Einführung in die Zahlentheorie

Sebastian Thomas

Manuskript (provisorisch)
Sommersemester 2013

Carl von Ossietzky Universität Oldenburg
Institut für Mathematik

Version: 22. Dezember 2013.

Dieses Vorlesungsmanuskript entstand während der Veranstaltung *Einführung in die Zahlentheorie*; gehalten an der Carl von Ossietzky Universität im Sommersemester 2013. Es befindet sich momentan noch im Aufbau.

Inhaltsverzeichnis

Vorwort

Dieses Manuskript ist provisorisch.
Mein Dank für Korrekturen gilt Florian Hörmeyer und Carina Mersmann.
Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Oldenburg, 2. Juli 2013
Sebastian Thomas

Kapitel I

Die ganzen Zahlen und verwandte Zahlbereiche

1 Die natürlichen Zahlen

Peanostrukturen

Wir formalisieren zunächst den Zählprozess, wie er etwa in der Grundschule oder sogar im Kindergarten erlernt wird.

(1.1) Definition (Peanostruktur)**.** Eine *Peanostruktur* besteht aus einer Menge N zusammen mit einer injektiven Abbildung $s\colon N \to N$ und einem Element $\alpha \in N \setminus \operatorname{Im} s$ so, dass folgendes Axiom gilt.

- *Induktionsaxiom.* Für jede Teilmenge U von N mit $\{\alpha\} \cup s(U) \subseteq U$ gilt $U = N$.

Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Peanostruktur als auch die unterliegende Menge mit N. Die Abbildung s wird *Nachfolgerabbildung* von N genannt. Das Element α wird *Anfangselement* von N genannt.
Für eine Peanostruktur N mit Nachfolgerabbildung s und Anfangselement α schreiben wir $\operatorname{suc} = \operatorname{suc}^N := s$ und $\operatorname{suc} n = \operatorname{suc}^N n := s(n)$ für $n \in N$ sowie $\mathfrak{a} = \mathfrak{a}^N := \alpha$. Für $n \in N$ nennen wir $\operatorname{suc} n$ den *Nachfolger* von n.

Das Induktionsaxiom für eine Peanostruktur N besagt also gerade, dass für jede Teilmenge U von N gilt: Wenn $\mathfrak{a} \in U$ ist und wenn für $n \in U$ auch stets $\operatorname{suc} n \in U$ gilt, dann ist bereits $U = N$. Auf dem Induktionsaxiom beruht das Induktionsprinzip, siehe Bemerkung (1.5).
Mit weiterführenden Mitteln der (axiomatischen) Mengenlehre konstruiert man die Menge $\mathbb{N}_0$ der *natürlichen Zahlen mit Null*, indem man $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, usw. setzt. Man kann dann zeigen, dass $\mathbb{N}_0$ eine Peanostruktur mit $\operatorname{suc} 0 = 1$, $\operatorname{suc} 1 = 2$, $\operatorname{suc} 2 = 3$, usw., und $\mathfrak{a}^N = 0$ wird. Wir verzichten hier auf einen formalen Beweis, da er den Rahmen dieser Veranstaltung sprengen würde. Es sei lediglich angemerkt, dass die Existenz der natürlichen Zahlen im Wesentlichen ein Axiom der Zermelo-Fraenkel-Mengenlehre ist: Die Existenz der natürlichen Zahlen folgt aus der Existenz einer unendlichen Menge, welche man per Axiom fordert.
Ebenso kann man zeigen, dass $\mathbb{N}$ zu einer Peanostruktur wird, siehe Aufgabe 2.

(1.2) Proposition. Es sei eine Peanostruktur N gegeben. Dann ist

$$N = \{\mathfrak{a}\} \dot\cup \operatorname{Im} \operatorname{suc}.$$

Beweis. Siehe Aufgabe 1(a). □

(1.3) Korollar. Es sei eine Peanostruktur N gegeben. Dann ist die Einschränkung

$$\operatorname{suc}|^{N \setminus \{\mathfrak{a}\}}\colon N \to N \setminus \{\mathfrak{a}\}$$

eine Bijektion.

