Kapitel 3

Die ganzen Zahlen

3.1 Konstruktion und Arithmetik

Lemma 3.1. *Auf* $\mathbb{N}_0 \times \mathbb{N}_0$ *wird durch*

$$(m,n) \sim (j,k) : \Longleftrightarrow \; m+k = n+j$$

eine Äquivalenzrelation definiert.

Beweis. Übung □

Jede Äquivalenzrelation S auf einer Menge X zerlegt die Menge X in paarweise disjunkte, nicht leere Teilmengen der Form

$$[x] := \{y \in X;\, ySx\} \qquad (x \in X),$$

die so genannten Äquivalenzklassen. $[x]$ heißt Äquivalenzklasse von x, und x heißt Repräsentant von $[x]$. Die Menge aller Äquivalenzklassen bezeichnen wie üblich mit X/S. (Vergleiche dazu Definition 1.24b.)

Definition 3.2. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist definiert durch

$$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0)/\sim \; \equiv \big\{[(m,n)];(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0\big\},$$

wobei $\sim$ wie in Lemma 3.1 definiert ist.

Wir führen jetzt auf $\mathbb{Z}$ eine Addition $\oplus$ und eine Multiplikation $\odot$ ein durch

$$[(j,k)] \oplus [(m,n)] := [(j+m, k+n)], \tag{3.1}$$

$$[(j,k)] \odot [(m,n)] := [(jm+kn, km+jn)]. \tag{3.2}$$

Lemma 3.3. *Die oben eingeführten Verknüpfungen* $\oplus$ *und* $\odot$ *auf* $\mathbb{Z}$ *sind wohldefiniert, d. h. sie sind unabhängig von der Wahl der Repräsentanten.*

Beweis. Wie beweisen die Unabhängigkeit von den Repräsentanten für die Addition. Seien dazu $[(j,k)] = [(j',k')]$ und $[(m,n)] = [(m',n')]$, dann ist zu zeigen

$$[(j,k)] \oplus [(m,n)] = [(j',k')] \oplus [(m',n')].$$

Nun gilt $(j,k) \sim (j',k')$, d. h. $j+k' = k+j'$ und wegen $(m,n) \sim (m',n')$ gilt $m+n' = n+m'$. Damit ist $(j+m)+(k'+n') = (k+n)+(j'+m')$, also $(j+m,k+n) \sim (j'+m',k'+n')$. Daraus folgt aber wie gewünscht

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

Rest Übung. □

Wir wissen bisher nur, dass $\oplus$ und $\odot$ innere Verknüpfungen auf $\mathbb{Z}$ sind Bevor wir aber ihre Eigenschaften näher untersuchen, wollen wir die zugehörigen Begriffe aus der Algebra einführen.

Definition 3.4. Sei R eine Menge, auf der zwei innere Verknüpfungen $+$ und $\cdot$ definiert sind. $(R,+,\cdot)$ heißt *Ring*, wenn $(R,+)$ eine abelsche Gruppe, $(R,\cdot)$ eine Halbgruppe ist und die *Distributivgesetze*

$$a\cdot(b+c) = (a\cdot b)+(a\cdot c), \quad (a+b)\cdot c = (a\cdot c)+(b\cdot c) \qquad (a,b,c \in R)$$

gelten. Man nennt R *kommutativ*, wenn $(R,\cdot)$ abelsch ist, und *unitär*, wenn $\#R > 1$ und $(R,\cdot)$ ein Monoid ist. R heißt *nullteilerfrei*, wenn aus $a\cdot b \in R$ mit $a\cdot b = 0$ folgt $a = 0$ oder $b = 0$.

Sind $(R,+,\cdot)$ und $(R',+',\cdot')$ Ringe, so heißt eine Abbildung $\varphi\colon R \to R'$ ein *Ringhomomorphismus*, wenn gilt

$$\varphi(a+b) = \varphi(a) +' \varphi(b) \text{ und } \varphi(a\cdot b) = \varphi(a)\cdot'\varphi(b) \qquad (a,b \in R). \tag{3.3}$$

In der Regel benutzt man dieselbe Notation für die Addition auf R und R' und ebenso für die Multiplikation auf R und R'. Man spricht also von zwei Ringen $(R,+,\cdot)$ und $(R',+,\cdot)$ oder kurz von zwei Ringen R und R'. Gleichung (3.3) hat dann die Form

$$\varphi(a+b) = \varphi(a)+\varphi(b) \text{ und } \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b) \qquad (a,b \in R).$$

Das neutrale Element der Addition nennt man *Nullelement*. Es wird grundsätzlich mit 0 bezeichnet. Das inverse Element von a bezüglich der Addition wird üblicherweise mit $-a$ bezeichnet und das neutrale Element bezüglich der Multiplikation, das so genannte *Einselement*, mit 1. Wenn in einem Ring mit Einselement zu $a \in R$ ein Element $b \in R$ existiert mit $a\cdot b = b\cdot a = 1$, dann heißt b inverses Element bezüglich der Multiplikation und wird mit a^{-1} bezeichnet.

Wie schon beim Rechnen in $\mathbb{N}_0$ schreibt man auch hier meistens ab anstelle von $a\cdot b$ und vereinbart „Punktrechnung geht vor Strichrechnung“.

Bemerkung 3.5. Ein Ringhomomorphismus $\varphi\colon R \to R'$ bildet das Nullelement in R auf das Nullelement in R' ab und für die Inversen gilt $\varphi(-a) = -\varphi(a)$.

In einem unitären Ring R sind analog zu Definition 2.17 die *Potenzen* erklärt.

Definition 3.6. Sei R ein unitärer Ring. Für $a \in R$ und $n \in \mathbb{N}_0$ ist die Potenz $a^n \in R$ definiert durch

$$a^0 := 1, \quad a^{n+1} := a^n \cdot a.$$

Bemerkung 3.7. In einem Ring R definiert man die Subtraktion $a - b$ für beliebige $a, b \in R$ durch $a - b := a + (-b)$. Im Gegensatz zur Subtraktion auf $\mathbb{N}_0$ (vgl. Bemerkung 2.20b) ist die Subtraktion auf einem Ring eine innere Verknüpfung.

Die wichtigsten Rechenregeln in Ringen sind im folgenden Lemma zusammengestellt:

Lemma 3.8. *In einem Ring R gelten für $a, b, c \in R$ die folgenden Regeln:*

(i) $a + c = b + c \implies a = b$ *(Kürzungsregel der Addition).*

(ii) *Die Gleichung $a + x = b$ hat genau eine Lösung $x \in R$, nämlich $x = b + (-a)$.*

(iii) $-0 = 0$, $-(-a) = a$, $-(a + b) = (-a) + (-b)$,

(iv) $a \cdot 0 = 0 \cdot a = 0$,

(v) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$,

(vi) $(-a) \cdot (-b) = a \cdot b$.

Beweis. Übung □

In einem unitären Ring R gilt immer $1 \neq 0$. Wäre nämlich $1 = 0$, dann folgte für jedes $a \in R$ nach Lemma 3.8(iv) $0 = 0 \cdot a = 1 \cdot a = a$, d. h. $\mathbb{R} = \{0\}$. Dies ist aber nach Definition eines unitären Rings ausgeschlossen.

Für die Potenzen haben wir analog zu Folgerung 2.18

Folgerung 3.9. *In einem Ring R gelten für alle $a, b \in R$, $k, n \in \mathbb{N}_0$ die Potenzgesetze:*

(i) $a^n a^k = a^{n+k}$,

(ii) $a^n b^n = (ab)^n$.

(iii) $(a^n)^k = a^{nk}$.

Nun betrachten wir $\mathbb{Z}$ mit den beiden inneren Verknüpfungen $\oplus$ und $\odot$.

Satz 3.10. $(\mathbb{Z}, \oplus, \odot)$ *ist ein kommutativer, unitärer Ring mit Nullelement* $[(0,0)]$. *Die inversen Elemente bezüglich der Addition sind gegeben durch* $-[(m,n)] = [(n,m)]$ *und das Einselement ist* $[(1,0)]$. *Die Gruppe* $(\mathbb{Z}, \oplus)$ *wird von* $\big\{[(n,0)]; n \in \mathbb{N}_0\big\}$ *erzeugt und es gibt eine disjunkte Zerlegung*

$$\mathbb{Z} = \big\{[(n,0)]; n \in \mathbb{N}_0\big\} \cup \big\{ -[(n,0)]; n \in \mathbb{N}\big\}. \tag{3.4}$$

Beweis. Aus Satz 2.13 folgt für alle $m, m', m'', n, n', n'' \in \mathbb{N}$:
Assiziativgesetz:

$$\begin{aligned}\big([(m,n)] + [(m',n')]\big) + [(m'',n'')] &= \big[\big((m+m') + m'', (n+n') + n''\big)\big] \\ &= \big[\big(m + (m' + m''), n + (n' + n'')\big)\big] \\ &= [(m,n)] + \big([(m',n')] + [(m'',n'')]\big),\end{aligned}$$

Kommutativgesetz:

$$[(m,n)]+[(m',n')]=[(m+m',n+n')]=[(m'+m,n'+n)]=[(m',n')]+[(m,n)],$$

Neutrales Element der Addition:

$$[(m,n)]+[(0,0)]=[(m+0,n+0)]=[(m,n)]..$$

Inverse Elemente bezüglich der Addition:

$$[(m,n)]+[(n,m)]=[(m+n,n+m)]=[(0,0)].$$

Demnach ist $(\mathbb{Z},\oplus)$ eine abelsche Gruppe. Ebenso ergibt sich aus Satz 2.16 für die Multiplikation:

Assiziativgesetz:

$$\begin{aligned}
&[(m,n)]\cdot\big([(m',n')]\cdot[(m'',n'')]\big)\\
&=[(m,n)]\cdot[(m'm''+n'n'',m'n''+n'm'')]\\
&=\big[\big(m(m'm'')+m(n'n'')+n(m'n'')+n(n'm''),m(m'n'')+m(n'm'')+n(m'm'')+n(n'n'')\big)\big]\\
&=\big[\big((mm')m''+(mn)'n''+(nm')n''+(nn')m'',(mm')n''+(mn')m''+(nm')m''+(nn')n''\big)\big]\\
&=[(mm'+nn',mn'+nm')]\cdot[(m'',n'')]\\
&=\big([(m,n)]\cdot[(m',n')]\big)\cdot[(m'',n'')].
\end{aligned}$$

Kommutativgesetz:

$$\begin{aligned}
[(m,n)]\cdot[(m',n')]&=[(mm'+nn',mn'+nm')]\\
&=[(m'm+n'n,n'm+m'n)]=[(m',n')]\cdot[(m,n)].
\end{aligned}$$

Distributivgesetz:

$$\begin{aligned}
&[(m,n)]\cdot([(m',n')]+[(m'',n'')])=[(m,n)]\cdot[(m'+m'',n'+n'')]\\
&=[(m(m'+m'')+n(n'+n''),m(n'+n'')+n(m'+m''))]\\
&=[(mm'+nn',mn'+nm')]+[(mm''+nn'',mn''+nm'')]\\
&=([(m,n)]\cdot[(m',n')])+([(m,n)]\cdot[(m'',n'')]).
\end{aligned}$$

Einselement:

$$[(n,m)]\cdot[(1,0)]=[(n\cdot1+m\cdot0,n\cdot0+m\cdot1)]=[(n,m)].$$

Folglich ist $\mathbb{Z}$ ein kommutativer, unitärer Ring.

