq bc && \text{(Definition).}
\end{aligned}$$

□

6. Exkurs zu algebraischen Strukturen

Definition I.6.1 (Verknüpfungen): Seien C eine Menge und $\circ$ eine Verknüpfung auf C, d. h. eine Abbildung $\circ\colon C \times C$. Zur besseren Lesbarkeit schreiben wir $a \circ b$ für $\circ(a, b)$.

(i) Die Verknüpfung heißt *assoziativ*, falls für alle Elemente a, b, c von C gilt, dass $(a \circ b) \circ c = a \circ (b \circ c)$.

(ii) Die Verknüfung heißt *kommutativ*, falls für alle Elemente a, b von C gilt, dass $a \circ b = b \circ a$.

(iii) Ein Element $e \in C$ heißt *neutrales Element*, falls für alle Elemente a von C gilt, dass $a \circ e = a = e \circ a$.

(iv) Gibt es in C ein neutrales Element und sind a und b weitere Elemente von C, so heißen a und b *invers zueinander*, falls $a \circ b = e = b \circ a$.

Neutrale Elemente sind eindeutig. Wäre nämlich e' ein weiteres neutrales Element in C, dann hätten wir $e' = e' \circ e = e$.

Ist die Verknüpfung assoziativ, so sind auch Inverse eindeutig. Wären nämlich a und b Elemente von C und invers zueinander und wäre b' ein weiteres Element von A mit $a \circ b' = e = b' \circ a$, dann hätten wir

$$b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = e \circ b' = b'.$$

Wir nennen b also *das* Inverse von a und schreiben $a^{-1} := b$. Ist die Verknüfpung additiv geschrieben (d. h. ist das Symbol „+“ statt „$\circ$“), dann schreiben wir auch $-a := b$.

Definition I.6.2 (Gruppe): Eine Menge G mit einer Verknüpfung $\circ\colon G \times G \to G$ heißt *Gruppe*, falls gilt:

(i) Die Verknüpfung ist assoziativ,

(ii) Es gibt ein neutrales Element $e \in G$,

(iii) Zu jedem Element $g \in G$ gibt es ein Inverses g^{-1}.

Wir schreiben $(G, \circ)$ für die Gruppe G. Sind keine Verwechslungen bezüglich der gewählten Verknüpfung zu befürchten, so schreiben wir für die Gruppe einfach nur G.

Eine Gruppe $(G, \circ)$ heißt *abelsche Gruppe*, falls die Verknüpfung kommutativ ist.

Beispiel I.6.3 (Gruppe oder nicht?): $(\mathbb{N}, +), (\mathbb{N}, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, +), (\mathbb{Q}, \cdot)$?

Beispiel I.6.4 (Einige Gruppen): (i) Sei n eine positive natürliche Zahl. Wir schreiben $[n] := \{1, \dots, n\}$. Die Menge $S_n := \{f\colon [n] \to [n] \mid f \text{ ist bijektiv}\}$ wird mit der Komposition von Abbildungen eine Gruppe.

Wir drücken eine Funktion $f\colon [n] \to [n]$ aus durch eine Wertetabelle, d. h.

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

Die zugehörige Funktion f ist bijektiv genau dann, wenn $f(1), f(2), \dots, f(n)$ paarweise verschieden sind.

Ist $k \leq n$ und sind $a_1, \dots, a_k \in [n]$, dann schreiben außerdem $(a_1 \dots a_k)$ für die Abbildung, die a_1 auf a_2, a_2 auf a_3, …, a_{k-1} auf a_k und a_k auf a_1 abbildet. Sind $a_1, \dots, a_k$ paarweise verschieden, so gehört die Abbildung zu S_n.

Ist beispielsweise $n = 3$, dann ist S_3 genau die Menge

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$$= \{\mathrm{id}, (23), (12), (123), (132), (13)\}.$$

Allgemein gilt $\#(S_n) = n!$.

(ii) Wir schreiben $\mathbb{Q}^{n\times n}$ für die Menge der $n \times n$-Matrizen mit rationalen Einträgen, d. h. für ein Element $A \in \mathbb{Q}^{n\times n}$ gibt es $a_{11}, \dots, a_{nn} \in \mathbb{Q}$, sodass

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Bezeichnet „+“ die Matrizenaddition (diese ist eintragsweise definiert), dann bildet $(\mathbb{Q}^{n\times n}, +)$ eine Gruppe. Genauso ist $\mathbb{Z}^{n\times n}$ zusammen mit der Matrizenaddition eine Gruppe.

(iii) Es bezeichne $\mathrm{Gl}_n(\mathbb{Q}) := \{A \in \mathbb{Q}^{n\times n} \mid \exists\, B \in \mathbb{Q}^{n\times n} : A \cdot B = B \cdot A = I_n\}$, wobei $I_n = \mathrm{diag}(1, 1, \dots, 1)$ die $n \times n$-Einheitsmatrix ist. Man kann zeigen, dass

$$\mathrm{Gl}_n(\mathbb{Q}) = \{A \in \mathbb{Q}^{n\times n} \mid \det(A) \neq 0\},$$

wobei $\det(A) := \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ die Determinante von A bezeichnet. Zusammen mit der Multiplikation von Matrizen bildet $\mathrm{Gl}_n(\mathbb{Q})$ eine

Gruppe (denn es gilt $\det(AB) = \det(A)\det(B)$). Sie heißt die *allgemeine lineare Gruppe* bzw. *general linear group*. Das Produkt C von zwei Matrizen $A = (a_{ij}), B = (b_{ij}) \in \mathrm{Gl}_n(\mathbb{Q})$ ist eintragsweise erklärt durch

$$C_{ij} := (A \cdot B)_{ij} := \sum_{k=1}^{n} a_{ik} b_{kj}, \qquad 1 \leq i, j \leq n$$

Achtung, die Reihenfolge von A und B spielt hier eine Rolle!

Ist beispielsweise $n = 2$ und sind $A = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right), B = \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right)$ Elemente von $\mathbb{Q}^{2\times 2}$, dann sind

$$\det(A) = a_1 d_1 - b_1 c_1,$$
$$A + B = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}, \qquad A \cdot B = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

Analog ist $\mathrm{Gl}_n(\mathbb{Z}) = \{A \in \mathbb{Z}^{n\times n} \mid \det(A) \in \{\pm 1\}\}$ zusammen mit der Matrizenmultiplikation eine Gruppe. Woher die andere Forderung für die Werte der Determinante kommt, wird später klar.

(iv) Die Menge $\mathrm{Sl}_n(\mathbb{Q}) := \{A \in \mathbb{Q}^{n\times n} \mid \det(A) = 1\}$ bildet zusammen mit der Multiplikation von Matrizen eine Gruppe. Sie heißt *spezielle lineare Gruppe*. Genau so ist $\mathrm{Sl}_n(\mathbb{Z})$ mit der Multiplikation von Matrizen eine Gruppe.

Notation I.6.5 (Potenzen): Seien $(G, \circ)$ eine Gruppe und g ein Element von G. Wir schreiben $g^2 := g \circ g$ und $g^k := g^{k-1} \circ g$ für eine natürliche Zahl k. Wird die Verknüpfung mit dem Symbol „+“ geschrieben, dann schreiben wir $2 \cdot g := g + g$ und $k \cdot g := (k-1) \cdot g + g$ für eine natürliche Zahl k. Schließlich definieren wir $g^0 := e$ bzw. $0 \cdot g = e$ in der additiven Schreibweise.

Definition I.6.6 (Ordnung): Seien $(G, \circ)$ eine Gruppe und g ein Element von G. Es bezeichne $M_g := \{k \in \mathbb{N} - \{0\} \mid g^k = e\}$. Dann heißt

$$\mathrm{ord}(g) := \begin{cases} \min M_g, & \text{falls } M_g \text{ nichtleer ist,} \\ \infty, & \text{sonst,} \end{cases}$$

die *Ordnung von g*.

Definition I.6.7 (Untergruppe): Seien $(G, \circ)$ eine Gruppe und H eine Teilmenge von G. Die Teilmenge H heißt *Untergruppe von G*, falls gilt:

(i) Das neutrale Element von G liegt auch in H,

(ii) Für alle $h_1, h_2 \in H$ gilt $h_1 \circ h_2 \in H$, (Abgeschlossenheit unter Verknüpfung)

(iii) Für alle $h \in H$ gilt $h^{-1} \in H$. (Abgeschlossenheit unter Inversen)

Insbesondere ist $(H, \circ)$ wieder eine Gruppe.

Bemerkung I.6.8 (Untergruppenkriterium): Seien $(G, \circ)$ eine Gruppe und $H \subseteq G$ eine Teilmenge. Es ist H eine Untergruppe von G genau dann, wenn gilt:

(1) H ist nichtleer,

(2) Für alle h_1, h_2 in H gehört auch $h_1 \circ h_2^{-1}$ zu H.

Beweis: Die Implikation „$\Rightarrow$“ ist klar. Für „$\Leftarrow$“ gehen wir die Definition einer Untergruppe durch. Zu (i): Ist H nichtleer, dann gibt es $h \in H$ und wegen (2) ist $h \circ h^{-1} = e \in H$.

Zu (iii): Ist $h \in H$, dann gilt $h^{-1} = e \circ h^{-1} \in H$ wegen (2) und (i).

Zu (ii): Sind schließlich $h_1, h_2 \in H$, dann gehört wegen (iii) schon h_2^{-1} zu H und nach (2) gehört wegen $h_1 \circ (h_2^{-1})^{-1} = h_1 \circ h_2$ auch $h_1 \circ h_2$ zu H. □

Definition I.6.9 (Ringe): Eine Menge R mit zwei Verknüpfungen „$\oplus$“ und „$\odot$“ heißt *Ring*, falls gilt:

(i) $(R, \oplus)$ ist eine abelsche Gruppe. Wir bezeichnen das neutrale Element von $(R, \oplus)$ mit 0

(ii) Die Verknüpfung „$\odot$“ ist assoziativ.

