Einführung in die elementare Zahlentheorie

Sascha Trostorff

4. Februar 2019

Inhaltsverzeichnis

I. Zahlenbereiche **3**

1. Die natürlichen Zahlen **4**

2. Die ganzen Zahlen **13**

3. Die rationalen Zahlen **18**

4. Die reellen Zahlen **23**

5. Stellenwertsysteme **27**

II. Teilbarkeit **34**

6. Teilbarkeit in Integritätsbereichen **35**

7. Euklidische Ringe **38**

III. Restklassenringe **47**

8. Der Ring $\mathbb{Z}_n$ **48**

9. Teilbarkeitsregeln **51**

10. Lineare Kongruenzen **53**

11. Elementare Sätze der Zahlentheorie **57**

Teil I.

Zahlenbereiche

1. Die natürlichen Zahlen

Definition (Peano-Axiome)**.** Es existiert eine Menge $\mathbb{N}$, die Menge der *natürlichen Zahlen,* mit folgenden Eigenschaften:

(P1) Es existiert eine injektive[1] Abbildung $\sigma : \mathbb{N} \to \mathbb{N}$, die *Nachfolgerabbildung.*

(P2) Es existiert ein Element in $\mathbb{N}$ - wir nennen es 0 -, das kein Nachfolger ist. Es gilt also

$$\forall n \in \mathbb{N} : \sigma(n) \neq 0.$$

(P3) Ist $M \subseteq \mathbb{N}$ eine Teilmenge mit den Eigenschaften:

(a) $0 \in M$,

(b) $\forall n \in M : \sigma(n) \in M$,

so gilt $M = \mathbb{N}$ (Induktionsaxiom).

Bemerkung 1.1. In der Literatur wird das Element, dass gemäß (P2) existiert, häufig 1 genannt.

Satz 1.2. *Es gilt*

$$\{m \in \mathbb{N}\,;\, \exists k \in \mathbb{N} : m = \sigma(k)\} \cup \{0\} = \mathbb{N}.$$

Insbesondere ist 0 *das einzige Element in* $\mathbb{N}$*, das kein Nachfolger ist.*

Beweis. Wir setzen

$$M \coloneqq \{m \in \mathbb{N}\,;\, \exists k \in \mathbb{N} : m = \sigma(k)\} \cup \{0\}.$$

Zunächst gilt $0 \in M$ per Definition. Ist weiter $n \in M$ so gilt $\sigma(n) \in \{m \in \mathbb{N}\,;\, \exists k \in \mathbb{N} : m = \sigma(k)\} \subseteq M$. Somit gilt nach (P3) $M = \mathbb{N}$. Ist nun $n \in \mathbb{N} = M$ ein Element, das kein Nachfolger ist, d.h.

$$n \notin \{m \in \mathbb{N}\,;\, \exists k \in \mathbb{N} : m = \sigma(k)\} = M \setminus \{0\},$$

so folgt $n = 0$. □

Sehr eng verknüpft mit dem Induktionsaxiom ist das Prinzip der Rekursion. Bevor wir dieses Prinzip diskutieren können, benötigen wir einige grundlegende Begriffe.

[1] Eine Abbildung $f : M \to N$ zwischen zwei Mengen M, N heißt *injektiv*, falls

$$\forall x, y \in M : f(x) = f(y) \Rightarrow x = y.$$

Definition. Es seien M, N nichtleere Mengen. Eine Teilmenge $R \subseteq M \times N$ heißt *binäre Relation zwischen M und N*. Wir definieren den *Definitionsbereich* von R durch

$$D(R) \coloneqq \{x \in M \,;\, \exists y \in N : (x, y) \in R\}\,.$$

Ferner nennen wir R eine *Funktion,* falls R *rechtseindeutig* ist, d.h.

$$\forall x \in M, y, z \in N : (x, y) \in R \wedge (x, z) \in R \Rightarrow y = z.$$

Somit ist bei einer Funktion R für $x \in D(R)$ das Element $y \in N$ mit $(x, y) \in R$ eindeutig bestimmt und wir schreiben $R(x) \coloneqq y$. Ist R eine Funktion, so schreiben wir auch $R : D(R) \subseteq M \to N$ und falls $D(R) = M$ auch kurz $R : M \to N$.

Satz 1.3 (Rekursion)**.** *Sei M eine nichtleere Menge und $x \in M$. Ferner seien für $n \in \mathbb{N}$ Funktionen $f_n : M \to M$ gegeben. Dann existiert genau eine Funktion $g : \mathbb{N} \to M$, so dass*

(a) $g(0) = x$,

(b) $\forall n \in \mathbb{N} : g(\sigma(n)) = f_n(g(n))$.

Beweis. Wir beweisen zunächst die Eindeutigkeit. Angenommen es gebe zwei Funktionen $g, \widetilde{g} : \mathbb{N} \to M$ mit den gewünschten Eigenschaften. Wir betrachten die Menge

$$K \coloneqq \{n \in \mathbb{N} \,;\, g(n) = \widetilde{g}(n)\}\,.$$

Offenbar gilt $0 \in K$, da $g(0) = x = \widetilde{g}(0)$. Sei nun $n \in K$. Dann gilt

$$g(\sigma(n)) = f_n(g(n)) = f_n(\widetilde{g}(n)) = \widetilde{g}(\sigma(n)),$$

und daher $\sigma(n) \in K$. Nach (P3) folgt daher $K = \mathbb{N}$ und somit $g = \widetilde{g}$.
Kommen wir nun zur Existenz einer solchen Funktion g. Dazu betrachten wir die folgende Menge von binären Relationen zwischen $\mathbb{N}$ und M:

$$\mathcal{R} \coloneqq \{R \subseteq \mathbb{N} \times M \,;\, (0, x) \in R, \forall n \in \mathbb{N} : (n, y) \in R \Rightarrow (\sigma(n), f_n(y)) \in R\}\,.$$

Diese Menge ist nichtleer, da $\mathbb{N} \times M \in \mathcal{R}$ gilt. Wir definieren nun die Relation

$$g \coloneqq \bigcap \mathcal{R} = \{(n, y) \in \mathbb{N} \times M \,;\, \forall R \in \mathcal{R} : (n, y) \in R\}\,.$$

Ziel ist es zu zeigen, dass g eine Funktion mit den gewünschten Eigenschaften ist.
Wir zeigen zunächst $g \in \mathcal{R}$:

- $(0, x) \in g$: Ist klar, da $(0, x) \in R$ für alle $R \in \mathcal{R}$.
- $(n, y) \in g \Rightarrow (\sigma(n), f_n(y)) \in g$: Ist $(n, y) \in g$, so gilt $(n, y) \in R$ für alle $R \in \mathcal{R}$. Damit folgt $(\sigma(n), f_n(y)) \in R$ für alle $R \in \mathcal{R}$ und damit $(\sigma(n), f_n(y)) \in g$.

Es gilt also $g \in \mathcal{R}$.
Außerdem gilt $D(g) = \mathbb{N}$: Da $g \in \mathcal{R}$ folgt $0 \in D(g)$. Sei nun $n \in D(g)$. Dann existiert $y \in M$ mit $(n, y) \in g$ und somit $(\sigma(n), f_n(y)) \in g$ da $g \in \mathcal{R}$. Damit ist $\sigma(n) \in D(g)$ und aus (P3) folgt $D(g) = \mathbb{N}$.
Wir zeigen nun abschließend, dass g eine Funktion ist. Betrachte dazu die Menge

$$K \coloneqq \{n \in \mathbb{N}\,;\, \forall y, z \in M : (n, y), (n, z) \in g \Rightarrow y = z\}\,.$$

Es gilt $0 \in K$: Wir wissen bereits $(0, x) \in g$. Annahme: Es gibt $y \neq x$ mit $(0, y) \in g$. Dann betrachten wir die Relation $\widetilde{g} \coloneqq g \setminus \{(0, y)\}$. Dann folgt $\widetilde{g} \in \mathcal{R}$ und $\widetilde{g} \subsetneq g$, was der Definition von g widerspricht. Somit gilt also $(0, y) \in g \Rightarrow y = x$, also $0 \in K$.
Sei $n \in K$. Dann gibt es genau ein Element $y \in M$ mit $(n, y) \in g$ (da $n \in D(g) = \mathbb{N}$). Da $g \in \mathcal{R}$, folgt $(\sigma(n), f_n(y)) \in g$. Somit genügt es $(\sigma(n), z) \in g \Rightarrow z = f_n(y)$ zu zeigen. Annahme: Es gibt $z \neq f_n(y)$ mit $(\sigma(n), z) \in g$. Dann betrachten wir die Relation $\widetilde{g} \coloneqq g \setminus \{(\sigma(n), z)\}$. Dann folgt $\widetilde{g} \in \mathcal{R}$ (beachte hierbei, dass $\sigma(n) \neq 0$ nach (P2), somit also $(0, x) \in \widetilde{g}$ gilt) mit $\widetilde{g} \subsetneq g$. Das widerspricht der Definition von g und damit folgt $\sigma(n) \in K$.
Mit (P3) folgt nun $K = \mathbb{N}$ und daher ist g eine Funktion.
Somit ist $g : \mathbb{N} \to M$ und es gilt $g(0) = x$ und $g(\sigma(n)) = f_n(g(n))$ für alle $n \in \mathbb{N}$. □

Mithilfe der Rekursion können wir nun die Addition auf den natürlichen Zahlen definieren.

Definition. Sei $k \in \mathbb{N}$. Wir definieren die Abbildung $(k+) : \mathbb{N} \to \mathbb{N}$ durch ($M = \mathbb{N}$ und $f_n = \sigma$ für $n \in \mathbb{N}$)

(a) $(k+)\,(0) \coloneqq k$,

(b) $\forall n \in \mathbb{N} : (k+)\,(\sigma(n)) \coloneqq \sigma\,((k+)\,(n))\,.$

Statt $(k+)(n)$ schreiben wir üblicherweise $k+n$. Es ist also $k+0 = k$ und $k+\sigma(n) = \sigma(k+n)$. Ferner setzen wir $1 \coloneqq \sigma(0)$ und erhalten so für $k \in \mathbb{N}$

$$\sigma(k) = \sigma(k+0) = k + \sigma(0) = k + 1.$$

Wir wollen nun einige Rechenregeln für die Addition beweisen.

Satz 1.4 (Rechenregeln für die Addition)**.** *Es gilt:*

(a) $\forall k, m, n \in \mathbb{N} : k + (m + n) = (k + m) + n$ *(Assoziativität),*

(b) $\forall k, n \in \mathbb{N} : k + n = n + k$ *(Kommutativität),*

(c) $\forall k, m, n \in \mathbb{N} : k + n = m + n \Rightarrow k = m$ *(Kürzbarkeit).*

(d) $\forall k, m \in \mathbb{N} : k + m = 0 \Rightarrow k = m = 0.$

Beweis. (a) Seien $k, m \in \mathbb{N}$ und betrachte $M \coloneqq \{n \in \mathbb{N}\,;\, k + (m + n) = (k + m) + n\}$. Es gilt $0 \in M$, da

$$k + (m + 0) = k + m = (k + m) + 0.$$

Sei $n \in M$. Dann gilt

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

also $\sigma(n) \in M$.

(b) Wir zeigen zunächst $k + 0 = 0 + k$ für alle $k \in \mathbb{N}$. Die Behauptung gilt offenbar für $k = 0$. Nehmen wir nun an, sie gelte für ein $k \in \mathbb{N}$. Dann gilt

$$\begin{aligned} 0 + \sigma(k) &= \sigma\left(0 + k\right) \\ &= \sigma(k + 0) \\ &= \sigma(k) \\ &= \sigma(k) + 0. \end{aligned}$$

Das beweist $k + 0 = 0 + k$ für alle $k \in \mathbb{N}$. Als nächstes zeigen wir $k + 1 = 1 + k$ für alle $k \in \mathbb{N}$. Für $k = 0$ haben wir die Behauptung bereits gezeigt. Gelte nun $k + 1 = 1 + k$ für ein $k \in \mathbb{N}$. Dann ist

$$\begin{aligned} \sigma(k) + 1 &= \sigma\left(\sigma(k)\right) \\ &= \sigma(k + 1) \\ &= \sigma(1 + k) \\ &= 1 + \sigma(k). \end{aligned}$$

Sei nun $k \in \mathbb{N}$ und betrachte die Menge $M \coloneqq \{n \in \mathbb{N}\,;\, k + n = n + k\}$. Wie wissen bereits, dass $0, \sigma(0) \in M$. Sei nun $n \in M$. Dann gilt mit (a)

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

und damit $\sigma(n) \in M$.

(c) Seien $k, m \in \mathbb{N}$. Wir betrachten die Menge $M \coloneqq \{n \in \mathbb{N}\,;\, k + n = m + n \Rightarrow k = m\}$. Es ist $0 \in M$ da $k = k + 0 = m + 0 = m$. Sei $n \in M$ und gelte $k + \sigma(n) = m + \sigma(n)$. Damit ist $\sigma(k + n) = \sigma(m + n)$ und somit $k + n = m + n$ nach (P1). Da $n \in M$ folgt $k = m$ und somit $\sigma(n) \in M$.

(d) Seien $k, m \in \mathbb{N}$ mit $k + m = 0$. Wir nehmen an $m \neq 0$. Dann existiert ein $n \in \mathbb{N}$ mit $m = \sigma(n)$ nach Satz 1.2. Damit gilt

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

Dies widerspricht (P2) und somit ist $m = 0$. Daher gilt auch $0 = k + m = k + 0 = k$. □

Über die Addition können wir nun die Ordnungsrelation $\leq$ auf $\mathbb{N}$ definieren.

Definition. Seien $m, n \in \mathbb{N}$. Wir definieren

$$m \leq n : \Leftrightarrow \exists k \in \mathbb{N} : m + k = n.$$

Wir beweisen zunächst, dass $\leq$ tatsächlich eine Ordnungsrelation auf $\mathbb{N}$ definiert. Dazu wiederholen wir kurz, was wir unter einer Ordnungsrelation verstehen.

Definition. Sei M eine Menge und $R \subseteq M \times M$. R heißt *Ordnungsrelation auf M,* falls

(a) R *reflexiv* ist, d.h. $\forall x \in M : (x, x) \in R$,

(b) R *antisymmetrisch* ist, d.h. $\forall x, y \in M : (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$,

(c) R *transitiv* ist, d.h. $\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.

Eine Ordnungsrelation R auf M heißt *Totalordnung*, falls $\forall x, y \in M : (x, y) \in R \vee (y, x) \in R$.

Satz 1.5. *Die Relation $\leq \subseteq \mathbb{N} \times \mathbb{N}$ ist eine Totalordnung auf $\mathbb{N}$.*

Beweis. $\leq$ reflexiv: Es gilt für $n \in \mathbb{N}$ stets $n \leq n$, da $n + 0 = n$.
$\leq$ antisymmetrisch: Seien $n, m \in \mathbb{N}$ mit $m \leq n$ und $n \leq m$. Dann existieren $k, \ell \in \mathbb{N}$ mit $m + k = n$ und $n + \ell = m$. Somit gilt aber

$$m + k + \ell = n + \ell = m = m + 0$$

und damit nach Satz 1.4 (c) $k + \ell = 0$. Aus Satz 1.4 (d) folgt nun $k = \ell = 0$ und daher $m = m + 0 = m + k = n$.
$\leq$ transitiv: Seien $k, m, n \in \mathbb{N}$ mit $k \leq m$ und $m \leq n$. Dann existieren $j, \ell \in \mathbb{N}$ mit $k + j = m$ und $m + \ell = n$. Damit folgt $n = m + \ell = k + j + \ell$, also $k \leq n$.
$\leq$ total: Sei $n \in \mathbb{N}$ und betrachte die Menge

$$M \coloneqq \{m \in \mathbb{N}\,;\, m \leq n \vee n \leq m\}\,.$$

Wir müssen $M = \mathbb{N}$ zeigen. Es gilt $0 \in M$, da $n = n + 0 = 0 + n$, also $0 \leq n$ gilt. Sei nun $m \in M$.
1.Fall: $m \leq n, m \neq n$: Es existiert $k \in \mathbb{N}$ mit $m + k = n$. Ferner ist $k \neq 0$, da sonst $m = n$. Daher existiert ein $\ell \in \mathbb{N}$ mit $k = \sigma(\ell)$. Dann gilt

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

also $\sigma(m) \leq n$, also $\sigma(m) \in M$.
2. Fall: $n \leq m$: Da per Definition $m \leq \sigma(m)$ gilt, folgt aus der Transitivität $n \leq \sigma(m)$ und damit $\sigma(m) \in M$.
Aus (P3) folgt nun $M = \mathbb{N}$. □

Satz 1.6. *Seien $k, m, n \in \mathbb{N}$. Dann gilt $k \leq m$ genau dann wenn $k + n \leq m + n$.*

Beweis. Sei $k \leq m$. Dann gibt es $\ell \in \mathbb{N}$ mit $k + \ell = m$. Demnach gilt $k + n + \ell = m + n$ und somit $k + n \leq m + n$. Gilt umgekehrt $k + n \leq m + n$, so existiert ein $\ell \in \mathbb{N}$ mit $k + n + \ell = m + n$. Nach Satz 1.4 (c) folgt hieraus $k + \ell = m$, also $k \leq m$. □

Definition. Für $n \in \mathbb{N}$ definieren wir die Mengen

$$\begin{aligned}
\mathbb{N}_{\geq n} &\coloneqq \{k \in \mathbb{N}\,;\, n \leq k\}\,,\\
\mathbb{N}_{>n} &\coloneqq \{k \in \mathbb{N}\,;\, n \leq k, k \neq n\} = \mathbb{N}_{\geq n} \setminus \{n\} = \mathbb{N}_{\geq \sigma(n)},\\
\mathbb{N}_{\leq n} &\coloneqq \{k \in \mathbb{N}\,;\, k \leq n\} = \mathbb{N} \setminus \mathbb{N}_{>n},\\
\mathbb{N}_{<n} &\coloneqq \{k \in \mathbb{N}\,;\, k \leq n, k \neq n\} = \mathbb{N}_{\leq n} \setminus \{n\}.
\end{aligned}$$

Wir können nun auch zeigen, dass $\leq$ eine Wohlordnung auf $\mathbb{N}$ definiert, d.h. das jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes Element besitzt.

Satz 1.7 (Prinzip des kleinsten Täters)**.** *Sei $M \subseteq \mathbb{N}$ nichtleer. Dann existiert ein kleinstes Element in M, d.h.*

$$\exists m \in M\, \forall n \in M : m \leq n$$

oder mit anderen Worten

$$\exists m \in M : M \subseteq \mathbb{N}_{\geq m}.$$

Beweis. Wir nehmen an, dass so ein Element nicht existiert. Es gilt also

$$\forall m \in M : \mathbb{N}_{<m} \cap M \neq \emptyset. \tag{1.1}$$

Betrachten wir die Menge $K \coloneqq \{n \in \mathbb{N}\,;\, \mathbb{N}_{\leq n} \subseteq \mathbb{N} \setminus M\}$. Dann ist $0 \in K$, da sonst $0 \in M$ gelten würde, was (1.1) widerspräche, da $\mathbb{N}_{<0} = \emptyset$. Sei nun $n \in K$. Wir nehmen an $\sigma(n) \notin K$. Das bedeutet, es gibt ein $k \in \mathbb{N}_{\leq \sigma(n)}$ mit $k \in M$. Da $\mathbb{N}_{\leq n} \subseteq \mathbb{N} \setminus M$ gilt, muss $k = \sigma(n) \in M$ gelten. Nun ist aber

$$\mathbb{N}_{<\sigma(n)} \cap M = \mathbb{N}_{\leq n} \cap M = \emptyset,$$

was (1.1) widerspricht. Somit ist also $\sigma(n) \in K$ und damit $K = \mathbb{N}$. Ist nun $n \in \mathbb{N} = K$, so gilt wegen $n \in \mathbb{N}_{\leq n} \subseteq \mathbb{N} \setminus M$, also $n \notin M$, was bedeutet, dass $M = \emptyset$ gilt. Das widerspricht der Annahme M nichtleer und damit muss unsere Annahme (1.1) falsch sein. □

Nun können wir auch das Schubfachprinzip beweisen.

Satz 1.8 (Schubfachprinzip)**.** *Seien $m, n \in \mathbb{N}$ mit $m > n$ und $f : \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$. Dann existieren $a, b \in \mathbb{N}_{\leq m}$ mit $a \neq b$ und $f(a) = f(b)$, d.h. f ist nicht injektiv.*

Beweis. Wir führen den Beweis per Induktion über n. Ist $n = 0$ so ist $m > 0$ und $f : \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq 0} = \{0\}$. Da $0, \sigma(0) \in \mathbb{N}_{\leq m}$ und $0 \neq \sigma(0)$ gilt, folgt die Behauptung. Wir nehmen nun an, dass die Behauptung für n gilt. Sei $m > \sigma(n)$ und $f : \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq \sigma(n)}$. Insbesondere ist $m > 0$ und somit gilt $m = \sigma(k)$ für ein $k > n$. Wir unterscheiden zwei Fälle:

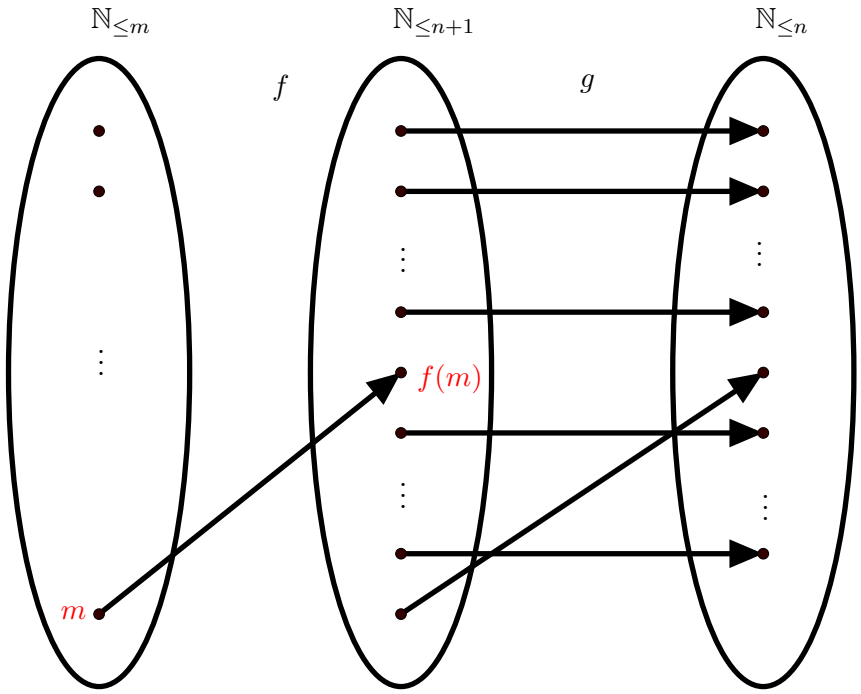
Fall 1 Es gibt $a \in \mathbb{N}_{\leq m}$ mit $a \neq m$ und $f(a) = f(m)$. In diesem Fall ist nichts zu zeigen.