Disjunkte Zerlegung (3.4): Für $[(j,k)]\in\mathbb{Z}$ mit $j,k\in\mathbb{N}_0$ tritt nach Satz 2.25 genau einer der beiden folgenden Fälle ein:

$$(ii)\ j\geq k\qquad(ii)\ j<k.$$

Zu (i): Ist $j\geq k$, dann existiert ein $x\in\mathbb{N}_0$ mit $j=k+x$, d. h. $j+0=k+x$, und damit ist $(j,k)\sim(x,0)$. Es gilt also $[(j,k)]=[(x,0)]\in\big\{[(n,0)];n\in\mathbb{N}_0\big\}$.

Zu (ii): $j < k$ bedeutet $j + x = k$ für ein $x \in \mathbb{N}$ und es folgt wie unter (i), dass $[(j,k)] = [(0,x)] = -[(x,0)] \in \big\{ -[(n,0)]; n \in \mathbb{N}\big\}$.

Damit ist $\mathbb{Z} \subset \big\{[(n,0)]; n \in \mathbb{N}_0\big\} \cup \big\{-[(n,0)]; n \in \mathbb{N}\big\}$ gezeigt. Die umgekehrte Inklusion ist klar.

Erzeuger von $(\mathbb{Z}, \oplus)$: Sei G eine beliebige Untergruppe von $(\mathbb{Z}, \oplus)$ mit $\big\{[(n,0)]; n \in \mathbb{N}_0\big\} \subset G$. Wegen $[(n,0)] \in G$ für alle $n \in \mathbb{N}$ müssen auch die inversen Elemente $-[(n,0)]$ für alle $n \in \mathbb{N}$ zu G gehören. Es gilt also $\big\{[(n,0)]; n \in \mathbb{N}_0\big\} \cup \big\{-[(n,0)]; n \in \mathbb{N}\big\} \subset G \subset \mathbb{Z}$ und mit (3.4) folgt $G = \mathbb{Z}$. □

Bemerkung 3.11. Die Gruppe $(\mathbb{Z}, \oplus)$ wird auch von $\big\{[(n,0)]; n \in \mathbb{N}\big\}$ erzeugt. Eine etwas andere Form der Zerlegung (3.4) ist

$$\mathbb{Z} = \big\{[(n,0)]; n \in \mathbb{N}\big\} \cup \{[(0,0)]\} \cup \big\{ -[(n,0)]; n \in \mathbb{N}\big\},$$

wobei die drei Mengen paarweise disjunkt sind.

Einbettung von $\mathbb{N}_0$ in $\mathbb{Z}$.

Gesucht ist ein Ersatz für $\mathbb{N}_0 \subset \mathbb{Z}$.

Lemma 3.12. *Die Abbildung* $\Phi\colon \mathbb{N}_0 \to \mathbb{Z}$, $n \mapsto [(n,0)]$ *ist injektiv und erfüllt für alle* $m, n \in \mathbb{N}_0$

(*i*) $\Phi(m+n) = \Phi(m) \oplus \Phi(n)$,

(*ii*) $\Phi(m \cdot n) = \Phi(m) \odot \Phi(n)$.

Beweis. Übung □

Bemerkungen 3.13. a) Aufgrund von Lemma 3.12 identifiziert man $m \in \mathbb{N}_0$ mit $\Phi(m) \in \mathbb{Z}$ und $\mathbb{N}_0$ mit $\Phi(\mathbb{N}_0) = \{[(n,0)]; n \in \mathbb{N}_0\}$. Man schreibt deshalb etwas ungenau, aber einprägsam $\mathbb{N}_0 \subset \mathbb{Z}$ anstelle von $\Phi(\mathbb{N}_0) \subset \mathbb{Z}$.

Sind $m, n \in \mathbb{N}_0$, dann kann man einmal $m + m$ im Sinne von Definition 2.11 in $\mathbb{N}_0$ bilden. Andererseits kann man auch $\Phi(m) \oplus \Phi(n)$ im Sinne von (3.1) in $\mathbb{Z}$ bilden. Wenn man nun m, n und $m + n$ mit $\Phi(m)$, $\Phi(n)$ bzw. $\Phi(m) \oplus \Phi(n)$ identifiziert, dann gilt nach Lemma 3.12(i) $m + n = m \oplus n$. Es spielt also keine Rolle, ob man m und n als Elemente von $\mathbb{N}_0$ auffasst und in $\mathbb{N}_0$ addiert oder als Elemente von $\mathbb{Z}$ auffasst und in $\mathbb{Z}$ addiert.

Deshalb werden wir im Folgenden $a \oplus b$ durch die einfachere Schreibweise $a + b$ ersetzen. Gehört mindestens einer der beiden Summanden a oder b zu $\mathbb{Z} \setminus \mathbb{N}_0$ dann ist $+$ als $\oplus$ zu lesen. Gilt dagegen $a, b \in \mathbb{N}_0$, dann ist Unterscheidung zwischen $+$ und $\oplus$ ist nicht notwendig. Dasselbe gilt natürlich auch für die Multiplikation, wo wir ab sofort nur noch $a \cdot b$ oder kürzer ab verwenden.

b) Die oben gemachten Aussagen zur Addition und Multiplikation lassen sich auch auf die Subtraktion ausdehnen. Für $m, n \in \mathbb{N}_0$ mit $m \leq n$ haben wir in Bemerkung 2.20b die Subtraktion definiert durch $n - m = x$, wobei $x \in \mathbb{N}_0$ eindeutig durch die Gleichung $m + x = n$ bestimmt ist. Für $\Phi(m), \Phi(n) \in \Phi(\mathbb{N}_0) \subset \mathbb{Z}$ ist die die Subtraktion nach

Bemerkung 3.7 durch $\Phi(n) - \Phi(m) := \Phi(n) + (-\Phi(m))$ definiert. Zwischen diesen beiden Definitionen besteht nun der folgende Zusammenhang

$$\begin{aligned}\Phi(n-m) = \Phi(x) &= \Phi(x) + \big(\Phi(m) + (-\Phi(m))\big)\\ &= \big(\Phi(x) + \Phi(m)\big) + (-\Phi(m)) = \Phi(x+m) + (-\Phi(m))\\ &= \Phi(n) + (-\Phi(m)) = \Phi(n) - \Phi(m).\end{aligned}$$

Es gilt also zusätzlich zu den Aussagen von Lemma 3.12

$$\Phi(n-m) = \Phi(n) - \Phi(m) \qquad (m, n \in \mathbb{N}_0, m \le n).$$

Wir haben stillschweigend von Beginn an für die Subtraktion in $\mathbb{N}_0$ und und $\mathbb{Z}$ dasselbe Symbol benutzt, obwohl das genau genommen erst jetzt gerechtfertigt ist.

3.2 Anordnung

Wir definieren jetzt auf $\mathbb{Z}$ eine Kleiner-oder-gleich-Relation $\circledleq$ durch

$$[(j,k)] \circledleq [(m,n)] :\iff j + n \le k + m.$$

Lemma 3.14. *a) Die Kleiner-oder-gleich-Relation $\circledleq$ auf $\mathbb{Z}$ ist wohldefiniert, d. h. sie ist unabhängig von der Wahl der Repräsentanten.*

b) Durch $\circledleq$ wird eine totale Ordnung im Sinne von Definition 1.61 auf $\mathbb{Z}$ definiert.

Beweis. Übung □

Bemerkung 3.15. Die zu $\circledleq$ gehörende strenge Ordnug $\circledless$ auf $\mathbb{Z}$ erfüllt demnach für alle $a, b \in \mathbb{Z}$ genau eine der drei Beziehungen (vgl. Lemma 1.62(iii))

$$a \circledless b, \quad a = b, \quad b \circledless a.$$

Lemma 3.16. *Die Abbildung $\Phi\colon \mathbb{N}_0 \to \mathbb{Z}$ aus Lemma 3.12 erfüllt außerdem*

(iii) $m \le n \iff \Phi(m) \circledleq \Phi(n)$,

(iv) $m < n \iff \Phi(m) \circledless \Phi(n)$.

Wir benutzen deshalb auch hier ab sofort die vereinfachte Schreibweise $\le$ und $<$ statt $\circledleq$ und $\circledless$ (vgl. Bemerkungen 3.13).

Definition 3.17. Sei $(R, +, \cdot)$ ein Ring und $\le$ eine totale Ordnung auf R sowie $<$ die zugehörige strenge Ordnung. Man nennt $<$ eine *Anordnung von R* oder $(R, <)$ einen *angeordneten Ring*, wenn für alle $a, b, c \in R$ gilt:

(i) $a < b \implies a + c < b + c$,

(ii) $a < b \wedge 0 < c \implies ac < bc \wedge ca < cb$.

Die Anordnung heißt *archimedisch*, wenn es zu allen $a, b \in R$ mit $a > 0, b > 0$ ein $n \in \mathbb{N}$ gibt mit $na > b$. Dabei ist $na \in R$ rekursiv definiert durch

$$0a := 0, \quad (n+1)a := na + a \quad (n \in \mathbb{N}_0).$$

In dieser Definition wird also verlangt, dass die arithmetische Struktur und die Ordnungsstruktur des Ringes miteinander verträglich sind. Die Elemente $a \in R$ mit $a > 0$ nennt man *positiv*, die mit $a < 0$ nennt man *negativ*. Weiter Eigenschaften eines angeordneten Ringes sind im folgenden Lemma zusammengestellt.