(iii) Es gelten die Distributivgesetze, d. h. für alle $x, y, z \in R$ sind

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Der Ring $(R, \oplus, \odot)$ heißt *Ring mit Eins* oder auch *unitaler Ring*, falls es $1 \in R$ gibt, sodass $1 \odot x = x = x \odot 1$.

Der Ring $(R, \oplus, \odot)$ heißt *kommutativer Ring* oder kurz *kommutativ*, wenn „$\odot$“ kommutativ ist.

Beispiel I.6.10 (Ring oder nicht?): $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}^{n\times n}, +, \cdot)$, $(\mathrm{Sl}_2(\mathbb{Z}), +, \cdot)$.

Beispiel I.6.11 (Beispiele für Ringe): Das Folgende sind Ringe:

(i) Die Menge $C([0,1]) = \{f\colon [0,1] \to \mathbb{R} \mid f \text{ stetig}\}$ bildet zusammen mit den punktweisen Verknüpfungen, die für $f, g \in C([0,1])$ definiert sind durch

$$f+g\colon [0,1] \longrightarrow \mathbb{R}, \qquad t \longmapsto f(t)+g(t),$$
$$f\cdot g\colon [0,1] \longrightarrow \mathbb{R}, \qquad t \longmapsto f(t)\cdot g(t),$$

einen Ring.

(ii) Die Menge

$$\mathbb{Q}[X] = \left\{ f = \sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{R} \right\}$$

heißt *Polynomring über* $\mathbb{Q}$. Er wird mit den Verknüpfungen, die für Polynome $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{j=0}^{m} b_j X^j \in \mathbb{Q}[X]$ erklärt sind durch

$$f+g := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i, \qquad f\cdot g := \sum_{i=0}^{n+m} a_i b_{n+m-i} X^i,$$

zu einem Ring. Ist $f = \sum_{i=0}^{n} a_i X^i$ ein Polynom, dann heißt

$$p_f\colon \mathbb{Q} \longrightarrow \mathbb{Q}, \qquad q \longmapsto \sum_{i=0}^{n} a_i q^i$$

die zugehörige Polynomfunktion. Man kann allgemeiner den Polynomring über einem beliebigen Ring erklären, jedoch muss man im Allgemeinen zwischen Polynomen und Polynomfunktionen unterscheiden.

Definition I.6.12 (Einheiten und Nullteiler): Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

(i) Die Menge $R^\times := \{a \in R \mid \exists\, b \in R : a\cdot b = b\cdot a = 1\}$ heißt *Einheitengruppe von* R. Tatsächlich ist $(R^\times, \cdot)$ eine Gruppe.

(ii) Ein Element a von R heißt *Nullteiler*, falls es $b \in R$ mit $a \cdot b = 0$ gibt.

Definition I.6.13 (Körper): Der Ring $(K, +, \cdot)$ heißt *Körper*, falls $(K, +, \cdot)$ ein kommutativer Ring mit Eins ist, sodass $K^\times = K - \{0\}$.

Beispiel I.6.14 (Körper oder nicht?): $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}^{n\times n}, +, \cdot)$, $(\mathbb{R}^{n\times n}, +, \cdot)$

Definition I.6.15 (Homomorphismen):

(i) Seien $(G, \circ)$ und $(H, \star)$ Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt *Gruppenhomomorphismus*, falls für alle $g_1, g_2 \in G$ gilt, dass

$$\varphi(g_1 \circ g_2) = \varphi(g_1) \star \varphi(g_2).$$

(ii) Seien $(R, +, \cdot)$ und $(S, \oplus, \odot)$ Ringe. Eine Abbildung $\varphi\colon R \to S$ heißt *Ringhomomorphismus*, falls für alle $a, b \in R$ gilt, dass

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b), \qquad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b).$$

(iii) Seien $(R, +, \cdot)$ und $(S, \oplus, \odot)$ unitale Ringe mit Einsen 1_R und 1_S. Eine Abbildung $\varphi\colon R \to S$ heißt *Homomorphismus von unitalen Ringen*, falls φ ein Ringhomomorphismus ist und $\varphi(1_R) = 1_S$ gilt.

(iv) Seien $(K, +, \cdot)$ und $(L, \oplus, \odot)$ Körper. Eine Abbildung $\varphi\colon K \to L$ heißt *Körperhomomorphismus*, falls φ ein Homomorphismus unitaler Ringe ist.

Bemerkung I.6.16 (Homomorphismen und neutrale Elemente): (i) Es seien $(G, \circ)$ und $(H, \star)$ Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt für die neutralen Elemente e_G von G und e_H von H, dass $\varphi(e_G) = e_H$ und außerdem gilt für alle $g \in G$, dass $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(ii) Die Abbildung $\varphi\colon (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, +, \cdot)$, $a \mapsto 0$ ist ein Ringhomomorphismus, aber kein Homomorphismus von unitalen Ringen.

Definition I.6.17 (Isomorphie): Zwei Gruppen bzw. Ringe bzw. unitale Ringe bzw. Körper C_1 und C_2 heißen isomorph, falls es Homomorphismen $\varphi\colon C_1 \to C_2$ und $\psi\colon C_2 \to C_1$ mit $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}$ gibt. In diesem Fall schreiben wir $C_1 \cong C_2$.

Bemerkung I.6.18 (Isomorphismen): Ist $\varphi\colon C_1 \to C_2$ ein Homomorphismus von Gruppen bzw. Ringen bzw. unitalen Ringen bzw. Körpern, dann gilt: φ ist ein Isomorphismus genau dann, wenn φ bijektiv ist.

Beweis: Die Implikation „$\Rightarrow$“ folgt aus der Definition von Bijektivität. Zur Implikation „$\Leftarrow$“: Ist φ bijektiv, dann gibt es eine Umkehrabbildung ψ zu φ, d. h. eine Abbildung $\psi\colon C_2 \to C_1$ mit $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}$. Wir zeigen exemplarisch für den Fall, dass C_1 und C_2 Gruppen sind„ dass dann auch ψ ein Homomorphismus ist. Seien also $h_1, h_2 \in C_2$. Dann gilt

$$\psi(h_1 \star h_2) = \psi\Big(\varphi[\psi(h_1)] \star \varphi[\psi(h_2)]\Big) = \psi\Big(\varphi(\psi(h_1) \circ \psi(h_2))\Big) = \psi(h_1) \circ \psi(h_2),$$

da $\psi \circ \varphi = \mathrm{id} = \varphi \circ \psi$. □

Definition I.6.19 (Nebenklassen): Seien G eine Gruppe und U eine Untergruppe. Auf G wird durch $g_1 \sim g_2$ genau dann, wenn $g_1^{-1}g_2 \in U$, eine Äquivalenzrelation erklärt. Für $g \in G$ definieren wir

$$[g] := g \cdot U := \{g' \sim g \mid g' \in G\},$$

die Äquivalenzklasse von g. Es gilt $[g] = \{g \cdot u \mid u \in U\}$.

Die Äquivalenzrelation „$\sim$“ gibt eine Partition von G, d. h. zwei Nebenklassen sind gleich oder disjunkt.

Bemerkung I.6.20 (Gleichmächtigkeit der Nebenklassen): Für jedes $g \in G$ ist die Abbildung

$$U \longrightarrow g \cdot U, \qquad u \longmapsto g \cdot u$$

eine Bijektion, denn $g\colon U \to U$, $g' \mapsto g^{-1} \cdot g'$ ist eine Umkehrabbildung. Insbesondere sind alle Nebenklassen gleichmächtig.

Satz I.6.21 (Satz von Lagrange): *Für jede Untergruppe U einer endlichen Gruppe G gilt: $\#(U)$ teilt $\#(G)$.*

Beweis: Es gelten $G = \bigcup_{g \in G} g \cdot U$ und $\#(g_1 \cdot G) = \#(g_2 \cdot G)$ für alle g_1, g_2 in G. Wir finden ein vollständiges Repräsentantensystem $\{g_1, \ldots, g_n\}$ für „$\sim$“, sodass

$$\#(G) = \#\Big(\dot{\bigcup_{i=1}^{n}} g_i \cdot G \Big) = \sum_{i=1}^{n} \#(g_i \cdot G) = \sum_{i=1}^{n} \#(H) = n \cdot \#(H). \qquad \square$$

Beispiel I.6.22 (Verknüpfungstafel): Sei $G = \{e_G, g_2, g_3, g_4, g_5, g_6\}$. Die folgende Tabelle heißt Verknüpfungstabelle von G:

	e	g_2	g_3	g_4	g_5	g_6
e	e	g_2	g_3	g_4		g_6
g_2	g_2	e		g_5	g_4	g_3
g_3	g_3	g_5	e	g_6	g_2	
g_4	g_4			e		
g_5	g_5	g_3			g_6	e
g_6	g_6				e	g_5

7. Von den rationalen Zahlen zu den reellen Zahlen

Sei P ein regelmäßiges Fünfeck von Seitenlänge 1. Wie lang ist die Diagonale d?

Proposition I.7.1: *Die Zahl d ist keine rationale Zahl.*

Beweis: Angenommen d wäre eine rationale Zahl, d. h. es gäbe eine natürliche Zahl k mit $d \cdot k$ eine natürliche Zahl. Durch Strecken mit Streckfaktor k erhält man ein regelmäßiges Fünfeck, bei dem Seiten- und Diagonalenlänge ganzzahlig sind, nämlich s_1 und d_1. Wegen der geometrischen Konstruktion gäbe es ein kleineres, regelmäßiges Fünfeck mit Seitenlängen $d_1 - s_1$ und Diagonalenlänge s_1 (beide wieder ganzzahlig). Dieses Vorgehen könnte beliebig oft iteriert werden. Die Seitenlängen würden dabei immer kleiner, aber blieben immer ganzzahlig. Aber das kann nicht sein. □

⚠Anzweifeln, dass alle Zahlen Brüche sind, konnte im antiken Griechenland mit dem Tod enden.