Fall 2 Für alle $a \in \mathbb{N}_{\leq m}$ mit $a \neq m$ gilt $f(a) \neq f(m)$. Wir definieren nun eine injektive Abbildung $g : \mathbb{N}_{\leq \sigma(n)} \setminus \{f(m)\} \to \mathbb{N}_{\leq n}$. Wir unterscheiden wiederum zwei Fälle.

Fall 2.1 $f(m) = \sigma(n)$. Dann betrachten wir die Abbildung $g : \mathbb{N}_{\leq \sigma(n)} \setminus \{f(m)\} \to \mathbb{N}_{\leq n}$ mit $g(j) \coloneqq j$.

Fall 2.2 $f(m) < \sigma(n)$. Dann betrachten wir die Abbildung $g : \mathbb{N}_{\leq \sigma(n)} \setminus \{f(m)\} \to \mathbb{N}_{\leq n}$ mit

$$g(j) = \begin{cases} j & \text{falls } j < \sigma(n), \\ f(m) & \text{falls } j = \sigma(n). \end{cases}$$



Nun ist in beiden Fällen $g \circ f|_{\mathbb{N}_{\leq k}} : \mathbb{N}_{\leq k} \to \mathbb{N}_{\leq n}$ wohldefiniert und $k > n$. Somit gibt es nach Induktionsvoraussetzung $a, b \in \mathbb{N}_{\leq k} \subseteq \mathbb{N}_{\leq m}$ mit $a \neq b$ und $g(f(a)) = g(f(b))$. Aus der Injektivität von g folgt nun $f(a) = f(b)$. □

Wir können nun als zweite Operation die Multiplikation auf $\mathbb{N}$ definieren.

Definition. Sei $k \in \mathbb{N}$. Wir definieren die Funktion $(k\cdot) : \mathbb{N} \to \mathbb{N}$ über ($M = \mathbb{N}$ und $f_m = (k+)$ für alle $m \in \mathbb{N}$)

(a) $(k\cdot)(0) \coloneqq 0$,

(b) $\forall n \in \mathbb{N} : (k\cdot)(\sigma(n)) \coloneqq (k+)((k\cdot)(n)) = k + (k\cdot)(n)$.

Statt $(k\cdot)(n)$ schreiben wir wieder üblicherweise $k \cdot n$. Ferner vereinbaren wir, dass $\cdot$ stärker bindet als $+$, d.h. es gilt $k \cdot n + m \coloneqq (k \cdot n) + m$ für $k, m, n \in \mathbb{N}$.

Satz 1.9 (Rechenregeln für die Multiplikation)**.** *Es gilt:*

(a) $\forall k, m, n \in \mathbb{N} : (m+n) \cdot k = m \cdot k + n \cdot k$ *(Distributivität),*

(b) $\forall k, m, n \in \mathbb{N} : (k \cdot m) \cdot n = k \cdot (m \cdot n)$ *(Assoziativität),*

(c) $\forall k, n \in \mathbb{N} : k \cdot n = n \cdot k$ *(Kommutativität),*

(d) $\forall k \in \mathbb{N}, n \in \mathbb{N}_{>0} : k \cdot n = 0 \Rightarrow k = 0$ *(Nullteilerfreiheit),*

(e) $\forall k, m \in \mathbb{N}, n \in \mathbb{N}_{>0} : k \cdot n = m \cdot n \Rightarrow k = m$ *(Kürzbarkeit).*

Beweis. (a) Seien $m, n \in \mathbb{N}$. Zunächst gilt

$$(m+n) \cdot 0 = 0 = 0 + 0 = m \cdot 0 + n \cdot 0.$$

Gilt nun $(m+n) \cdot k = m \cdot k + n \cdot k$ für ein $k \in \mathbb{N}$, so folgt mit Satz 1.4 (b)

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

(b) Seien $k, m \in \mathbb{N}$. Zunächst gilt

$$(k \cdot m) \cdot 0 = 0 = k \cdot 0 = k \cdot (m \cdot 0).$$

Ist $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ für ein $n \in \mathbb{N}$, so folgt mit (a)

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

(c) Der Beweis erfolgt in 4 Schritten:

(i) Als erstes zeigen wir $0 \cdot k = 0$ für alle $k \in \mathbb{N}$. Für $k = 0$ gilt die Formel offensichtlich, da $0 \cdot 0 = 0$. Gelte sie nun für ein $k \in \mathbb{N}$. Dann ist

$$0 \cdot \sigma(k) = 0 + 0 \cdot k = 0 \cdot k = 0.$$

(ii) Nun beweisen wir $1 \cdot k = k$ für alle $k \in \mathbb{N}$. Ist $k = 0$ so gilt $1 \cdot 0 = 0$ per Definition. Gelte nun $1 \cdot k = k$ für ein $k \in \mathbb{N}$. Dann ist

$$1 \cdot \sigma(k) = 1 + 1 \cdot k = 1 + k = k + 1 = \sigma(k).$$

(iii) Schließlich können wir nun die Behauptung beweisen. Sei $k \in \mathbb{N}$. Dann gilt $k \cdot 0 = 0 = 0 \cdot k$ (siehe (i)). Gilt nun $k \cdot n = n \cdot k$ für ein $n \in \mathbb{N}$, so folgt mit (a),(i) und (ii):

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

(d) Seien $k \in \mathbb{N}, n \in \mathbb{N}_{>0}$ mit $k \cdot n = 0$. Nach Satz 1.2 gibt es $\ell \in \mathbb{N}$ mit $n = \sigma(\ell)$. Daher gilt

$$0 = k \cdot n = k \cdot \sigma(\ell) = k + k \cdot \ell.$$

Nach Satz 1.4 (d) folgt hieraus $k = 0$.

(e) Seien $k, m \in \mathbb{N}$, $n \in \mathbb{N}_{>0}$ und $k \cdot n = m \cdot n$. Da $\leq$ eine Totalordnung ist, gilt $k \leq m$ oder $m \leq k$. Wir nehmen o.E. an, dass $k \leq m$ gilt. Dann gibt es $\ell \in \mathbb{N}$ mit $m = k + \ell$. Dann gilt

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

Mit Satz 1.4 folgt hieraus

$$0 = \ell \cdot n$$

und nach (d) gilt dann $\ell = 0$. Somit ist $m = k + 0 = k$. □

2. Die ganzen Zahlen

In diesem Abschnitt wollen wir die ganzen Zahlen mithilfe der natürlichen Zahlen definieren. Dafür benötigen wir Äquivalenzklassen. Wir wiederholen daher noch einmal, was wir unter einer Äquivalenzrelation verstehen.

Definition. Sei M eine Menge und $R \subseteq M \times M$. R heißt *Äquivalenzrelation auf M,* falls

(a) R reflexiv ist,

(b) R *symmetrisch* ist, d.h. $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$,

(c) R transitiv ist.

Ist R eine Äquivalenzrelation auf M, so heißt für $x \in M$ die Menge $[x]_R \coloneqq \{y \in M \mid (x, y) \in R\}$ *Äquivalenzklasse* und x ein *Repräsentant der Äquivalenzklasse.* Ferner definieren wir die Menge

$$M/_R \coloneqq \{[x]_R \mid x \in M\}.$$

Statt $(x, y) \in R$ schreiben wir auch hier häufig xRy.

Wir definieren nun eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.

Definition. Wir definieren $\sim_{\mathbb{Z}} \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ durch

$$(k, \ell) \sim_{\mathbb{Z}} (m, n) \colon \Leftrightarrow k + n = \ell + m.$$

Satz 2.1. *$\sim_{\mathbb{Z}}$ definiert eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.*

Beweis. Die Reflexivität und Symmetrie von $\sim_{\mathbb{Z}}$ ist offensichtlich. Seien nun $k, \ell, m, n, x, y \in \mathbb{N}$ mit $(k, \ell) \sim_{\mathbb{Z}} (m, n)$ und $(m, n) \sim_{\mathbb{Z}} (x, y)$. Dann gilt unter Verwendung von Satz 1.4

$$k + n + y = \ell + m + y = \ell + n + x.$$

Hieraus folgt (ebenfalls aus Satz 1.4) $k + y = \ell + x$, also $(k, \ell) \sim_{\mathbb{Z}} (x, y)$. Damit ist $\sim_{\mathbb{Z}}$ auch transitiv und somit eine Äquivalenzrelation. □

Definition. Die Menge der *ganzen Zahlen* $\mathbb{Z}$ ist definiert als

$$\mathbb{Z} \coloneqq \mathbb{N} \times \mathbb{N}/_{\sim_{\mathbb{Z}}}.$$

Wir können nun die Addition, die Multiplikation und die die Ordnung $\leq$ auf $\mathbb{Z}$ wie folgt definieren.

Satz 2.2. *Wir definieren für* $k, \ell, m, n \in \mathbb{N}$

$$[(k,\ell)]_{\sim_{\mathbb{Z}}} + [(m,n)]_{\sim_{\mathbb{Z}}} \coloneqq [(k+m, \ell+n)]_{\sim_{\mathbb{Z}}}.$$

Dann ist $+$ *wohldefiniert. Ferner ist* $(\mathbb{Z}, +)$ *eine abelsche Gruppe mit neutralem Element* $[(0,0)]_{\sim_{\mathbb{Z}}}$ *und inversem Element* $[(\ell,k)]_{\sim_{\mathbb{Z}}}$ *zu* $[(k,\ell)]_{\sim_{\mathbb{Z}}}$.

Beweis. Wir zeigen die Wohldefiniertheit. Seien $(a,b) \sim_{\mathbb{Z}} (k,\ell)$ und $(x,y) \sim_{\mathbb{Z}} (m,n)$. Dann gilt

$$k + m + y + b = a + \ell + x + n = \ell + n + x + a,$$

also $(k+m, \ell+n) \sim_{\mathbb{Z}} (x+a, y+b)$. Somit ist $+$ wohldefiniert. Ferner ist $+$ assoziativ und kommutativ nach Satz 1.4. Offenbar ist $[(0,0)]_{\sim_{\mathbb{Z}}}$ das neutrale Element. Außerdem gilt

$$[(k,\ell)]_{\sim_{\mathbb{Z}}} + [(\ell,k)]_{\sim_{\mathbb{Z}}} = [(k+\ell, \ell+k)]_{\sim_{\mathbb{Z}}} = [(0,0)]_{\sim_{\mathbb{Z}}},$$

wobei dir letze Gleichheit wegen

$$k + \ell + 0 = k + \ell = \ell + k = \ell + k + 0$$

folgt. □

Satz 2.3. *Für* $k, \ell, m, n \in \mathbb{N}$ *definieren wir*

$$[(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(m,n)]_{\sim_{\mathbb{Z}}} \coloneqq [(k \cdot m + \ell \cdot n, k \cdot n + \ell \cdot m)]_{\sim_{\mathbb{Z}}}.$$

Dann ist $\cdot$ *wohldefiniert. Ferner gelten das Distributivgesetz, das Assoziativgesetz und das Kommutativgesetz (vgl. Satz 1.9). Ferner ist* $[(\sigma(0),0)]_{\sim_{\mathbb{Z}}}$ *das neutrale Element bzgl* $\cdot$.

Beweis. Wir zeigen zunächst, dass $\cdot$ wohldefiniert ist. Seien dazu $(a,b) \sim_{\mathbb{Z}} (k,\ell)$ und $(x,y) \sim_{\mathbb{Z}} (m,n)$. Dann gilt

$$\begin{aligned}
(k \cdot m + \ell \cdot n) + (a \cdot y + b \cdot x) + a \cdot n &= k \cdot m + (\ell + a) \cdot n + a \cdot y + b \cdot x \\
&= k \cdot m + (b + k) \cdot n + a \cdot y + b \cdot x \\
&= k \cdot (m+n) + b \cdot (n + x) + a \cdot y \\
&= k \cdot (m+n) + b \cdot (y + m) + a \cdot y \\
&= (k+b) \cdot m + k \cdot n + b \cdot y + a \cdot y \\
&= (\ell + a) \cdot m + k \cdot n + b \cdot y + a \cdot y \\
&= \ell \cdot m + k \cdot n + b \cdot y + a \cdot (m+y) \\
&= \ell \cdot m + k \cdot n + b \cdot y + a \cdot (x+n) \\
&= (k \cdot n + \ell \cdot m) + (a \cdot x + b \cdot y) + a \cdot n
\end{aligned}$$

und somit

$$(k \cdot m + \ell \cdot n) + (a \cdot y + b \cdot x) = (k \cdot n + \ell \cdot m) + (a \cdot x + b \cdot y),$$

also $(k \cdot m + \ell \cdot n, k \cdot n + \ell \cdot m) \sim_{\mathbb{Z}} (a \cdot x + b \cdot y, a \cdot y + b \cdot x)$. Seien nun $k, \ell, m, n, x, y \in \mathbb{N}$. Dann gilt

$$\begin{aligned}
[(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot \Big([(m,n)]_{\sim_{\mathbb{Z}}} + [(x,y)]_{\sim_{\mathbb{Z}}} \Big) &= [(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(m+x, n+y)]_{\sim_{\mathbb{Z}}} \\
&= [(k \cdot (m+x) + \ell \cdot (n+y), k \cdot (n+y) + \ell \cdot (m+x))]_{\sim_{\mathbb{Z}}} \\
&= [(k \cdot m + \ell \cdot n, k \cdot n + \ell \cdot m)]_{\sim_{\mathbb{Z}}} + [(k \cdot x + \ell \cdot y, k \cdot y + \ell \cdot x)]_{\sim_{\mathbb{Z}}} \\
&= [(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(m,n)]_{\sim_{\mathbb{Z}}} + [(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(x,y)]_{\sim_{\mathbb{Z}}} .
\end{aligned}$$

Außerdem gilt

$$\begin{aligned}
&[(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot \Big([(m,n)]_{\sim_{\mathbb{Z}}} \cdot [(x,y)]_{\sim_{\mathbb{Z}}} \Big) \\
&= [(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(m \cdot x + n \cdot y, m \cdot y + n \cdot x)]_{\sim_{\mathbb{Z}}} \\
&= [(k \cdot (m \cdot x + n \cdot y) + \ell \cdot (m \cdot y + n \cdot x), k \cdot (m \cdot y + n \cdot x) + \ell \cdot (m \cdot x + n \cdot y))]_{\sim_{\mathbb{Z}}} \\
&= [((k \cdot m + \ell \cdot n) \cdot x + (k \cdot n + \ell \cdot m) \cdot y, (k \cdot m + \ell \cdot n) \cdot y + (k \cdot n + \ell \cdot m) \cdot x)]_{\sim_{\mathbb{Z}}} \\
&= [(k \cdot m + \ell \cdot n, k \cdot n + \ell \cdot m)]_{\sim_{\mathbb{Z}}} \cdot [(x,y)]_{\sim_{\mathbb{Z}}} \\
&= \Big([(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(m,n)]_{\sim_{\mathbb{Z}}} \Big) \cdot [(x,y)]_{\sim_{\mathbb{Z}}} .
\end{aligned}$$

Die Kommutativität von $\cdot$ ist klar. Ferner gilt

$$[(k,\ell)]_{\sim_{\mathbb{Z}}} \cdot [(\sigma(0),0)]_{\sim_{\mathbb{Z}}} = [(k \cdot \sigma(0) + k \cdot 0, k \cdot 0 + \ell \cdot \sigma(0))]_{\sim_{\mathbb{Z}}} = [(k,\ell)]_{\sim_{\mathbb{Z}}} .$$ □

Satz 2.4. *Wir definieren* $\leq \subseteq \mathbb{Z} \times \mathbb{Z}$ *durch*

$$[(k,\ell)]_{\sim_{\mathbb{Z}}} \leq [(m,n)]_{\sim_{\mathbb{Z}}} :\Leftrightarrow k + n \leq \ell + m.$$

Dann ist $\leq$ *wohldefiniert und eine Totalordnung auf* $\mathbb{Z}$.

Beweis. Seien $k, \ell, m, n \in \mathbb{N}$ so dass $k + n \leq \ell + m$. Seien ferner $\widetilde{k}, \widetilde{\ell}, \widetilde{m}, \widetilde{n} \in \mathbb{N}$ mit $(\widetilde{k}, \widetilde{\ell}) \sim_{\mathbb{Z}} (k, \ell)$ und $(\widetilde{m}, \widetilde{n}) \sim_{\mathbb{Z}} (m, n)$. Dann ist mit Satz 1.6

$$\widetilde{k} + \widetilde{n} + \ell + m = \widetilde{\ell} + k + \widetilde{m} + n \leq \widetilde{\ell} + \widetilde{m} + \ell + m$$

und somit

$$\widetilde{k} + \widetilde{n} \leq \widetilde{\ell} + \widetilde{m}.$$

Somit ist $\leq$ wohldefiniert. Die Reflexivität von $\leq$ ist klar. Sei nun $[(k,\ell)]_{\sim_{\mathbb{Z}}} \leq [(m,n)]_{\sim_{\mathbb{Z}}}$ und $[(m,n)]_{\sim_{\mathbb{Z}}} \leq [(k,\ell)]_{\sim_{\mathbb{Z}}}$. Dann ist $k + n = \ell + m$ und somit $(k,\ell) \sim_{\mathbb{Z}} (m,n)$, also $[(m,n)]_{\sim_{\mathbb{Z}}} = [(k,\ell)]_{\sim_{\mathbb{Z}}}$. Somit ist $\leq$ antisymmetrisch. Gilt $[(k,\ell)]_{\sim_{\mathbb{Z}}} \leq [(m,n)]_{\sim_{\mathbb{Z}}}$ und $[(m,n)]_{\sim_{\mathbb{Z}}} \leq [(x,y)]_{\sim_{\mathbb{Z}}}$ so ist

$$k + y + n \leq \ell + m + y \leq \ell + x + n$$

und daher $k + y \leq \ell + x$ nach Satz 1.6. Das zeigt die Transitivität. Die Totalität von $\leq$ folgt unmittelbar aus der Totalität von $\leq$ auf $\mathbb{N}$. □

Wir wollen nun noch die natürlichen Zahlen in die ganzen Zahlen strukturverträglich einbetten.

Satz 2.5. *Die Abbildung*

$$\begin{aligned}\iota : \mathbb{N} &\to \mathbb{Z}\\ n &\mapsto [(n,0)]_{\sim_{\mathbb{Z}}}\end{aligned}$$

ist injektiv. Ferner gilt für $m, n \in \mathbb{N}$:

(a) $\iota(m+n) = \iota(m) + \iota(n)$,

(b) $\iota(m \cdot n) = \iota(m) \cdot \iota(n)$,

(c) $m \leq n \Leftrightarrow \iota(m) \leq \iota(n)$.

Beweis. Seien $m, n \in \mathbb{N}$. Ist $\iota(n) = \iota(m)$ so gilt $(n,0) \sim_{\mathbb{Z}} (m,0)$ also $n = n+0 = 0+m = m$. Somit ist ι injektiv. Ferner gilt

$$\iota(m+n) = [(m+n,0)]_{\sim_{\mathbb{Z}}} = [(m,0)]_{\sim_{\mathbb{Z}}} + [(n,0)]_{\sim_{\mathbb{Z}}} = \iota(m) + \iota(n)$$

und

$$\iota(m) \cdot \iota(n) = [(m,0)]_{\sim_{\mathbb{Z}}} \cdot [(n,0)]_{\sim_{\mathbb{Z}}} = [(m \cdot n + 0 \cdot 0, m \cdot 0 + 0 \cdot n)]_{\sim_{\mathbb{Z}}} = [(m \cdot n, 0)]_{\sim_{\mathbb{Z}}} = \iota(m \cdot n).$$

Außerdem ist

$$\iota(m) \leq \iota(n) \Leftrightarrow m + 0 \leq n + 0 \Leftrightarrow m \leq n. \qquad \square$$

Bemerkung 2.6. Im folgenden werden wir $\mathbb{N}$ stets als Teilmenge von $\mathbb{Z}$ auffassen, d.h. wir unterscheiden nicht zwischen n und $\iota(n)$. In diesem Sinne gilt dann $\mathbb{Z} = \mathbb{Z}_{\geq 0} \cup \mathbb{Z}_{\leq 0}$, da $\leq$ eine Totalordnung auf $\mathbb{Z}$ definiert. Für $k = [(m,n)]_{\sim_{\mathbb{Z}}} \in \mathbb{Z}_{\geq 0}$ gilt dann $n \leq m$ und somit gibt es $\ell \in \mathbb{N}$ mit $n + \ell = m$, was nichts anderes bedeutet als $(m,n) \sim_{\mathbb{Z}} (\ell, 0)$ und damit $k = \iota(\ell)$. Somit ist also im Sinne unserer Identifikation $\mathbb{Z}_{\geq 0} = \mathbb{N}$. Analog gilt für $k = [(m,n)]_{\sim_{\mathbb{Z}}} \in \mathbb{Z}_{\leq 0}$ die Beziehung $m \leq n$ und somit finden wir $\ell \in \mathbb{N}$ mit $m + \ell = n$, was $(m,n) \sim_{\mathbb{Z}} (0, \ell)$ zeigt, also $k = [(0,\ell)]_{\sim_{\mathbb{Z}}}$. Außerdem definieren wir für $[(m,n)]_{\sim_{\mathbb{Z}}} \in \mathbb{Z}$

$$-[(m,n)]_{\sim_{\mathbb{Z}}} \coloneqq [(n,m)]_{\sim_{\mathbb{Z}}} = [(m,n)]_{\sim_{\mathbb{Z}}} \cdot [(0,\sigma(0))]_{\sim_{\mathbb{Z}}} \in \mathbb{Z}.$$

Gemäß unserer obigen Überlegungen ist dann

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}).$$

Ferner schreiben wir wie üblich $k - n$ statt $k + (-n)$ für $k, n \in \mathbb{Z}$.

Noch wollen wir noch einige Eigenschaften der algebraischen Operationen auf $\mathbb{Z}$ thematisieren.

Satz 2.7. *Seien $k, m, n \in \mathbb{Z}$. Dann gilt*

(a) $k \cdot m = 0 \Rightarrow k = 0 \vee m = 0$,

(b) $k \leq m \Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : k + \ell = m$,

(c) $k \leq m \Leftrightarrow k + n \leq m + n$,

(d) für $n \in \mathbb{Z}_{>0}$ gilt $k \leq m \Leftrightarrow k \cdot n \leq m \cdot n$,

(e) für $n \in \mathbb{Z}_{<0}$ gilt $k \leq m \Leftrightarrow m \cdot n \leq k \cdot n$,

(f) für $n \neq 0$ gilt $k = m \Leftrightarrow k \cdot n = m \cdot n$.