Lemma 3.18. *In einem angeordneten, unitären Ring $(R, <)$ gilt für alle $a, b, c, d \in R$:*

(i) $a < b \iff -b < -a$,

(ii) $a < b \wedge c < d \implies a + c < b + d$,

(iii) $0 \leq a < b \wedge 0 \leq c < d \implies ac < bd$,

(iv) $a < b \wedge c < 0 \implies ac > bc \wedge ca > cb$.

(v) *Es gilt $a^2 > 0$ für alle $a \in R$, $a \neq 0$. Speziell ist $1 > 0$.*

(vi) *Sei $0 < a < b$, so dass die inversen Elemente bezüglich der Multiplikation $a^{-1} \in R$ und $b^{-1} \in R$ existieren. Dann gilt $0 < b^{-1} < a^{-1}$.*

(vii) *R ist nullteilerfrei, d. h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$.*

Beweis. (vi): Die inversen Elemente der Multiplikation sind durch die Gleichungen $a^{-1}a = aa^{-1} = 1$ definiert. Aus $a^{-1} < 0$ würde $1 = aa^{-1} < a \cdot 0 = 0$ im Widerspruch zu (v) folgen. Also hat man $a^{-1} > 0$ und ebenso $b^{-1} > 0$. Mit Definition 3.17(ii) ergibt sich dann $a^{-1}a < a^{-1}b$ und weiter $(a^{-1}a)b^{-1} < (a^{-1}b)b^{-1}$ sowie

$$b^{-1} = (a^{-1}a)b^{-1} < (a^{-1}b)b^{-1} = a^{-1}(bb^{-1}) = a^{-1}.$$

(vii): Sind $a \neq 0$ und $b \neq 0$, so folgt $a > 0$ oder $a < 0$ und $b > 0$ oder $b < 0$. Man erhält damit $ab > 0$ oder $ab < 0$ aus Definition 3.17(ii) bzw. Aussage (iv) dieses Lemmas. In jedem Fall gilt $ab \neq 0$.

Rest Übung □

Aus den Rechenregeln für die strenge Ordnung $<$ ergeben sich unmittelbar die folgenden Eigenschaften der zugehörigen schwachen Ordnung.

Folgerung 3.19. *Sei $(R, <)$ ein angeordneter, unitärer Ring und $\leq$ die zugehörige schwache Ordnung, dann gilt für alle $a, b, c, d \in R$:*

(i) $a \leq b \implies a + c \leq b + c$,

(ii) $a \leq b \wedge 0 \leq c \implies ac \leq bc \wedge ca \leq cb$.

(iii) $a \leq b \iff -b \leq -a$,

(iv) $a \leq b \wedge c \leq d \implies a + c \leq b + d$,

(v) $0 \leq a \leq b \wedge 0 \leq c \leq d \implies ac \leq bd$,

(vi) $a \leq b \wedge c \leq 0 \implies ac \geq bc \wedge ca \geq cb$.

(vii) *Es gilt $a^2 \geq 0$ für alle $a \in R$.*

In einem angeordneten Ring kann man den Betrag eines Ringelementes definieren.

Definition 3.20. Sei $(R, <)$ ein angeordneter Ring. Für $a \in R$ definiert man den *Betrag* $|a| \in R$ durch

$$|a| := \begin{cases} a, & a \geq 0, \\ -a, & a < 0. \end{cases}$$

Lemma 3.21. *Sei $(R, <)$ ein angeordneter, unitärer Ring. Für alle $a, b \in R$ gilt:*

(i) $|a| \geq 0$,

(ii) $|-a| = |a|$,

(iii) $-|a| \leq a \leq |a|$, $-|a| \leq -a \leq |a|$,

(iv) $|a| = 0 \iff a = 0$.

(v) *Ist $b \geq 0$, dann gilt* $|a| \leq b \iff -b \leq a \leq b$

(vi) $|ab| = |a| \cdot |b|$,

(vii) $|a^{-1}| = |a|^{-1}$, *falls $a^{-1} \in R$ existiert,*

(viii) $|a + b| \leq |a| + |b|$ *(Dreiecksungleichung),*

(ix) $|a - b| \geq \big||a| - |b|\big|$.

Beweis. Wir benutzen hier die Rechenregeln in Ringen (Lemma 3.8) ohne im Einzelnen darauf hinzuweisen. (i), (ii) beweist man durch Fallunterscheidung $a \geq 0$ und $a < 0$ mittels der Definition des Betrags und Lemma 3.18(i). Ebenso erhält man die Ungleichung $a \leq |a|$ in (iii). Ersetzt man man hierin a durch $-a$, so folgt mit (ii) $-a \leq |-a| = |a|$. Damit sind zwei der vier Ungleichungen bewiesen. Wendet man auf diese Folgerung 3.19(iii) an, so erhält man auch noch die restlichen beiden.

(iv): Ist $|a| = 0$, so gilt nach (iii) $0 = -0 = -|a| \leq a \leq |a| = 0$ und aus der Antisymmetrie von $\leq$ folgt $a = 0$. Die umgekehrte Richtung ist klar.

(v): Sei $|a| \leq b$. Nach Folgerung 3.19(iii) gilt $-b \leq -|a|$, und aus (iii) folgt dann $-b \leq -|a| \leq a \leq |a| \leq b$, d. h. es ist $-b \leq a \leq b$. Gilt umgekehrt $-b \leq a \leq b$, dann gilt nach Folgerung 3.19(iii) auch $-b \leq -a \leq b$. Für $a \geq 0$ ist nun $|a| = a \leq b$ und für $a < 0$ ist $|a| = -a \leq b$, so dass in beiden Fällen $|a| \leq b$ gilt.

(vi): Man unterscheidet die vier Fälle

$$a \geq 0 \wedge b \geq 0, \quad a \geq 0 \wedge b < 0, \quad a < 0 \wedge b \geq 0, \quad a < 0 \wedge b < 0$$

unter Verwendung von Folgerung 3.19(v).

(vii): Aus $1 = |1| = |a \cdot a^{-1}| = |a| \cdot |a^{-1}|$ und $1 = |1| = |a^{-1} \cdot a| = |a^{-1}| \cdot |a|$ ergibt sich mit der Definition der inversen Elemente $|a^{-1}| = |a|^{-1}$.

(viii): Aus $a \leq |a|$ und $b \leq |b|$ folgt $a + b \leq |a| + |b|$. Wegen $-|a| \leq a$ und $-|b| = b$ (nach (iii)) hat man auch $-(|a| + |b|) = -|a| + (-|b|) \leq a + b$. Daraus erhält man $|a + b| \leq |a| + |b|$ mit (v).

(ix): Aus (viii) und (ii) ergibt sich

$$|b| + |a - b| \geq |b + (a - b)| = |a|, \quad |a| + |a - b| = |a| + |b - a| \geq |a + (b - a)| = |b|.$$

Also hat man $|a-b| \geq |a|-|b|$ und $|a-b| \geq |b|-|a| = -(|a|-|b|)$. Daraus folgt $|a-b| \geq \big||a|-|b|\big|$ mit (v). □

Wir beweisen noch zwei Folgerungen aus der archimedischen Eigenschaft in Definition 3.17.

Lemma 3.22. *Sei $(R,<)$ ein archimedisch angeordneter, unitärer Ring.*
a) Für alle $a \in R$ mit $a \geq -1$ und alle $n \in \mathbb{N}_0$ gilt die Bernoullische *Ungleichung*

$$(1+a)^n \geq 1+na.$$

b) Zu $a \in R, a > 1$ und $b \in R$ existiert ein $n \in \mathbb{N}$ mit $a^n > b$.

Beweis. a) Wir verwenden eine Induktion nach n, wobei $n = 0$ trivial ist. Sei nun $(1+a)^n \geq 1+na$ für ein $n \in \mathbb{N}$, dann folgt wegen $1+a \geq 0$ und $a^2 \geq 0$ (Folgerung 3.19)

$$\begin{aligned}(1+a)^{n+1} &= (1+a)^n \cdot (1+a) \geq (1+na)\cdot(1+a)\\ &= 1+(n+1)a+a^2 \geq 1+(n+1)a.\end{aligned}$$

b) Wegen $a-1 > 0$ existiert aufgrund der archimedischen Eigenschaft ein $n \in \mathbb{N}$ mit $n(a-1) > b$. Aus a) folgt nun

$$a^n = (1+(a-1))^n \geq 1+n(a-1) > n(a-1) > b.$$ □

Nach den theoretischen Grundlagen der angeordneten Ringe kommen wir nun zur Anwendung auf $\mathbb{Z}$.

Satz 3.23. *$(\mathbb{Z},<)$ ist ein archimedisch angeordneter Ring. Für alle $a,b \in \mathbb{Z}$ gilt*

(i) $a \leq b \iff b-a \in \mathbb{N}_0$,

(ii) $a < b \iff b-a \in \mathbb{N}$.

Weiter gilt

(iii) $\mathbb{N}_0 = \{a \in \mathbb{Z}; a \geq 0\}$,

(iv) $\mathbb{N} = \{a \in \mathbb{Z}; a > 0\}$.

In der Formulierung von Satz 3.23 haben wir konsequent $\mathbb{N}_0$ und $\Phi(\mathbb{N}_0)$ sowie $\mathbb{N}$ und $\Phi(\mathbb{N})$ identifiziert (vgl. Bemerkungen 3.13. So ist (i) zu verstehen als $a \leq b \iff b-a \in \Phi(\mathbb{N}_0)$ und entsprechend für die anderen Aussagen. Wir werden im Folgenden darauf nicht mehr hinweisen.

Beweis. Wir wissen bereits, dass $\leqslant$ eine totale Ordnung auf $\mathbb{Z}$ ist (Lemma 3.14). Wir müssen deshalb nur noch zeigen, dass (i)–(iv), die Bedingungen von Definition 3.17(i), (ii) und die archimedische Eigenschaft erfüllt sind.

(i): Wir machen zur Verdeutlichung hier noch einmal die Unterscheidung zwischen $+$ und $\oplus$ sowie $\leq$ und $\leqslant$ und zwischen $\mathbb{N}_0$ und $\Phi(\mathbb{N}_0)$.