Beweis. Siehe Aufgabe 1(b). □

(1.4) Definition (Vorgängerabbildung)**.** Es sei eine Peanostruktur N gegeben. Die *Vorgängerabbildung* von N ist gegeben durch

$$\operatorname{prec} = (\operatorname{suc}|^{N\setminus\{\alpha\}})^{-1}\colon N \setminus \{\alpha\} \to N.$$

Für $n \in N$ nennen wir $\operatorname{prec} n$ den *Vorgänger* von n.

Induktion und Rekursion

(1.5) Bemerkung (Induktionsprinzip)**.** Es seien eine Peanostruktur N und für jedes $n \in N$ eine Aussage φ_n gegeben. Ferner gelte φ_α und es folge aus der Gültigkeit von φ_n für $n \in N$ stets die Gültigkeit von $\varphi_{\operatorname{suc} n}$. Dann gilt φ_n für alle $n \in N$.

Beweis. Es sei $U := \{n \in N \mid \varphi_n \text{ gilt}\}$. Da φ_α gilt, ist $\alpha \in U$. Für alle $n \in U$ ist ferner φ_n gültig, nach Annahme also auch $\varphi_{\operatorname{suc} n}$, d.h. $\operatorname{suc} n \in U$. Wir erhalten $U = N$ nach dem Induktionsaxiom, d.h. φ_n ist gültig für alle $n \in N$. □

In Bemerkung (1.5) nennt man φ_α den *Induktionsanfang* und φ_n für $n \in N$ die *Induktionsannahme* für den *Induktionsschluss* $\varphi_n \Rightarrow \varphi_{\operatorname{suc} n}$.
Äquivalent können wir in Bemerkung (1.5) auch annehmen, dass φ_α gilt, und dass für alle $n \in N \setminus \{\alpha\}$ aus der Gültigkeit von $\varphi_{\operatorname{prec} n}$ auch die Gültigkeit von φ_n folgt, vgl. Proposition (1.2).
Es seien Mengen I und X gegeben. Wir erinnern daran, dass eine Familie in X über I eine Teilmenge x von $I \times X$ ist, mit der Zusatzbedingung, dass es für alle $i \in I$ genau ein $y \in X$ mit $(i, y) \in x$ gibt. Wir schreiben dann üblicherweise $x_i = y$ und $(x_i)_{i\in I} = x$.

(1.6) Satz (Rekursionssatz)**.** Es sei eine Peanostruktur N gegeben. Für jede Menge X, jede Abbildung $t\colon X \to X$ und jedes Element $a \in X$ gibt es genau eine Familie $x = (x_n)_{n\in N}$ in X mit $x_\alpha = a$ und $x_{\operatorname{suc} n} = t(x_n)$ für $n \in N$.

Beweis. Um die Existenz von x zu zeigen, setzen wir

$$I := \{y \subseteq N \times X \mid (\alpha, a) \in y \text{ und für } (n, b) \in y \text{ ist auch } (\operatorname{suc} n, t(b)) \in y\}$$