Beweis. Seien $k = [(a,b)]_{\sim_{\mathbb{Z}}}$, $m = [(x,y)]_{\sim_{\mathbb{Z}}}$, $n = [(c,d)]_{\sim}$.

(a) Wir nehmen an, dass $m \neq 0$ und $k \cdot m = 0$ gilt. Das heißt $x \neq y$ und $a \cdot x + b \cdot y = a \cdot y + b \cdot x$. Wir unterscheiden zwei Fälle: Sei zunächst $a \leq b$. Dann gibt es ein $\ell \in \mathbb{N}$ mit $a + \ell = b$. Demnach ist

$$a \cdot x + (a + \ell) \cdot y = a \cdot y + (a + \ell) \cdot x,$$

woraus $\ell \cdot y = \ell \cdot x$ folgt. Da $x \neq y$ ist, folgt somit nach Satz 1.9 (d) $\ell = 0$ also $a = b$. Der Fall $b \leq a$ funktioniert analog. Somit ist also $a = b$ und daher $(a,b) \sim_{\mathbb{Z}} (0,0)$, also $k = 0$.

(b) Es gilt

$$k \leq m \Leftrightarrow a+y \leq b+x \Leftrightarrow \exists \ell \in \mathbb{N} = \mathbb{Z}_{\geq 0} : a+y+\ell = b+x \Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : [(a+\ell, b)]_{\sim_{\mathbb{Z}}} = [(x,y)]_{\sim_{\mathbb{Z}}}.$$

(c) Es gilt nach Satz 1.6

$$k + n \leq m + n \Leftrightarrow a + c + y + d \leq b + d + x + c \Leftrightarrow a + y \leq b + x \Leftrightarrow k \leq m.$$

(d) Da $n \in \mathbb{Z}_{>0}$ gibt es $\ell \in \mathbb{N}_{>0}$ mit $n = [(\ell, 0)]_{\sim_{\mathbb{Z}}}$. Nach Satz 1.9 gilt

$$k \cdot n \leq m \cdot n \Leftrightarrow a \cdot \ell + y \cdot \ell \leq b \cdot \ell + x \cdot \ell \Leftrightarrow (a + y) \cdot \ell \leq (b + x) \cdot \ell \Leftrightarrow a + y \leq b + x \Leftrightarrow k \leq m.$$

(e) Ist $n \in \mathbb{Z}_{<0}$, so gilt $n = [(0, \ell)]_{\sim_{\mathbb{Z}}} = -\ell$ für ein $\ell \in \mathbb{N}_{>0}$. Damit gilt wiederum mit Satz 1.9

$$m \cdot n \leq k \cdot n \Leftrightarrow y \cdot \ell + a \cdot \ell \leq x \cdot \ell + b \cdot \ell \Leftrightarrow (y + a) \cdot \ell \leq (x + b) \cdot \ell \Leftrightarrow y + a \leq x + b \Leftrightarrow k \leq m.$$

(f) Das folgt unmittelbar aus der Antisymmetrie von $\leq$ und aus (d), falls $n > 0$ oder (e), falls $n < 0$ gilt. □

3. Die rationalen Zahlen

Wie schon bei den ganzen Zahlen, führen wir auch die rationalen Zahlen als Äquivalenzklassen ein. Wir definieren dazu die folgende Relation auf $\mathbb{Z} \times \mathbb{Z}_{>0}$.

Definition. Wir definieren $\sim_{\mathbb{Q}} \subseteq (\mathbb{Z} \times \mathbb{Z}_{>0}) \times (\mathbb{Z} \times \mathbb{Z}_{>0})$ durch

$$(x, n) \sim_{\mathbb{Q}} (y, m) : \Leftrightarrow x \cdot m = y \cdot n.$$

Satz 3.1. *Die Relation $\sim_{\mathbb{Q}}$ ist eine Äquivalenzrelation.*

Beweis. Die Relation ist offensichtlich reflexiv und symmetrisch. Seien nun $x, y, z \in \mathbb{Z}$ und $n, m, k \in \mathbb{Z}_{>0}$ mit $(x, n) \sim_{\mathbb{Q}} (y, m)$ und $(y, m) \sim_{\mathbb{Q}} (z, k)$. Dann gilt

$$x \cdot k \cdot m = y \cdot n \cdot k = z \cdot n \cdot m$$

und somit $x \cdot k = z \cdot n$ nach Satz 2.7 (f). Also ist $\sim_{\mathbb{Q}}$ transitiv. □

Definition. Die Menge $\mathbb{Q}$ der rationalen Zahlen definieren wir als die Faktormenge

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}_{>0} / \sim_{\mathbb{Q}}.$$

Wie schon in $\mathbb{Z}$ beginnen wir, die Ordnung $\leq$ auf $\mathbb{Q}$ fortzusetzen.

Satz 3.2. *Wir definieren die Relation $\leq \subseteq \mathbb{Q} \times \mathbb{Q}$ durch*

$$[(x, n)]_{\sim_{\mathbb{Q}}} \leq [(y, m)]_{\sim_{\mathbb{Q}}} : \Leftrightarrow x \cdot m \leq y \cdot n.$$

Dann ist $\leq$ wohldefiniert und eine Totalordnung auf $\mathbb{Q}$.

Beweis. Seien $x, y, \widetilde{x}, \widetilde{y} \in \mathbb{Z}$ und $n, m, \widetilde{n}, \widetilde{m} \in \mathbb{Z}_{>0}$ so dass $(x, n) \sim_{\mathbb{Q}} (\widetilde{x}, \widetilde{n})$, $(y, m) \sim_{\mathbb{Q}} (\widetilde{y}, \widetilde{m})$ und $x \cdot m \leq y \cdot n$ gilt. Dann ist nach Satz 2.7 (d)

$$\widetilde{x} \cdot \widetilde{m} \cdot n \cdot m = x \cdot \widetilde{n} \cdot \widetilde{m} \cdot m \leq y \cdot n \cdot \widetilde{m} \cdot \widetilde{n} = \widetilde{y} \cdot m \cdot \widetilde{n} \cdot n$$

und somit gilt wiederum nach Satz 2.7 (d)

$$\widetilde{x} \cdot \widetilde{m} \leq \widetilde{y} \cdot \widetilde{n}.$$

Das beweist, dass $\leq$ wohldefiniert ist. Offenbar ist $\leq$ reflexiv. Die Antisymmetrie folgt aus der Definition von $\sim_{\mathbb{Q}}$. Seien nun $x, y, z \in \mathbb{Z}$ und $n, m, k \in \mathbb{Z}_{>0}$ mit $x \cdot m \leq y \cdot n$ und $y \cdot k \leq z \cdot m$. Dann ist

$$x \cdot k \cdot m \leq y \cdot n \cdot k \leq z \cdot m \cdot n$$

und somit $x \cdot k \leq z \cdot n$. Somit ist $\leq$ eine Ordnungsrelation. Die Totalität folgt unmittelbar aus der Totalität von $\leq$ auf $\mathbb{Z}$. □

Nun kommen wir zur Addition und zur Multiplikation.

Satz 3.3. *Für $x, y \in \mathbb{Z}$ und $n, m \in \mathbb{Z}_{>0}$ definieren wir*

$$[(x,n)]_{\sim_{\mathbb{Q}}} + [(y,m)]_{\sim_{\mathbb{Q}}} \coloneqq [(x \cdot m + y \cdot n, n \cdot m)]_{\sim_{\mathbb{Q}}}.$$

Dann ist $+$ wohldefiniert, und $(\mathbb{Q}, +)$ eine abelsche Gruppe mit neutralem Element $[(0, \sigma(0))]_{\sim_{\mathbb{Q}}}$ und $[(-x, n)]_{\sim_{\mathbb{Q}}}$ als inversem Element zu $[(x,n)]_{\sim_{\mathbb{Q}}}$.

Beweis. Zunächst bemerken wir, dass nach Satz 2.7 für $n, m \in \mathbb{Z}_{>0}$ auch $n \cdot m > 0$ gilt. Seien nun $x, y, \widetilde{x}, \widetilde{y} \in \mathbb{Z}$ und $n, m, \widetilde{n}, \widetilde{m} \in \mathbb{Z}_{>0}$ mit $(x,n) \sim_{\mathbb{Q}} (\widetilde{x}, \widetilde{n})$ und $(y,m) \sim_{\mathbb{Q}} (\widetilde{y}, \widetilde{m})$. Dann ist

$$\begin{aligned}(\widetilde{x} \cdot \widetilde{m} + \widetilde{y} \cdot \widetilde{n}) \cdot (n \cdot m) &= \widetilde{x} \cdot \widetilde{m} \cdot n \cdot m + \widetilde{y} \cdot \widetilde{n} \cdot n \cdot m \\ &= x \cdot \widetilde{n} \cdot \widetilde{m} \cdot m + y \cdot \widetilde{m} \cdot \widetilde{n} \cdot n \\ &= (x \cdot m + y \cdot n) \cdot (\widetilde{n} \cdot \widetilde{m})\end{aligned}$$

und somit $(\widetilde{x} \cdot \widetilde{m} + \widetilde{y} \cdot \widetilde{n}, \widetilde{n} \cdot \widetilde{m}) \sim_{\mathbb{Q}} (x \cdot m + y \cdot n, n \cdot m)$ und demnach ist $+$ wohldefiniert. Für $x, y, z \in \mathbb{Z}$ und $n, m, k \in \mathbb{Z}_{>0}$ gilt

$$\begin{aligned}\Big([(x,n)]_{\sim_{\mathbb{Q}}} + [(y,m)]_{\sim_{\mathbb{Q}}}\Big) + [(z,k)]_{\sim_{\mathbb{Q}}} &= [(x \cdot m + y \cdot n, n \cdot m)]_{\sim_{\mathbb{Q}}} + [(z,k)]_{\sim_{\mathbb{Q}}} \\ &= [((x \cdot m + y \cdot n) \cdot k + z \cdot (n \cdot m), n \cdot m \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot m \cdot k + y \cdot k \cdot n + z \cdot m \cdot n, n \cdot m \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot m \cdot k + (y \cdot k + z \cdot m) \cdot n, n \cdot m \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x,n)]_{\sim_{\mathbb{Q}}} + [(y \cdot k + z \cdot m, m \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x,n)]_{\sim_{\mathbb{Q}}} + \Big([(y,m)]_{\sim_{\mathbb{Q}}} + [(z,k)]_{\sim_{\mathbb{Q}}}\Big).\end{aligned}$$

Die Kommutativität von $+$ ist klar. Ferner gilt

$$[(x,n)]_{\sim_{\mathbb{Q}}} + [(0,\sigma(0))]_{\sim_{\mathbb{Q}}} = [(x \cdot \sigma(0) + 0 \cdot n, n \cdot \sigma(0))]_{\sim_{\mathbb{Q}}} = [(x,n)]_{\sim_{\mathbb{Q}}}$$

und

$$[(x,n)]_{\sim_{\mathbb{Q}}} + [(-x,n)]_{\sim_{\mathbb{Q}}} = [(x \cdot n + (-x) \cdot n, n \cdot n)]_{\sim_{\mathbb{Q}}} = [(0, n \cdot n)]_{\mathbb{Q}} = [(0, \sigma(0))]_{\sim\mathbb{Q}},$$

da $(0,m) \sim_{\mathbb{Q}} (0, \sigma(0))$ für alle $m \in \mathbb{Z}_{>0}$ gilt. □

Satz 3.4. *Für $x, y \in \mathbb{Z}$ und $n, m \in \mathbb{Z}_{>0}$ definieren wir*

$$[(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(y,m)]_{\sim_{\mathbb{Q}}} \coloneqq [(x \cdot y, n \cdot m)]_{\sim_{\mathbb{Q}}}.$$

Dann ist $\cdot$ wohldefiniert und $(\mathbb{Q}, +, \cdot)$ ist ein Körper mit neutralem Element $[(\sigma(0), \sigma(0))]_{\sim_{\mathbb{Q}}}$ bzgl $\cdot$. Ferner ist das inverse Element zu $[(x,n)]_{\sim_{\mathbb{Q}}}$ mit $x \neq 0$ bzgl $\cdot$ gegeben durch

$$[(x,n)]_{\sim_{\mathbb{Q}}}^{-1} \coloneqq \begin{cases} [(n,x)]_{\sim_{\mathbb{Q}}} & \text{falls } x > 0, \\ [(-n,-x)]_{\sim_{\mathbb{Q}}} & \text{falls } x < 0. \end{cases}$$

Beweis. Seien $x, y, \widetilde{x}, \widetilde{y} \in \mathbb{Z}$ und $n, m, \widetilde{n}, \widetilde{m} \in \mathbb{Z}_{>0}$ mit $(x,n) \sim_{\mathbb{Q}} (\widetilde{x}, \widetilde{n})$ und $(y,m) \sim_{\mathbb{Q}} (\widetilde{y}, \widetilde{m})$. Dann ist

$$\widetilde{x} \cdot \widetilde{y} \cdot n \cdot m = x \cdot y \cdot \widetilde{n} \cdot \widetilde{m}$$

also $(\widetilde{x} \cdot \widetilde{y}, \widetilde{n} \cdot \widetilde{m}) \sim_{\mathbb{Q}} (x \cdot y, n \cdot m)$ und somit ist $\cdot$ wohldefiniert. Die Assoziativität und Kommutativität von $\cdot$ ist klar. Seien nun $x, y, z \in \mathbb{Z}$ und $n, m, k \in \mathbb{Z}_{>0}$. Dann gilt

$$\begin{aligned}[(x,n)]_{\sim_{\mathbb{Q}}} \cdot \Big([(y,m)]_{\sim_{\mathbb{Q}}} + [(z,k)]_{\sim_{\mathbb{Q}}}\Big) &= [(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(y \cdot k + z \cdot m, m \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot y \cdot k + x \cdot z \cdot m, n \cdot m \cdot k)]_{\sim_{\mathbb{Q}}}.\end{aligned}$$

Andererseits ist

$$\begin{aligned}\Big([(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(y,m)]_{\sim_{\mathbb{Q}}}\Big) + \Big([(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(z,k)]_{\sim_{\mathbb{Q}}}\Big) &= [(x \cdot y, n \cdot m)]_{\sim_{\mathbb{Q}}} + [(x \cdot z, n \cdot k)]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot y \cdot n \cdot k + x \cdot z \cdot n \cdot m, n \cdot m \cdot n \cdot k)]_{\sim_{\mathbb{Q}}}.\end{aligned}$$

Nun gilt

$$(x \cdot y \cdot k + x \cdot z \cdot m) \cdot n \cdot m \cdot n \cdot k = (x \cdot y \cdot k \cdot n + x \cdot z \cdot m \cdot n) \cdot m \cdot n \cdot k$$

also $(x \cdot y \cdot k + x \cdot z \cdot m, n \cdot m \cdot k) \sim_{\mathbb{Q}} (x \cdot y \cdot n \cdot k + x \cdot z \cdot n \cdot m, n \cdot m \cdot n \cdot k)$, was die Distributivität beweist.
Ferner gilt

$$[(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(\sigma(0), \sigma(0))]_{\sim_{\mathbb{Q}}} = [(x \cdot \sigma(0), n \cdot \sigma(0))]_{\sim_{\mathbb{Q}}} = [(x,n)]_{\sim_{\mathbb{Q}}}$$

und

$$[(x,n)]_{\sim_{\mathbb{Q}}} \cdot [(x,n)]_{\sim_{\mathbb{Q}}}^{-1} = \begin{cases} [(x \cdot n, n \cdot x)]_{\sim_{\mathbb{Q}}} & \text{falls } x > 0, \\ [(x \cdot (-n), n \cdot (-x))]_{\sim_{\mathbb{Q}}} & \text{falls } x < 0 \end{cases} = [(\sigma(0), \sigma(0))]_{\sim_{\mathbb{Q}}},$$

da $(y,y) \sim_{\mathbb{Q}} (\sigma(0), \sigma(0))$ für alle $y \in \mathbb{Z}_{>0}$. □

Wir wollen nun die Menge $\mathbb{Z}$ in $\mathbb{Q}$ einbetten.

Satz 3.5. *Die Abbildung*

$$\begin{aligned}\iota : \mathbb{Z} &\to \mathbb{Q} \\ x &\mapsto [(x, \sigma(0))]_{\sim_{\mathbb{Q}}}\end{aligned}$$

ist injektiv. Ferner gilt für $x, y \in \mathbb{Z}$: $\iota(x+y) = \iota(x)+\iota(y)$, $\iota(x \cdot y) = \iota(x) \cdot \iota(y)$, sowie $x \leq y \Leftrightarrow \iota(x) \leq \iota(y)$.

Beweis. Seien $x, y \in \mathbb{Z}$. Dann folgt aus $\iota(x) = \iota(y)$

$$x \cdot \sigma(0) = y \cdot \sigma(0)$$

und damit $x = y$. Somit ist ι injektiv. Ferner gilt

$$\begin{aligned}\iota(x) + \iota(y) &= [(x, \sigma(0))]_{\sim_{\mathbb{Q}}} + [(y, \sigma(0))]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot \sigma(0) + y \cdot \sigma(0), \sigma(0) \cdot \sigma(0))]_{\sim_{\mathbb{Q}}}\end{aligned}$$

$$= [(x + y, \sigma(0))]_{\sim_{\mathbb{Q}}} = \iota(x + y)$$

sowie

$$\begin{aligned}\iota(x) \cdot \iota(y) &= [(x, \sigma(0))]_{\sim_{\mathbb{Q}}} \cdot [(y, \sigma(0))]_{\sim_{\mathbb{Q}}} \\ &= [(x \cdot y, \sigma(0))]_{\sim_{\mathbb{Q}}} = \iota(x \cdot y).\end{aligned}$$

Außerdem gilt

$$\iota(x) \leq \iota(y) \Leftrightarrow x \cdot \sigma(0) \leq y \cdot \sigma(0) \Leftrightarrow x \leq y. \qquad \square$$

Bemerkung 3.6. Auch hier wollen wir $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auffassen. Ferner schreiben wir statt $[(x, n)]_{\sim_{\mathbb{Q}}}$ üblicherweise $\frac{x}{n}$ und statt $\frac{x}{n} \sim_{\mathbb{Q}} \frac{y}{m}$ schreiben wir $\frac{x}{n} = \frac{y}{m}$. Ferner gilt $\frac{x}{n} > 0 \Leftrightarrow x > 0$, $\frac{x}{n} = 0 \Leftrightarrow x = 0$ und $\frac{x}{n} < 0 \Leftrightarrow x < 0$.

Lemma 3.7. *Sei $p \in \mathbb{Q}_{\geq 0}$. Dann existiert ein $n \in \mathbb{N}$ mit $p < n$.*

Beweis. In der Tat, ist $p = \frac{m}{a}$ für $m \in \mathbb{N}, \sigma(b) = a \in \mathbb{N}_{>0}$ so gilt $p < \sigma(m)$, da

$$0 < a \Rightarrow 0 < a + b \cdot m \Rightarrow m < a + b \cdot m + m = a + m \cdot a = \sigma(m) \cdot a \Rightarrow p < \sigma(m). \qquad \square$$

Satz 3.8. *Seien $k, m, n \in \mathbb{Q}$. Dann gilt*

(a) $k \cdot m = 0 \Rightarrow k = 0 \vee m = 0$,

(b) $k \leq m \Leftrightarrow \exists j \in \mathbb{Q}_{\geq 0} : k + j = m$,

(c) $k \leq m \Leftrightarrow k + n \leq m + n$,

(d) für $n \in \mathbb{Q}_{>0}$ gilt $k \leq m \Leftrightarrow k \cdot n \leq m \cdot n$,

(e) für $n \in \mathbb{Q}_{<0}$ gilt $k \leq m \Leftrightarrow m \cdot n \leq k \cdot n$,

(f) für $n \neq 0$ gilt $k = m \Leftrightarrow k \cdot n = m \cdot n$.

Beweis. Sei $k = \frac{x}{a}, m = \frac{y}{b}$ und $n = \frac{z}{c}$.

(a) Ist $k \cdot m = 0$, so ist $x \cdot y = 0$. Dann gilt nach Satz 2.7 (a) $x = 0$ oder $y = 0$ und somit $k = 0$ oder $m = 0$.

(b) Es gilt nach Satz 2.7 (b)

$$\begin{aligned}k \leq m &\Leftrightarrow x \cdot b \leq y \cdot a \\ &\Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : x \cdot b + \ell = y \cdot a \\ &\Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : (x \cdot b \cdot a + \ell \cdot a) \cdot b = y \cdot (a \cdot a \cdot b) \\ &\Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : \frac{x \cdot b \cdot a + \ell \cdot a}{a \cdot a \cdot b} = \frac{y}{b} \\ &\Leftrightarrow \exists \ell \in \mathbb{Z}_{\geq 0} : \frac{x}{a} + \frac{\ell}{a \cdot b} = \frac{y}{b}\end{aligned}$$

$$\Rightarrow \exists j \in \mathbb{Q}_{\geq 0} : k + j = m.$$

Ist umgekehrt $k + j = m$ für ein $j = \frac{p}{d} \in \mathbb{Q}_{>0}$ so ist $\frac{x \cdot d + p \cdot a}{a \cdot d} = \frac{y}{b}$, also $(x \cdot d + p \cdot a) \cdot b = y \cdot a \cdot d$. Hieraus folgt $x \cdot d \cdot b \leq y \cdot a \cdot d$ nach Satz 2.7 (d) und somit $x \cdot b \leq y \cdot a$, also $k \leq m$, wiederum nach Satz 2.7 (d).

(c) Es gilt nach Satz 2.7 (c)

$$k+n \leq m+n \Leftrightarrow \frac{x \cdot c + z \cdot a}{a \cdot c} \leq \frac{y \cdot c + z \cdot b}{b \cdot c} \Leftrightarrow (x \cdot c + z \cdot a) \cdot b \cdot c \leq (y \cdot c + z \cdot b) \cdot a \cdot c \Leftrightarrow x \cdot b \leq y \cdot a \Leftrightarrow k \leq m.$$

(d) Es gilt nach Satz 2.7 (d)

$$k \cdot n \leq m \cdot n \Leftrightarrow \frac{x \cdot z}{a \cdot c} \leq \frac{y \cdot z}{b \cdot c} \Leftrightarrow x \cdot z \cdot b \cdot c \leq y \cdot z \cdot a \cdot c \Leftrightarrow x \cdot b \leq y \cdot a \Leftrightarrow k \leq m.$$

(e) Es gilt nach Satz 2.7 (e)

$$m \cdot n \leq k \cdot n \Leftrightarrow \frac{y \cdot z}{b \cdot c} \leq \frac{x \cdot z}{a \cdot c} \Leftrightarrow y \cdot z \cdot a \cdot c \leq x \cdot z \cdot b \cdot c \Leftrightarrow x \cdot b \leq y \cdot a \Leftrightarrow k \leq m.$$

(f) Das folgt unmittelbar aus der Antisymmetrie von $\leq$ und (d), falls $n > 0$ oder (e), falls $n < 0$ gilt. □

Bemerkung 3.9. Mit allen diesen Eigenschaften ist $(\mathbb{Q}, +, \cdot, \leq)$ ein geordneter Körper.