Sei $a = [(m,n)] \lesseqgtr b = [(m',n')]$, dann gilt mit einem $x \in \mathbb{N}_0$ und der Äquivalenzrelation $\sim$ aus Lemma 3.1

$$\begin{aligned} a \lesseqgtr b &\iff m + n' \leq n + m' \iff m + n' + x = n + m' \\ &\iff (m+x, n) \sim (m', n') \iff [(m,n)] \oplus [(x,0)] = [(m',n')] \\ &\iff [(m',n')] - [(m,n)] = [(x,0)] \iff b - a \in \Phi(\mathbb{N}_0) \end{aligned}$$

(ii) beweist man wie (i) mit einem $x \in \mathbb{N}$.

(iii) und (iv) folgen aus (i) bzw. (ii) für $a = 0$.

Def. 3.17(i): Ab jetzt benutzen wir nur noch die vereinfachten Schreibweisen $+$, $\cdot$, $<$ usw. und identifizieren $\mathbb{N}_0$ mit $\Phi(\mathbb{N}_0)$

Die Behauptung folgt nun unmittelbar aus (ii), denn

$$a < b \overset{\text{(ii)}}{\iff} b - a \in \mathbb{N} \iff (b+c) - (a+c) \in \mathbb{N} \overset{\text{(ii)}}{\iff} (a+c) < (b+c).$$

Def. 3.17(ii): Dies folgt ebenfalls aus (ii), denn wegen $c > 0$ gilt

$$a < b \overset{\text{(ii)}}{\iff} b - a \in \mathbb{N} \iff (b-a) \cdot c = b \cdot c - a \cdot c \in \mathbb{N} \overset{\text{(ii)}}{\iff} a \cdot c < b \cdot c.$$

Archimedische Eigenschaft: Zunächst beachte man, dass die in Definition 3.17 definierte Multiplikation na mit $n \in \mathbb{N}_0$ und $a \in R$ im Falle $R = \mathbb{Z}$ mit der Ringmultiplikation $[(n,0)] \odot a$ oder vereinfacht geschrieben $n \cdot a$ bzw. na übereinstimmt (Beweis durch vollständige Induktion nach n).

Wegen $a, b > 0$ sind $a, b \in \mathbb{N}$. Wählt man nun z. B. $n := b + 1 \in \mathbb{N}$, dann gilt wegen $a \geq 1$

$$na = (b+1)a \geq (b+1) \cdot 1 > b. \qquad \square$$

Bemerkungen 3.24. a) In Satz 3.10 haben wir die disjunkte Zerlegung $\mathbb{Z} = \mathbb{N}_0 \cup (-\mathbb{N})$ bewiesen. Danach gilt für jedes $a \in \mathbb{Z}$ genau eine der beiden Darstellungen

$$a = n \text{ für ein } n \in \mathbb{N}_0, \qquad a = -m \text{ für ein } m \in \mathbb{N}.$$

Nach Satz 3.23 gilt nun genauer, dass die linke Darstellung genau dann gilt, wenn $a \geq 0$ ist, und die rechte gilt dann und nur dann, wenn $a < 0$ ist. Dies entspricht genau der üblichen Vorstellung der ganzen Zahlen.

b) Die Aussage „Die Gruppe $(\mathbb{Z}, \oplus)$ wird von $\{[(n,0)]; n \in \mathbb{N}_0\}$ erzeugt“ in Satz 3.10 können wir jetzt auch so lesen, dass die Gruppe $(\mathbb{Z}, +)$ von $\mathbb{N}_0$ erzeugt wird. $(\mathbb{Z}, +)$ ist also die kleinste Gruppe, die $\mathbb{N}_0$ enthält.

3.3 Teilbarkeit — EUKLIDischer Algorithmus

Definition 3.25. Sei R ein kommutativer, unitärer Ring.

Ein Element $a \in R$ heißt *Einheit* in R, wenn ein $b \in R$ mit $ab = 1$ existiert. Man nennt $a \in R$ einen *Teiler* von $b \in R$ bzw. b ein *Vielfaches* von a und schreibt $a \mid b$, wenn ein $x \in R$ mit $ax = b$ existiert. Ein Element $a \in R \setminus \{0\}$ heißt *irreduzibel*, wenn

a keine Einheit ist und aus $a = bc$ mit $b, c \in R$ folgt, dass b oder c eine Einheit ist. $a \in R \setminus \{0\}$ heißt *Primelement*, wenn a keine Einheit ist und aus $a \mid (bc)$ mit $b, c \in R$ bereits $a \mid b$ oder $a \mid c$ folgt.

Man nennt R einen *Integritätsring*, wenn R *nullteilerfrei* ist, d. h. aus $a, b \in R \setminus \{0\}$ folgt $ab \neq 0$. Ein Paar (R, δ) heißt EUKLID*ischer Ring*, wenn R ein Integritätsring ist und $\delta\colon R \setminus \{0\} \to \mathbb{N}$ eine Abbildung mit der Eigenschaft, dass es zu je zwei Elementen $a, b \in R$ mit $b \neq 0$ stets Elemente $q, r \in R$ gibt, so dass

$$a = qb + r \quad \text{mit} \quad r = 0 \quad \text{oder} \quad \delta(r) < \delta(b).$$

Wir werden jetzt $\mathbb{Z}$ in Hinblick auf auf die oben definierten Eigenschaften untersuchen. Wir beginnen mit einigen Aussagen zur Teilbarkeit.

Lemma 3.26. *a) Für alle $j, k, l, m, n \in \mathbb{Z}$ gilt:*

(i) $m \mid n \iff -m \mid n \iff m \mid (-n) \iff (-m) \mid (-n) \iff |m| \,\big|\, |n|$,

(ii) $(\pm 1) \mid m$, $(\pm m) \mid m$, $m \mid 0$,

(iii) $l \mid m \wedge m \mid n \implies l \mid n$ *(Transitivität),*

(iv) $m \mid n \wedge n \neq 0 \implies |m| \leq |n|$,

(v) $m \mid n \wedge n \mid m \implies m = n \vee m = -n$,

(vi) $m \mid n \implies m \mid nk$,

(vii) $m \mid n \implies mj \mid nj$,

(viii) $mj \mid nj \wedge j \neq 0 \implies m \mid n$,

(ix) $l \mid m \wedge l \mid n \implies l \mid (jm + kn)$.

b) Die Einheiten des Ringes $\mathbb{Z}$ sind ± 1.

Beweis. a) Die Aussagen (i), (ii), und (iii) folgen unmittelbar aus der Definition.

(iv) Aus $m \mid n$ folgt zunächst $|m| \,\big|\, |n|$ und dann $|m|x = |n|$ mit $x \in \mathbb{Z}$. Wegen $|m| \geq 0$ und $|n| > 0$ muss $x \in \mathbb{N}$ gelten. Ist $x = 1$ so ist $|m| = |n|$ und wir sind fertig. Andernfalls ist $x = x' + 1$ für ein $x' \in \mathbb{N}$ und $|n| = |m|(x'+1) = |m|x' + |m| = |n|$. Wegen $|m|x' \in \mathbb{N}_0$ folgt $|m| \leq |n|$.

(v) Ist $m = 0$ oder $n = 0$, dann folgt aus $0 \mid n$ bzw. $0 \mid m$ mit Lemma 3.8(iv) sofort $m = n = 0$. Anderenfalls erhält man aus (iv), dass sowohl $|m| \leq |n|$ als auch $|n| \leq |m|$ gilt. Damit ist $|m| = |n|$, d, h. $m = n \vee m = -n$.

(vi) $mx = n$ impliziert $m(xk) = nk$.

(vii) $mx = n$ führt zu $(mj)x = nj$, also $mj \mid nj$.

(viii) Aus $(mj)x = (mx)j = nj$ erhält man $mx = n$, also $m \mid n$ mit der Nullteilerfreiheit von $\mathbb{Z}$ (siehe Lemma 3.18(vii) und Satz 3.23).

(ix) $lx = m$ und $ly = n$ implizieren $l(xj + yk) = mj + nk$.

b) Wegen $1 \cdot 1 = (-1) \cdot (-1) = 1$ sind 1 und -1 Einheiten von $\mathbb{Z}$. Umgekehrt existiere zu $m \in \mathbb{Z}$ ein $n \in \mathbb{Z}$ mit $mn = 1$. Aus der Definition von Teiler und a)(ii) folgt $m \mid 1$ und $1 \mid m$. Mit a)(v) folgt daraus die Behauptung, nämlich $m = 1$ oder $m = -1$. □

Satz 3.27 (EUKLIDischer Algorithmus)**.** *Zu $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit der Eigenschaft*

$$a = qb + r \quad \textit{und} \quad 0 \leq r < |b|. \tag{3.5}$$

$(\mathbb{Z}, |\cdot|)$ ist ein EUKLID*ischer Ring.*

Bemerkung 3.28. a) Am ersten Teil des Beweise erkennt man, dass für $a, b \in \mathbb{N}_0$, $b \neq 0$, auch $q \in \mathbb{N}_0$ gilt.

b) Formel (3.5) kann man als „Division mit Rest“ interpretieren und in der Form

$$a : b = q \text{ Rest } r \qquad (0 \leq r < |b|).$$

schreiben.

Wir werden sehen, dass der *Euklid*ische Algorithmus von zentraler Bedeutung für das Rechnen mit ganzen Zahlen ist. Er hat aber auch Anwendungen im praktischen Leben. Im Bankenbereich rechnet man lieber mit Integer-Größen als mit Real-Größen, da Integer-Größen weniger Speicherplatz benötigen und keine Rundungsfehler auftreten können. Geldbeträge kann man immer ganzzahlig darstellen, wenn man mit der kleinsten Einheit, in der EU also mit Cent, rechnet. Andererseits benötigt man aber auch nicht-ganzzahlige Werte, z. B. beim Umrechnen von einer Währung in eine andere oder bei der Zinsberechnung. Will man etwa $155,75\,€$ in US-$ umrechnen, so müsste man (Kurs vom 02.06.2003)

$$15575 \cdot 1,1718 = 18250,785$$

rechnen, was man aber mit Integer-Größen nicht kann. Man rechnet deshalb

$$15575 \cdot 11718 = 182507850$$

und teilt das Ergebnis mit Rest durch 10000, also

$$181921950 = 10000 \cdot 18250 + 7850.$$

Den Rest 7850 betrachtet man für die Rundung und erhält

$$15575\,\text{Euro-Cent} = 18251\,\text{US-Cent} \quad \text{oder} \quad 155,75\,€ = 182,51\,\$.$$

Bei dieser Form der Rechnung hat man jederzeit volle Kontrolle über die zu berücksichtigenden Nachkommastellen und die Rundung, was bei großen Geldbeträgen natürlich von Bedeutung ist.