Im Folgenden wollen wir $\mathbb{Q}$ zur Zahlengerade vervollständigen.

Bemerkung I.7.2 (Betrag und Ordnung):

(i) Für alle $x \in \mathbb{Q}$ und $a \in \mathbb{Q}_{\geq 0}$ gilt $|x| \leq a$ genau dann, wenn $-a \leq x \leq a$,

(ii) Für alle $x \in \mathbb{Q}$ gilt $-|x| \leq x \leq |x|$.

Beweis: (i) Ist $x \geq 0$, dann gilt $x = |x|$ und aus $0 \leq x$ und $0 \leq a$ folgt $-a \leq 0 \leq x$. Ist $x \leq 0$, dann ist $|x| = -x$ und $-x \leq a$ gilt genau dann, wenn $x \geq -a$, d. h. $x \leq 0 \leq a$.

(ii) Folgt aus (i) mit $a = |x|$. □

Proposition I.7.3 (Eigenschaften des Betrags): *Der Betrag $|\cdot|$ und die Metrik d auf $\mathbb{Q}$ haben die folgenden Eigenschaften:*

(i) *Für alle $x \in \mathbb{Q}$ gilt $|x| \geq 0$ und $|x| = 0$ genau dann, wenn $x = 0$.*[1]

(ii) *Für alle $x, y \in \mathbb{Q}$ gilt $|x \cdot y| = |x||y|$.*[2]

(iii) *Für alle $x, y \in \mathbb{Q}$ gilt $|x + y| \leq |x| + |y|$.*

[1] Diese Eigenschaft heißt „Positive Definitheit“.
[2] Diese Eigenschaft heißt „Homogenität“.

Beweis: (i) Es gilt $|x| \geq 0$, da $x \leq 0$ genau dann gilt, wenn $-x \geq 0$ (siehe Bemerkung I.5.10) und $|x| = 0$ gilt genau dann, wenn $x = 0$, per Definition.

(ii) Wir unterscheiden die vier Fälle (1) $x, y \geq 0$, (2) $x, y \leq 0$, (3) $x \geq 0$ und $y \leq 0$ sowie (4) $x \leq 0$, $y \geq 0$. Exemplarisch betrachten wir (3): Nach Bemerkung I.5.10 gilt $x \cdot y \leq 0$, d. h.

$$|x \cdot y| = -x \cdot y = x \cdot (-y) = |x| \cdot |y|.$$

(iii) Einerseits gilt $x+y \leq |x|+|y|$ nach Bemerkung I.7.2 (ii) und Bemerkung I.5.10, und andererseits gilt $x + y \geq |-|x| - |y|$ nach Bemerkung I.7.2 (ii) und Bemerkung I.5.10. Jetzt folgt die Aussage aus Bemerkung I.7.2 (i). □

Proposition I.7.4 (Eigenschaften der Metrik): *Für alle $x, y, z \in \mathbb{Q}$ gilt:*

(i) *Es gilt $d(x, y) \geq 0$ und $d(x, y) = 0$ genau dann, wenn $x = y$,*

(ii) *Es gilt $d(x, y) = d(y, x)$,*

(iii) *Es gilt $d(x, z) \leq d(x, y) + d(y, z)$.*

Die Eigenschaften haben dieselben Namen wie die entsprechenden Eigenschaften des Betrags.

Beweis: (i) Folgt aus Proposition I.7.3.

(ii) Wir rechnen nach, dass

$$d(x, y) = |x - y| = |(-1) \cdot (y - x)| = |-1| \cdot |y - x| = |y - x|.$$

(iii) Mit I.7.3 (iii) sehen wir, dass

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

□

Erinnerung I.7.5: Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in $\mathbb{Q}$, d. h. für jede natürliche Zahl n gilt $x_n \in \mathbb{Q}$.

(i) Die Folge $(x_n)_{n\in\mathbb{N}}$ heißt *Cauchyfolge*, falls es für jede natürliche Zahl k einen Index N gibt, sodass $|x_n - x_m| < 1/k$ für alle $n, m \geq N$.
Setze $C := \{x := (x_n)_{n\in\mathbb{N}} \mid x \text{ ist Cauchyfolge}\}$.

(ii) Sind $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ Folgen und $\lambda \in \mathbb{Q}$, dann sind auch

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}},$$
$$\lambda \cdot (x_n)_{n\in\mathbb{N}} := (\lambda x_n)_{n\in\mathbb{N}}, \qquad (x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n \cdot y_n)_{n\in\mathbb{N}}$$

Folgen.

(iii) Die Folge $(x_n)_{n\in\mathbb{N}}$ heißt *Nullfolge*, falls es für jede natürliche Zahl k einen Index N gibt, sodass $|x_n| < 1/k$ für alle $n \geq N$.

Wir erinnern außerdem an die Definition eines Vektorraums über einem Körper: Sind K ein Körper und $(V, +)$ eine abelsche Gruppe und gibt es eine äußere Verknüpfung

$$\cdot : K \times V \longrightarrow V, \qquad (\alpha, v) \longmapsto \alpha v$$

die für alle $v, w \in V$ und $\alpha, \beta \in K$ leistet, dass $1v = v$, $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$, $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ und $\alpha \cdot (v + w) = \alpha \cdot v + \beta \cdot v$, dann heißt $(V, +, \cdot)$ ein Vektorraum über K.

Definition I.7.6 (Äquivalenzrelation): Auf C aus Erinnerung I.7.5 erklärt

$$x \sim y :\Leftrightarrow x - y \text{ ist eine Nullfolge}$$

eine Äquivalenzrelation. Wir setzen $\mathbb{R} := C/\!\sim$

Bemerkung I.7.7: (i) Sind $x = (x_n)_{n\in\mathbb{N}}$ und $y = (y_n)_{n\in\mathbb{N}}$ Elemente von C, dann gilt $x \sim y$ genau dann, wenn $x - y$ zu

$$N := \{x = (x_n)_{n\in\mathbb{N}} \in C \mid x \text{ ist Nullfolge}\}$$

gehört.

(ii) Die Definitionen aus Erinnerung I.7.5(ii) erklären Verknüpfungen „+“, „·“ auf C, die C zu einem unitalen Ring machen. Die Folge $(0, 0, \dots)$ ist das Nullelement von C, die Folge $(1, 1, \dots)$ ist die Eins von C.

Wir wollen im Folgenden auch den Quotienten $C/\!\sim$ zu einem Ring machen und setzen an zu definieren, was wir uns wünschen würden:

$$[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}] := [(x_n + y_n)_{n\in\mathbb{N}}], \qquad [(x_n)_{n\in\mathbb{N}}] \cdot [(y_n)_{n\in\mathbb{N}}] := [(x_n y_n)_{n\in\mathbb{N}}]$$

Dass das tatsächlich kein Unsinn ist, und dass diese Verknüpfungen $C/\!\sim$ zu einem Ring machen, überlegen wir uns im Folgenden.

Vorüberlegung I.7.8: Seien $(R, +, \cdot)$ ein Ring und $S \subseteq R$ eine Teilmenge. Auf R erklärt $r_1 \sim r_2 :\Leftrightarrow r_1 - r_2 \in S$ eine Relation. Wann handelt es sich dabei um eine Äquivalenzrelation? In diesem Fall: Wann definiert die Ringstruktur auf R auch eine Ringstruktur auf $R/\sim$, d. h. wann sind

$$[r_1] + [r_2] := [r_1 + r_2], \qquad [r_1] \cdot [r_2] := [r_1 \cdot r_2]$$

wohldefiniere Verknüpfungen auf $R/\sim$ und wann ist $R/\sim$ ausgestattet mit diesen Verknüpfungen selbst ein Ring?

Der Reihe nach. Wann ist die Relation eine Äquivalenzrelation? Wir brauchen dazu das Folgende:

- Für alle $r \in R$ muss $r \sim r$ gelten, d. h. wir brauchen $r - r = 0_R \in S$. Das ist (genau) dann erfüllt, wenn $0 \in S$.
- Für $r_1, r_2 \in R$ mit $r_1 \sim r_2$ brauchen wir $r_2 \sim r_1$. Wegen $r_1 \sim r_2$ per Definition genau dann, wenn $r_1 - r_2 \in S$ und $r_2 \sim r_1$ per Definition genau dann, wenn $r_2 - r_1 = -(r_1 - r_2) \in S$, ist das erfüllt, wenn S abgeschlossen unter additiven Inversen ist.
- Für $r_1, r_2, r_3 \in R$ mit $r_1 \sim r_2$ und $r_2 \sim r_3$ muss gelten, dass auch $r_1 \sim r_3$. Da $r_1 \sim r_2$ genau dann, wenn $r_1 - r_2 \in S$, $r_2 \sim r_3$ genau dann, wenn $r_2 - r_3 \in S$ und $r_1 \sim r_3$ genau dann, wenn $r_1 - r_3 = (r_1 - r_2) + (r_2 - r_3)$ ist das erfüllt, wenn S abgeschlossen bezüglich Addition ist.

Wir fassen zusammen: Ist $(S, +)$ eine Untergruppe von R, dann ist „$\sim$“ eine Äquivalenzrelation auf R. Wir haben verwendet, dass $(R, +)$ eine Gruppe ist. Die Umkehrung gilt auch.

Sei nun S eine Untergruppe von R. Wann ist die angegebene Addition wohldefiniert? Für r_1, r_2, r_1' und r_2' aus R mit $r_1 \sim r_1'$ und $r_2 \sim r_2'$ brauchen wir, dass $r_1 + r_2 \sim r_1' + r_2'$. Per Definition heißt $r_1 \sim r_1'$ genau, dass $r_1 - r_1' \in S$ und $r_2 \sim r_2'$ heißt genau, dass $r_2 - r_2' \in S$. Aber dann ist

$$r_1 + r_2 - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in S,$$

da $(R, +)$ eine abelsche Gruppe und S eine Untergruppe von $(R, +)$ ist. Hier brauchen wir also keine zusätzlichen Forderungen.