4. Die reellen Zahlen

Abschließend wollen wir nun noch die reellen Zahlen aus den rationalen Zahlen konstruieren. Dazu bedienen wir uns des Konzepts der Dedekind-Schnitte.

Definition. Eine Teilmenge $A \subseteq \mathbb{Q}$ heißt *Dedekind-Schnitt,* falls

(a) $A \neq \emptyset$ und $\mathbb{Q} \setminus A \neq \emptyset$,

(b) $\forall p \in A, q \in \mathbb{Q} : q \leq p \Rightarrow q \in A$,

(c) A besitzt kein größtes Element, d.h. $\forall p \in A \exists q \in A : p < q$.

Beispiel 4.1. Ist $x \in \mathbb{Q}$ so ist $A \coloneqq \{p \in \mathbb{Q} \,|\, p < x\}$ ein Dedekind-Schnitt (fur Eigenschaft (c) setze $q \coloneqq \frac{x+p}{2}$). Ebenso ist

$$A \coloneqq \left\{p \in \mathbb{Q} \,|\, p \leq 0 \vee p^2 < 2\right\}$$

ein Dedekind-Schnitt. In der Tat ist $0 \in A$ und $2 \in \mathbb{Q} \setminus A$ und somit gilt Eigenschaft (a). Sei $p \in A$ und $q \leq p$. Ist $q \leq 0$ so gilt $q \in A$. Ist $q > 0$ so gilt $p > 0$ und $p^2 < 2$ und daher

$$q^2 = q \cdot q \leq p \cdot p = p^2 < 2,$$

nach Satz 3.8 (d), also gilt auch $q \in A$ in diesem Fall. Wir zeigen nun noch Eigenschaft (c). Sei $p \in A$. Ist $p \leq 0$ so setzten wir $q \coloneqq 1$. Ist $p > 0$ so setzen wir

$$q \coloneqq \frac{2(p+1)}{p+2}.$$

Dann gilt

$$q - p = \frac{2(p+1) - p(p+2)}{p+2} = \frac{2 - p^2}{p+2} > 0,$$

also $p < q$ und

$$2 - q^2 = \frac{2(p+2)^2 - 4(p+1)^2}{(p+2)^2} = \frac{2(p^2+4p+4) - 4(p^2+2p+1)}{(p+2)^2} = \frac{4 - 2p^2}{(p+2)^2} = \frac{2(2-p^2)}{(p+2)^2} > 0,$$

also $q \in A$.

Definition. Wir nennen die Menge

$$\mathbb{R} \coloneqq \{A\,;\, A \subseteq \mathbb{Q} \text{ Dedekind-Schnitt}\}$$

die Menge der *reellen Zahlen.*

Satz 4.2. *Wir definieren die Relation* $\leq \subseteq \mathbb{R} \times \mathbb{R}$ *durch*

$$A \leq B :\Leftrightarrow A \subseteq B.$$

Dann ist $\leq$ *eine totale Ordnungsrelation. Zudem ist* $\mathbb{R}$ *unbeschränkt, d.h. für alle* $A \in \mathbb{R}$ *existieren* $B, C \in \mathbb{R}$ *mit*

$$B < A < C.$$

Ferner ist für jede beschränkte Menge $\mathcal{A} \subseteq \mathbb{R}$ *die Menge*

$$A_{\sup} \coloneqq \bigcup_{A \in \mathcal{A}} A$$

ein Dedekind-Schnitt und $A_{\sup}$ *ist die kleinste obere Schranke von* $\mathcal{A}$ *(d.h.* $\mathbb{R}$ *ist supremums-vollständig).*

Beweis. Die Eigenschaften einer Ordnungsrelation sind klar. Wir zeigen nun, dass je zwei Elemente $A, B \in \mathbb{R}$ vergleichbar sind. Wir unterscheiden zwei Fälle. Ist $A \setminus B = \emptyset$, so gilt $A \subseteq B$ und daher $A \leq B$. Existiere nun ein $p \in A \setminus B$ und sei $q \in B$. Dann gilt entweder $q > p$ oder $q \leq p$, da $\leq$ eine Totalordnung auf $\mathbb{Q}$ ist. Wäre $p < q$ so folgt nach Eigenschaft (b), dass $p \in B$ gilt, was der Wahl von p widerspricht. Somit gilt also $q \leq p$ und daher wieder nach (b) $q \in A$. Da $q \in B$ beliebig war, folgt $B \subseteq A$ also $B \leq A$.
Sei nun $A \in \mathbb{R}$. Für $b \in A$ und $c \in \mathbb{Q} \setminus A$ setzen wir

$$B \coloneqq \{p \in \mathbb{Q}\,;\, p < b\}$$
$$C \coloneqq \{p \in \mathbb{Q}\,;\, p < c + 1\}.$$

Dann sind $B, C \in \mathbb{R}$ und es gilt $B \subseteq A \subseteq C$ nach Eigenschaft (b) für den Dedekind-Schnitt A (für $A \subseteq C$ nehmen wir an, dass es $x \in A$ mit $x \notin C$ gibt. Dann folgt $c + 1 \leq x$ und somit $c \in A$ wegen (b)). Offenbar gilt $B \neq A$, da $b \in A$ aber $b \notin B$. Außerdem gilt $C \neq A$, da $c \in C$ aber $c \notin A$ gilt.
Sei abschließend $\mathcal{A} \subseteq \mathbb{R}$ nach oben beschränkt, d.h. es existiert $B \in \mathbb{R}$ mit

$$\forall A \in \mathcal{A} : A \leq B.$$

Wir setzen

$$A_{\sup} \coloneqq \bigcup_{A \in \mathcal{A}} A$$

und beweisen zunächst, dass $A_{\sup} \in \mathbb{R}$:
Eigenschaft (a): Es ist $A_{\sup} \neq \emptyset$, da $A \neq \emptyset$ für $A \in \mathcal{A}$. Ebenso gilt $\mathbb{Q} \setminus A_{\sup} = \bigcap_{A \in \mathcal{A}} \mathbb{Q} \setminus A \supseteq \mathbb{Q} \setminus B \neq \emptyset$.
Eigenschaft (b): Ist $p \in A_{\sup}$ und $q \in \mathbb{Q}$ mit $q \leq p$, so existiert ein $A \in \mathcal{A}$ mit $p \in A$ und daher auch $q \in A \subseteq A_{\sup}$.
Eigenschaft (c): Ist $p \in A_{\sup}$ so gibt es $A \in \mathcal{A}$ mit $p \in A$ und daher ein $q \in A \subseteq A_{\sup}$ mit $p < q$.
Da offenbar $A \subseteq A_{\sup}$ für jedes $A \in \mathcal{A}$ gilt, ist $A_{\sup}$ eine obere Schranke von $\mathcal{A}$. Ist C eine weitere obere Schranke, so gilt für alle $A \in \mathcal{A}$

$$A \subseteq C$$

und somit

$$A_{\sup} = \bigcup_{A \in \mathcal{A}} A \subseteq C$$

und daher ist $A_{\sup}$ die kleinste obere Schranke, also das Supremum von $\mathcal{A}$. □

Definition. Wir definieren die Einbettung $\iota : \mathbb{Q} \to \mathbb{R}$ durch

$$\iota(p) \coloneqq \{x \in \mathbb{Q}\,;\, x < p\}\,.$$

Satz 4.3. *Für $p, q \in \mathbb{Q}$ gilt $\iota(p) < \iota(q)$ genau dann, wenn $p < q$. Insbesondere ist ι injektiv. Außerdem ist $\mathbb{Q}$ ordnungsdicht in $\mathbb{R}$, d.h. für zwei Elemente $A, B \in \mathbb{R}$ mit $A < B$ existiert ein $p \in \mathbb{Q}$ mit*

$$A < \iota(p) < B.$$

Beweis. Seien $p, q \in \mathbb{Q}$. Gilt $p < q$ so folgt unmittelbar $\iota(p) \subsetneq \iota(q)$, da $p \in \iota(q) \setminus \iota(p)$. Gelte nun umgekehrt $\iota(p) < \iota(q)$. Nach Voraussetzung gibt es $r \in \iota(q) \setminus \iota(p)$, also $p \leq r < q$, was $p < q$ impliziert. Gilt $\iota(p) = \iota(q)$ folgt $p = q$ da sonst $p < q$ oder $q < p$ und daher $\iota(p) < \iota(q)$ oder $\iota(q) < \iota(p)$ folgen würde.
Seien nun $A, B \in \mathbb{R}$ mit $A < B$. Dann exitsiert ein $q \in B \setminus A$. Daher existiert ein $p \in B$ mit $q < p$ (Eigenschaft (c)). Nun gilt für $x \in \iota(p)$ dass $x < p$ und somit $x \in B$ folgt (Eigenschaft (b)), also $\iota(p) \leq B$. Außerdem ist $p \in B \setminus \iota(p)$, also gilt $\iota(p) < B$. Ebenso gilt für $x \in A$, dass $x < p$ ist (sonst wäre $p \leq x$, also $p \in A$ und damit $q \in A$, da $q < p$), also gilt $A \subseteq \iota(p)$. Da $q \in \iota(p) \setminus A$ folgt $A < \iota(p)$ und damit die Behauptung. □

Theorem 4.4. *Es existieren zwei eindeutig bestimmte Operationen $+, \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ so, dass $(\mathbb{R}, +, \cdot, \leq)$ ein geordneter Körper ist und*

$$\iota : \mathbb{Q} \to \mathbb{R}$$

ein Körper-Homomorphismus ist, der die Ordnung bewahrt.

Als letzte Operation führen wir nun noch das Potenzieren ein.

Definition. Sei $x \in \mathbb{R}$. Wir definieren die Funktion $x^{(\cdot)} : \mathbb{N} \to \mathbb{R}$ rekursiv durch

(a) $x^{(0)} \coloneqq 1$,

(b) $\forall n \in \mathbb{N} :\ x^{(n+1)} \coloneqq x^{(n)} \cdot x$.

Ferner definieren wir für $x \neq 0$ und $n \in \mathbb{N}$

$$x^{(-n)} \coloneqq \left(x^{-1}\right)^{(n)}.$$

Statt $x^{(k)}$ schreiben wir wie üblich x^k.

Satz 4.5. *Seien $x, y \in \mathbb{R}$ mit $x, y \neq 0$. Dann gelten:*

(a) $\forall k \in \mathbb{Z} :\ x^k \neq 0$.

(b) $\forall k \in \mathbb{Z} :\ x > 0 \Rightarrow x^k > 0$.

(c) $\forall k \in \mathbb{Z} :\ (x \cdot y)^k = x^k \cdot y^k$.

(d) $\forall k, \ell \in \mathbb{Z} :\ x^k \cdot x^\ell = x^{k+\ell}$.

(e) $\forall k, \ell \in \mathbb{Z}: \left(x^k\right)^\ell = x^{k\cdot\ell}$.

(f) $\forall k \in \mathbb{Z}: x \in \mathbb{Q} \Rightarrow x^k \in \mathbb{Q}$.

(g) $\forall k \in \mathbb{N}: x \in \mathbb{Z} \Rightarrow x^k \in \mathbb{Z}$.

(h) $\forall k \in \mathbb{N}: x \in \mathbb{N} \Rightarrow x^k \in \mathbb{N}$.

Beweis. (a) Es gilt $x^0 = 1 \neq 0$ und aus $x^n \neq 0$ für $n \in \mathbb{N}$ folgt $x^{n+1} = x^n \cdot x \neq 0$. Damit folgt mit Induktion $x^n \neq 0$ für alle $n \in \mathbb{N}$. Hieruas folgt ebenso $x^{-n} = \left(x^{-1}\right)^n \neq 0$, da $x^{-1} \neq 0$.

(b) Es gilt $x^0 = 1 > 0$ und aus $x^n > 0$ für $n \in \mathbb{N}$ folgt $x^{n+1} = x^n \cdot x > 0$. Damit folgt mit Induktion $x^n > 0$ für alle $n \in \mathbb{N}$. Hieruas folgt ebenso $x^{-n} = \left(x^{-1}\right)^n > 0$, da $x^{-1} > 0$.

(c) Es gilt $(x \cdot y)^0 = 1 = x^0 \cdot y^0$ und aus $(x \cdot y)^n = x^n \cdot y^n$ für $n \in \mathbb{N}$ folgt $(x \cdot y)^{n+1} = (x^n \cdot y^n) \cdot (x \cdot y) = x^{n+1} \cdot y^{n+1}$ also folgt die Behauptung für alle $n \in \mathbb{N}$. Wegen $(x \cdot y)^{-n} = \left((x \cdot y)^{-1}\right)^n = \left(x^{-1} \cdot y^{-1}\right)^n = \left(x^{-1}\right)^n \cdot \left(y^{-1}\right)^n = x^{-n} \cdot y^{-n}$ folgt die Behauptung für alle Exponenten.

(d) Sei $k \in \mathbb{Z}$. Es gilt $x^k \cdot x^0 = x^k = x^{k+0}$ und aus $x^k \cdot x^n = x^{k+n}$ für $n \in \mathbb{N}$ folgt $x^k \cdot x^{n+1} = x^k \cdot x^n \cdot x = x^{k+n} \cdot x = x^{k+n+1}$ also folgt die Behauptung für alle $n \in \mathbb{N}$. Außerdem gilt für $n \geq k$:

$$x^k \cdot x^{-n} = x^k \cdot \left(x^{-1}\right)^n = x^k \cdot \left(x^{-1}\right)^{k+n-k} = x^k \cdot \left(x^{-1}\right)^k \cdot \left(x^{-1}\right)^{n-k} = 1^k \cdot x^{k-n} = x^{k-n}$$

und für $n < k$

$$x^k \cdot x^{-n} = x^{k-n+n} \cdot x^{-n} = x^{k-n} \cdot x^n \cdot x^{-n} = x^{k-n}.$$

(e) Sei $k \in \mathbb{Z}$. Es gilt $\left(x^k\right)^0 = 1 = x^{k\cdot 0}$ und aus $\left(x^k\right)^n = x^{k\cdot n}$ für $n \in \mathbb{N}$ folgt $\left(x^k\right)^{n+1} = \left(x^k\right)^n \cdot x^k = x^{k\cdot n} \cdot x^k = x^{k\cdot(n+1)}$ also folgt die Behauptung für alle $n \in \mathbb{N}$. Da

$$x^k \cdot x^{-k} = x^k \cdot \left(x^{-1}\right)^k = 1^k = 1,$$

folgt

$$x^{-k} = \left(x^k\right)^{-1}$$

und damit

$$\left(x^k\right)^{-n} = \left(x^{-k}\right)^n = x^{-k\cdot n} = x^{k\cdot(-n)}.$$

(f) Sei $x \in \mathbb{Q}$ mit $x \neq 0$. Dann gilt $x^0 = 1 \in \mathbb{Q}$ und aus $x^n \in \mathbb{Q}$ für $n \in \mathbb{N}$ folgt $x^{n+1} = x^n \cdot x \in \mathbb{Q}$ und damit $x^n \in \mathbb{Q}$ für alle $n \in \mathbb{N}$. Da $x^{-1} \in \mathbb{Q}$ folgt $x^{-n} = \left(x^{-1}\right)^n \in \mathbb{Q}$ für alle $n \in \mathbb{N}$.

(g) Sei $x \in \mathbb{Z}$ mit $x \neq 0$. Dann gilt $x^0 = 1 \in \mathbb{Z}$ und aus $x^n \in \mathbb{Z}$ für $n \in \mathbb{N}$ folgt $x^{n+1} = x^n \cdot x \in \mathbb{Z}$ und damit $x^n \in \mathbb{Z}$ für alle $n \in \mathbb{N}$.

(h) Sei $x \in \mathbb{N}$ mit $x \neq 0$. Dann gilt $x^0 = 1 \in \mathbb{N}$ und aus $x^n \in \mathbb{N}$ für $n \in \mathbb{N}$ folgt $x^{n+1} = x^n \cdot x \in \mathbb{N}$ und damit $x^n \in \mathbb{N}$ für alle $n \in \mathbb{N}$.

□

5. Stellenwertsysteme

In diesem Abschnitt wollen wir uns mit Stellenwertsystemen und Darstellungen reeller Zahlen beschäftigen. Bekannt sind zum Beispiel das Dezimalsystem, das Binärsystem oder das Hexadezimalsystem. All diese Darstellungssysteme beruhen auf der Wahl einer natürlichen Zahl als Basis. Wir werden diese Basis $b \in \mathbb{N}_{>1}$ beliebig wählen und von so genannten b-adischen Darstellungen sprechen. Zunächst benötigen wir einige Vorbereitungen. Der Einfachheit halber werden wir uns nur auf nichtnegative Zahlen beschränken (für negative Zahlen setzt man einfach ein $-$ mit dazu).

Satz 5.1 (Division mit Rest)**.** *Seien $p, q \in \mathbb{R}_{\geq 0}$ mit $q \neq 0$. Dann existieren $m \in \mathbb{N}$ und $r \in \mathbb{R}_{\geq 0}$ mit $r < q$, so dass*

$$p = m \cdot q + r.$$

Beweis. Nach der Ordnungsdichtheit von $\mathbb{Q}$ und Lemma 3.7 existiert eine Zahl $n \in \mathbb{N}$ mit

$$p \cdot q^{-1} < n$$

also $p < n \cdot q$. Mit anderen Worten: Die Menge $M \coloneqq \{n \in \mathbb{N}\,;\, p < n \cdot q\}$ ist nichtleer und besitzt nach Satz 1.7 ein kleinstes Element $m' \in \mathbb{N}$. Offenbar ist $m' \neq 0$, da sonst $p < 0 \cdot q = 0$, was $p \geq 0$ widerspricht. Somit ist also $m' = m + 1$ für ein $m \in \mathbb{N}$ und da $m < m'$, folgt $m \notin M$, da m' minimal war. Es ist also

$$m \cdot q \leq p < (m+1) \cdot q.$$

Wir setzen

$$r = p - m \cdot q \geq 0.$$

Damit gilt

$$m \cdot q + r = p < (m+1) \cdot q = m \cdot q + q$$

und somit $r < q$. □

Satz 5.2. *Sei $q \in \mathbb{R}_{>0}$. Seien ferner $m, \widetilde{m} \in \mathbb{N}$ und $r, \widetilde{r} \in \mathbb{R}_{\geq 0}$ mit $r, \widetilde{r} < q$ und*

$$m \cdot q + r = \widetilde{m} \cdot q + \widetilde{r}.$$

Dann gilt $m = \widetilde{m}$ und $r = \widetilde{r}$.

Beweis. Da $\leq$ eine Totalordnung auf $\mathbb{R}$ bildet gilt entweder $r \leq \widetilde{r}$ oder $\widetilde{r} \leq r$. Gelte o.E. $r \leq \widetilde{r}$. Dann ist $\widetilde{r} - r \geq 0$ und somit

$$0 \leq \widetilde{r} - r = m \cdot q - \widetilde{m} \cdot q = (m - \widetilde{m}) \cdot q. \tag{5.1}$$

Andererseits ist $\widetilde{r} - r < q$ und somit gilt

$$0 \leq m - \widetilde{m} < 1.$$

Da $m - \widetilde{m} \in \mathbb{N}$, folgt $m = \widetilde{m}$. Hieraus folgt mit (5.1) $r = \widetilde{r}$. □

Die letzten beide Sätze besagen also, dass man für $p, q \in \mathbb{R}_{\geq 0}$ mit $q \neq 0$ eindeutig bestimmte Zahlen $m \in \mathbb{N}, r \in \mathbb{R}_{\geq 0}$ mit $r < q$ findet, so dass

$$p = m \cdot q + r$$

gilt. Wir wollen diese Zahlen nun benennen.

Definition. Seien $p, q \in \mathbb{R}_{\geq 0}$ mit $q \neq 0$. Seien ferner $m \in \mathbb{N}$ und $r \in \mathbb{R}_{\geq 0}$ mit $r < q$ so dass $p = m \cdot q + r$. Dann definieren wir

$$p \operatorname{div} q \coloneqq m,$$
$$p \bmod q \coloneqq r.$$

Wir beginnen nun die b-adische Darstellung für eine Zahl $m \in \mathbb{N}$ zu definieren.

Satz 5.3. *Sei $m \in \mathbb{N}$. Wir definieren rekursiv die Funktion $r : \mathbb{N} \to \mathbb{N}$ durch*

(a) $r_0 \coloneqq m$,

(b) $\forall n \in \mathbb{N} : \; r_{n+1} \coloneqq r_n \operatorname{div} b$.

Wir definieren ferner $a_n \coloneqq r_n \bmod b$ für $n \in \mathbb{N}$. Dann existiert ein $n_0 \in \mathbb{N}$ mit $r_n = a_n = 0$ für alle $n \geq n_0$ und für so ein n_0 gilt

$$m = \sum_{k=0}^{n_0 - 1} a_k b^k.$$

Beweis. Die Menge $\{r_n \, ; \, n \in \mathbb{N}\}$ besitzt nach Satz 1.7 ein kleinstes Element r_{n_0}. Dann gilt

$$r_{n_0} = r_{n_0+1} \cdot b + a_{n_0} \geq r_{n_0+1} \cdot b.$$

Ist $r_{n_0+1} \neq 0$, so folgt

$$r_{n_0} > r_{n_0+1}$$

im Widerspruch zur Minimalität von r_{n_0}. Also ist $r_{n_0+1} = 0$ und aufgrund der Minimalität $r_{n_0} \leq r_{n_0+1} = 0$ auch $r_{n_0} = 0$. Damit gilt aber ebenso $a_{n_0+1} = 0$. Ist nun $r_{n_0+k} = 0$ für ein $k \in \mathbb{N}_{\geq 1}$, so folgt $r_{n_0+k+1} = 0 \operatorname{div} b = 0$ und daher ist $r_n = 0$ für alle $n \geq n_0$. Damit gilt auch $a_n = r_n \bmod b = 0$ für alle $n \geq n_0$.
Wir erhalten somit

$$\begin{aligned}
m &= r_1 \cdot b + a_0 \\
&= (r_2 \cdot b + a_1) \cdot b + a_0 = r_2 \cdot b^2 + \sum_{k=0}^{1} a_k b^k \\
&\vdots \\
&= r_{n_0} \cdot b^{n_0} + \sum_{k=0}^{n_0 - 1} a_k \cdot b^k \\
&= \sum_{k=0}^{n_0 - 1} a_k \cdot b^k
\end{aligned}$$

□

Definition. Ist $m \in \mathbb{N}$, $b \in \mathbb{N}_{>1}$ und $a_0, \ldots, a_{n_0-1} \in \mathbb{N}_{<b}$ gemäß Satz 5.3, so schreiben wir

$$m = (a_{n_0-1} \cdots a_0)_b$$

und nennen dies die *b-adische Darstellung von m* oder *Darstellung von m zur Basis b.*

Beispiel 5.4. (a) Wählen wir $b = (\sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma)\,(0)$, so sprechen wir von der Dezimaldarstellung. Da diese nur aus Elementen kleiner als b besteht, genügt es endliche viele Symbole für die Elemente kleiner als b zu wählen. Wir wählen natürlich die gewöhnlichen Ziffern $0, 1, 2, \ldots, 9$ und erhalten somit die gewünschte Darstellung. So folgt etwa für $m = b$

$$r_1 = m \operatorname{div} b = 1,\ a_0 = 0$$
$$r_2 = r_1 \operatorname{div} b = 0,\ a_1 = 1$$

und damit $b = (10)_b$. Die Darstellung zu dieser Basis nennen wir *Dezimaldarstellung* und wir vereinbaren, dass alle natürlichen Zahlen (wenn nicht anders angegeben) bzgl dieser Basis dargestellt sind.