Definition 3.29. Sind $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, so nennt man $d \in \mathbb{N}_0$ den *größten gemeinsamen Teiler* von $a_1, a_2, \ldots, a_k$ und schreibt $d = \text{ggT}(a_1, a_2, \ldots, a_k)$, wenn $d \mid a_j$ für alle $j = 1, 2, \ldots, k$, und aus $d' \in \mathbb{Z}$ mit $d' \mid a_j$, $j = 1, 2, \ldots, k$, stets $d' \mid d$ folgt.

Bemerkung 3.30. a) Der größte gemeinsame Teiler (im Folgenden meist mit ggT abgekürzt) ist eindeutig bestimmt. Sind nämlich d und d' größte gemeinsame Teiler von $a_1, a_2, \ldots, a_k$, so folgt $d \mid d'$ und $d' \mid d$, also $d' = d$ wegen $d, d' \in \mathbb{N}_0$ und Lemma 3.26(v).

b) Hinsichtlich der Existenz des ggT gilt Folgendes. Sind $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ und ist $a_{j_0} \neq 0$ für ein $j_0 \in \{1, 2, \ldots, k\}$, dann ist die Menge der gemeinsamen Teiler

$$T := \big\{a \in \mathbb{N}_0; a \mid a_j \text{ für alle } j \in \{1, 2, \ldots, k\}\big\}$$

nach oben beschränkt, z. B. ist $|a_{j_0}|$ eine obere Schranke, und $d := \mathrm{ggT}(a_1, a_2, \ldots, a_k)$ ist das letzte Element dieser Menge. Damit ist d die größte Zahl, die alle a_j teilt, woraus sich der Name „größter gemeinsamer Teiler“ ableitet. Man könnte in diesem Fall den größten gemeinsamen Teiler anschaulicher durch $d = \max T$ definieren.

Ist allerdings $a_j = 0$ für alle j, dann ist $d = \mathrm{ggT}(0, 0, \ldots, 0) = 0$, während $T = \mathbb{N}_0$ ist. In diesem Fall macht eine Definition von d über das Maximum von T keinen Sinn.

c) Offensichtlich ändert sich der ggT nicht, wenn man die Reihenfolge der a_j ändert oder doppelte Werte streicht, z. B. ist

$$\mathrm{ggT}(a_1, a_2, \ldots, a_k) = \mathrm{ggT}(a_2, a_1, \ldots, a_k),$$
$$\mathrm{ggT}(a, a, \ldots, a) = \mathrm{ggT}(a).$$

Außerdem gilt

$$\mathrm{ggT}(a) = \mathrm{ggT}(a, 0) = |a| \qquad (a \in \mathbb{Z}).$$

Mit dem folgenden iterierten EUKLIDischen Algorithmus geben wir nun ein konstruktives Verfahren zur Bestimmung des ggT zweier Zahlen $a, b \in \mathbb{Z}$ an.

Satz 3.31 (Iterierter EUKLIDischer Algorithmus)**.** *Seien $a, b \in \mathbb{Z} \setminus \{0\}$ mit $|a| > |b|$, dann existieren ein $k \in \mathbb{N}_0$ und ganze Zahlen*

$$r_0 > r_1 > \cdots r_k > r_{k+1} = 0,$$

die die Bedingungen

(i) $r_0 = |a|$, $r_1 = |b|$,

(ii) $r_j = q_j r_{j+1} + r_{j+2}$ *mit* $q_j \in \mathbb{N}_0$ *und* $0 \leq r_{j+2} < r_{j+1}$, $(j = 0, 1 \ldots, k-1)$,

erfüllen. Es gilt

$$\mathrm{ggT}(a, b) = r_k$$

und es existieren $x, y \in \mathbb{Z}$ mit der Eigenschaft

$$\mathrm{ggT}(a, b) = xa + yb. \tag{3.6}$$

Beweis. Nach Satz 3.27 sind für $r_{j+1} \neq 0$ die q_j und r_{j+2} in (ii) eindeutig durch r_j und r_{j+1} bestimmt. Man kann also die r_j durch (i) und (ii) rekursiv definieren, so lange in (ii) $r_{j+1} \neq 0$ ist.

Wegen $r_0 > r_1 > r_2 \cdots \geq 0$ bricht das Verfahren nach endlich vielen Schritten mit $r_{k+1} = 0$ ab für ein $k \leq |b|$.

Wir zeigen nun die Existenz von $n_j, m_j \in \mathbb{Z}$ mit

$$r_j = n_j \cdot a + m_j \cdot b \qquad (j = 0, 1, \ldots, k+1). \tag{3.7}$$

Dazu nehmen wir an, dass die Aussage falsch ist, d. h. es gibt ein $j_0 \in \{0, 1, \ldots, k+1\}$, für das (3.7) nicht gilt. Wir wählen das kleinste j_0 mit dieser Eigenschaft. Wegen

$$r_0 = |a| = (\pm 1) \cdot a + 0 \cdot b$$
$$r_1 = |b| = 0 \cdot a + (\pm 1) \cdot b$$

ist (3.7) für $j = 0, 1$ richtig, d. h. $2 \leq j_0 \leq k+1$. Setzen wir nun $j_0 = \nu + 2$ für ein $\nu \in \{0, 1, \ldots k-1\}$, dann ist $r_{\nu+1} > r_{j_0} \geq r_k > 0$ und man kann $r_{\nu+2}$ nach (ii) bilden. Nutzt man außerdem aus, dass für r_ν und $r_{\nu+1}$ die Darstellung (3.7) gültig ist (Minimalität von j_0), dann folgt

$$\begin{aligned} r_{j_0} = r_{\nu+2} &= r_\nu - q_\nu r_{\nu+1} \\ &= n_\nu a + m_\nu b - q_\nu (n_{\nu+1} a + m_{\nu+1} b) \\ &= (n_\nu - q_\nu n_{\nu+1}) a + (m_\nu - q_\nu m_{\nu+1}) b \\ &= n_{j+2} a + m_{j+2} b, \end{aligned}$$

wobei wir $n_{\nu+2} := n_\nu - q_\nu n_{\nu+1}$ und $m_{\nu+2} := m_\nu - q_\nu m_{\nu+1}$ gesetzt haben. Wegen $n_{\nu+2}, m_{\nu+2} \in \mathbb{Z}$ ist damit aber (3.7) auch für $\nu + 2 = j_0$ richtig, im Widerspruch zur Wahl von j_0. Damit ist die Darstellung (3.7) bewiesen.

Als nächstes zeigen wir $r_k \mid a$ und $r_k \mid b$. Zunächst gilt $r_k \mid r_{k-1}$ wegen $r_{k-1} = q_{k-1} r_k + r_{k+1} = q_{k-1} r_k$. Daraus folgt weiter induktiv mit Lemma 3.26(v)

$$\begin{aligned} r_k \mid r_{k-2} &= q_{k-2} r_{k-1} + r_k \\ r_k \mid r_{k-3} &= q_{k-3} r_{k-2} + r_{k-1} \\ &\vdots \end{aligned}$$

und man erhält schließlich $r_k \mid r_1$ und $r_k \mid r_0$. Wegen $r_1 = |b|$ und $r_0 = |a|$ gilt deshalb $r_k \big| |b|$ und $r_k \big| |a|$, also mit Lemma 3.26(i) auch $r_k \mid b$ und $r_k \mid a$. Somit ist r_k ein gemeinsamer Teiler von a und b.

Zum Nachweis von $r_k = \mathrm{ggT}(a, b)$ zu zeigen, wählen wir nun noch einen beliebigen Teiler d' von a und b. Für diesen Teiler gilt nach Lemma 3.26(v) auch $d' \mid (xa + yb)$ für alle $x, y \in \mathbb{Z}$ und mit der Darstellung (3.7) von r_k folgt $d' \mid r_k$, d. h. $r_k = \mathrm{ggT}(a, b)$. Mit (3.7) erhält man daraus auch noch (3.6). □

Bemerkung 3.32. Der Algorithmus in Satz 3.31 führt ohne Veränderung auch für $|a| < |b|$ zum Ziel. In diesem Fall erhält man als Reste $r_0 = |a|$, $r_1 = |b|$, $r_2 = |a|$ und von da ab verläuft alles wie im Fall $|a| > |b|$.

Beispiel 3.33. Das folgende Zahlenbeispiel zeigt den iterierten EUKLIDischen Algorithmus für die Zahlen $a = 3112$, $b = 574$. Wir zeigen außerdem, wie man aus dem

Algorithmus die Darstellung (3.6) erhält.

$$
\begin{array}{rl}
 & r_0 = 3112 \\
 & r_1 = 574 \\
3112 = 5 \cdot 574 + 242, & r_2 = 242 \\
574 = 2 \cdot 242 + 90, & r_3 = 90 \\
242 = 2 \cdot 90 + 62, & r_4 = 62 \\
90 = 1 \cdot 62 + 28, & r_5 = 28 \\
62 = 2 \cdot 28 + 6, & r_6 = 6 \\
28 = 4 \cdot 6 + 4, & r_7 = 4 \\
6 = 1 \cdot 4 + 2, & \mathbf{r_8 = 2 = ggT(a, b)} \\
4 = 2 \cdot 2 + 0, & r_9 = 0.
\end{array} \tag{3.8}
$$

Daraus folgt

$$
\begin{aligned}
\mathrm{ggT}(3112, 574) &= \underline{2} \\
&= 6 - 1 \cdot \underline{4} \\
&= 6 - 1 \cdot (28 - 4 \cdot 6) = 5 \cdot \underline{6} - 28 \\
&= 5 \cdot (62 - 2 \cdot 28) - 28 = 5 \cdot 62 - 11 \cdot \underline{28} \\
&= 5 \cdot 62 - 11 \cdot (90 - 1 \cdot 62) = 16 \cdot \underline{62} - 11 \cdot 90 \\
&= 16 \cdot (242 - 2 \cdot 90) - 11 \cdot 90 = 16 \cdot 242 - 43 \cdot \underline{90} \\
&= 16 \cdot 242 - 43 \cdot (574 - 2 \cdot 242) = 102 \cdot \underline{242} - 43 \cdot 574 \\
&= 102 \cdot (3112 - 5 \cdot 574) - 43 \cdot 574 = 102 \cdot 3112 - 553 \cdot 574.
\end{aligned}
$$

Dabei werden die unterstrichenen Zahlen jeweils durch eine Zeile auf der linken Seite von Schema (3.8) ersetzt.