Wann ist die angegebene Multiplikation wohldefiniert? Für r_1, r_2, r_1' und r_2' wie oben brauchen wir, dass $r_1 r_2 \sim r_1' r_2'$. Per Definition heißt $r_1 \sim r_1'$ genau, dass es $s_1 \in S$ mit $r_1 = r_1' + s$ gibt; genau so heißt $r_2 \sim r_2'$ genau, dass es $s_2 \in S$ mit $r_2 = r_2' + s_2$ gibt. Jetzt ist

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

und wir brauchen, dass $r_1' s_2 + r_2' s_1 + s_1 s_2$ zu S gehört. Das ist jedenfalls erfüllt, wenn für alle $r \in R$ und alle $s \in S$ gilt, dass $rs \in S$.

Definition I.7.9 (Ideal): Sei $(R, +, \cdot)$ ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *Ideal*, falls $(S, +)$ eine Untergruppe von $(R, +)$ ist und falls für alle $r \in R$ und $s \in S$ gilt, dass $rs \in S$.

Satz I.7.10 (Quotienten für algebraische Strukturen):

(i) *Seien $(A, +)$ eine abelsche Gruppe und $S \subseteq A$ eine Untergruppe. Dann ist „$\sim$“ aus Vorüberlegung I.7.8 eine Äquivalenzrelation und durch*

$$[g_1] + [g_2] := [g_1 + g_2]$$

für $g_1, g_2 \in A$ wird eine wohldefinierte Verknüpfung auf $A/\sim$ erklärt, die $A/\sim$ zu einer abelschen Gruppe macht.

(ii) *Seien $(R, +, \cdot)$ ein kommutativer Ring und $S \subseteq R$ ein Ideal. Dann ist „$\sim$“ aus Vorüberlegung I.7.8 eine Äquivalenzrelation und durch*

$$[g_1] + [g_1] := [g_1 + g_2], \qquad [g_1] \cdot [g_2] := [g_1 \cdot g_2]$$

für $g_1, g_2 \in R$ werden wohldefinierte Verknüpfungen auf $R/\sim$ erklärt, die $R/\sim$ zu einem kommutativen Ring machen.

(iii) *Seien V ein Vektorraum über einem Körper K und $U \subseteq V$ ein Untervektorraum. Dann ist „$\sim$“ aus Vorüberlegung I.7.8 eine Äquivalenzrelation und durch*

$$[v] + [w] := [v + w], \qquad \lambda \cdot [v] := [\lambda v]$$

für $v, w \in V$ und $\lambda \in K$ werden wohldefinierte Verknüpfungen auf $V/\sim$ erklärt, die $V/\sim$ zu einem Vektorraum über K machen.

Wir schreiben auch $A/S := A/\sim$, $R/S := R/\sim$ und $V/U := V/\sim$.

Beweis: Da wir bereits wissen, dass die Verknüpfungen in (i) und (ii) wohldefiniert sind; für (i) und (ii) müssen wir uns also nur noch überlegen, dass die Verknüpfungen assoziativ, kommutativ (und gegebenenfalls distributiv) sind, und was jeweils das neutrale Element beziehungsweise was jeweils die Inversen sind. Da wir repräsentantenweise rechnen und wir über die Verknüpfungen auf A respektive R bereits gut bescheid wissen, gibt es die entsprechenden Eigenschaften der Verknüpfungen auf A/S beziehungsweise R/S gratis. Offensichtlich ist $[0]$ das neutrale Element von A/S beziehungsweise von R/S bezüglich „+“ und für $[a] \in A/S$ beziehungsweise $[a] \in R/S$ ist $[-a]$ das additive Inverse.

Für (iii) müssen wir uns noch überlegen, dass die Skalarmultiplikation wohldefiniert ist. Das ist mittlerweile eine Routine-Übung und deshalb kein Problem für die Leserin beziehungsweise den Leser. □

Korollar I.7.11: *Der Quotient $\mathbb{R} = C/N$ wird mit „+“ und „·“ aus Erinnerung I.7.5 zu einem kommutativen Ring.*

Beweis: Wir haben lediglich zu zeigen, dass N ein Ideal in C ist. Aus der Analysis I ist bekannt, dass Summen von Nullfolgen wieder Nullfolgen sind, die konstante Folge $(0, 0, \dots)$ ist eine Nullfolge, außerdem ist für eine Nullfolge $(x_n)_{n\in\mathbb{N}}$ ebenfalls $(-x_n)_{n\in\mathbb{N}}$ eine Nullfolge. Schließlich ist das Produkt einer Cauchyfolge und einer Nullfolge wieder eine Nullfolge und wir sind fertig. □

Proposition I.7.12 ($\mathbb{R}$ als Körpererweiterung von $\mathbb{Q}$): *Die Abbildung*

$$\iota\colon \mathbb{Q} \longrightarrow \mathbb{R}, \qquad q \longmapsto [(q, q, \dots)]$$

ist ein Homomorphismus von Ringen.

In $\mathbb{R}$ hat jedes Element $r = [(x_n)_{n\in\mathbb{N}}] \neq [(0, 0, \dots)]$ ein Inverses bezüglich Multiplikation, d. h. $(\mathbb{R}, +, \cdot)$ ist ein Körper. Damit wird ι zu einer Einbettung von Körpern und wir können $\mathbb{Q}$ vermöge ι als Teilkörper von $\mathbb{R}$ auffassen.

Beispiel I.7.13:
(i) $x = (1, 1{,}1, 1{,}101, 1{,}101\,001, 1{,}101\,001\,000\,1, \dots)$ ist eine Cauchyfolge und definiert somit eine reelle Zahl.

(ii) $x = (0{,}9, 0{,}99, 0{,}999, 0{,}9999, \dots)$ ist eine Cauchyfolge und definiert die gleiche reelle Zahl wie $\iota(1) = (1, 1, 1, \dots)$, denn $|x_n - 1| \to 0$.

(iii) $x = (1, 3/2, 5/3, 8/5, 13/8, 21/13, \dots) = (a_k/a_{k+1})_{k\in\mathbb{N}}$ ist eine Cauchyfolge, wobei $(a_k)_{k\in\mathbb{N}}$ die Fibonacci-Folge bezeichnet, d. h. $a_0 = a_1 = 1$, $a_{k+2} = a_{k+1} + a_k$.

Definition I.7.14 (Anordnung, Norm und Abstand auf $\mathbb{R}$): Für eine reelle Zahl $r := [(x_n)_{n\in\mathbb{N}}]$ definiere

$$r > 0 :\Longleftrightarrow\ \exists\, K, N \in \mathbb{N} :\ \forall\, n \geq N : x_n > \frac{1}{K}.$$

Diese Festsetzung ist unabhängig vom gewählten Vertreter. Sind $r_1 = [(x_n)_{n\in\mathbb{N}}]$ und $r_2 := [(y_n)_{n\in\mathbb{N}}]$ zwei reelle Zahlen, definiere

$$r_1 < r_2 :\Longleftrightarrow\ |r_2 - r_1| > 0, \qquad (r_1 \leq r_2 :\Longleftrightarrow\ r_1 = r_2 \vee r_1 < r_2).$$

Hierbei wird $|r|$ definiert wie in Definition I.5.9.

Bemerkung I.7.15 (Ordnung und Betrag): Seien $r = [(x_n)_{n\in\mathbb{N}}]$ und $s = [(y_n)_{n\in\mathbb{N}}]$ reelle Zahlen.

(i) Es gilt $r > s$ genau dann, wenn es einen Index N gibt derart, dass für alle $n, m \geq N$ gilt, dass $x_n > y_n$,

(ii) Es gilt $|r| = [|x_n|_{n\in\mathbb{N}}]$,

(iii) Es gilt genau dann $|r| < \varepsilon \in \mathbb{Q}$, falls es einen Index N gibt derart, dass für alle $n, m \geq N$ gilt ,dass $|r_n| < \varepsilon$.

Bemerkung I.7.16 (Der Betrag als Norm): Die eben definiere Relation „$\leq$“ ist eine totale Ordnung auf $\mathbb{R}$. Für den Betrag gelten folgende Regeln:

(i) Für alle $r \in \mathbb{R}$ ist $|r| \geq 0$ und $|r| = 0$ genau dann, wenn $r = 0$,

(ii) Für alle $r_1, r_2 \in \mathbb{R}$ gilt $|r_1 r_2| = |r_1||r_2|$,

(iii) Für alle $r_1, r_2 \in \mathbb{R}$ gilt $|r_1 + r_2| \leq |r_1| + |r_2|$.

Der Beweis geht ähnlich wie für die rationalen Zahlen.

Definition I.7.17 (Metrik): Sei X eine Menge. Eine Funktion $d\colon X \times X \to \mathbb{R}_{\geq 0}$ heißt *Metrik auf* X, falls gilt:

(i) Für alle $x, y \in X$ ist $d(x, y) \geq 0$ und es gilt $d(x, y) = 0$ genau dann, wenn $x = y$,

(ii) Für alle $x, y \in X$ ist $d(x, y) = d(y, x)$,

(iii) Für alle $x, y, z \in X$ gilt $d(x, z) \leq d(x, y) + d(y, z)$.

Bemerkung I.7.18 (Betragsmetrik auf den reellen Zahlen): Die Abbildung

$$d\colon \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}, \qquad (x, y) \longmapsto |x - y|$$

ist eine Metrik auf den reellen Zahlen,

Satz I.7.19: *Der Körper der reellen Zahlen ist vollständig, d. h. jede Cauchyfolge in* $\mathbb{R}$ *konvergiert.*

Beweis: Sei $r = (r_i)_{i\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{R}$. Jedes Folgenglied r_i können wir schreiben als $r_i = [(x_{i,n})_{n\in\mathbb{N}}]$ mit einer Cauchyfolge $(x_{i,n})_{n\in\mathbb{N}}$ in $\mathbb{Q}$. Dann haben wir das Folgende:

(i) Da jede Folge $(x_{i,n})_{n\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{Q}$ ist, gibt es für jede natürliche Zahl ℓ einen Index $N_i(\ell)$, sodass für alle $n, m \geq N_i(\ell)$ gilt, dass $|x_{i,n} - x_{i,m}| < 1/\ell$.