(b) $m = 72$, $b = 2$. Dann gilt

$$\begin{aligned} r_1 &= 72 \operatorname{div} 2 = 36,\ a_0 = 0, \\ r_2 &= 36 \operatorname{div} 2 = 18,\ a_1 = 0, \\ r_3 &= 18 \operatorname{div} 2 = 9,\ a_2 = 0, \\ r_4 &= 9 \operatorname{div} 2 = 4,\ a_3 = 1, \\ r_5 &= 4 \operatorname{div} 2 = 2,\ a_4 = 0, \\ r_6 &= 2 \operatorname{div} 2 = 1,\ a_5 = 0, \\ r_7 &= 1 \operatorname{div} 2 = 0,\ a_6 = 1 \end{aligned}$$

und damit

$$72 = (1001000)_2.$$

(c) $m = 211, b = 16$. Als Symbole wählen wir neben $0, \ldots, 9$ noch $A, \ldots, F$. Dann gilt

$$r_1 = 211 \operatorname{div} 16 = 13,\ a_0 = 3,$$
$$r_2 = 13 \operatorname{div} 16 = 0,\ a_1 = 13$$

und damit

$$211 = (D3)_{16}.$$

Als nächstes definieren wir die b-adische Darstellung für $x \in \mathbb{R}_{<1}$.

Satz 5.5. *Sei $x \in]0, 1[$. Wir definieren rekursiv die Funktionen $r_- : \mathbb{N} \to \mathbb{R}$ durch*

(a) $r_0 \coloneqq x$,

(b) $\forall n \in \mathbb{N}_{>0} : r_{-(n+1)} \coloneqq r_{-n} \cdot b \bmod 1$.

und setzen $a_{-(n+1)} \coloneqq r_{-n} \cdot b \operatorname{div} 1$ *für* $n \in \mathbb{N}$. *Dann gilt* $a_{-k} \in \mathbb{N}_{<b}$ *für* $k \in \mathbb{N}_{\geq 1}$ *und*

$$x = \sum_{k=1}^{\infty} a_{-k} b^{-k}.$$

Beweis. Es gilt

$$b > r_{-n} \cdot b = a_{-(n+1)} + r_{-(n+1)} \geq a_{-(n+1)}$$

für alle $n \in \mathbb{N}$. Nun beweisen wir

$$\forall n \in \mathbb{N}_{\geq 1} : \; x - \sum_{k=1}^{n} a_{-k} \cdot b^{-k} = r_{-n} \cdot b^{-n}.$$

Für $n = 1$ gilt

$$x - a_{-1} b^{-1} = b^{-1}(x \cdot b - a_{-1}) = r_{-1} \cdot b^{-1}.$$

Gilt die Formel für ein $n \in \mathbb{N}$, so folgt

$$\begin{aligned} x - \sum_{k=1}^{n+1} a_{-k} \cdot b^{-k} &= x - \sum_{k=1}^{n} a_{-k} \cdot b^{-k} - a_{-(n+1)} \cdot b^{-(n+1)} \\ &= r_{-n} \cdot b^{-n} - a_{-(n+1)} \cdot b^{-(n+1)} \\ &= b^{-(n+1)}(r_{-n} \cdot b - a_{-(n+1)}) \\ &= b^{-(n+1)} \cdot r_{-(n+1)} \end{aligned}$$

und damit gilt die Formel für alle $n \in \mathbb{N}$. Da $r_{-n} < 1$ für alle $n \in \mathbb{N}$ und $b^{-1} < 1$ gilt, folgt nach einem Satz aus der Analysis

$$x - \sum_{k=1}^{n} a_{-k} \cdot b^{-k} = r_{-n} \cdot b^{-n} \to 0 \quad (n \to \infty)$$

und somit die Behauptung. □

Definition. Sei $y \in \mathbb{R}_{\geq 0}$. Wir setzen $m \coloneqq y \operatorname{div} 1 \in \mathbb{N}$ und $x \coloneqq y \bmod 1 \in]0, 1[$. Seien $a_0, \ldots, a_{n_0 - 1}$ und $a_{-1}, a_{-2}, \ldots$ gemäß Satz 5.3 und Satz 5.5 gewählt. Wir schreiben

$$y = (a_{n_0 - 1} \cdots a_0, a_{-1} a_{-2} \cdots)_b$$

und nennen dies *die b-adische Darstellung von y.*

Beispiel 5.6. (a) $b = 10$ und $y = \frac{1}{3}$. Dann gilt $m = \frac{1}{3} \operatorname{div} 1 = 0$ und $x = \frac{1}{3} \bmod 1 = \frac{1}{3}$. Es gilt

$$\begin{aligned} r_{-1} &= \frac{1}{3} \cdot 10 \bmod 1 = \frac{1}{3}, \; a_{-1} = \frac{1}{3} \cdot 10 \operatorname{div} 1 = 3, \\ r_{-2} &= \frac{1}{3} \cdot 10 \bmod 1 = \frac{1}{3}, \; a_{-2} = \frac{1}{3} \cdot 10 \operatorname{div} 1 = 3, \\ &\vdots \end{aligned}$$

und daher

$$\frac{1}{3} = (0, 33333 \ldots)_{10}.$$

(b) $b = 5$ und $y = \frac{1}{3}$. Es gilt wie oben $m = 0$ und $x = \frac{1}{3}$ sowie

$$\begin{aligned} r_{-1} &= \frac{1}{3} \cdot 5 \bmod 1 = \frac{2}{3},\ a_{-1} = \frac{1}{3} \cdot 5 \operatorname{div} 1 = 1, \\ r_{-2} &= \frac{2}{3} \cdot 5 \bmod 1 = \frac{1}{3},\ a_{-2} = \frac{2}{3} \cdot 5 \operatorname{div} 1 = 3, \\ &\vdots \end{aligned}$$

und daher

$$\frac{1}{3} = (0,1313\ldots)_5.$$

(c) $b = 10$ und $y = \sqrt{2}$. Es gilt für $m = y \operatorname{div} 1 \in \mathbb{N}$ und $x = y \bmod 1 \in \mathbb{R}_{<1}$ die Gleichung $\sqrt{2} = m + x$ und somit

$$2 = (m + x)^2.$$

Wäre $m = 0$, so wäre $x > 1$, wäre $m \geq 2$, so wäre $2 < (m + x)^2$. Somit muss $m = 1$ gelten und $x = \sqrt{2} - 1$. Nun gilt

$$r_{-1} = \left(\sqrt{2} - 1\right) \cdot 10 \bmod 1,\ a_{-1} = (\sqrt{2} - 1) \cdot 10 \operatorname{div} 1$$

also

$$\begin{aligned} &\left(\sqrt{2} - 1\right) \cdot 10 = a_{-1} + r_{-1} \\ \Leftrightarrow &\sqrt{2} \cdot 10 = a_{-1} + r_{-1} + 10 \\ \Leftrightarrow &2 \cdot 10^2 = (a_{-1} + r_{-1} + 10)^2 \\ \Leftrightarrow &2 \cdot 10^2 = (a_{-1} + r_{-1})^2 + 20 \cdot (a_{-1} + r_{-1}) + 10^2 \\ \Leftrightarrow &10^2 = (a_{-1} + r_{-1})((a_{-1} + r_{-1}) + 20). \end{aligned}$$

Man sucht nun $a_{-1} \in \mathbb{N}, r_{-1} < 1$, so dass diese Gleichung gilt. Da $r_{-1} < 1$ suchen wir also das größte $a_{-1} \in \mathbb{N}$ mit

$$10^2 \geq a_{-1} \cdot (a_{-1} + 20).$$

Durch probieren erhalten wir $a_{-1} = 4$ und damit

$$10^2 = (4 + r_{-1}) \cdot (r_{-1} + 24) = r_{-1}^2 + 28r_{-1} + 96 \Rightarrow r_{-1}^2 + 28r_{-1} = 4.$$

Nun ist

$$r_{-2} = r_{-1} \cdot 10 \bmod 1,\ a_{-2} = r_{-1} \cdot 10 \operatorname{div} 1,$$

also $r_{-1} \cdot 10 = r_{-2} + a_{-2}$. Mulitplizieren wir die obige Gleichung mit 10^2 so erhalten wir

$$\begin{aligned} 400 &= (10r_{-1})^2 + 280 \cdot 10 \cdot r_{-1} \\ &= (r_{-2} + a_{-2})^2 + 280 \cdot (r_{-2} + a_{-2}) \\ &= (r_{-2} + a_{-2})\,(r_{-2} + a_{-2} + 280)\,. \end{aligned}$$

Offensichtlich ist $a_{-2} = 1$ und wir erhalten

$$119 = r_{-2}^2 + 281 r_{-2}.$$

Mit $r_{-2} \cdot 10 = r_{-3} + a_{-3}$ folgt nach Multiplikation mit 10^2

$$11900 = (r_{-3} + a_{-3})(r_{-3} + a_{-3} + 2810).$$

Durch probieren erhalten wir $a_{-3} = 4$, denn

$$4 \cdot 2814 = 11256 < 11900$$

usw. Wir erhalten also

$$\sqrt{2} = (1, 414 \dots)_{10},$$

wobei wir sehen werden, dass diese Dartstellung niemals periodisch wird.

Satz 5.7. *Sei $y \in \mathbb{R}_{\geq 0}$, $b \in \mathbb{N}_{>1}$ und $y = (a_{n_0-1} \cdots a_0, a_{-1} \cdots)_b$ die b-adische Darstellung von y. Dann gilt $y \in \mathbb{Q}$ genau dann, wenn es $k_0, \tau \in \mathbb{N}_{>0}$ gibt so, dass*

$$a_{-(k+\tau)} = a_{-k} \quad (k \geq k_0).$$

In diesem Fall können für $y = \frac{m}{c}$ die Zahlen $k_0, \tau \leq c$ gewählt werden.

Beweis. Offenbar reicht es, die Behauptung für $y \in \mathbb{R}_{<1}$ zu zeigen. Wir nehmen zunächst an, dass y rational ist, also $y = \frac{m}{c}$ für gewisse $m, c \in \mathbb{N}$ mit $c > 0$ und $m < c$, da $y < 1$. Wir betrachten nun die Folge $(r_{-n})_{n \in \mathbb{N}}$ aus Satz 5.5. Da $a_{-(n+1)} = r_{-n} \cdot b \operatorname{div} 1$ gilt, reicht es die Behauptung für r_{-n} statt für a_{-n} zu zeigen. Wir betrachten dazu die Folge $\widetilde{r}_{-n} \coloneqq r_{-n} \cdot c < c$ und zeigen $\widetilde{r}_{-n} \in \mathbb{N}$ für alle $n \in \mathbb{N}$. Für $n = 0$ gilt

$$\widetilde{r}_0 = r_0 \cdot c = y \cdot c = m \in \mathbb{N}.$$

Gelte nun $\widetilde{r}_{-n} \in \mathbb{N}$. Dann gilt wegen $r_{-n} \cdot b = a_{-n} + r_{-(n+1)}$ auch

$$\widetilde{r}_{-n} \cdot b = a_{-(n+1)} \cdot c + \widetilde{r}_{-(n+1)}$$

und damit

$$\widetilde{r}_{-(n+1)=} = \widetilde{r}_{-n} \cdot b - a_{-(n+1)} \cdot c \in \mathbb{N}.$$

Somit gilt also

$$\widetilde{r}_{-} : \mathbb{N} \to \mathbb{N}_{<c}.$$

Nach Schubfachprinzip Satz 1.8 existieren also $1 \leq k_0 \leq c$ und $k_1 \leq c+1$ mit $k_0 < k_1$ und $\widetilde{r}_{-k_0} = \widetilde{r}_{-k_1}$. Mit $\tau \coloneqq k_1 - k_0$ gilt also

$$\widetilde{r}_{-k_0} = \widetilde{r}_{-(k_0+\tau)}$$

und somit auch

$$r_{-k_0} = \frac{\widetilde{r}_{-k_0}}{c} = \frac{\widetilde{r}_{-(k_0+\tau)}}{c} = r_{-(k_0+\tau).}$$

Wir zeigen nun per Induktion

$$\forall k \in \mathbb{N}_{\geq k_0} : \; r_{-k} = r_{-(k+\tau)}.$$

Für $k = k_0$ haben wir das eben gezeigt. Gelte nun $r_{-k} = r_{-(k+\tau)}$ für ein $k \geq k_0$. Dann folgt $a_{-(k+1)} = a_{-(k+1+\tau)}$ und daher

$$r_{-(k+1)} = r_{-k} \cdot b - a_{-(k+1)} = r_{-(k+\tau)} \cdot b - a_{-(k+1+\tau)} = r_{-(k+1+\tau)},$$

was die Behauptung zeigt.
Gelte nun

$$a_{-k} = a_{-(k+\tau)} \quad (k \geq k_0).$$

Nach Satz 5.5 gilt

$$\begin{aligned} y &= \sum_{k=1}^{\infty} a_{-k} b^{-k} \\ &= \sum_{k=1}^{k_0-1} a_{-k} b^{-k} + \sum_{k=k_0}^{\infty} a_{-k} b^{-k} \\ &= \sum_{k=1}^{k_0-1} a_{-k} b^{-k} + a_{-k_0} \sum_{n=0}^{\infty} b^{-(k_0+n\cdot\tau)} + \ldots + a_{-(k_0+\tau-1)} \sum_{n=0}^{\infty} b^{-(k_0+\tau-1+n\cdot\tau)}. \end{aligned}$$

Es genügt also zu zeigen

$$\sum_{n=0}^{\infty} b^{-(s+n\cdot\tau)} \in \mathbb{Q} \quad (k_0 \leq s \leq k_0 + \tau - 1).$$

Dazu verwenden wir die Formel für die geometrische Reihe aus der Analysis. Es gilt

$$\sum_{n=0}^{\infty} b^{-(s+n\cdot\tau)} = b^{-s} \sum_{n=0}^{\infty} \frac{1}{(b^\tau)^n} = b^{-s} \frac{1}{1 - \frac{1}{b^\tau}} \in \mathbb{Q}$$

und hieraus folgt die Behauptung. □

Teil II.

Teilbarkeit

6. Teilbarkeit in Integritätsbereichen

Definition. Sei R eine Menge und $\oplus : R \times R \to R$, $\circ : R \times R \to R$ zwei Operationen. Dann heißt $(R, \oplus, \circ)$ *Ring*, falls

(a) $(R, \oplus)$ ist eine *abelsche Gruppe,* d.h.

(i) $\oplus$ ist assoziativ,

(ii) $\exists 0 \in R \forall x \in R : \ 0 \oplus x = x \oplus 0 = x$,

(iii) $\forall x \in R \exists -x \in R : \ x \oplus (-x) = (-x) \oplus x = 0$,

(iv) $\oplus$ ist kommutativ.

(b) $\circ$ ist assoziativ,

(c) $\oplus$ und $\circ$ sind distributiv, d.h.

$$\forall x, y, z \in R : \ (x \oplus y) \circ z = (x \circ z) \oplus (y \circ z),$$
$$\forall x, y, z \in R : \ x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z).$$

Ein Ring $(R, \oplus, \circ)$ heißt *Ring mit Eins* (oder *unitärer Ring*), falls

$$\exists 1 \in R \forall x \in R : \ 1 \circ x = x \circ 1 = x.$$

Ein Ring $(R, \oplus, \circ)$ heißt *kommutativer Ring,* falls $\circ$ kommutativ ist.
Ein kommutativer Ring mit Eins $(R, \oplus, \circ)$ heißt *Integritätsbereich,* falls $1 \neq 0$ und R *nullteilerfrei* ist, d.h.

$$\forall x, y \in R : \ x \circ y = 0 \Rightarrow x = 0 \vee y = 0.$$

Bemerkung 6.1. Die Inversen $-x$ und die Elemente 1 und 0 sind eindeutig bestimmt.

Beispiel 6.2. (a) Jeder Körper ist ein Integritätsbereich, insbesondere also $\mathbb{Q}$ und $\mathbb{R}$. Außerdem ist $\mathbb{Z}$ ein Integritätsbereich, $\mathbb{N}$ hingegen nicht.

(b) Sei $\mathbb{K}$ ein Körper. Wir definieren

$$\mathbb{K}[X] \coloneqq \left\{ (a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}_{>n_0} : a_n = 0 \right\}$$

versehen mit den Operationen

$$(a_n)_{n \in \mathbb{N}} \oplus (b_n)_{n \in \mathbb{N}} \coloneqq (a_n + b_n)_{n \in \mathbb{N}},$$

$$(a_n)_{n\in\mathbb{N}} \circ (b_n)_{n\in\mathbb{N}} := \left(\sum_{j=0}^{n} a_j \cdot b_{n-j}\right)_{n\in\mathbb{N}}.$$

Dann ist $\mathbb{K}[X]$ ein Integritätsbereich, der sog. *Polynomring über* $\mathbb{K}$. Für ein Element $(a_n)_n \in \mathbb{K}[X]$ schreiben wir auch

$$a_0 + a_1 X + a_2 X^2 + \ldots + a_{n_0} X^{n_0},$$

wobei $a_{n_0} \neq 0$ und $a_n = 0$ für $n > n_0$.

Sei im Weiteren $(R, \oplus, \circ)$ stets ein Integritätsbereich.

Definition. Seien $a, b \in R \setminus \{0\}$.

(a) Man sagt *a teilt b* (oder *a ist ein Teiler von b*), falls es ein Element $k \in R$ gibt mit $a \circ k = b$. Notation: $a \mid b$.

(b) Ein Element $a \in R \setminus \{0\}$ heißt *Einheit,* falls $a \mid 1$. Die Menge aller Einheiten in R bezeichnen wir mit R^*.

(c) a und b heißen *assoziiert,* wenn $a \mid b$ und $b \mid a$ gilt. Notation $a \sim b$.

(d) Ein Element $a \in R \setminus \{0\}$ heißt *irreduzibel,* falls $a \notin R^*$ und

$$\forall b \in R : b \mid a \Rightarrow (b \in R^* \vee a \mid b)\,.$$

(e) Ein Element $p \in R \setminus \{0\}$ heißt *prim*, falls $p \notin R^*$ und

$$\forall a, b \in R :\ p \mid a \circ b \Rightarrow (p \mid a \ \vee\ p \mid b).$$

(f) Ein Element $c \in R \setminus \{0\}$ heißt *größter gemeinsamer Teiler von a und b,* falls $c \mid a$ und $c \mid b$ und

$$\forall d \in R : d \mid a \wedge d \mid b \Rightarrow d \mid c.$$

(g) Ein Element $c \in R \setminus \{0\}$ heißt *kleinstes gemeinsames Vielfaches von a und b,* falls $a \mid c$ und $b \mid c$ und

$$\forall d \in R : a \mid d \wedge b \mid d \Rightarrow c \mid d.$$

Bemerkung 6.3. (a) Die Einheiten in R sind genau die bzgl $\circ$ invertierbaren Elemente.

(b) Ist $p \in R$ prim, so ist p irreduzibel, denn für $b \in R$ mit $b \mid p$ existiert $a \in R$ mit $a \circ b = p$. Damit gilt insbesondere $p \mid a \circ b$ und daher $p \mid a$ oder $p \mid b$. Im Fall $p \mid a$ gilt $a = p \circ k$ für ein $k \in R$ und daher

$$p = a \circ b = p \circ k \circ b$$

und da $p \neq 0$, folgt $1 = k \circ b$ und damit $b \in R^*$.

(c) Es gibt Integritätsbereiche, in denen irreduzibele Elemente nicht prim sind. Betrachte zum Beispiel

$$R \coloneqq \{a + b\mathrm{i}\sqrt{5}\,;\, a, b \in \mathbb{Z}\}$$

als Unterring von $\mathbb{C}$. Dann ist $2 \in R$ irreduzibel, aber nicht prim. In der Tat gilt

$$2 \cdot 3 = (1 - \mathrm{i}\sqrt{5})(1 + \mathrm{i}\sqrt{5}).$$

also $2 \mid (1 - \mathrm{i}\sqrt{5}) \cdot (1 + \mathrm{i}\sqrt{5})$, aber $2 \nmid (1 - \mathrm{i}\sqrt{5})$ und $2 \nmid (1 + \mathrm{i}\sqrt{5})$ (Übung!). Um zu zeigen, dass 2 irreduzibel ist, nehmen wir an es gibt $x, y \in R \setminus R^*$ mit $2 = x \cdot y$. Dann gilt

$$4 = |x|^2 \cdot |y|^2$$

und somit $|x|^2 \in \{1, 2, 4\}$. Ist $|x|^2 = 1$, so gilt also mit $x = a + \mathrm{i}b\sqrt{5}$, dass $a^2 + 5b^2 = 1$ und daher $x = \pm 1$ also $x \in R^*$. Analog folgt aus $|x|^2 = 4$, dass $y \in R^*$. Somit verbleibt also $|x|^2 = a^2 + 5b^2 = 2$, was allerdings für $a, b \in \mathbb{Z}$ nicht vorkommen kann. Somit ist 2 also irreduzibel.