Will man den größten gemeinsamen Teiler von mehr als zwei Zahlen bestimmen, dann kann man das folgende Lemma verwenden.

Lemma 3.34. *Sind $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ und ist $d = \mathrm{ggT}(a_1, a_2, \ldots, a_{k-1})$, dann ist $\mathrm{ggT}(a_1, a_2, \ldots, a_k) = \mathrm{ggT}(d, a_k)$.*

Beweis. Sei $d' := \mathrm{ggT}(d, a_k)$, dann gilt wegen $d' \mid d$ und $d \mid a_j$ für alle $j = 1, 2, \ldots, k-1$ auch $d' \mid a_j$ für alle $j = 1, 2, \ldots, k$ (Lemma 3.26(iii)). Ist jetzt $d'' \in \mathbb{N}_0$ mit $d'' \mid a_j$ für alle $j = 1, 2, \ldots, k$, dann gilt einmal $d'' \mid d$, da $d = \mathrm{ggT}(a_1, a_2, \ldots, a_{k-1})$, und andererseits gilt natürlich $d'' \mid a_k$. Daraus folgt aber $d'' \mid d'$, da $d' = \mathrm{ggT}(d, a_k)$, und damit ist $d' = \mathrm{ggT}(a_1, a_2, \ldots, a_k)$. □

Als weitere Anwendung von Satz 3.31 beweisen wir

Satz 3.35. *Seien $a_1, a_2 \ldots, a_k \in \mathbb{Z}$ mit $d = \mathrm{ggT}(a_1, a_2 \ldots, a_k)$, dann gilt*

$$\mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_k := \{x_1a_1 + x_2a_2 + \cdots x_ka_k \in \mathbb{Z}; x_j \in \mathbb{Z},\ j = 1, 2, \ldots, k\} = \mathbb{Z}d.$$

Beweis. Sei zunächst $k = 2$.

„$\subset$“ Sei $x \in \mathbb{Z}a_1 + \mathbb{Z}a_2$, d. h. $x = n_1a_1 + n_2a_2$ für gewisse $n_1, n_2 \in \mathbb{Z}$. Wegen $d \mid a_1$ und $d \mid a_2$ existieren $c_1, c_2 \in \mathbb{Z}$ mit $dc_1 = a_1$ und $dc_2 = a_2$. Also ist

$$x = n_1a_1 + n_2a_2 = n_1dc_1 + n_2dc_2 = (n_1c_1 + n_2c_2)d \in \mathbb{Z}d.$$

„$\supset$“ Ist nun $x \in \mathbb{Z}d$, also $x = nd$ für ein $n \in \mathbb{Z}$, dann existieren nach (3.6) $n_1, n_2 \in \mathbb{Z}$ mit $d = n_1a_1 + n_2a_2$ und es folgt

$$x = nd = n(n_1a_1 + n_2a_2) = (nn_1)a_1 + (nn_2)a_2 \in \mathbb{Z}a_1 + \mathbb{Z}a_2.$$

Für beliebige $k \in \mathbb{N}$ beweisen wir die Aussage durch vollständige Induktion. Dabei ist der Fall $k = 1$, also $\mathbb{Z}a_1 = \mathbb{Z}\,\mathrm{ggT}(a_1)$ wegen $\mathrm{ggT}(a_1) = |a_1| = \pm a_1$ unmittelbar klar.

Beim Induktionsschluss von k nach $k + 1$ benutzen wir Lemma 3.34 und den Fall $k = 2$. Mit $d' := \mathrm{ggT}(a_1, a_2, \ldots, a_k)$ folgt die Behauptung damit aus

$$\mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_{k+1} = (\mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_k) + \mathbb{Z}a_{k+1}$$

$$= \mathbb{Z}d' + \mathbb{Z}a_{k+1} = \mathbb{Z}\,\mathrm{ggT}(d', a_{k+1}) = \mathbb{Z}\,\mathrm{ggT}(a_1, a_2, \ldots, a_{k+1}). \qquad \square$$

Als direkte Anwendung erhalten wir eine Aussage über die Lösbarkeit von DIOPHANT*ischen Gleichungen*, d. h. von Gleichungen über $\mathbb{Z}$.

Folgerung 3.36. *Seien $a_1, a_2, \ldots, a_k, b \in \mathbb{Z}$. Eine lineare* DIOPHANT*ische Gleichung*

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$$

besitzt genau dann eine Lösung $(x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k$, wenn

$$\mathrm{ggT}(a_1, a_2 \ldots, a_k) \mid b.$$

Außerdem benötigen wir für später noch

Folgerung 3.37. *Seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$ (solche Zahlen heißen auch* teilerfremd*). Ist $c \in \mathbb{Z}$ mit $a \mid bc$, dann gilt $a \mid c$.*

Beweis. Nach Satz 3.35 gilt

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\,\mathrm{ggT}(a, b) = \mathbb{Z} \cdot 1 = \mathbb{Z}$$

und wir haben für geeignete $x, y \in \mathbb{Z}$ die Darstellung $1 = xa + yb$ und nach Multiplikation mit c

$$c = cxa + cyb. \tag{3.9}$$

Gilt nun $a \mid bc$, dann teilt a die rechte Seite von (3.9) und damit auch c. $\square$

In der Schule bestimmt man den größten gemeinsamen Teiler zweier Zahlen meist aus der Primfaktorzerlegung, die wir später noch behandeln werden. Für große Zahlen, z. B. 100-stellige, ist es aber sehr viel schwieriger, die Primfaktorzerlegungen zu bestimmen als den größten gemeinsamen Teiler. Der iterierte EUKLIDische Algorithmus in Satz 3.31 liefert ein sehr leicht zu programmierendes Verfahren, das auch für große Zahlen schnell zum Ziel führt.

Wir betrachten als nächstes eine Darstellung der ganzen Zahlen, die für das praktische Rechnen unverzichtbar ist.

Satz 3.38 (Satz von der g-adischen Darstellung)**.** *Sei $g \in \mathbb{N}$, $g \geq 2$. Jede jede Zahl $a \in \mathbb{Z}$, $a \neq 0$, besitzt eine eindeutige Darstellung der Form*

$$a = \varepsilon \sum_{j=0}^{N} r_j g^j \tag{3.10}$$

mit $\varepsilon \in \{-1, +1\}$, $N \in \mathbb{N}_0$ und $0 \leq r_j < g$, $r_N \neq 0$. Die r_j kann man rekursiv berechnen aus

$$|a| = q_0 g + r_0, \;\; q_j = q_{j+1} g + r_{j+1} \quad (j \in \mathbb{N}). \tag{3.11}$$

Hat a die Darstellung (3.10)*, dann schreibt man $a = \varepsilon(r_N, r_{N-1}, \ldots, r_1, r_0)_g$.*

Beweis. Die r_j, q_j in (3.11) sind wegen $0 \leq r_j < g$ durch den EUKLIDischen Algorithmus (Satz 3.27) wohldefiniert. Nun gilt für alle $n \in \mathbb{N}_0$

$$\begin{aligned} |a| &= r_0 + q_0 g \\ &= r_0 + (r_1 + q_1 g) g \\ &= r_0 + r_1 g + q_1 g^2 \\ &= r_0 + r_1 g + (r_2 + q_2 g) g^2 \\ &= r_0 + r_1 g + r_2 g^2 + q_2 g^3 \\ &= \cdots\cdots\cdots\cdots\cdots\cdots \\ &= \sum_{j=0}^{n} r_j g^j + q_n g^{n+1}. \end{aligned} \tag{3.12}$$

(Einen exakten Beweis dieser Darstellung kann man leicht mit vollständiger Induktion führen.)

Wegen $\sum_{j=0}^{n} r_j g^j \geq 0$ erhält man aus (3.12) $|a| \geq q_n g^{n+1}$. Wäre jetzt $q_n \neq 0$, d. h. $q_n \geq 1$ für alle $n \in \mathbb{N}_0$ (beachte Bemerkung 3.28), dann folgte $|a| \geq g^{n+1}$ für alle $n \in \mathbb{N}_0$ im Widerspruch zu Lemma 3.22b. (An dieser Stelle des Beweises werden die Voraussetzung $g \geq 2$ und die archimedische Eigenschaft der Anordnung von $\mathbb{Z}$ (vgl. Satz 3.23) benutzt.)

Wählt man nun $N \in \mathbb{N}_0$ als die kleinste natürliche Zahl mit $q_N = 0$, dann folgt aus (3.12) mit $n = N$

$$|a| = \sum_{j=0}^{N} r_j g^j, \qquad a = \varepsilon \sum_{j=0}^{N} r_j g^j.$$

Dabei ist $r_N \neq 0$, denn aus $r_N = 0$ folgte $q_{N-1} = q_N g + r_N = 0 \cdot g + 0 = 0$ im Widerspruch zur Minimalität von N. Damit ist die Existenz der Darstellung (3.10) gezeigt.