(ii) Da $(r_i)_{i\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{R}$ ist, gibt es für jede natürliche Zahl ℓ einen Index $M(\ell)$ sodass für alle $i, j \geq M$ gilt, dass $|r_i - r_j| < 1/\ell$.

Wir suchen jetzt eine reelle Zahl r, gegen die die Folge $(r_i)_{i\in\mathbb{N}}$ konvergiert, d. h. für die Folge $(r_i)_{i\in\mathbb{N}}$ soll gelten: Für jede natürliche Zahl k gibt es einen Index $N(k)$ sodass für alle $i, j \geq N(k)$ gilt, dass $|r - r_i| < 1/k$. Dazu definieren wir eine neue Folge rationaler Zahlen $(y_k)_{k\in\mathbb{N}}$ per $y_k := x_{k,N(k)}$. Für diese Folge zeigen wir:

(1) $(y_k)_{k\in\mathbb{N}}$ ist Cauchyfolge in $\mathbb{Q}$,

(2) Es gilt $r_i \to r := [(y_k)_{k\in\mathbb{N}}]$.

Zu (1): Ist ℓ eine natürliche Zahl, wähle N_0 so, dass $|r_i - r_j| < 1/(3\ell)$ für alle $i, j \geq N_0$ und setze $N_1 := \max\{N_0, 3\ell\}$. Dann gilt für alle $k, m \geq N_1$, dass

$$\begin{aligned}|y_k - y_m| &= |x_{k,N_k(k)} - x_{m,N_m(m)}| \\ &\leq |x_{k,N_k(k)} - x_{k,t}| + |x_{k,t} - x_{m,t}| + |x_{m,N_m(m)} - x_t| \leq \frac{1}{k} + \frac{1}{3\ell} + \frac{1}{m} \leq \frac{1}{\ell}.\end{aligned}$$

Wähle jetzt t so, dass $|x_{k,t} - x_{m,t}| < 1/(3\ell)$, also zum Beispiel $t \geq M(3\ell)$. Das geht, da $|r_k - r_m| < 1/(3\ell)$. Dann ist $|y_k - y_m| < 1/\ell$. Da das Vorgehen nicht von ℓ abhängt, gilt die Aussage für jede natürliche Zahl ℓ und damit ist $(y_k)_{k\in\mathbb{N}}$ eine Cauchyfolge.

Zu (2): Sei ℓ eine beliebge natürliche Zahl. Wir zeigen für einen noch zu bestimmenden Index N, dass $|r - r_n| < 1/\ell$ für alle $n \geq N$. Wir wissen aus (1), dass $(y_k)_{k\in\mathbb{N}}$ eine Cauchyfolge ist. Wir können deshalb einen Index N_1 finden, sodass für alle $k, m \geq N$ gilt, dass $|y_k - y_m| < 1/(2\ell)$. Setzen wir $N := \max\{2\ell, N_1\}$, dann gilt für alle $n \geq N$ und alle $m \geq \max\{N_1, N_n(n)\}$, dass

$$|x_{n,m} - y_m| \leq |x_{n,m} - x_{n,N_n(n)}| + |x_{n,N_n(n)} - y_m| \leq \frac{1}{n} + |y_n - y_m| < \frac{1}{\ell},$$

d. h. $|r_n - r| < 1/\ell$ und wir sind fertig. □

Kapitel II.

Teilbarkeitslehre

1. Euklidischer Algorithmus

Definition II.1.1 (Teiler): Seien a und b ganze Zahlen. Gibt es eine ganze Zahl c, sodass $a = bc$, dann heißt b *Teiler von* a. Man sagt auch b *teilt* a und schreibt $b \mid a$.

Beispiel II.1.2: Die Teiler von 6 sind ± 1, ± 2, ± 3 und ± 6.

Bemerkung II.1.3 (Endlichkeit der Teilermenge): Sind $0 \neq a$ eine ganze Zahl und b ein Teiler von a, dann folgt $|b| \leq |a|$, denn ist $a = bc$, dann ist $|a| = |b||c| \geq |b|$, denn wegen $a \neq 0$ sind auch $b, c \neq 0$.

Definition II.1.4 (ggT, kgV und mod): Seien a und b ganze Zahlen und m eine natürliche Zahl.

(i) Die Zahl $\mathrm{ggT}(a,b) := \max\{k \in \mathbb{Z} \mid k \mid a \text{ und } k \mid b\}$ heißt *größter gemeinsamer Teiler von a und b* und ist es auch.

(ii) Gilt $\mathrm{ggT}(a,b) = 1$, dann heßen a und b teilerfremd.

(iii) Die Zahl $\mathrm{kgV}(a,b) := \min\{v \in \mathbb{N} \mid a \mid v \text{ und } b \mid v\}$ heißt *kleinstes gemeinsames Vielfaches von a und b* und ist es auch.

(iv) Wir schreiben $a \equiv b \pmod{m}$, falls m die Differenz $a - b$ teilt.

Bemerkung II.1.5 (Kongruenz-Rechenregeln): Seien a, a', b, b' ganze Zahlen und m eine natürliche Zahl. Gilt $a \equiv a' \pmod{m}$ sowie $b \equiv b' \pmod{m}$, dann gelten

$$a+b \equiv a'+b' \pmod{m}, \qquad a-b \equiv a'-b' \pmod{m}, \qquad ab \equiv a'b' \pmod{m}.$$

Den Beweis für diese Aussagen haben sie bereits auf Blatt 6 in Aufgabe 1 gegeben.

Proposition II.1.6 (Existenz der Gaußklammer): *Für jede nicht-negative reelle Zahl x gibt es eine ganze Zahl k_0, sodass $k_0 \leq x$ und $k_0+1 > x$. Insbesondere gilt dann:*

(i) *Für alle ganzen Zahlen k mit $k \leq k_0$ ist $k \leq x$,*

(ii) *Für alle ganzen Zahlen k mit $k \geq k_0 + 1$ ist $k > x$.*

Also ist $k_0 = \max\{k \in \mathbb{Z} \mid k \leq x\}$.

Beweis: Wir unterscheiden zwei Fälle. Ist $x \geq 0$, dann definieren wir

$$M := \{k \in \mathbb{Z} \mid k > x\} \subseteq \mathbb{N}.$$

Nach dem Prinzip des kleinsten Täters hat M ein kleinstes Element k_0'. Für $k_0 := k_0' - 1$ gilt $k_0 \notin M$, d. h. $k_0 \leq x$ und $k_0' = k_0 + 1 \in M$, d. h. $k_0 + 1 > x$.

Ist $x < 0$, so erhalten wir wie im ersten Fall eine ganze Zahl k_0', sodass $k_0' \leq -x \leq k_0' + 1$, also $-k_0' \geq x \geq -k_0' - 1$. Für $k_0 := -k_0' - 1$ gilt also $k_0 < x \leq k_0 + 1$. Ist x keine ganze Zahl, dann leistet $k_0 = -k_0' - 1$ das Gewünschte, ist x eine ganze Zahl, dann leistet $-k_0'$ das Gewünschte. □

Definition II.1.7: In der Situation von Proposition II.1.6 heißt $\lfloor x \rfloor := k_0$ auch *Gaußklammer von x.*

Aus dem Beweis von Proposition II.1.6 folgt für $x \geq 0$, dass

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor - 1, & \text{falls } x \notin \mathbb{Z}, \\ -\lfloor x \rfloor, & \text{falls } x \in \mathbb{Z}. \end{cases}$$

Einsetzen für $x < 0$ von $-x$ ergibt die Aussage für $x \in \mathbb{R}$.

Beispiel II.1.8: Für $x = 1{,}2$ gilt $\lfloor 1{,}2 \rfloor = 1$ und es ist $\lfloor -1{,}2 \rfloor = -2 = -\lfloor 1{,}2 \rfloor - 1$. Für $x = 1$ haben wir $\lfloor -1 \rfloor = -1 = -\lfloor 1 \rfloor$.

Proposition II.1.9 (Teilen mit Rest): *Seien a und b ganze Zahlen und b nicht Null. Dann existieren eindeutig bestimmte ganze Zahlen q, r mit $a = qb + r$ und $0 \leq r < b - 1$. Die Zahl r heißt dann* Rest der Division von a durch b.

Beweis: Setze $q := \lfloor a/b \rfloor$. Dann ist $q \leq a/b < q + 1$, was äquivalent ist zu $bq \leq a < bq + b$ und das wiederum ist äquivalent zu $0 \leq a - bq < b$. Wählen wir jetzt $r := a + bq$, dann leistet (q, r) das Gewünschte.

Zur Eindeutigkeit:Gilt $0 \leq a - qb < b - 1$, dann haben wir die folgenden Konsequenzen:

(i) Zunächst ist $qb \leq a$, also $q \leq a/b$,

(ii) Dann ist $a - b + 1 < qb$, d. h. $q > a/b - 1 + 1/b > a/b - 1$.