Lemma 6.4. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $R \setminus \{0\}$. Außerdem gilt für $a, b \in R \setminus \{0\}$*

$$a \sim b \Leftrightarrow \exists c \in R^* : a = c \circ b.$$

Beweis. Der Nachweis der Äquivalenzrelation ist Übungsaufgabe. Gilt $a \sim b$, so folgt $a = c \circ b$ und $b = d \circ a$ für $c, d \in R \setminus \{0\}$. Damit gilt

$$b = d \circ a = d \circ c \circ b$$

und somit

$$d \circ c = 1,$$

also ist $c \in R^*$. Ist umgekehrt $a = c \circ b$ für ein $c \in R^*$, so gilt $b \mid a$ und da c invertierbar ist, auch $a \mid b$ also $a \sim b$. □

Satz 6.5. *Seien $a, b \in R \setminus \{0\}$ und $c, c' \in R \setminus \{0\}$. Sei weiter c ein* ggT *(*kgV*) von a und b. Dann ist c'* ggT *(*kgV*) von a und b genau dann, wenn $c \sim c'$.*

Beweis. Ist c' ggT von a und b, so gilt insbesondere $c' \mid a$ und $c' \mid b$ und damit auch $c' \mid c$. Ebenso folgt aber auch $c \mid c'$ und daher gilt $c \sim c'$. Ist andererseits $c' \sim c$, so gilt insbesondere $c' \mid c$. Damit gilt $c' \mid a$ und $c' \mid b$. Ist k ein weiterer Teiler von a und b so folgt $k \mid c$ und da $c \mid c'$, folgt $k \mid c'$, also ist c' ggT von a und b. Für kgV folgt die Behauptung analog. □

7. Euklidische Ringe

Wir wollen uns nun mit Strukturen beschäftigen, in denen größte gemeinsame Teiler immer existieren und sich auch algorithmisch berechnen lassen. Sei generell $(R, \oplus, \circ)$ ein Integritätsbereich.

Definition. $(R, \oplus, \circ)$ heißt *euklidischer Ring,* falls es eine *Gradfunktion* $\delta : R \to \mathbb{N}$ mit folgenden Eigenschaften gibt:

(a) $\delta(0) = 0$,

(b) für alle $x, y \in R$ mit $y \neq 0$ existieren $q, r \in R$ mit $x = q \circ y \oplus r$ und $\delta(r) < \delta(y)$,

(c) für $x, y \in R$ mit $y \neq 0$ gilt $\delta(x) \leq \delta(x \circ y)$.

Bemerkung 7.1. Es gilt $\delta(x) = 0 \Leftrightarrow x = 0$. In der Tat, ist $\delta(x) = 0$ und $x \neq 0$, so existiert nach (b) $q, r \in R$ mit

$$0 = q \circ x \oplus r$$

und $\delta(r) < \delta(x) = 0$, was nicht möglich ist.

Satz 7.2. $(\mathbb{Z}, +, \cdot)$ *ist ein euklidischer Ring mit* $\delta(x) \coloneqq |x|$.

Beweis. Eigenschaften (a) und (c) sind klar. Für (b) seien $x, y \in \mathbb{Z}$ mit $y \neq 0$. Setze $q \coloneqq |x| \operatorname{div} |y|$ und $r = |x| \bmod |y|$. Dann gilt $\delta(r) = |r| = r < |y| = \delta(y)$. Außerdem ist

$$|x| = q \cdot |y| + r.$$

Sind $x, y \geq 0$, so ist die Behauptung gezeigt. Ist $x \leq 0, y > 0$ so gilt

$$x = -|x| = -q \cdot y - r$$

und $\delta(-r) = \delta(r) < \delta(y)$. Ist $x \geq 0$ und $y < 0$ so folgt

$$x = |x| = -q \cdot y + r$$

und für $x, y \leq 0$ gilt

$$x = -|x| = -q \cdot |y| - r = q \cdot y - r.$$

Das beweist Eigenschaft (b). □

Wir wollen nun noch zeigen, dass auch $\mathbb{K}[X]$ für $\mathbb{K}$ Körper ein euklidischer Ring ist. Dazu definieren wir zunächst den Grad eines Polynoms.

Definition. Wir definieren

$$\gamma : \mathbb{K}[X] \to \mathbb{Z}_{\geq -1}$$

durch

$$\gamma((a_n)_{n\in\mathbb{N}}) \coloneqq \begin{cases} \max\{n \in \mathbb{N}\,;\, a_n \neq 0\} & \text{falls } (a_n)_n \neq (0)_n, \\ -1 & \text{sonst.} \end{cases}$$

Lemma 7.3. *Seien $p, q \in \mathbb{K}[X]$. Dann gelten*

(a) $\gamma(p+q) \leq \max\{\gamma(p), \gamma(q)\}$,

(b) $\gamma(p \cdot q) = \gamma(p) + \gamma(q)$.

Beweis. (a) Sei o.E. $\gamma(p) \leq \gamma(q)$. Dann gilt $a_k = b_k = 0$ für alle $k > \gamma(q) \geq \gamma(p)$ und damit auch $a_k + b_k = 0$ für $k > \gamma(q)$. Damit ist $\gamma(p+q) \leq \gamma(q) = \max\{\gamma(p), \gamma(q)\}$.

(b) Sei $r \coloneqq p \cdot q$. Es gilt

$$r_{\gamma(p)+\gamma(q)} = \sum_{j=0}^{\gamma(p)+\gamma(q)} a_j \cdot b_{\gamma(p)+\gamma(q)-j} = \sum_{j=0}^{\gamma(p)} a_j \cdot b_{\gamma(p)+\gamma(q)-j} = a_{\gamma(p)} \cdot b_{\gamma(q)} \neq 0$$

und daher $\gamma(r) \geq \gamma(p) + \gamma(q)$. Außerdem gilt für alle $n \in \mathbb{N}_{\geq 1}$

$$r_{\gamma(p)+\gamma(q)+n} = \sum_{j=0}^{\gamma(p)+\gamma(q)+n} a_j \cdot b_{\gamma(p)+\gamma(q)+n-j} = \sum_{j=0}^{\gamma(p)} a_j \cdot b_{\gamma(p)+\gamma(q)+n-j} = 0$$

und somit $\gamma(r) \leq \gamma(p) + \gamma(q)$.

□

Korollar 7.4. *Es gilt $\mathbb{K}[X]^* = \mathbb{K} \setminus \{0\}$, wobei wir Elemente aus $x \in \mathbb{K}$ mit dem Polynom $(x, 0, 0, 0, \ldots)$ identifizieren.*

Beweis. Ist $x \in \mathbb{K} \setminus \{0\}$, so gilt $x \cdot x^{-1} = 1$ und daher $x \mid 1$ also ist x eine Einheit. Ist umgekehrt $p \in K[X]^*$ so existiert ein $q \in K[X]$ mit $p \cdot q = 1$. Dann gilt

$$0 = \gamma(1) = \gamma(p \cdot q) = \gamma(p) + \gamma(q) \geq \gamma(p),$$

da $q \neq 0$ und somit $\gamma(q) \geq 0$. Damit folgt $\gamma(p) = 0$ und somit $p = (x, 0, 0, \ldots)$ für ein $x \in \mathbb{K} \setminus \{0\}$. □

Satz 7.5. *$(\mathbb{K}[X], +, \cdot)$ ist ein euklidischer Ring mit $\delta(p) \coloneqq \gamma(p) + 1$.*

Beweis. Die Eigenschaft (a) ist klar nach Definition von γ. Die Eigenschaft (c) folgt aus

$$\delta(p \cdot q) = \gamma(p \cdot q) + 1 = \gamma(p) + 1 + \gamma(q) \geq \gamma(p) + 1 = \delta(p)$$

für $q \neq 0$. Kommen wir nun zur Eigenschaft (b). Seien $p, q \in \mathbb{K}[X]$ mit $q \neq 0$. Wir betrachten die Menge

$$M \coloneqq \{n \in \mathbb{N} \mid \exists s, r \in \mathbb{K}[X] : p = s \cdot q + r \wedge \gamma(r) = n - 1\}.$$

Dann ist $M \neq \emptyset$, da $p = 0 \cdot q + p$ und daher $\gamma(p) + 1 \in M$. Nach Satz 1.7 existiert ein minimales Element $n_0 \in M$ und damit Polynome $s, r \in \mathbb{K}[X]$ mit $p = s \cdot q + r$ und $\gamma(r) = n_0 - 1$. Wir zeigen nun $n_0 - 1 < \gamma(q)$. Sei dazu $q = (a_n), s = (b_n)$ und $r = (c_n)$. Wir nehmen an: $n_0 - 1 = \gamma(r) \geq \gamma(q)$ und setzen $\widetilde{s} \coloneqq (d_n)$ mit

$$d_n \coloneqq \begin{cases} c_{\gamma(r)} \cdot a_{\gamma(q)}^{-1} & \text{falls } n = \gamma(r) - \gamma(q), \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt $\gamma(\widetilde{s}) = \gamma(r) - \gamma(q)$ und

$$\begin{aligned} p &= s \cdot q + r \\ &= (s + \widetilde{s}) \cdot q + (r - \widetilde{s} \cdot q). \end{aligned}$$

Nun ist $\gamma(r - \widetilde{s} \cdot q) \leq \max\{\gamma(r), \gamma(\widetilde{s} \cdot q)\} = \max\{\gamma(r), \gamma(\widetilde{s}) + \gamma(q)\} = \max\{\gamma(r), \gamma(r)\} = \gamma(r)$. Allerdings gilt

$$(r - \widetilde{s} \cdot q)_{\gamma(r)} = c_{\gamma(r)} - \sum_{j=0}^{\gamma(r)} d_j \cdot a_{\gamma(r)-j} = c_{\gamma(r)} - d_{\gamma(r)-\gamma(q)} \cdot a_{\gamma(q)} = 0$$

und somit $\gamma(r - \widetilde{s} \cdot q) < \gamma(r)$. Das widerspricht der Minimalität von n_0. Somit gilt also

$$p = s \cdot q + r$$

mit $\delta(r) = \gamma(r) + 1 = n_0 < \gamma(q) + 1 = \delta(q)$. □

Sei im Weiteren $(R, +, \cdot)$ stets ein euklidischer Ring. Wir zeigen nun, wie man in euklidischen Ringen einen größten gemeinsamen Teiler berechnen kann.

Theorem 7.6 (Euklidischer Algorithmus)**.** *Seien $a, b \in R \setminus \{0\}$. Wir definieren rekursiv die Elemente $r_n \in R$ und $s_n \in R$ dusch*

$$\begin{aligned} a &= s_0 \cdot b + r_0, \ \delta(r_0) < \delta(b) \\ b &= s_1 \cdot r_0 + r_1, \ \delta(r_1) < \delta(r_0) \\ r_{n-1} &= s_{n+1} \cdot r_n + r_{n+1}, \ \delta(r_{n+1}) < \delta(r_n), \end{aligned}$$

solange $\delta(r_n) > 0$. Da $(\delta(r_n))_{n \in \mathbb{N}}$ absteigend in $\mathbb{N}$ ist, gibt es $n \in \mathbb{N}$ mit $\delta(r_n) > 0$ und $\delta(r_{n+1}) = 0$. Dann ist r_n ggT von a und b.

Beweis. Es gilt $r_{n+1} = 0$ und daher

$$r_{n-1} = s_{n+1} \cdot r_n$$

also $r_n \mid r_{n-1}$. Außerdem gilt

$$r_{n-2} = s_n r_{n-1} + r_n$$

und daher $r_n \mid r_{n-2}$. Induktiv folgt $r_n \mid r_{n-1}, \ldots, r_n \mid r_0$ und somit auch $r_n \mid b$ und $r_n \mid a$. Damit ist r_n gemeinsamer Teiler. Ist nun $d \in R$ mit $d \mid a$ und $d \mid b$, so folgt wegen

$$r_0 = a - s_0 \cdot b$$

auch $d \mid r_0$ und dann auch (wegen $r_1 = b - s_1 \cdot r_0$) $d \mid r_1$. Induktiv folgt hieraus $d \mid r_n$ und somit ist r_n ggT von a und b. □

Bemerkung 7.7. Der ggT und das kgV sind nach Satz 6.5 bis auf Einheiten eindeutig bestimmt, sofern sie existieren. Im euklidischen Ring $(\mathbb{Z}, +, \cdot)$ sind 1 und -1 die einzigen Einheiten. Für zwei ganze Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ setzen wir $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ als die entsprechenden natürlichen Zahlen.

Beispiel 7.8. (a) Wir betrachten die Zahlen $n = 11.427.780$ und $m = 141.050$. Wir berechnen den ggT über den euklidischen Algorithmus. Es gilt

$$\begin{aligned} 11427780 &= 81 \cdot 141050 + 2730 \\ 141050 &= 51 \cdot 2730 + 1820 \\ 2730 &= 1 \cdot 1820 + 910 \\ 1820 &= 2 \cdot 910 + 0 \end{aligned}$$

und damit gilt $\mathrm{ggT}(11427780, 141050) = 910$.

(b) Wir rechnen in $\mathbb{R}[X]$. Betrachte die Polynome $p = X^4 + X^3 + X - 1$ und $q = 3X^5 + 3X^4 - 4X^3 - X^2 + X$. Dann gilt

$$\begin{aligned} 3X^5 + 3X^4 - 4X^3 - X^2 + X &= 3X \cdot \left(X^4 + X^3 + X - 1\right) + \left(-4X^3 - 4X^2 + 4X\right) \\ X^4 + X^3 + X - 1 &= -\frac{1}{4}X \cdot \left(-4X^3 - 4X^2 + 4X\right) + \left(X^2 + X - 1\right) \\ -4X^3 - 4X^2 + 4X &= -4X \cdot \left(X^2 + X - 1\right) + 0 \end{aligned}$$

und somit $X^2 + X - 1$ ein ggT. Alle übrigen ggT haben die Form

$$aX^2 + aX - a$$

für $a \in \mathbb{R} \setminus \{0\}$.

Korollar 7.9 (Lemma von Bézout)**.** *Seien $a, b \in R \setminus \{0\}$. Sei d ein* ggT *von a und b. Dann existieren $x, y \in R$ mit*

$$d = x \cdot a + y \cdot b.$$

Beweis. Es gilt $d \sim r_n$ wobei r_n wie in Theorem 7.6 definiert ist. Damit ist $d = c \cdot r_n$ für $c \in R^*$ und somit genügt es die Behauptung für r_n zu beweisen. Es gilt durch Rückwärtsrechnen im euklidischen Algorithmus

$$\begin{aligned} r_n &= r_{n-2} - s_n r_{n-1} \\ &= r_{n-2} - s_n(r_{n-3} - s_{n-1} r_{n-2}) \\ &= (1 + s_n s_{n-1}) r_{n-2} - s_n r_{n-3} \\ &\vdots \\ &= x \cdot a + y \cdot b. \end{aligned}$$

□

Beispiel 7.10. Wir betrachten wieder die Zahlen $n = 11.427.780$ und $m = 141.050$. Dann gilt

$$910 = 2730 - 1 \cdot 1820$$

$$\begin{aligned}
&= 2730 - 1 \cdot (141050 - 51 \cdot 2730) \\
&= 52 \cdot 2730 - 1 \cdot 141050 \\
&= 52 \cdot (11427780 - 81 \cdot 141050) - 1 \cdot 141050 \\
&= 52 \cdot 11427780 - 4213 \cdot 141050.
\end{aligned}$$

Korollar 7.11 (Lemma von Euklid)**.** *Seien $c, a, b \in R \setminus \{0\}$ so, dass $c \mid a \cdot b$. Sei 1 ein* ggT *von c und a. Dann gilt $c \mid b$. Insbesondere sind alle irreduziblen Elemente prim.*

Beweis. Es existieren $x, y \in R$ mit

$$1 = x \cdot a + y \cdot c.$$

Außerdem existiert $d \in R$ mit $c \cdot d = a \cdot b$. Dann gilt

$$\begin{aligned}
b = b \cdot 1 &= b \cdot (x \cdot a + y \cdot c) \\
&= x \cdot a \cdot b + y \cdot b \cdot c \\
&= x \cdot c \cdot d + y \cdot b \cdot c \\
&= (x \cdot d + y \cdot b) \cdot c,
\end{aligned}$$

also $c \mid b$.
Sei $p \in R \setminus \{0\}$ irreduzibel und gelte $p \mid a \cdot b$. Wir nehmen an, dass $p \nmid a$. Dann ist 1 ein ggT von p und a da p nur Einheiten und zu p assoziierte Teiler besitzt. Da $p \nmid a$ können aber nur die Einheiten gemeinsame Teiler von p und a sind und damit ist 1 ein ggT von a und p. Dann gilt aber $p \mid b$ nach dem oben Gezeigten und daher ist p prim. □

Theorem 7.12. *Sei $a \in R \setminus \{0\}$. Dann existieren irreduzible Elemente $p_1, \ldots, p_k \in R \setminus \{0\}$ und eine Einheit $\varepsilon \in R^*$ mit*

$$a = \varepsilon \cdot p_1 \cdot \ldots \cdot p_k.$$

Sind ferner $q_1, \ldots, q_\ell \in R \setminus \{0\}$ irreduzibel und $\widetilde{\varepsilon} \in R^*$ mit $a = \widetilde{\varepsilon} \cdot q_1 \cdot \ldots \cdot q_\ell$ so gilt $k = \ell$ und es existiert eine bijektive Abbildung $\pi : \{1, \ldots, k\} \to \{1, \ldots, k\}$ so, dass

$$p_i \sim q_{\pi(i)} \quad (i \in \{1, \ldots, k\}).$$

Beweis. Wir beweisen zunächst die Existenz solch einer Zerlegung in irreduzible Elemente. Wir nehmen an, es gibt Elemente in $R \setminus \{0\}$ die sich nicht auf diese Weise zerlegen lassen, d.h.

$$M \coloneqq \{b \in R \setminus \{0\}\,;\, b \text{ nicht zerlegbar}\}$$

ist nichtleer. Wähle $b \in M$ mit $\delta(b)$ minimal. Da b selbst nicht irreduzibel und keine Einheit ist, gilt $b = c \cdot d$ für gewisse $c, d \in R \setminus R^*$. Nach Eigenschaft (b) existieren $q, r \in R$ mit

$$c = q \cdot b + r \text{ und } \delta(r) < \delta(b).$$

Nun ist

$$c = q \cdot b + r = q \cdot c \cdot d + r$$

und daher

$$r = (1 - q \cdot d) \cdot c.$$

Da $d \notin R^*$ folgt $1 - q \cdot d \neq 0$ und somit

$$\delta(c) \leq \delta(r) < \delta(b).$$

Analog zeigt man $\delta(d) < \delta(b)$ und da $\delta(b)$ minimal war, folgt $c, d \notin M$. Somit lassen sich c und d als Produkte irreduzibler Elemente und Einheiten darstellen aber damit auch $b = c \cdot d$. Widerspruch!
Kommen wir nun zu verschiedenen Zerlegungen: Gelte also

$$\varepsilon \cdot p_1 \cdot \ldots \cdot p_k = \widetilde{\varepsilon} \cdot q_1 \cdot \ldots \cdot q_\ell.$$

Wir nehmen ohne Einschränkung $\ell \leq k$ an. Es ist $p_1 \mid q_1 \cdot \ldots \cdot q_\ell$ und da p_1 prim ist, folgt $p_1 \mid q_{\pi(1)}$ für ein $\pi(1) \in \{1, \ldots, \ell\}$. Da $q_{\pi(1)}$ irreduzibel ist und p_1 keine Einheit, folgt $q_{\pi(1)} \mid p_1$ und daher $p_1 \sim q_{\pi(1)}$. Also gilt $p_1 = \varepsilon_1 \cdot q_{\pi(1)}$ für eine Einheit ε_1 und somit

$$\varepsilon \cdot \varepsilon_1 \cdot p_2 \cdot \ldots \cdot p_k = \widetilde{\varepsilon} \cdot \prod_{i=1, i \neq \pi(1)}^{\ell} q_i.$$

Man fährt nun so fort mit p_2, p_3 etc. bis keine $q_i's$ mehr vorhanden sind. Dann folgt

$$\widetilde{\varepsilon}^{-1} \cdot \varepsilon \cdot \varepsilon_1 \cdot \ldots \cdot \varepsilon_\ell \cdot p_{\ell+1} \cdot \ldots \cdot p_k = 1.$$

Wäre $k > \ell$, so würde folgen, dass p_k eine Einheit wäre, was Definition von irreduzibel widerspricht. Somit kann nur der Fall $k = \ell$ auftreten. □

Korollar 7.13. *Seien $a, b \in R \setminus \{0\}$ mit Zerlegungen*

$$a = \varepsilon \cdot p_1 \cdot \ldots \cdot p_k$$
$$b = \widetilde{\varepsilon} \cdot q_1 \cdot \ldots \cdot q_\ell$$

gemäß Theorem 7.12. Dann gilt $a \mid b$ genau dann, wenn es eine injektive Abbildung $\tau : \{1, \ldots, k\} \to \{1, \ldots, \ell\}$ gibt mit

$$p_i \sim q_{\tau(i)} \quad (i \in \{1, \ldots, k\}).$$

Beweis. Gilt $a \mid b$, so existiert $c \in R$ mit $a \cdot c = b$. Wir zerlegen c in irreduzible Elemente und eine Einheit δ, also $c = \delta \cdot p_{k+1} \cdot \ldots \cdot p_{k+m}$ und erhalten so

$$b = a \cdot c = \delta \cdot \varepsilon \cdot p_1 \cdot \ldots \cdot p_k \cdot p_{k+1} \cdot \ldots \cdot p_{k+m}.$$

Nach Theorem 7.12 gilt $k + m = \ell$ und es existiert eine bijektive Abbildung $\pi : \{1, \ldots, k+m\} \to \{1, \ldots, \ell\}$ mit

$$p_i \sim q_{\pi(i)}$$

für alle $i \in \{1, \ldots, k+m\}$. Die Abbildung $\tau \coloneqq \pi|_{\{1,\ldots,k\}}$ liefert dann die Behauptung.
Existiert umgekehrt so eine Abbildung τ, so gilt

$$\varepsilon_i p_i = q_{\tau(i)}$$

für Einheiten ε_i und damit gilt

$$a \cdot \widetilde{\varepsilon} \cdot \prod_{i=1}^{k} \varepsilon_i \prod_{j \notin \{\tau(1),\ldots,\tau(k)\}} q_j = b,$$

also $a \mid b$. □

Korollar 7.14. *Seien $a, b, c \in R \setminus \{0\}$ mit Zerlegungen*

$$\begin{aligned} a &= \varepsilon \cdot p_1 \cdot \ldots \cdot p_k, \\ b &= \delta \cdot q_1 \cdot \ldots \cdot q_\ell, \\ c &= \kappa \cdot r_1 \cdot \ldots \cdot r_m, \end{aligned}$$

gemäß Theorem 7.12. Dann ist c ein ggT *von a und b genau dann, wenn es zwei injektive Abbildungen $\gamma_1 : \{1,\ldots,m\} \to \{1,\ldots,k\}$ und $\gamma_2 : \{1,\ldots,m\} \to \{1,\ldots,\ell\}$ gibt, so dass*

$$r_i \sim p_{\gamma_1(i)} \sim q_{\gamma_2(i)} \quad (i \in \{1,\ldots,m\})$$

und

$$\forall i \in \{1,\ldots,k\} \setminus \{\gamma_1(1),\ldots,\gamma_1(m)\}, j \in \{1,\ldots,\ell\} \setminus \{\gamma_2(1),\ldots,\gamma_2(m)\} : p_i \nsim q_j.$$

Beweis. Sei zunächst c ein ggT von a und b. Dann existieren nach Korollar 7.13 zwei injektive Abbildungen γ_1, γ_2, die die erste Bedingung erfüllen. Wir zeigen nun, dass diese auch die zweite Bedingung erfüllen. Dazu nehmen wir an, es existieren $i \in \{1,\ldots,k\} \setminus \{\gamma_1(1),\ldots,\gamma_1(m)\}$ und $j \in \{1,\ldots,\ell\} \setminus \{\gamma_2(1),\ldots,\gamma_2(m)\}$ mit $p_i \sim q_j$. Wir betrachten $d \coloneqq c \cdot p_i$. Dann gilt $d \mid a$ und $d \mid b$ aber nicht $d \mid c$, was der Definition des ggT widerspricht.
Existieren nun umgekehrt die zwei injektiven Abbildungen γ_1, γ_2, so ist c ein gemeinsamer Teiler von a und b nach Korollar 7.13. Wir definieren nun

$$a' \coloneqq \prod_{i \notin W(\gamma_1)} p_i, \quad b' \coloneqq \prod_{j \notin W(\gamma_2)} q_j.$$

Dann gilt

$$c \cdot a' \sim a, \quad c \cdot b' \sim b.$$

Ferner haben nach Korollar 7.13 die Elemente a' und b' nur Einheiten als gemeinsame Teiler und daher ist 1 ein ggT von a' und b'. Damit ist aber nach $c = c \cdot 1$ ein ggT von $c \cdot a'$ und $c \cdot b'$ (vgl. Übung) und damit auch von den jeweiligen assoziierten Elementen a und b. Also ist c ein ggT von a und b. □

Beispiel 7.15. Wir betrachten wieder $n = 11.427.780$ und $m = 141.050$. Es gilt

$$\begin{aligned} n &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 23 \\ m &= 2 \cdot 5 \cdot 5 \cdot 7 \cdot 13 \cdot 31 \end{aligned}$$

und daher

$$\mathrm{ggT}(n, m) = 2 \cdot 5 \cdot 7 \cdot 13 = 910.$$

Wir wollen uns abschließend mit dem kgV beschäftigen. Dazu benötigen wir das folgende Lemma.