Eindeutigkeit der Darstellung: Sei $a = \varepsilon \sum_{j=0}^{N} r_j g^j = \varepsilon' \sum_{j=0}^{M} r'_j g^j$. Indem wir gegebenenfalls Nullen ergänzen, können wir $N = M$ annehmen und erhalten

$$0 = |a| - |a| = \sum_{j=0}^{N} (r_j - r'_j) g^j.$$

Nehmen wir jetzt an, dass die beiden Darstellungen verschieden sind, dann ist die Menge $U := \{j \in \{0,1,\dots,N\}; r_j \neq r'_j\}$ nicht leer und mit $m := \min U$ gilt dann

$$0 = g^m(r_m - r'_m) + g^{m+1}x = g^m[(r_m - r'_m) + gx], \quad x := \sum_{j=m+1}^{N} (r_j - r'_j)g^{j-m-1} \in \mathbb{Z}.$$

Da $\mathbb{Z}$ nullteilerfrei ist, folgt $(r_m - r'_m) + gx = 0$, daraus weiter $g \big| |r_m - r'_m|$ und nach Lemma 3.26(iv) ist deshalb $g \leq |r_m - r'_m|$. Andererseits gilt aber nach Definition von r_m und r'_m

$$-g < -r'_m \leq -r'_m + r_m < g,$$

also $|r_m - r'_m| < g$. Dies ist ein Widerspruch und somit muss $U = \emptyset$ sein. Es folgt $r_j = r'_j$ für alle j und wegen $a \neq 0$ auch $\varepsilon = \varepsilon'$. Also ist die Darstellung eindeutig. □

Man nennt (3.10) die *g-adische Darstellung von a*. Üblich ist natürlich $g = 10$, aber auch die *Binärdarstellung*, d. h. $g = 2$, die *Oktaldarstellung* mit $g = 8 = 2^3$ und die *Hexadezimaldarstellung*, $g = 16 = 2^4$, spielen in der Praxis eine wichtige Rolle.

Beispiel 3.39. a) $g = 2$, $a = 75$.

$$\begin{aligned}
75 &= 1 + 37 \cdot 2 \\
&= 1 + (1 + 18 \cdot 2) \cdot 2 \\
&= 1 + 1 \cdot 2 + 18 \cdot 2^2 \\
&= 1 + 1 \cdot 2 + (0 + 9 \cdot 2) \cdot 2^2 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 9 \cdot 2^3 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + (1 + 4 \cdot 2) \cdot 2^3 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 4 \cdot 2^4 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + (0 + 2 \cdot 2) \cdot 2^4 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 2 \cdot 2^5 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + (0 + 1 \cdot 2) \cdot 2^5 \\
&= 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6.
\end{aligned}$$

Damit haben wir dir Binärdarstellung (Darstellung im Dualsystem)

$$75 = (1,0,0,1,0,1,1)_2.$$

b) $g = 12$, $a = 173$.

$$\begin{aligned}
173 &= 5 + 14 \cdot 12 \\
&= 5 + (2 + 1 \cdot 12) \cdot 12 \\
&= 5 + 2 \cdot 12 + 1 \cdot 12^2.
\end{aligned}$$

Die Darstellung in 12-adischen System lautet also

$$173 = (1,2,5)_{12}.$$

Aus der g-adischen Darstellung lassen sich verschiedene Teilbarkeitskriterien ableiten. Eines der bekanntesten ist das Quersummenkriterium im Dezimalsystem (10-adischen System).

Lemma 3.40. *Eine Zahl $a = \pm\sum_{j=0}^{N} r_j 10^j \in \mathbb{Z}$ im Dezimalsystem ist genau dann durch 3 bzw. 9 teilbar, wenn die Quersumme*

$$Q := \sum_{j=0}^{N} r_j \in \mathbb{N}_0$$

durch 3 bzw. 9 teilbar ist.

Beweis. Aus $10 = 9+1$ folgt durch Induktion die Existenz von $x_j \in \mathbb{Z}$ mit $10^j = 9x_j+1$, $j \in \mathbb{N}_0$. Also hat man

$$\pm a = \sum_{j=0}^{N} r_j 10^j = \sum_{j=0}^{N} (9x_j + 1) r_j = 9\Big(\sum_{j=0}^{N} x_j r_j\Big) + Q.$$

Demnach ist $9 \mid a$ äquivalent $9 \mid Q$ und $3 \mid a$ zu $3 \mid Q$. □

An der g-adischen Darstellung kann man das übliche schriftliche Additionsverfahren herleiten. Seien

$$a = \sum_{j=0}^{N} a_j g^j, \quad b = \sum_{j=0}^{N} b_j g^j \qquad (0 \le a_j, b_j < g)$$

Darstellungen von $a, b \in \mathbb{Z}$. Definiert man c_j, $j = 0, 1, \ldots, N$ durch

$$a_0 + b_0 = c_0 + \varepsilon_0 g,\ \varepsilon_0 \in \{0,1\},\ 0 \le c_0 < g,$$
$$a_j + b_j + \varepsilon_{j-1} = c_j + \varepsilon_j g,\ \varepsilon_j \in \{0,1\},\ 0 \le c_j < g,\ 1 \le j \le N,$$

Dann ist

$$a + b = \sum_{i=0}^{N} c_i g^i + \varepsilon_N g^{N+1}$$

die g-adische Darstellung von $a + b$.

Lemma 3.41. *$\mathbb{Z}$ ist abzählbar unendlich.*

Beweis. Nach Satz 3.27 (siehe auch Bemerkung 3.28a) besitzt jedes $n \in \mathbb{N}_0$ eine eindeutige Darstellung

$$n = 2x + \eta,\ x \in \mathbb{N}_0,\ \eta \in \{0,1\}.$$

Damit definieren wir die Abbildung

$$\varphi\colon \mathbb{N}_0 \to \mathbb{Z},\ n \mapsto \begin{cases} x, & \eta = 0, \\ -x-1, & \eta = 1. \end{cases}$$

Offenbar ist φ bijektiv und damit ist $\mathbb{Z}$ abzählbar unendlich. □

3.4 Primzahlen

Wir kommen nun zu den Grundbausteinen der multiplikativen Struktur der natürlichen Zahlen, den so genannten Primzahlen.

Definition 3.42. Eine natürliche Zahl $p \in \mathbb{N}$, $p \neq 1$, heißt *Primzahl*, wenn p nur 1 und p als positive Teiler hat. Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet. Eine natürliche Zahl $n \in \mathbb{N}$, $n \neq 1$, die nicht Primzahl ist, heißt *zusammengesetzt*.

Man kann Definition 3.42 auch so formulieren: Ist $p \in \mathbb{N}$, $p \neq 1$ mit $p = rs$ für $r, s \in \mathbb{N}$, dann folgt $r = 1$ oder $s = 1$. In der Algebra nennt man Elemente mit dieser Eigenschaft *irreduzibel*. Denn Zusammenhang mit den *Primelementen* der Algebra werden wir in Satz 3.46 kennen lernen.

Lemma 3.43. *Für $n \in \mathbb{N}$, $n \neq 1$, sei*

$$M = \{m \in \mathbb{N}; m \mid n \text{ und } m \neq 1\}.$$

Dann ist $M \neq \emptyset$ und das erste Element q von M ist eine Primzahl, die n teilt. q heißt kleinster Primteiler *von n.*

Beweis. Wegen $n \in M$ gilt $M \neq \emptyset$, so dass das erste Element q von M nach Satz 2.26c existiert. Wäre q keine Primzahl, so würde ein $s \in \mathbb{N}$ mit $s \mid q$ und $s \neq 1$, $s \neq q$ existieren. Nach Lemma 3.26(iii) gilt damit aber $s \mid n$, also $s \in M$. Aus Lemma 3.26(iv) folgt aber andererseits $s < q$ im Widerspruch zur Wahl von q. □

Satz 3.44 (Satz von Euklid)**.** *Die Menge $\mathbb{P}$ aller Primzahlen ist unendlich.*

Beweis. $p_0 = 2$ ist eine Primzahl, denn $q \mid 2$ mit $q \in \mathbb{N}$ impliziert $1 \leq q \leq 2$, also $q = 1$ oder $q = 2$. Es gilt also $\mathbb{P} \neq \emptyset$. Wenn wir annehmen, dass $\mathbb{P}$ endlich ist, dann existieren ein $n \in \mathbb{N}_0$ und ein bijektive Abbildung $\varphi\colon A_{n+1} \to \mathbb{P}$. Setzt man nun $\varphi(j) = p_j$ für $j = 0, 1, \ldots, n$ und $m := p_0 p_1 \cdots p_n + 1$, dann ist $m \in \mathbb{N}$ und $m > 1$. Ist q der kleinste Primteiler von m nach Lemma 3.43, dann ist $q \in \mathbb{P} = \varphi(A_{n+1}) = \{p_0, p_1, \ldots, p_n\}$ und es folgt $q \mid (p_0 p_1 \cdots p_n)$. Aus $q \mid m$ und $q \mid (p_0 p_1 \cdots p_n)$ erhält man nun mit Lemma 3.26(ix) $q \mid (m - p_0 p_1 \cdots p_n)$, also $q \mid 1$. Dies bedeutet $q = 1$ und ist ein Widerspruch zu $q \in \mathbb{P}$. □

Eine Verschärfung des Satzes von Euklid ist der *Primzahlsatz* der analytischen Zahlentheorie, unabhängig von J. Hadamard und C. de La Vallée Poussin 1896 bewiesen:

$$\pi_N := \sharp\{p \in \mathbb{P}; p \leq N\} \approx \frac{N}{\log N}, \text{ d. h. } \lim_{N\to\infty} \frac{\pi_N}{N/\log N} = 1.$$

Als beweistechnisches Hilfsmittel zeigen wir als nächstes

Lemma 3.45. *Für $p \in \mathbb{P}$ und $m \in \mathbb{Z}$ gilt*

$$p \nmid m \iff \mathrm{ggT}(p, m) = 1.$$

Euklid (von Alexandria)
geb. ca. 325 v. C.
gest. ca. 265 v. C. in Alexandria

Jacques Salomon Hadamard
geb. 8.12.1865 in Versailles
gest. 17.10.1963 in Paris

Charles-Jean Baron de la Vallée Poussin
geb. 14.8.1866 in Löwen
gest. 2.3.1962 in Löwen

Beweis. Wir zeigen dazu

$$\mathrm{ggT}(p,m) \neq 1 \iff p \mid m.$$

$\Longrightarrow$: Sei $d := \mathrm{ggT}(p,m) \neq 1$, dann gilt $d \mid p$ und $d \mid m$. Wegen $d \neq 1$ und $p \in \mathbb{P}$ muss $d = p$ gelten und wir haben $p \mid m$.

$\Longleftarrow$: Gilt umgekehrt $p \mid m$, dann ist p ein gemeinsamer Teiler von p und m und es gilt $\mathrm{ggT}(p,m) = p > 1$. □

Als eine wichtige Charakterisierung der Primzahlen beweisen wir nun, dass im Ring der ganzen Zahlen die aus der Algebra bekannte Begriffe *irreduzibel* und *Primelement* äquivalent sind.