Insgesamt haben wir $q \leq a/b < q + 1$, also gibt Proposition II.1.6, dass $q = \lfloor a/b \rfloor$. □

Beispiel II.1.10: Wir wollen den größten gemeinsamen Teiler von $a = 10$ und $b = 7$ bestimmen.

$$\begin{aligned} 10 &= 1 \cdot 10 + 0 \cdot 7 \\ 7 &= 0 \cdot 10 + 1 \cdot 7 \\ 3 &= 1 \cdot 10 - 1 \cdot 7 \\ 1 &= -2 \cdot 10 + 3 \cdot 7 \\ 0 &= 7 \cdot 10 - 10 \cdot 7. \end{aligned}$$

Definition II.1.11 (Euklidischer Algorithmus): Seien a und b natürliche Zahlen mit $b \leq a$ und $b \neq 0$. Dann haben wir

$$a = 1 \cdot a + 0 \cdot b, \qquad b = 0 \cdot a + 1 \cdot b.$$

Seien $a_1 := a$, $a_2 := b$, $x_1 := 1$, $x_2 := 0$, $y_1 := 0$ und $y_2 := 1$. Wir definieren solange $b > 0$ iterativ Gleichungen $a_n = x_n a + y_n b$ wie folgt: Sind die Gleichungen

$$a_{n-2} = x_{n-2}a + y_{n-2}b, \qquad a_{n-1} = x_{n-1}a + y_{n-1}b$$

gegeben, setze $q_n := \lfloor a_{n-2}/a_{n-1} \rfloor$, $a_n := a_{n-2} - q_n a_{n-1}$, $x_n := x_{n-2} - q_n x_{n-1}$ sowie $y_n := y_{n-2} - q_n y_{n-1}$ und erhalte $a_n = x_n a + y_n b$.

Satz II.1.12 (über den Euklidischen Algorithmus): *Für den Algorithmus aus Definition II.1.11 gilt:*

(i) *Es gibt einen Index N, sodass $a_N = 0$. Somit ist der Algoritmus terminierend.*

(ii) *Für den Index N aus* (i) *gilt* $a_{N-1} = \mathrm{ggT}(a, b)$.

(iii) *Wir haben die Gleichung* $\mathrm{ggT}(a, b) = x_{N-1}a + y_{N-1}b$.

Beweis: (i) In jedem Schritt des Algorithmus gilt $a_n = a_{n-2} \pmod{a_{n-1}}$, d. h. $a_n < a_{n-1}$. Da alle a_n natürliche Zahlen sind, wir in endlich vielen Schritten $a_N = 0$ erreicht.

(ii) Setze $g := \mathrm{ggT}(a, b)$. Wegen $a_{N-1} = x_N a + y_N b$ folgt $g \mid a_{N-1}$. Jetzt zeigen wir $q_{N-1} \mid a$ und $q_{N-1} \mid b$ – daraus folgt mit der Definition des ggT, dass $a_{N-1} \leq g$. Dazu zeigen wir per vollständiger Induktion, dass $a_{N-1} \mid a_{N-i}$ für $i \geq 1$. Für $i = 1$ ist die Behauptung evident. Für $i = 2$ haben wir $0 = a_N = a_{N-2} - q_N q_{N-1}$, d. h. $a_{N-2} = q_N a_{N-1}$.

Es gelte jetzt $a_{N-1} \mid a_{N-j}$ für alle $j \leq i$. Für $a_{N-(i+1)}$ finden wir

$$a_{N-(i-1)} = a_{N-(i+1)} - q_{N-(i-1)} a_{N-i},$$

d. h. $a_{N-(i+1)} = a_{N-(i-1)} + q_{N-(i-1)} a_{N-i}$ und da $a_{N-(i-1)}$ und a_{N-i} von a_{N-1} geteilt werden, wird auch $a_{N-(i+1)}$ von a_{N-1} geteilt.

(iii) Diese Aussage folgt aus (ii) und $a_{N-1} = x_{N-1} a + y_{N-1} b$. □

Korollar II.1.13 (Lemma von Bézout): *Seien a und b von Null verschiedene ganze Zahlen. Dann gibt es ganze Zahlen k und ℓ, sodass*

$$\mathrm{ggT}(a, b) = ka + \ell b.$$

2. Der Chinesische Restsatz

Erinnerung: Sei m eine natürliche Zahl. Auf $\mathbb{Z}$ wird durch „$a \equiv b \pmod m$, falls $m \mid a - b$“ eine Äquivalenzrelation erklärt. Die Menge der Äquivalenzklassen ist

$$\mathbb{Z}/m\mathbb{Z} := \{[a] \mid a \in \mathbb{Z}\} = \{[0], \ldots, [m-1]\}.$$

Es gilt $[a]_m := [a] = \{a + mk \mid k \in \mathbb{Z}\} = \{a' \in \mathbb{Z} \mid a' \equiv a \pmod m\}$. Mit der wohldefinierten repräsentantenweisen Addition und der wohldefinierten repräsentantenweisen Multiplikation wird $\mathbb{Z}/m\mathbb{Z}$ zu einem kommutativen unitalen Ring.

Proposition II.2.1 (Einheiten in $\mathbb{Z}/m\mathbb{Z}$): *Sei m eine natürliche Zahl. Eine Restklasse $[a] \in \mathbb{Z}/m\mathbb{Z}$ ist (multiplikativ) invertierbar genau dann, wenn $\mathrm{ggT}(a, m) = 1$.*

Aus der obigen Proposition lesen wir ab, dass

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

Beweis: Eine Restklasse $[a]$ ist invertierbar genau dann, wenn es $b \in \mathbb{Z}$ mit $ab \equiv 1 \pmod{m}$ gibt, was genau dann der Fall ist, wenn es ganze Zahlen b und k mit $ab - 1 = km$ gibt.

„$\Rightarrow$“: Sei $g := \mathrm{ggT}(a, m) \in \mathbb{N}_{>0}$. Falls $[a]$ invertierbar ist und b, k ganze Zahlen mit $ab - 1 = km$ sind, dann wird $ab - km = 1$ von g geteilt, d. h. $g = 1$.

„$\Leftarrow$“: Ist $\mathrm{ggT}(a, m) = 1$, dann liefert das Lemma von Bézout die Existenz von ganzen Zahlen k, ℓ mit $ka + \ell m = 1$, d. h. $ka \equiv 1 \pmod{m}$ und damit ist $[k]$ das multiplikative Inverse von $[a]$. □

Korollar II.2.2 (Rechentricks für teilerfremde Zahlen):

(i) *Seien a, b ganze Zahlen und m eine 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 zwei ganze Zahlen mit $\mathrm{ggT}(m_1, m_2) = 1$ und sei a eine ganze Zahl. Aus $m_1 \mid a$ und $m_2 \mid a$ folgt $m_1 m_2 \mid a$.*

Beweis: (i) Nach Proposition II.2.1 gehören $[a]_m$ und $[b]_m$ zu $\mathbb{Z}/m\mathbb{Z}^\times$. In $\mathbb{Z}/m\mathbb{Z}^\times$ haben wir $[ab]_m = [a]_m[b]_m \in \mathbb{Z}/m\mathbb{Z}^\times$, was wir zeigen wollten.

(ii) Ohne Einschränkung seien m_1 und m_2 zwei positive natürliche Zahlen. Wir rechnen modulo m_2, d. h. im Folgenden steht $[a]$ für $[a]_{m_2}$. Nach Proposition II.2.1 gehört $[m_1]$ zu $\mathbb{Z}/m_2\mathbb{Z}^\times$, d. h. es gibt eine ganze Zahl m_1' sodass $[m_1][m_1'] = [1]$. Wegen $m_1 \mid a$ gibt es eine ganze Zahl k mit $a = km_1$ und damit erhalten wir $[m_1'][a] = [m_1'][m_1][k] = [k]$.

Andererseits folgt aus $m_2 \mid a$, dass $[a] = 0$, d. h. $[k] = 0$, d. h. $m_2 \mid k$ und damit wird a von $m_1 m_2$ geteilt. □

Beispiel II.2.3 (Ein Brahmagupta-Problem nach Ore): Gibt es eine natürliche Zahl n, die die Kongruenzen

$$\begin{aligned} n &\equiv 1 \pmod{2} \\ n &\equiv 2 \pmod{3} \\ n &\equiv 3 \pmod{4} \\ n &\equiv 4 \pmod{5} \\ n &\equiv 5 \pmod{6} \\ n &\equiv 0 \pmod{7} \end{aligned}$$

löst? Man nennt ein solches Problem ein „Problem simultaner Kongruenzen“.

Satz II.2.4 (Chinesischer Restsatz): *Seien $m_1, \ldots, m_r$ paarweise teilerfremde positive natürliche Zahlen (d. h.* $\mathrm{ggT}(m_i, m_j) = 1$ *für $i \neq j$) und $a_1, \ldots, a_r$ beliebige ganze Zahlen. Dann gilt:*

(i) *Es gibt eine ganze Zahl x, sodass für alle $i \in \{1, \ldots, n\}$ gilt, dass $x \equiv a_i \pmod{m_i}$.*

(ii) *Ist $m := \prod_{i=1}^{r} m_i$ und ist x_0 eine Lösung des simultanten Kongruenzproblems, dann sind alle Elemente von $\{x_0 + km \mid k \in \mathbb{Z}\}$ Lösungen des simultanen Kongruenzproblems.*

(iii) *Die Menge aus* (ii) *ist sogar die Lösungsmenge des simultanen Kongruenzproblems, d. h. man erhält so alle ganzzahligen Lösungen des Problems.*

Beweis: (i) Können wir für jedes $j \in \{1, \ldots, r\}$ eine ganze Zahl A_j mit

$$A_j \equiv \begin{cases} 1 \pmod{m_j}, \\ 0 \pmod{m_i}, \quad \text{für } i \neq j, \end{cases}$$

finden, dann gilt für $x := \sum_{i=1}^{r} A_j a_j$, dass $x \equiv a_j \pmod{m_j}$ für $1 \leq j \leq r$.

Tatsächlich geht das: Wir setzen $M_j := m/m_j = \prod_{1 \leq i \leq r, j \neq j} m_i$. Dann gilt $M_j \equiv 0 \pmod{m_i}$ für $i \in \{1, \ldots, n\}$ mit $i \neq j$ nach Korollar II.2.2(ii) und außerdem gilt $\mathrm{ggT}(M_j, m_j) = 1$ nach Korollar II.2.2(i).

Wegen $\mathrm{ggT}(M_j, m_j) = 1$ finden wir eine ganze Zahl M_j' mit $M_j M_j' \equiv 1 \pmod{m_j}$. Nun leistet $A_j := M_j M_j'$ das Gewünschte.

(ii) Für jedes $j \in \{1, \ldots, r\}$ gilt $x = x_0 + km \equiv x_0 \equiv a_j \pmod{m_j}$.