Lemma 7.16. *Seien $a, b, d \in R \setminus \{0\}$ so, dass 1 ein* ggT *von a und b ist und $a \mid d$ und $b \mid d$. Dann gilt $a \cdot b \mid d$.*

Beweis. Wir zerlegen a, b, d gemäß Theorem 7.12 in

$$\begin{aligned} a &= \varepsilon \cdot p_1 \cdot \ldots \cdot p_k, \\ b &= \delta \cdot p_{k+1} \cdot \ldots \cdot p_{k+\ell}, \\ d &= \kappa \cdot q_1 \cdot \ldots \cdot q_n. \end{aligned}$$

Da 1 ein ggT von a und b ist, folgt $p_j \nsim p_{k+i}$ für alle $j \in \{1, \ldots, k\}$ und $i \in \{1, \ldots, \ell\}$. Außerdem existieren injektive Abbildungen $\gamma_1 : \{1, \ldots, k\} \to \{1, \ldots, n\}$ und $\gamma_2 : \{k+1, \ldots, k+\ell\} \to \{1, \ldots, n\}$ so, dass

$$\begin{aligned} p_j &\sim q_{\gamma_1(j)} \\ p_{k+i} &\sim q_{\gamma_2(k+i)}. \end{aligned}$$

Da $p_j \nsim p_{k+i}$, folgt $\gamma_1(j) \neq \gamma_2(k+i)$ und damit ist $\gamma : \{1, \ldots, k+\ell\} \to \{1, \ldots, m\}$ mit

$$\gamma(i) = \begin{cases} \gamma_1(i) & i \in \{1, \ldots, k\}, \\ \gamma_2(i) & i \in \{k+1, \ldots, k+\ell\} \end{cases}$$

injektiv mit

$$p_i \sim q_{\gamma(i)}$$

für alle i. Damit folgt $a \cdot b \mid d$. □

Satz 7.17. *Seien $a, b \in R \setminus \{0\}$. Sei c ein* ggT *von a und b. Dann existiert $f \in R \setminus \{0\}$ mit $c \cdot f = a \cdot b$. Dann ist f ein* kgV *von a und b.*

Beweis. Da c ein gemeinsamer Teiler von a und b ist, existieren $\widetilde{a}, \widetilde{b} \in R \setminus \{0\}$ mit

$$a = \widetilde{a} \cdot c \text{ und } b = \widetilde{b} \cdot c.$$

Da c ein ggT von a und b ist, folgt, dass 1 ein ggT von $\widetilde{a}$ und $\widetilde{b}$ ist. In der Tat, ist d ein gemeinsamer Teiler von $\widetilde{a}$ und $\widetilde{b}$ so gilt $d \cdot c \mid a$ und $d \cdot c \mid b$ und damit $d \cdot c \mid c$ und daher ist d eine Einheit. Es gilt

$$c \cdot f = a \cdot b = \widetilde{a} \cdot \widetilde{b} \cdot c \cdot c$$

und damit

$$f = \widetilde{a} \cdot \widetilde{b} \cdot c = a \cdot \widetilde{b} = \widetilde{a} \cdot b$$

also $a \mid f$ und $b \mid f$. Ist nun g ein gemeinsames Vielfaches von a und b, so folgt insbesondere $c \mid g$ und damit existiert $\widetilde{g} \in R \setminus \{0\}$ mit

$$g = \widetilde{g} \cdot c.$$

Dann gilt $\widetilde{a} \cdot c = a \mid g = \widetilde{g} \cdot c$ und daher $\widetilde{a} \mid \widetilde{g}$ und ebenso $\widetilde{b} \mid \widetilde{g}$. Nach Lemma 7.16 folgt nun $\widetilde{a} \cdot \widetilde{b} \mid \widetilde{g}$ und daher ist

$$f = \widetilde{a} \cdot \widetilde{b} \cdot c \mid \widetilde{g} \cdot c = g$$

also ist f ein kgV von a und b. □

Beispiel 7.18. (a) Wir betrachten wiederum die Zahlen $n = 11.427.780$ und $m = 141.050$. Dann gilt

$$\begin{aligned}\mathrm{kgV}(n,m) &= \frac{n \cdot m}{910} \\ &= \frac{2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 23 \cdot 2 \cdot 5 \cdot 5 \cdot 7 \cdot 13 \cdot 31}{2 \cdot 5 \cdot 7 \cdot 13} \\ &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 23 \cdot 31 \\ &= 1.771.305.900.\end{aligned}$$

(b) Wir rechnen in $\mathbb{R}[X]$ und betrachte die Polynome $p = X^4 + X^3 + X - 1$ und $q = 3X^5 + 3X^4 - 4X^3 - X^2 + X$. Dann ist

$$p \cdot q = 3X^9 + 6X^8 - X^7 - 2X^6 - 6X^4 + 3X^3 + 2X^2 - X$$

und somit ist

$$3X^9+6X^8-X^7-2X^6-6X^4+3X^3+2X^2-X : X^2+X-1 = 3X^7+3X^6-X^5+2X^4-3X^3-X^2+X$$

ein kgV von p und q.

Teil III.

Restklassenringe

8. Der Ring $\mathbb{Z}_n$

Wir hatten gesehen, dass wir für $x \in \mathbb{Z}$ und $n \in \mathbb{N}_{\geq 1}$ Zahlen $y, r \in \mathbb{Z}$ mit $|r| < n$ finden so dass

$$x = y \cdot n + r.$$

Wir wollen uns nun mit diesen Resten r befassen. Durchweg sei $n \in \mathbb{N}_{\geq 1}$.

Definition. Wir definieren auf $\mathbb{Z}$ die Relation $\equiv_{\mathrm{mod}\, n}$ durch

$$m \equiv k \pmod{n} :\Leftrightarrow \exists a \in \mathbb{Z} : m - k = a \cdot n.$$

Dann definiert $\equiv_{\mathrm{mod}\, n}$ ein Äquivalenzrelation (Übung!) auf $\mathbb{Z}$ und wir setzen

$$\mathbb{Z}_n := \mathbb{Z}/\equiv_{\mathrm{mod}\, n}.$$

Bemerkung 8.1. Es gilt $n \mid m \Leftrightarrow m \equiv 0 \pmod{n}$.

Satz 8.2. *Wir definieren die Operationen $+$ und $\cdot$ auf $\mathbb{Z}_n$ durch*

$$[m] + [k] := [m + k]$$
$$[m] \cdot [k] := [m \cdot k].$$

Dann sind $+$ und $\cdot$ wohldefiniert und $(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit Eins.

Beweis. Seien $m, k, \widetilde{m}, \widetilde{k} \in \mathbb{Z}$ mit $m \equiv \widetilde{m} \pmod{n}$ und $k \equiv \widetilde{k} \pmod{n}$. Dann gilt

$$m - \widetilde{m} = a \cdot n, \quad k - \widetilde{k} = b \cdot n$$

für geeignete $a, b \in \mathbb{Z}$. Dann gilt

$$(m + k) - (\widetilde{m} + \widetilde{k}) = (a - b) \cdot n$$

also $m + k \equiv \widetilde{m} + \widetilde{k} \pmod{n}$. Ebenso gilt

$$(m \cdot k) - (\widetilde{m} \cdot \widetilde{k}) = (m - \widetilde{m}) \cdot k + (k - \widetilde{k}) \cdot \widetilde{m} = (k \cdot a + b \cdot \widetilde{m}) \cdot n.$$

Somit sind beide Operationen wohldefiniert. Die Kommutativität, Assoziativität und Distributivität folgen unmittelbar aus den Rechenregeln der Addition und Multiplikation für ganze Zahlen. Die neutralen Elemente bzgl. $+$ und $\cdot$ sind $[0]$ bzw. $[1]$ und zu $[m]$ ist $[-m]$ das inverse Element bezüglich $+$. □

Satz 8.3. *$\mathbb{Z}_n$ ist genau dann ein Integritätsbereich (also ein nullteilerfreier kommutativer Ring mit Eins), wenn n eine Primzahl ist.*

Beweis. Sei zunächst $\mathbb{Z}_n$ ein Integritätsbereich und $m \in \mathbb{N}_{>0}$ mit $m \mid n$. Dann gibt es $k \in \mathbb{N}_{>0}$ mit $m \cdot k = n$. Dann ist

$$[m] \cdot [k] = [m \cdot k] = [n] = 0$$

und damit gilt $[m] = 0$ oder $[k] = 0$. Da $0 < m, k \leq n$, folgt hieraus $m = n$ oder $k = n$. Damit ist n irreduzibel, also eine Primzahl.
Sei nun n prim und $m, k \in \mathbb{Z}$ mit

$$[m \cdot k] = [m] \cdot [k] = 0.$$

Dann gilt $m \cdot k = a \cdot n$ für ein $a \in \mathbb{Z}$. Ist $a = 0$, so folgt $k = 0$ oder $m = 0$. Ist $a \neq 0$, so gilt $n \mid m \cdot k$ und da n prim ist, folgt mit Korollar 7.11 $n \mid m$ oder $n \mid k$. Damit gilt aber $m \equiv 0 \pmod{n}$ oder $k \equiv 0 \pmod{n}$. Also ist $\mathbb{Z}_n$ ein Integritätsbereich. □

- **Einschub**

  Wir wollen noch eine Folgerung aus dem Schubfachprinzip nachtragen. Dazu definieren wir zunächst, was wir unter einer endlichen Menge verstehen.

  Definition. Eine Menge M heißt *endlich*, falls es ein $n \in \mathbb{N}$ und eine bijektive Abbildung $f : M \to \mathbb{N}_{<n}$ gibt.

  Lemma 8.4. *Sei M eine endliche Menge und $n, m \in \mathbb{N}$ und $f : M \to \mathbb{N}_{<n}, g : M \to \mathbb{N}_{<m}$ bijektive Abbildungen. Dann gilt $m = n$ und wir definieren $|M| := n$, die* Kardinalität *(oder* Mächtigkeit*) von M.*

  Beweis. Ist $m \neq n$ so gilt $m < n$ oder $n < m$. Sei o.E. $m < n$. Dann ist nach Satz 1.8 $f \circ g^{-1} : \mathbb{N}_{<m} \to \mathbb{N}_{<n}$ nicht injektiv, was allerdings der Bijektivität von $f \circ g^{-1}$ widerspricht. □

  Satz 8.5. *Seien M, N endliche Mengen mit $|M| = |N|$ und $f : M \to N$. Dann ist f injektiv genau dann wenn f surjektiv ist.*

  Beweis. Zunächst existiert ein $n \in \mathbb{N}$ und bijektive Abbildungen $g : M \to \mathbb{N}_{<n}$, $h : N \to \mathbb{N}_{<n}$. Da f genau dann injektiv bzw. surjektiv ist, wenn $h \circ f \circ g^{-1} : \mathbb{N}_{<n} \to \mathbb{N}_{<n}$ injektiv bzw. surjektiv ist, können wir o.E. annehmen, dass $f : \mathbb{N}_{<n} \to \mathbb{N}_{<n}$.
  Sei f injektiv. Wir nehmen an, dass f nicht surjektiv ist. Dann gibt es ein $j \in \mathbb{N}_{<n}$ mit $j \notin f[\mathbb{N}_{<n}]$. Betrachte die injektive Abbildung

  $$\begin{aligned} g : \mathbb{N}_{<n} \setminus \{j\} &\to \mathbb{N}_{<n-1} \\ \ell &\mapsto \begin{cases} \ell & \text{falls } \ell < j \\ \ell - 1 & \text{falls } \ell > j. \end{cases} \end{aligned}$$

  Dann ist nach Voraussetzung $g \circ f : \mathbb{N}_{<n} \to \mathbb{N}_{<n-1}$ injektiv, was jedoch Satz 1.8 widerspricht. Somit ist f surjektiv.

Sei nun f surjektiv. Dann ist für alle $m \in \mathbb{N}_{<n}$ die Menge $\{k \in \mathbb{N}_{<n} \mid f(k) = m\}$ nichtleer. Demnach existiert nach Satz 1.7 ein kleinstes Element. Wir setzen

$$\begin{aligned} g : \mathbb{N}_{<n} &\to \mathbb{N}_{<n} \\ m &\mapsto \min\{k \in \mathbb{N}_{<n} \mid f(k) = m\} \end{aligned}$$

und erhalten so

$$f(g(m)) = m \quad (m \in \mathbb{N}_{<n}).$$

Somit ist g injektiv und nach dem bisher Gezeigten auch surjektiv. Seien nun $k, \widetilde{k} \in \mathbb{N}_{\leq n}$ mit $f(k) = f(\widetilde{k})$ und gelte o.E. $k \leq \widetilde{k}$. Da g surjektiv ist, existiert $m \in \mathbb{N}_{<n}$ mit $g(m) = \widetilde{k}$. Dann gilt

$$f(k) = f(\widetilde{k}) = f(g(m)) = m,$$

und somit nach der Definition von g

$$\widetilde{k} = g(m) \leq k.$$

Somit ist also $k = \widetilde{k}$, die Funktion f also injektiv. □

Korollar 8.6. *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Ist $\mathbb{Z}_n$ ein Körper, so ist es insbesondere ein Integritätsbereich und damit ist n prim nach Satz 8.3. Sei nun n prim. Wir zeigen, dass $[m] \neq [0]$ ein multiplikatives Inverses besitzt. Wir betrachten die Abbildung

$$\begin{aligned} f : \mathbb{N}_{<n} &\to \mathbb{N}_{<n} \\ k &\mapsto (m \cdot k) \bmod n. \end{aligned}$$

Diese Abbildung ist injektiv. In der Tat folgt aus $(m \cdot k) \bmod n = (m \cdot \widetilde{k}) \bmod n$ für $k, \widetilde{k} \in \mathbb{N}_{<n}$ mit $\widetilde{k} \leq k$ dass $m \cdot (k - \widetilde{k}) \bmod n = 0$, also

$$[m] \cdot [k - \widetilde{k}] = [0].$$

Da $\mathbb{Z}_n$ ein Integritätsbereich ist (Satz 8.3) und $m \not\equiv 0 \pmod n$, folgt $k - \widetilde{k} \equiv 0 \pmod n$. Da $0 \leq k - \widetilde{k} < n$, folgt $k = \widetilde{k}$ also ist f injektiv und somit auch surjektiv nach Satz 8.5. Somit existiert insbesondere ein $k \in \mathbb{N}_{<n}$ mit $m \cdot k \bmod n = 1$. Damit ist $[k]$ das multiplikative Inverse von $[m]$ und damit ist $\mathbb{Z}_n$ ein Körper. □

9. Teilbarkeitsregeln

Sei $b \in \mathbb{N}_{>1}$. Aus Abschnitt 5 wissen wir, dass wir jeder natürlichen Zahl $n \in \mathbb{N}$ ihre b-adische Darstellung zuordnen können. Mit anderen Worten: wir schreiben

$$n = \sum_{k=0}^{n_0} a_k b^k$$

für geeignete Zahlen $a_0, \ldots, a_{n_0} \in \mathbb{N}_{<g}$ mit $a_{n_0} \neq 0$. Wir wollen nun einige Teilbarkeitsregeln mithilfe der b-adischen Darstellung beweisen.

Satz 9.1 (Quersummenregel)**.** *Sei $d \in \mathbb{N}_{\geq 1}$ mit $d \mid b-1$. Sei ferner $n \in \mathbb{N}$ und $n = \sum_{k=0}^{n_0} a_k b^k$ dessen b-adische Darstellung. Dann gilt $d \mid n$ genau dann, wenn $d \mid \sum_{k=0}^{n_0} a_k$.*

Beweis. Da $d \mid b-1$ existiert $a \in \mathbb{N}_{>0}$, so dass $d \cdot a = b-1$, oder mit anderen Worten $b \equiv 1 \pmod{d}$. Induktiv folgt hieraus

$$b^k \equiv 1 \pmod{d}$$

für alle $k \in \mathbb{N}$. Somit gilt

$$n \equiv \sum_{k=0}^{n_0} a_k \pmod{d}.$$

Somit gilt nun also

$$d \mid n \Leftrightarrow n \bmod d = 0 \Leftrightarrow \sum_{k=0}^{n_0} a_k \bmod d = 0 \Leftrightarrow d \mid \sum_{k=0}^{n_0} a_k. \qquad \square$$

Satz 9.2 (Alternierende Quersumme)**.** *Sei $d \in \mathbb{N}_{\geq 1}$ mit $d \mid b+1$. Sei ferner $n \in \mathbb{N}$ und $n = \sum_{k=0}^{n_0} a_k b^k$ dessen b-adische Darstellung. Dann gilt $d \mid n$ genau dann, wenn $d \mid \sum_{k=0}^{n_0} (-1)^k a_k$.*

Beweis. Da $d \mid b+1$, gilt $b \equiv -1 \pmod{d}$ und induktiv folgt hieraus

$$b^k \equiv (-1)^k \pmod{d}$$

für alle $k \in \mathbb{N}$. Damit gilt

$$n \equiv \sum_{k=0}^{n_0} (-1)^k a_k \pmod{d}$$

und somit folgt die Behauptung. $\square$

Satz 9.3. *Sei $d \in \mathbb{N}_{\geq 1}$ mit $d \mid b^j$ für ein $j \in \mathbb{N}$. Sei ferner $n \in \mathbb{N}$ und $n = \sum_{k=0}^{n_0} a_k b^k$ dessen b-adische Darstellung. Dann gilt $d \mid n$ genau dann, wenn $d \mid \sum_{k=0}^{\min\{n_0, j-1\}} a_k b^k$.*

Beweis. Da $d \mid b^j$ folgt induktiv

$$b^k \equiv 0 \pmod{d}$$

für alle $k \in \mathbb{N}_{\geq j}$. Somit ist

$$n \equiv \sum_{k=0}^{\min\{n_0, j-1\}} a_k b^k \pmod{d}$$

woraus die Behauptung folgt. □

10. Lineare Kongruenzen

In diesem Abschnitt wollen wir uns mit der Lösbarkeit linearer Kongruenzen beschäftigen, d.h. wir stellen die Frage, ob für gegebene Zahlen $n \in \mathbb{N}_{\geq 1}, a, b \in \mathbb{Z}$ Lösungen $x \in \mathbb{Z}$ der Kongruenz

$$a \cdot x \equiv b \pmod{n}$$

existieren und wenn ja, wie viele. Wir beginnen zunächst mit der Lösbarkeit linearer Kongruenzen. Für das einfachere Rechnen setzen wir

$$\mathrm{ggT}(0, n) := n$$

für alle $n \in \mathbb{N}_{\geq 1}$.

Satz 10.1. *Seien $n \in \mathbb{N}_{\geq 1}, a, b \in \mathbb{Z}$. Die lineare Kongruenz*

$$a \cdot x \equiv b \pmod{n}$$

hat genau dann eine Lösung $x \in \mathbb{Z}$, wenn $\mathrm{ggT}(a, n) \mid b$.