Satz 3.46. *Eine Zahl $p \in \mathbb{N}$, $p \neq 1$, ist genau dann eine Primzahl, wenn für alle $m, n \in \mathbb{N}$ mit $p \mid mn$ gilt*

$$p \mid m \quad \textit{oder} \quad p \mid n. \tag{3.13}$$

Beweis. $\Longleftarrow$: Sei $p \in \mathbb{N}$, $p \neq 1$, derart, dass für alle $m, n \in \mathbb{N}$ mit $p \mid mn$ Aussage (3.13) gilt. Um zu zeigen, dass p eine Primzahl ist, nehmen wir an, dass p die Darstellung $p = rs$ mit $r, s \in \mathbb{N}$ hat und zeigen $r = 1$ oder $s = 1$.

Da die Darstellung $p = rs$ insbesondere $p \mid rs$ impliziert, erhalten wir aus der Voraussetzung $p \mid r$ oder $p \mid s$. Gelte o. B. d. A. $p \mid s$, dann hat s die Darstellung $s = pl$ mit einen $l \in \mathbb{N}$ und es gilt $p = rpl$. Die Nullteilerfreiheit von $\mathbb{Z}$ liefert nun $1 = rl$, d. h. $r \mid 1$, und mit Lemma 3.26(iv) folgt dann $r = 1$.

$\Longrightarrow$: Wir müssen zeigen, dass aus $p \mid mn$ und $p \nmid m$ stets $p \mid n$ folgt. Da wir nach Lemma 3.45 $p \nmid m$ äquivalent durch $\mathrm{ggT}(p, m) = 1$ gilt ersetzen können, erhalten wir diese Aussage unmittelbar aus Folgerung 3.37 mit $a = p$, $b = m$, und $c = n$. □

Folgerung 3.47. *a) Sind $p \in \mathbb{P}$, $n_0, n_1, \ldots, n_m \in \mathbb{N}$ für ein $m \in \mathbb{N}$ mit*

$$p \mid (n_0 n_1 \cdots n_m),$$

dann teilt p mindestens einen der Faktoren $n_0, n_1, \ldots, n_m$.

b) Sind $q, p_0, p_1, \ldots, p_m \in \mathbb{P}$ für ein $m \in \mathbb{N}$, dann gilt

$$q \mid (p_0 p_1 \cdots p_m)$$

dann und nur dann, wenn $q = p_j$ für ein $j \in \{0, 1, \ldots, m\}$.

Beweis. a) Mit Satz 3.46 durch vollständige Induktion über m.

b) Aus $q \mid (p_0 p_1 \cdots p_m)$ folgt mit Teil a) zunächst $q \mid p_j$ für ein $j \in \{0, 1, \ldots, m\}$ und da p_j eine Primzahl ist, muss $q = 1$ oder $q = p_j$ gelten, wobei der erste Fall wegen $q \in \mathbb{P}$ ausscheidet. Die Umkehrung erhält man unmittelbar aus Lemma 3.26(ii), (vi). □

Bemerkung 3.48. Häufig benutzt man das Induktionsprinzip in der folgenden Form:

Ist $M \subset \mathbb{N}_0$ mit

$$0 \in M \text{ und } (k \in M \text{ für alle } k \in \mathbb{N}_0, k \leq n \implies n+1 \in M), \text{ dann ist } M = \mathbb{N}_0.$$

Beim Induktionsschluss nimmt man also an, dass die Aussage $A(k)$ für alle $k \leq n$ richtig ist und zeigt damit die Gültigkeit von $A(n+1)$.

Zum Beweis dieser Form des Induktionsprinzips nimmt man $M \neq \mathbb{N}_0$ an und betrachtet die Menge $C := \mathbb{N}_0 \setminus M$. Aufgrund der Annahme $M \neq \mathbb{N}_0$ ist C nicht leer und besitzt nach Satz 2.26c ein erstes Element j, das wegen $0 \in M$ nicht 0 sein kann. Setzen wir $n + 1 = j$, dann ist also $k \in M$ für alle $k \leq n$ und nach Voraussetzung an M folgt $n + 1 = j \in M$ als Widerspruch zur Definition von j.

Diese Form des Induktionsprinzips kann man ebenfalls mit einer beliebigen natürlichen Zahl n_0 beginnen. In diesem Fall hat man die Bedingung $k \leq n$ durch $n_0 \leq k \leq n$ zu ersetzen.

Eine wichtige Anwendung der Teilbarkeitstheorie ist

Satz 3.49 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n > 1$ lässt sich als endliches Produkt von Primzahlen darstellen, d. h. es gibt ein $s \in \mathbb{N}_0$ sowie Primzahlen $p_0, p_1, \ldots, p_s$ mit*

$$n = p_0 p_1 \cdots p_s. \tag{3.14}$$

Unter der Zusatzbedingung $p_0 \leq p_1 \leq \ldots \leq p_s$ ist die Darstellung eindeutig.

Beweis. Existenz: Wir benutzen das Induktionsprinzip in der Form aus Bemerkung 3.48 mit dem Induktionsanfang $n = 2$. Da 2 eine Primzahl ist, ist in diesem Fall nichts weiter zu beweisen. Wir machen jetzt die Induktionsannahme, dass die gesuchte Darstellung für alle natürlichen Zahlen $2 \leq k \leq n$ und ein festes $n \geq 2$ gilt, und zeigen die Gültigkeit für $n+1$. Ist $n+1$ eine Primzahl, so sind wir fertig. Andernfalls sei q der kleinste Primteiler von $n+1$, also $n+1 = qm$ für ein $m \in \mathbb{N}$ mit $2 \leq m \leq n$. Nach Induktionsvoraussetzung kann man m in der Form

$$m = p_0 p_1 \cdots p_s$$

darstellen mit $s \in \mathbb{N}$ sowie $p_0, p_1, \ldots, p_s \in \mathbb{P}$. Für $n+1$ ist dann

$$n + 1 = q p_0 p_1 \cdots p_s$$

die gesuchte Darstellung.

Eindeutigkeit: Wir verwenden wieder eine Induktion nach n, wobei $n = 2$ trivial ist. Sei jetzt die Darstellung von $k \in \mathbb{N}$ als Primzahlprodukt eindeutig für $k = 2, 3, \ldots, n$ und sei

$$n + 1 = p_0 p_1 \cdots p_s = q_0 q_1 \cdots q_t$$

mit Primzahlen p_i, q_j, die der Bedingung $p_0 \leq p_1 \leq \ldots \leq p_s$ bzw. $q_0 \leq q_1 \leq \ldots \leq q_t$ genügen. Wegen $p_0 \mid (p_0 p_1 \cdots p_s)$ gilt natürlich auch $p_0 \mid (q_0 q_1 \cdots q_t)$ und mit Folgerung 3.47b schließt man $p_0 = q_j \geq q_0$ für ein $j \in \{0, 1, \ldots, t\}$. Analog erhält man $q_0 \geq p_0$ und damit $p_0 = q_0$.

Ist nun $s = 0$, dann muss auch $t = 0$ sein, denn andernfalls erhielten wir aus

$$n + 1 = p_0 = p_0 \cdot q_1 q_2 \cdots q_t$$

einen Widerspruch zu $p_0 \in \mathbb{P}$. Damit ist aber $n+1 = p_0$ die eindeutige Darstellung von $n+1$. Ebenso behandelt man den Fall $t = 0$.

Seien jetzt $s > 0$ und $t > 0$, dann können wir den Faktor p_0 aus der Gleichung

$$n + 1 = p_0 p_1 \cdots p_s = p_0 q_1 \cdots q_t$$

herauskürzen und erhalten

$$k := p_1 \cdots p_s = q_1 \cdots q_t$$

mit $2 \leq k \leq n$ nach Lemma 3.26(iv). Auf k können wir jetzt die Induktionsvoraussetzung anwenden und erhalten $s = t$ sowie $p_j = q_j$ für $1 \leq j \leq s$. Damit ist die Eindeutigkeit gezeigt. □

Fasst man in der Darstellung (3.14) gleiche Faktoren zu Potenzen zusammen, dann erhält man die so genannte kanonische Primfaktorzerlegung einer Zahl.

Folgerung 3.50. *Jede natürliche Zahl $n > 1$ lässt sich als endliches Produkt von Primzahlpotenzen darstellen, d. h. es gibt ein $r \in \mathbb{N}_0$ sowie paarweise verschiedene $q_0, q_1, \ldots, q_r \in \mathbb{P}$ und $\nu_0, \nu_1, \ldots, \nu_r \in \mathbb{N}$ mit*

$$n = q_0^{\nu_0} q_1^{\nu_1} \cdots q_r^{\nu_r}.$$

Dabei gilt $\nu_j = \max\{k \in \mathbb{N}; q_j^k \mid n\}$. Unter der Zusatzbedingung $q_0 < q_1 < \cdots < q_r$ ist die Darstellung eindeutig.

Beachtet man, dass sich jede ganze Zahl $k \in \mathbb{Z}$ schreiben lässt als $k = \varepsilon|k|$ mit $\varepsilon \in \{-1, 1\}$ und $|k| \in \mathbb{N}$, dann erhält man aus Satz 3.49 bzw. Folgerung 3.50

Folgerung 3.51. *Jede ganze Zahl $k \in \mathbb{Z} \setminus \{-1, 0, 1\}$ lässt sich darstellen als*

$$k = \varepsilon p_0 p_1 \cdots p_s. \tag{3.15}$$

mit $\varepsilon \in \{-1, 1\}$, $s \in \mathbb{N}_0$ sowie $p_0, p_1, \ldots, p_s \in \mathbb{P}$. Unter der Zusatzbedingung $p_0 \leq p_1 \leq \ldots \leq p_s$ ist die Darstellung eindeutig.

Außerdem besitzt k eine Darstellung als endliches Produkt von Primzahlpotenzen, d. h. es gibt ein $r \in \mathbb{N}_0$, paarweise verschiedene $q_0, q_1, \ldots, q_r \in \mathbb{P}$ und $\nu_0, \nu_1, \ldots, \nu_r \in \mathbb{N}$ mit

$$k = \varepsilon q_0^{\nu_0} q_1^{\nu_1} \cdots q_r^{\nu_r}.$$

Dabei gilt $\nu_j = \max\{k \in \mathbb{N}; q_j^k \mid k\}$. Unter der Zusatzbedingung $q_0 < q_1 < \cdots < q_r$ ist die Darstellung eindeutig.