(iii) Seien x und x_0 Lösungen des simultanen Kongruenzproblems. Dann gilt für jedes $j \in \{1, \ldots, r\}$ dass $x - x_0 \equiv a_j - a_j \equiv 0 \pmod{m_j}$, d. h. wir haben für jedes $j \in \{1, \ldots, r\}$, dass $m_j \mid x - x_0$. Nach Korollar II.2.2 wird $x - x_0$ von $m = \prod_{i=1}^{r} m_i$ geteilt, also gibt es eine ganze Zahl k mit $x - x_0 = km$. Damit ist alles gezeigt. □

Bemerkung II.2.5: Seien wiederum $m_1, \ldots, m_r$ paarweise teilerfremde ganze Zahlen und $m := \prod_{i=1}^{r} m_i$. Der Chinesische Restsatz sagt uns, dass es für jeden Rest $x \pmod{m}$ ein eindeutig bestimmtes r-Tupel

$$(a_1 \pmod{m_1}, \ldots, a_r \pmod{m_r}) \in \mathbb{Z}/m_1\mathbb{Z} \times \ldots \mathbb{Z}/m_r\mathbb{Z}$$

mit $x \equiv a_j \pmod{m_j}$ für alle $1 \leq j \leq r$ gibt.

Korollar II.2.6 (aus dem Chinesischen Restsatz): *Aus dem Beweis des Chinesischen Restsatzes erhält man folgende Methode zur Lösung des simultanen Kongruenzproblems*

$$x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}.$$

(i) *Setze* $m := \prod_{i=1}^{r} m_i$,

(ii) *Für* $j \in \{1, \ldots, r\}$, *setze* $M_j := m/m_j = \prod_{1 \leq i \leq r, i \neq j} m_j$,

(iii) *Bestimme* $M_j' \in \mathbb{Z}$ *mit* $M_j M_j' \equiv 1 \pmod{m_j}$ *(zum Beispiel mit dem Euklidischen Algorithmus),*

(iv) *Setze* $A_j := M_j M_j'$.

Dann ist $x = \sum_{i=1}^{r} A_i a_i$ *eine Lösung des simultanen Kongruenzproblems.*

Proposition II.2.7 (Reste-Abbildung): *Seien* m_i *und* m *positive natürliche Zahlen so, dass* m *von* m_i *geteilt wird. Die Abbildung*

$$p\colon \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_i\mathbb{Z}, \qquad [a]_m \longmapsto [a]_{m_i}$$

ist ein wohldefinierter Homomorphismus von unitalen Ringen. Außerdem ist p *surjektiv.*

Beweis: Für die Wohdefiniertheit seien a und a' ganze Zahlen mit $[a]_m = [a']_m$. Dann wird $a - a'$ von m geteilt und wegen $m_i \mid m$ haben wir erst Recht $m_i \mid a - a'$, d. h. $[a]_{m'}$.

Für $[a]_m$ und $[b]_m$ aus $\mathbb{Z}/m\mathbb{Z}$ gilt

$$p([a]_m + [b]_m) = p([a+b]_m) = [a+b]_{m_i} = [a]_{m_i} + [b]_{m_i} = p([a]_m) + p([b]_m),$$

d. h. p ist ein Homomorphismus der abelschen Gruppen $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m_i\mathbb{Z}, +)$. Analog zeigt man, dass $p([a]_m[b]_m) = p([a]_m)p([b]_m)$, was p zu einem Ringhomomorphismus macht. Wegen $p([1]_m) = [1]_{m_i}$ ist p sogar ein Homomorphismus unitaler Ringe.

Schließlich ist p surjektiv, denn ist $[a]_{m_i} \in \mathbb{Z}/m_i\mathbb{Z}$ gegeben, dann ist $[a]_m$ ein Urbild. □

Bemerkung II.2.8: (i) Sind $(R_1, +, \cdot)$ und $(R_2, +, \cdot)$ unitale Ringe, dann ist auch

$$R_1 \times R_2 := \{(a, b) \mid a \in R_1, b \in R_2\}$$

zusammen mit den Verknüpfungen

$$(a, b) + (a', b') := (a + a', b + b'), \qquad (a, b) \cdot (a', b') := (aa', bb')$$

ein unitaler Ring. Es sind $(0_{R_1}, 0_{R_2})$ und $(1_{R_1}, 1_{R_2})$ die neutralen Elemente bezüglich „+“ beziehungsweise „·“.

(ii) Sind $R_1, \ldots, R_k$ unitale Ringe, dann wird auch $\prod_{i=1}^{k} R_i$ durch die komponentenweisen Verknüpfungen zu einem unitalen Ring.

Satz II.2.9 (Chinesischer Resatz): *Seien $m_1, \ldots, m_r$ paarweise teilerfremde positive natürliche Zahlen und $m := \prod_{i=1}^{r}$. Dann ist der Ringhomomorphismus*

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

aus Proposition II.2.7 ein Isomorphismus. Insbesondere haben wir die Isomorphie von Ringen $\mathbb{Z}/m\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$.

Beweis: Der Beweis von Satz II.2.4 greift. Wir können jetzt allerdings einen alternativen, kürzeren Beweis geben. Zunächst ist p injektiv, denn für r-Tupel $([a]_{m_1}, \ldots, [a]_{m_r}) = ([a']_{m_1}, \ldots, [a']_{m_r})$, dann gilt für jedes $i \in \{1, \ldots, r\}$, dass $a - a'$ von m_i geteilt wird, d. h. $a - a'$ wird auch von m geteilt und damit gilt $[a]_m = [a]_{m'}$. Wegen

$$\#\mathbb{Z}/m\mathbb{Z} = m = \prod_{i=1}^{r} m_i = \prod_{i=1}^{r} \#\mathbb{Z}/m_i\mathbb{Z} = \#\prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$$

ist p auch surjektiv. □

Bemerkung II.2.10: Der alternative Beweis ist zwar kürzer, liefert aber kein Verfahren wie in Korollar II.2.6, um die Urbilder zu bestimmen.

Beispiel II.2.11: Ist $p\colon \mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ wie in Satz II.2.9 ein Isomorphismus?

Nein! Wegen $p([12]_{24}) = ([0]_6, [0]_4)$ kann p nicht injektiv sein und die simultane Kongruenz

$$\begin{aligned} x &\equiv 4 \pmod 6 \\ x &\equiv 3 \pmod 4 \end{aligned}$$

kann keine Lösung haben, denn gäbe es eine, dann hätten wir $x \equiv 4 \equiv 0 \pmod 2$ und $x \equiv 3 \equiv 1 \pmod 2$, was nicht sein kann.

Beispiel II.2.12: Wir suchen eine natürliche Zahl n, die die simultanen Kongruenzen

$$\begin{aligned} n \equiv 1 \pmod 2, \qquad n \equiv 2 \pmod 3, \qquad n \equiv 3 \pmod 4 \\ n \equiv 4 \pmod 5 \qquad n \equiv 5 \pmod 6 \qquad n \equiv 0 \pmod 7 \end{aligned}$$

löst. Allerdings sind 2, 3, 4, 5, 6 und 7 nicht paarweise teilerfremd.

Da aber 3, 4, 5 und 7 teilerfremd sind, gibt es nach dem Chinesischen Restsatz eine natürliche Zahl n, die

$$n \equiv 2 \pmod 3, \qquad n \equiv 3 \pmod 4,$$
$$n \equiv 4 \pmod 5, \qquad n \equiv 0 \pmod 7$$

löst. Für dieses n gilt weiterhin, dass $n \equiv 3 \equiv 1 \pmod 2$, da 2 ein Teiler von 4 ist. Weil jetzt $n \equiv 1 \pmod 2$ und $n \equiv 2 \pmod 3$ liefert der Chinesische Restsatz, dass $n \equiv 5 \pmod 6$, d. h. es gibt eine natürliche Zahl n, die die simultanen Kongruenzen löst. Die Lösungen dieses Systems von Kongruenzen können wir jetzt mit dem Chinesischen Restsatz bestimmen:

(i) Wir setzen $m_1 := 3$, $m_2 := 4$, $m_3 := 5$, $m_4 := 7$ sowie $m := \prod_{i=1}^{4} m_i = 420$.

(ii) Wir setzen $M_i := m/m_i$, d. h. $M_1 = 140$, $M_2 = 105$, $M_3 = 84$, $M_4 = 60$. Wir haben

$$M_1 \equiv 2 \pmod 3, \qquad M_2 \equiv 1 \pmod 4,$$
$$M_3 \equiv 4 \pmod 5, \qquad M_4 \equiv 4 \pmod 7.$$

(iii) Wähle $M_1' = 2$, $M_2' = 1$, $M_3' = 4$ und $M_4' = 2$. Dann gilt $M_i M_i' \equiv 1 \pmod{m_i}$ für $1 \leq i \leq 4$.

(iv) Mithilfe des Euklidischen Algorithmus bestimmen wir $A_1 = 280$, $A_2 = 105$, $A_3 = 336$ und $A_4 = 120$.

(v) Wähle $x = 280 \cdot 2 + 105 \cdot 3 + 336 \cdot 4 + 120 \cdot 0 = 2219$.

Da alle Lösungen äquivalent modulo 420 sind, ist 119 die kleinste Lösung des „Eierproblems“.

3. Primzahlen

Beispiel II.3.1 (Primfaktorzerlegungen): Die natürliche Zahl 12 hat die Teiler $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. Wollen wir 12 als Produkt natürlicher Zahlen schreiben, dann haben wir (bis auf Reihenfolge) die Möglichkeiten $12 = 2 \cdot 6$ und $12 = 3 \cdot 4$. Beide Faktorisierungen lassen sich weiterzerlegen zu $12 = 3 \cdot 2^2$.

Definition II.3.2 (Primzahl): Eine natürliche Zahl $n > 1$ heißt *Primzahl*, falls sich n nicht als Produkt zweier kleinerer natürlicher Zahlen schrieben lässt. Die Menge der Primzahlen heißt $\mathbb{P}$, d. h. $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$.