Beweis. Sei $x \in \mathbb{Z}$ eine Lösung. Dann existiert ein $k \in \mathbb{Z}$ mit $a \cdot x - b = k \cdot n$, oder $b = a \cdot x - k \cdot n$. Nun gilt $\mathrm{ggT}(a, n) \mid a \cdot x$ und $\mathrm{ggT}(a, n) \mid k \cdot n$ und somit $\mathrm{ggT}(a, n) \mid b$. Sei umgekehrt $\mathrm{ggT}(a, n) \mid b$. Dann gibt es $\ell \in \mathbb{Z}$ mit $\ell \cdot \mathrm{ggT}(a, n) = b$. Nach Korollar 7.9 gibt es $j, k \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = j \cdot a + k \cdot n$ und damit

$$a \cdot \ell \cdot j + \ell \cdot k \cdot n = \ell \cdot \mathrm{ggT}(a, n) = b,$$

oder, mit anderen Worten

$$a \cdot \ell \cdot j \equiv b \pmod{n},$$

also ist $\ell \cdot j$ eine Lösung. □

Satz 10.2. *Seien $n \in \mathbb{N}_{\geq 1}, a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) \mid b$. Sei $x_1 \in \mathbb{Z}$ so dass $a \cdot x_1 \equiv b \pmod{n}$ (eine solche Lösung existiert nach Satz 10.1). Dann gilt*

$$\{x \in \mathbb{Z} \mid a \cdot x \equiv b \pmod{n}\} = \left\{ x_1 + k \frac{n}{\mathrm{ggT}(a, n)} \;\middle|\; k \in \mathbb{Z} \right\}.$$

Beweis. Sei zunächst $x = x_1 + k \frac{n}{\mathrm{ggT}(a,n)}$ für ein $k \in \mathbb{Z}$. Dann gilt

$$\begin{aligned} a \cdot x &\equiv a \cdot x_1 + a \cdot k \frac{n}{\mathrm{ggT}(a, n)} \pmod{n} \\ &\equiv b + \frac{a}{\mathrm{ggT}(a, n)} \cdot k \cdot n \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

Somit ist x also eine Lösung. Sei nun umgekehrt $x \in \mathbb{Z}$ eine Lösung. Dann gilt

$$a \cdot (x - x_1) \equiv 0 \pmod{n},$$

also existiert $j \in \mathbb{Z}$ mit $a \cdot (x - x_1) = j \cdot n$. Wir schreiben $a = \widetilde{a} \cdot \mathrm{ggT}(a, n)$ und $n = \widetilde{n} \cdot \mathrm{ggT}(a, n)$ mit $\widetilde{a} \in \mathbb{Z}$,$\widetilde{n} \in \mathbb{N}_{\geq 1}$. Dann gilt $\mathrm{ggT}(\widetilde{a}, \widetilde{n}) = 1$ und

$$\widetilde{a} \cdot (x - x_1) = j \cdot \widetilde{n}.$$

Somit gilt

$$\widetilde{a} = \mathrm{ggT}(\widetilde{a}, j \cdot \widetilde{n}) = \mathrm{ggT}(\widetilde{a}, j),$$

also $\widetilde{a} \mid j$ und somit gibt es $\ell \in \mathbb{Z}$ mit $\widetilde{a} \cdot \ell = j$. Hieraus ergibt sich

$$x = x_1 + \ell \cdot \widetilde{n} = x_1 + \ell \cdot \frac{n}{\mathrm{ggT}(a, n)}.$$ □

Hieraus können wir nun eine Folgerung über die Lösbarkeit von Diophantischen Gleichungen ziehen.

Korollar 10.3 (Diophantische Gleichungen)**.** *Seien $a \in \mathbb{Z}, b \in \mathbb{N}_{\geq 1}$ und $c \in \mathbb{Z}$ und betrachte die* diophantische Gleichung

$$a \cdot x + b \cdot y = c.$$

Diese Gleichung besitzt genau dann eine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, wenn $\mathrm{ggT}(a, b) \mid c$. Ist $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ eine Lösung, so ist jede weitere Lösung von der Form

$$(x, y) = \left(x_1 + k \cdot \frac{b}{\mathrm{ggT}(a, b)}, y_1 - k \cdot \frac{a}{\mathrm{ggT}(a, b)} \right)$$

für $k \in \mathbb{Z}$.

Beweis. $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ ist genau dann eine Lösung, wenn

$$a \cdot x \equiv c \pmod{b}.$$

Dann existiert nach Satz 10.1 genau dann eine Lösung $x \in \mathbb{Z}$ der Kongruenz, wenn $\mathrm{ggT}(a, b) \mid c$. Das beweist den ersten Teil. Existiert nun eine Lösung (x_1, y_1) der diophantischen Gleichung, so gilt nach Satz 10.2 für jede weitere Lösung x der Kongruenz

$$x = x_1 + k \cdot \frac{b}{\mathrm{ggT}(a, b)}$$

für ein $k \in \mathbb{Z}$. Hieraus folgt dann

$$\begin{aligned} b \cdot y &= c - a \cdot x \\ &= c - a \cdot x_1 - a \cdot k \cdot \frac{b}{\mathrm{ggT}(a, b)} \\ &= b \cdot \left(y_1 - k \cdot \frac{a}{\mathrm{ggT}(a, b)} \right) \end{aligned}$$

und somit $y = y_1 - k \cdot \frac{a}{\mathrm{ggT}(a,b)}$. □

Zum Abschluss dieses Abschnitts wollen wir uns mit Systemen linearer Kongruenzen befassen. Wir beginnen zunächst mit Frage, wie Lösungen aussehen, so welche existieren.

Satz 10.4 (Chinesischer Restsatz; Teil 1)**.** *Seien $m_1, \dots, m_n \in \mathbb{N}_{\geq 1}$ und $a_1, \dots, a_n \in \mathbb{Z}$. Existiert ein $x_1 \in \mathbb{Z}$ mit*

$$\forall i \in \{1, \dots, n\} : x_1 \equiv a_i \pmod{m_i}$$

so gilt

$$\{x \in \mathbb{Z} \mid \forall i \in \{1, \dots, n\} : x \equiv a_i \pmod{m_i}\} = \{x_1 + j \operatorname{kgV}(m_1, \dots, m_n) \mid j \in \mathbb{Z}\}.$$

Beweis. Sei zunächst $x \equiv x_1 \pmod{\operatorname{kgV}(m_1, \dots, m_n)}$. Dann existiert ein $j \in \mathbb{Z}$ so dass

$$x = x_1 + j \cdot \operatorname{kgV}(m_1, \dots, m_n).$$

Damit gilt für $i \in \{1, \dots, n\}$

$$x \equiv x_1 \equiv a_i \pmod{m_i},$$

da $m_i \mid \operatorname{kgV}(m_1, \dots, m_n)$. Sei nun umgekehrt $x \equiv a_i \pmod{m_i}$ für alle $i \in \{1, \dots, n\}$. Dann gilt $x \equiv x_1 \pmod{m_i}$, also $m_i \mid x - x_1$ für alle $i \in \{1, \dots, n\}$. Gemäß der Definition des kleinsten gemeinsamen Vielfachen folgt $\operatorname{kgV}(m_1, \dots, m_n) \mid x - x_1$, also $x \equiv x_1 \pmod{\operatorname{kgV}(m_1, \dots, m_n)}$. □

Wir kommen nun zur Existenz von Lösungen.

Satz 10.5 (Chinesischer Restsatz; Teil 2)**.** *Seien $m_1, \dots, m_n \in \mathbb{N}_{\geq 1}$ mit $\operatorname{ggT}(m_i, m_j) = 1$ für $i \neq j$. Seien weiter $a_1, \dots, a_n \in \mathbb{Z}$. Dann existiert ein $x \in \mathbb{Z}$ mit*

$$\forall i \in \{1, \dots, n\} : x \equiv a_i \pmod{m_i}.$$

Beweis. Sei $i \in \{1, \dots, n\}$ und setze $k_i \coloneqq \prod_{j \neq i} m_j$. Dann gilt $\operatorname{ggT}(k_i, m_i) = 1$. Nach Satz 10.1 existiert ein $x_i \in \mathbb{Z}$ mit

$$k_i \cdot x_i \equiv 1 \pmod{m_i}.$$

Wir setzen nun $x \coloneqq \sum_{i=1}^{n} a_i \cdot k_i \cdot x_i$. Dann gilt für $j \in \{1, \dots, n\}$, da $m_j \mid k_i$ für $i \neq j$,

$$x = \sum_{i=1}^{n} a_i \cdot k_i \cdot x_i \equiv a_j \cdot k_j \cdot x_j \equiv a_j \pmod{m_j}$$

und somit löst x das System linearer Kongruenzen. □

Der Beweis des Chinesischen Restsatzes liefert gleichzeitig eine Methode zur Berechnung der Lösung.

Beispiel 10.6. Gesucht sind alle Lösungen des Systems

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 5 \pmod{11}. \end{aligned}$$

Es gilt $m \coloneqq \mathrm{kgV}(3,7,11) = 3 \cdot 7 \cdot 11 = 231$ und $k_1 = 7 \cdot 11 = 77$, $k_2 = 3 \cdot 11 = 33$, $k_3 = 3 \cdot 7 = 21$. Es gilt

$$k_1 \cdot x_1 = 77 \cdot x_1 \equiv -x_1 \pmod 3.$$

Somit löst $x_1 \coloneqq -1$ die Kongruenz $k_1 \cdot x_1 \equiv 1 \pmod 3$. Ebenso erhalten wir

$$k_2 \cdot x_2 = 33 \cdot x_2 \equiv -2 \cdot x_2 \pmod 7$$

und damit $x_2 \coloneqq -4$ und

$$k_3 \cdot x_3 = 21 \cdot x_3 \equiv -x_3 \pmod{11}$$

und somit $x_3 \coloneqq -1$. Damit ist

$$\begin{aligned} x = \sum_{i=1}^{3} a_i \cdot k_i \cdot x_i &= 1 \cdot 77 \cdot (-1) + 3 \cdot 33 \cdot (-4) + 5 \cdot 21 \cdot (-1) \\ &= -77 - 396 - 105 \equiv 154 + 66 + 126 = 346 \equiv 115 \pmod{231} \end{aligned}$$

eine Lösung des Systems linearer Kongruenzen und die Lösungsmenge ist somit

$$\{115 + k \cdot 231 \mid k \in \mathbb{Z}\}.$$

Bemerkung 10.7. Für $m_1, \ldots, m_n \in \mathbb{N}_{\geq 2}$ mit $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$ und $m \coloneqq \prod_{i=1}^{n} m_i$ ist die Abbildung

$$\begin{aligned} f : \mathbb{Z}_m &\to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \\ [x]_{\equiv m} &\mapsto \left([x]_{\equiv m_1}, \ldots, [x]_{\equiv m_n}\right) \end{aligned}$$

bijektiv. In der Tat folgt aus Satz Satz 10.5 die Surjektivität und aus Satz Satz 10.4 die Injektivität dieser Abbildung.

11. Elementare Sätze der Zahlentheorie

Definition. Wir definieren die *Euler'sche φ-Funktion* durch

$$\begin{aligned}\varphi : \mathbb{N}_{>0} &\to \mathbb{N} \\ n &\mapsto \left|\{m \in \mathbb{N}_{<n} \mid \mathrm{ggT}(m,n) = 1\}\right|.\end{aligned}$$

Bemerkung 11.1. Ist p prim, so ist $\varphi(p) = p-1$. Für $n \in \mathbb{N}$ gilt $\varphi(n) = |\mathbb{Z}_n^*|$, die Anzahl der Einheiten in $\mathbb{Z}_n$.

Lemma 11.2. *(a) Seien $m, n \in \mathbb{N}_{>0}$ mit $\mathrm{ggT}(m,n) = 1$. Dann gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.*

(b) Sei p Primzahl und $n \in \mathbb{N}_{>0}$. Dann gilt $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Beweis. (a) Wir betrachten die Abbildung

$$\begin{aligned}f : \mathbb{Z}_{m\cdot n} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ [x]_{\equiv_{m\cdot n}} &\mapsto \left([x]_{\equiv_m}, [x]_{\equiv_n}\right).\end{aligned}$$

Diese ist nach chinesischem Restsatz bijektiv (vgl Bemerkung 10.7). Damit ist die Restriktion von f auf $\mathbb{Z}_{m\cdot n}^*$ injektiv. Wir zeigen nun

$$f\left(\mathbb{Z}_{m\cdot n}^*\right) = \mathbb{Z}_m^* \times \mathbb{Z}_n^*.$$

Es gilt für $x \in \mathbb{N}$

$$\mathrm{ggT}(x, m\cdot n) = \mathrm{ggT}(x,m) \cdot \mathrm{ggT}(x,n),$$

da $\mathrm{ggT}(m,n) = 1$. Damit ist aber

$$\begin{aligned}[x]_{\equiv_{m\cdot n}} \in \mathbb{Z}_{m\cdot n}^* &\Leftrightarrow \mathrm{ggT}(x, m\cdot n) = 1 \\ &\Leftrightarrow \mathrm{ggT}(x,m) = 1 \text{ und } \mathrm{ggT}(x,n) = 1 \\ &\Leftrightarrow \left([x]_{\equiv_m}, [x]_{\equiv_n}\right) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*\end{aligned}$$

was die Behauptung zeigt. Damit ist $f : \mathbb{Z}_{m\cdot n}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bijektiv und daher

$$\varphi(m\cdot n) = |\mathbb{Z}_{m\cdot n}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m)\cdot\varphi(n).$$

(b) Es gilt für $m \in \mathbb{N}_{<p^n}$:

$$\mathrm{ggT}(m, p^n) \neq 1 \Leftrightarrow p \mid m,$$

da jeder nichttriviale Teiler von p^n den Primfaktor p enthalten muss. Nun gilt aber

$$p \mid m \Leftrightarrow m \in \left\{0\cdot p, 1\cdot p, \ldots, (p^{n-1}-1)\cdot p\right\}.$$

Das sind genau p^{n-1} Elemente und damit gilt

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1). \qquad \square$$

Bemerkung 11.3. Über die Primfaktorzerlegung lässt scih nun $\varphi(n)$ für alle $n \in \mathbb{N}_{\geq 1}$ ausrechnen. Zum Beispiel ist

$$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5) = 2^2 \cdot (2-1) \cdot (3-1) \cdot (5-1) = 32.$$

Satz 11.4 (Satz von Euler-Fermat)**.** *Sei $n \in \mathbb{N}_{>0}$ und $a \in \mathbb{Z}$ mit* $\mathrm{ggT}(a, n) = 1$*. Dann gilt*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Beweis. Gemäß der Definition von φ existieren genau $\varphi(n)$ Zahlen $0 < r_1 < \ldots < r_{\varphi(n)} < n$ mit $\mathrm{ggT}(r_i, n) = 1$ für $i \in \{1, \ldots, \varphi(n)\}$. Demnach existiert eine Permutation $\beta : \{1, \ldots, \varphi(n)\} \to \{1, \ldots, \varphi(n)\}$ so dass $r_i \cdot r_{\beta(i)} \equiv 1 \pmod{n}$ gilt. Damit gilt

$$\prod_{i=1}^{\varphi(n)} r_i^2 = \prod_{i=1}^{\varphi(n)} r_i \cdot \prod_{i=1}^{\varphi(n)} r_{\beta(i)} \equiv 1 \pmod{n}.$$

Wir betrachten nun die Abbildung

$$\begin{aligned} \sigma : \left\{r_1, \ldots, r_{\varphi(n)}\right\} &\to \mathbb{Z}_n^* \\ r_i &\mapsto [a \cdot r_i]_{\mathrm{mod}\, n}. \end{aligned}$$

Diese ist wohldefiniert, da

$$\mathrm{ggT}(a \cdot r_i, n) = \mathrm{ggT}(r_i, n) = 1,$$

also ist $[a \cdot r_i]_{\mathrm{mod}\, n}$ eine Einheit in $\mathbb{Z}_n$. Außerdem ist σ injektiv, denn es gilt

$$\sigma(r_i) = \sigma(r_j) \Leftrightarrow a \cdot r_i \equiv a \cdot r_j \pmod{n} \Leftrightarrow a \cdot (r_i - r_j) \equiv 0 \pmod{n}.$$

Da $\mathrm{ggT}(a, n) = 1$ folgt wiederum, dass $[a]_{\mathrm{mod}\, n} \in \mathbb{Z}_n^*$ also invertierbar ist und daher gilt folgt $r_i - r_j \equiv 0 \pmod{n}$. Da $0 < r_i, r_j < n$, folgt hieraus $r_i = r_j$ und somit die Injektivität von σ. Da $|\mathbb{Z}_n^*| = \varphi(n)$, ist σ auch surjektiv nach Satz 8.5. Da außerdem $[r_i]_{\mathrm{mod}\, n} \in \mathbb{Z}_n^*$ für alle $i \in \{1, \ldots, \varphi(n)\}$ existiert zu jedem $j \in \{1, \ldots, \varphi(n)\}$ genau ein $i \in \{1, \ldots, \varphi(n)\}$ mit

$$a \cdot r_i \equiv r_j \pmod{n}$$

und somit ist

$$\prod_{i=1}^{\varphi(n)} a \cdot r_i \equiv \prod_{j=1}^{\varphi(n)} r_j.$$

Damit gilt

$$a^{\varphi(n)} \equiv a^{\varphi(n)} \cdot \prod_{i=1}^{\varphi(n)} r_i^2 \equiv \left(\prod_{i=1}^{\varphi(n)} a \cdot r_i\right)\left(\prod_{i=1}^{\varphi(n)} r_i\right) \equiv \prod_{i=1}^{\varphi(n)} r_i^2 \equiv 1 \pmod{n}. \qquad \square$$

Korollar 11.5 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl und $a \in \mathbb{Z}$. Dann gilt*

$$a^p \equiv a \pmod{p}.$$

Beweis. Da p prim ist, gilt entweder $\mathrm{ggT}(|a|, p) = 1$ oder $\mathrm{ggT}(|a|, p) = p$. Für den Fall, dass $\mathrm{ggT}(|a|, p) = 1$ folgt aus Satz 11.4

$$a^p = a \cdot a^{p-1} = a \cdot a^{\varphi(p)} \equiv a \pmod{p}.$$

Ist $\mathrm{ggT}(|a|, p) = p$, so gilt $a = k \cdot p$ für ein $k \in \mathbb{Z}$. Damit gilt

$$a^p = k^p \cdot p^p \equiv 0 \equiv a \pmod{p}. \qquad \square$$

Satz 11.6 (Satz von Wilson)**.** *Sei $p \in \mathbb{N}_{\geq 2}$. Ist p prim so gilt $(p-1)! \equiv -1 \pmod{p}$. Ist p nicht prim, so gilt* $(p-1)! \equiv \begin{cases} 2 & \text{falls } p = 4, \\ 0 & \text{sonst} \end{cases} \pmod{p}$.

Beweis. Sei p prim. Wir betrachten die Fälle $p = 2$ und $p = 3$ gesondert. Es gilt

$$(2-1)! = 1 \equiv -1 \pmod{2}$$

und

$$(3-1)! = 2 \equiv -1 \pmod{3}.$$

Sei also nun $p \geq 5$ prim. Dann ist nach Korollar 8.6 $\mathbb{Z}_p$ ein Körper. Demnach existiert zu jedem $[a]_{\mathrm{mod}\, p} \in \mathbb{Z}_p \setminus \{0\}$ genau ein $[k]_{\mathrm{mod}\, p} \in \mathbb{Z}_p \setminus \{0\}$ mit $a \cdot k \equiv 1 \pmod{p}$. Nun gilt $a \equiv k \pmod{p}$ genau dann wenn $a^2 \equiv 1 \pmod{p}$, was äquivalent ist zu

$$0 \equiv a^2 - 1 \equiv (a-1) \cdot (a+1) \pmod{p}.$$

Da $\mathbb{Z}_p$ nullteilerfrei ist, folgt $a \equiv 1$ oder $a \equiv -1 \pmod{p}$. Wir betrachten nun die Menge $M \coloneqq \mathbb{Z}_p \setminus \{0, -1, 1\}$ und erhalten $|M| = p - 3$. Ferner lässt sich M in $\frac{p-3}{2}$ Paare der Form $([a]_{\mathrm{mod}\, p}, [a]^{-1}_{\mathrm{mod}\, p})$ zerlegen (beachte, $[a]_{\mathrm{mod}\, p} \neq [a]^{-1}_{\mathrm{mod}\, p}$). Somit gilt

$$\prod_{[a]_{\mathrm{mod}\, p} \in M} [a]_{\mathrm{mod}\, p} = [1]_{\mathrm{mod}\, p}.$$

Insbesondere folgt

$$2 \cdot \ldots \cdot p - 2 \equiv 1 \pmod{p}$$

und da $p - 1 \equiv -1 \pmod{p}$ folgt

$$(p-1)! \equiv -1 \pmod{p}.$$

Sei nun p nicht prim. Wir unterscheiden folgende Fälle:

(A) $p = m \cdot n$ mit $m < n$. Dann gilt wegen $1 < m < n < p$, dass $m \cdot n \mid (p-1)!$ und daher $(p-1)! \equiv m \cdot n = p \equiv 0 \pmod{p}$.

(B) $p = m^2$ für m prim. Ist $m \geq 3$, so folgt $0 < m < 2m^{k-1} < m^k = p$ und daher $2p = 2m^k = 2m^{k-1} \cdot m \mid (p-1)!$ und somit $(p-1)! \equiv 2p \equiv 0 \pmod{p}$. Für den Fall $m = 2$, also $p = 4$ gilt

$$(p-1)! = 3! = 6 \equiv 2 \pmod{4}. \qquad \square$$

Satz 11.7 (Satz von Euler)**.** *Sei p eine ungerade Primzahl. Dann existiert $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod{p}$ genau dann wenn $p \equiv 1 \pmod{4}$.*

Beweis. Sei $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod{p}$. Dann gilt $\mathrm{ggT}(x,p) = 1$ (sonst wäre $x^2 \equiv 0$) und somit ist einerseits

$$x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und andererseits nach Satz 11.4

$$x^{p-1} \equiv 1 \pmod{p}.$$

Damit ist also

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und damit gilt $p \mid \left(1 - (-1)^{\frac{p-1}{2}}\right)$. Ist $\frac{p-1}{2}$ ungerade, so gilt $1 - (-1)^{\frac{p-1}{2}} = 1 - (-1) = 2$, und damit $p \mid 2$, was zum Widerspruch führt. Somit ist also $\frac{p-1}{2}$ gerade, also ist

$$\frac{p-1}{2} = 2 \cdot k$$

für ein $k \in \mathbb{N}$ und daher

$$p - 1 = 4 \cdot k \equiv 0 \pmod{4}.$$

Sei nun umgekehrt $p \equiv 1 \pmod{4}$. Dann ist $\frac{p-1}{2}$ gerade und es gilt

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-1) \\
&= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdot \ldots \cdot (p-1) \\
&\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \left(-\frac{p-3}{2}\right) \cdot \ldots \cdot (-2) \cdot (-1) \pmod{p} \\
&\equiv \underbrace{(-1)^{\frac{p-1}{2}}}_{=1} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.
\end{aligned}$$

Andererseits ist nach Satz 11.6 $(p-1)! \equiv -1 \pmod{p}$ und somit

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$ □

Korollar 11.8. *Es existieren unendlich viele Primzahlen p mit $p \equiv 1 \pmod{4}$.*

Beweis. Angenommen, es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$ mit $p_i \equiv 1 \pmod{4}$. Wir setzen $k \coloneqq \left(\prod_{i=1}^{n} p_i\right)^2 + 1 \in \mathbb{N}$. Sei p ein Primteiler von k. Dann ist insbesondere $p \neq p_i$ für alle $i \in \{1, \ldots, n\}$. Außerdem gilt $k \equiv 0 \pmod{p}$ und somit

$$\left(\prod_{i=1}^{n} p_i\right)^2 \equiv -1 \pmod{p}.$$

Damit gilt aber nach Satz 11.7 $p \equiv 1 \pmod{4}$, was zum Widerspruch führt. □