Satz II.3.3 (von Euklid, ca 300 v. Chr.): *Es gibt unendlich viele Primzahlen.*

Proposition II.3.4: *Eine natürliche Zahl n größer als Eins ist prim genau dann, wenn gilt: Sind a und b natürliche Zahlen und wird ab von n geteilt, dann wird a von n geteilt oder b wird von n geteilt.*

Beweis: „⇐“: Angenommen, n erfüllt die rechte Seite. Seien a und b natürliche Zahlen und gelte $n = ab$. Dann sind a und b kleinergleich n. Da außerdem ab von n geteilt würde, würde nach Voraussetzung a von n oder b von n geteilt. Ohne Einschränkung gelte $n \mid a$. Dann wäre $n \leq a$ und insgesamt hätten wir $n = a$. Folglich lässt sich n nicht als Produkt von zwei kleineren natürlichen Zahlen schreiben und ist damit prim.

„⇒“: Angenommen n wäre prim und es gäbe natürliche Zahlen a und b, sodass ab von n geteilt würde. Dann wäre $ab = kn$ für eine geeignete natürliche Zahl k.

Wäre $\mathrm{ggT}(a, n) = 1$, dann gäbe es nach dem Lemma von Bézout ganze Zahlen r und s, sodass $1 = rn + sa$, d. h. wir hätten

$$b = brn + bsa = brn + skn = (br + sk)n$$

und wäre n ein Teiler von b.

Wäre $g := \mathrm{ggT}(a, n) > 1$, dann würde n von g geteilt und da n prim ist, wäre $g = n$. Wegen $n = g = \mathrm{ggT}(a, n)$ würde dann aber auch a von n geteilt.□

Proposition II.3.5 (Existenz von Primteilern): *Jede natürliche Zahl $n > 1$ hat einen* Primteiler*, d. h. einen Teiler, der eine Primzahl ist.*

Beweis: Seien $n > 1$ und $T_n := \{k \in \mathbb{N} \mid k > 1 \text{ und } k \text{ teilt } n\}$. Wegen $n \in T_n$ wäre T_n nichtleer. Nach dem Prinzip des kleinsten Täters hat T_n ein kleinstes Element und dieses muss eine Primzahl sein. □

Beweis (des Satzes von Euklid): Angenommen, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_k$, wobei k eine natürliche Zahl ist. Setze $N := \prod_{i=1}^{k} p_i + 1$. Nach Proposition II.3.5 hätte N einen Primteiler $q = p_i$ für ein geeignetes $1 \leq i \leq k$, aber wegen $N \equiv 1 \pmod{p_i}$ für $1 \leq i \leq n$ könnte keine der Primzahlen ein Teiler von N sein. □

Satz II.3.6 (Fundamentalsatz der Arithmetik):

(i) *Jede natürliche Zahl $n \neq 0$ lässt sich als Produkt*

$$n = \prod_{i=1}^{k} p_i \qquad (k \in \mathbb{N}) \tag{II.1}$$

von Primzahlen $p_1, \ldots, p_k$ schreiben. Per Definition des Produktes ist das leere Produkt $\prod_{i=1}^{0} p_i = \prod_{i \in \varnothing} p_i = 1$.

(ii) *Die Darstellung in Gl.* (II.1) *ist eindeutig bis auf Reihenfolge der p_i's.*

Die Zerlegung aus Gl. (II.1) *heißt* Primfaktorzerlegung von n.

Beweis: (i) Wir zeigen die Behauptung per Induktion nach n. Für $n = 1$ ist nichts zu zeigen.

Die Aussage gelte nun für eine natürliche Zahl n. Nach Proposition II.3.5 hat $n+1$ einen Primteiler, d. h. es gibt eine Primzahl p_1 und eine natürliche Zahl $n' < n+1$, sodass $n+1 = p_1 n'$. Nach Induktionsvoraussetzung hat n' eine Primfaktorzerlegung, sagen wir $n' = \prod_{i=2}^{\ell} p_i$. Dann ist $n+1 = \prod_{i=1}^{\ell} p_i$ und $n+1$ hat eine Primfaktorzerlegung.

(ii) Angenommen die natürliche Zahl n hätte zwei Primfaktorzerlegungen $n = p_1 \cdots p_r = q_1 \cdots q_s$. Wir zeigen die Eindeutigkeit per Induktion über $k := \min\{r, s\}$. Ist $k = 0$, so ist $n = 1$, d. h. r und s müssen beide Null sein. Ist $k = 1$, dann ist n eine Primzahl, r und s müssen beide Eins sein und $n = p_1 = q_1$.

Die Aussage gelten nun für eine natürliche Zahl k. Ohne Einschränkung gelte $r = k+1 \leq s$. Wir zeigen, dass $p_1 = q_j$ für irgendein $j \in \{1, \ldots, s\}$ und benutzen dafür, dass für Primzahlen p und q genau dann $p \mid q$ gilt, wenn $p = q$.

Angenommen, es gäbe kein $j \in \{1, \ldots, s\}$, sodass $p_1 \mid q_j$. Da nach Voraussetzung gilt, dass $p_1 \cdots p_r = q_1 \cdots q_s$, hätten wir $p_1 \mid q_1 \cdots q_s$. Da q_1 nach Voraussetzung nicht von p_1 geteilt wird und weil p_1 prim ist, hätten wir $p_1 \mid q_2 \cdots q_s$. Induktiv erhielten wir, dass $p_1 \mid q_s$ im Widerspruch zur Voraussetzung. Unsere Annahme war also falsch, und p_1 taucht in der zweiten Primfaktorzerlegung von n als Faktor auf.

Durch Änderung der Reihenfolge können wir erreichen, dass $p_1 = q_1$, d. h. $p_2 \cdots p_r = q_2 \cdots q_s$. Nach Induktionsvoraussetzung ist $r - 1 = s - 1$ und nach eventueller Umsortierung gilt $p_2 = q_2, \ldots, p_r = q_s$. □

Lemma II.3.7 (Kleiner Satz von Fermat[1]): *Für jede Primzahl p gilt: Ist a eine ganze Zahl mit* $\mathrm{ggT}(a, p) = 1$*, dann ist* $a^{p-1} \equiv 1 \pmod{p}$.

Sie haben diese Aussage auf dem neunten Übungsblatt bewiesen. Das entscheidende Werkzeug im Beweis war, dass $\mathbb{Z}/p\mathbb{Z}^\times$ die Ordnung $p-1$ hat.

Für später bemerken wir Folgendes: Ist jetzt n irgendeine natürliche Zahl und a eine ganze Zahl so, dass $[a] \in \mathbb{Z}/n\mathbb{Z}^\times$, dann gibt es eine ganze Zahl b, sodass $[a][b] = 1$, d. h. es gibt außerdem eine ganze Zahl k, sodass $1 = ab + kn$, d. h. $\mathrm{ggT}(a, n) = 1$.

[1] Pierre de Fermat, französischer Jurist und Hobbymathematiker, lebte von 1607 bis 1655.

Definition II.3.8 (Eulersche φ-Funktion): Die Funktion

$$\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}, \quad n \longmapsto \#(\mathbb{Z}/n\mathbb{Z}^\times) = \#(\{a \in \mathbb{N} \mid 0 \leq a \leq n-1, \mathrm{ggT}(a,n) = 1\})$$

heißt *Eulersche φ-Funktion.*

Beispiel II.3.9: Es sind $\varphi(5) = 4$ und $\varphi(6) = 2$.

Proposition II.3.10 (Berechnung von $\varphi(n)$):

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

(ii) *Sind p eine Primzahl und e eine natürliche Zahl, dann ist*

$$\varphi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right).$$

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

Beweis: Aussagen (i) und (ii) folgen aus der Definition. Zu (iii): Nach dem Chinesischen Restsatz gilt

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Es gilt sogar $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, denn $(a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ist invertierbar genau dann, wenn es $(a',b') \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ gibt, sodass $aa' = 1$ und $bb' = 1$. Aber das ist äquivalent dazu, dass $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $b \in \mathbb{Z}/m\mathbb{Z}^\times$. Insbesondere gilt deshalb

$$\varphi(nm) = \#(\mathbb{Z}/nm\mathbb{Z})^\times = \#(\mathbb{Z}/n\mathbb{Z})^\times \#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(n)\varphi(m). \qquad \square$$

Beispiel II.3.11: Für $n = 72$ berechnen wir wegen $72 = 8 \cdot 9$, dass

$$\varphi(72) = \varphi(8 \cdot 9) = \varphi(2^3)\varphi(3^2) = (8-4) \cdot (9-3) = 4 \cdot 6 = 24.$$

Satz II.3.12 (von Euler): *Seien n eine natürliche Zahl und a eine ganze Zahl mit $\mathrm{ggT}(a,n) = 1$. Dann ist $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Beweis: Genau wie im Beweis des kleinen Fermatschen Satzes betrachten wir die Gruppe $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ und die von $[a]$ erzeugte Untergruppe

$$\langle [a] \rangle = \{[a]^k \mid k \in \mathbb{Z}\} =: U.$$

Nach dem Satz von Lagrange ist $\mathrm{ord}([a]) = \#(U)$ ein Teiler der Gruppenordnung $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$, d. h. es gibt eine natürliche Zahl c sodass $c\,\mathrm{ord}([a]) = \varphi(n)$. Deswegen ist

$$a^{\varphi(n)} \equiv a^{c\,\mathrm{ord}([a])} \equiv (a^{\mathrm{ord}([a])})^c \equiv 1 \pmod{n}. \qquad \square$$

Für den Beweis brauchten wir zwingend, dass $\mathrm{ggT}(a, n) = 1$, damit $[a]$ zu $\mathbb{Z}/n\mathbb{Z}^\times$ gehört.

Bemerkung II.3.13 (RSA-Verfahren[2]): 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.[3]

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.[4]

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

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

[4] 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.