und

$$x := \bigcap I.$$

Zunächst zeigen wir, dass x das bzgl. Inklusion kleinste Element von I ist. Für alle $y \in I$ ist $(\alpha, a) \in y$, also auch $(\alpha, a) \in \bigcap I = x$. Für $(n, b) \in x = \bigcap I$ gilt $(n, b) \in y$ für alle $y \in I$, also auch $(\operatorname{suc} n, t(b)) \in y$ für alle $y \in I$ und damit $(\operatorname{suc} n, t(b)) \in \bigcap I = x$. Folglich ist $x \in I$. Wegen $x = \bigcap I \subseteq y$ für alle $y \in I$ ist x ferner das bzgl. Inklusion kleinste Element von I.
Als nächstes wollen wir zeigen, dass x eine Familie in X über N ist, also dass es für alle $n \in N$ genau ein $b \in X$ mit $(n, b) \in x$ gibt. Hierzu führen wir Induktion nach n.
Wegen $x \in I$ ist $(\alpha, a) \in x$. Für die Eindeutigkeit sei ein beliebiges $a' \in X$ mit $(\alpha, a') \in x$ gegeben und es sei $x' := x \setminus \{(\alpha, a')\}$, so dass $x = x' \dot\cup \{(\alpha, b)\}$ gilt. Da x das bzgl. Inklusion kleinste Element von I ist, impliziert dies $x' \notin I$. Für $(n, b) \in x' \subset x$ gilt jedoch $(\operatorname{suc} n, t(b)) \in x$; und wegen $\alpha \notin \operatorname{Im}\operatorname{suc}$ sogar $(\operatorname{suc} n, t(b)) \in x \setminus \{(\alpha, a')\} = x'$. Dies bedeutet jedoch, dass $(\alpha, a) \notin x'$ ist. Wegen $(\alpha, a) \in x = x' \dot\cup \{(\alpha, a')\}$ folgt $(\alpha, a) = (\alpha, a')$, also $a' = a$. Insgesamt haben wir gezeigt, dass es genau ein $b \in X$ mit $(\alpha, b) \in x$ gibt.
Es sei ein beliebiges $n \in N$ gegeben und es gebe genau ein $b \in X$ mit $(n, b) \in x$. Wegen $x \in I$ folgt dann $(\operatorname{suc} n, t(b)) \in x$. Für die Eindeutigkeit sei ein beliebiges $c' \in X$ mit $(\operatorname{suc} n, c') \in x$ gegeben und es sei $x' := x \setminus \{(\operatorname{suc} n, c')\}$, so dass $x = x' \dot\cup \{(\operatorname{suc} n, c')\}$ gilt. Da x das bzgl. Inklusion kleinste Element von I ist, impliziert dies $x' \notin I$. Es gilt jedoch $(\alpha, a) \in x$; und wegen $\alpha \notin \operatorname{Im}\operatorname{suc}$ sogar $(\alpha, a) \in x \setminus \{(\operatorname{suc} n, c')\} = x'$. Für $(m, d) \in x' \subset x$ gilt ferner $(\operatorname{suc} m, t(d)) \in x$. Für $(m, d) \in x' \subset x$ mit $m \neq n$ folgt wegen der Injektivität der Nachfolgerfunktion aber $\operatorname{suc} m \neq \operatorname{suc} n$, es ist also sogar $(\operatorname{suc} m, t(d)) \in x \setminus \{(\operatorname{suc} n, c')\} = x'$. Folglich gibt es ein $d \in X$ mit $(n, d) \in x' \subset x$ und $(\operatorname{suc} n, t(d)) \notin x'$. Die Induktionsvoraussetzung impliziert nun aber $d = b$. Somit haben wir $(n, b) \in x'$ und $(\operatorname{suc} n, t(b)) \notin x'$. Wegen $(\operatorname{suc} n, t(b)) \in x = x' \dot\cup \{(\operatorname{suc} n, c')\}$ folgt $(\operatorname{suc} n, t(b)) = (\operatorname{suc} n, c')$, also $c' = t(b)$. Insgesamt haben wir gezeigt, dass es genau ein $c \in X$ mit $(\operatorname{suc} n, c) \in x$ gibt.

Nach dem Induktionsprinzip (1.5) gibt es also für jedes $n \in N$ genau ein $b \in X$ mit $(n, b) \in x$, d.h. x ist eine Familie in X über N. Nach Konstruktion gilt ferner: Es ist $(\alpha, a) \in x$, d.h. $x_\alpha = a$. Für $n \in N$ ist $(n, x_n) \in x$, also ist auch $(\operatorname{suc} n, t(x_n)) \in x$, d.h. $x_{\operatorname{suc} n} = t(x_n)$.
Um die Eindeutigkeit zu zeigen, sei eine beliebige Familie $x' = (x'_n)_{n \in N}$ in X gegeben. Dann gilt $x'_\alpha = a = x_\alpha$. Für $n \in N$ mit $x'_n = x_n$ folgt ferner

$$x'_{\operatorname{suc} n} = t(x'_n) = t(x_n) = x_{\operatorname{suc} n}.$$

Nach dem Induktionsprinzip (1.5) gilt daher $x'_n = x_n$ für alle $n \in N$, also $x' = x$. □

Anstelle der Aussage in Satz (1.6) kann man (mit der dort verwendeten Notation) auch sagen, dass es genau eine Familie $x = (x_n)_{n \in N}$ in X mit

$$x_n = \begin{cases} a, & \text{falls } n = \alpha, \\ \operatorname{suc}(x_{\operatorname{prec} n}), & \text{falls } n \neq \alpha, \end{cases}$$

für $n \in N$ gibt.

(1.7) Korollar. Es sei eine Peanostruktur N gegeben. Für jede Menge X, jede Abbildung $t\colon X \to X$ und jedes Element $a \in X$ gibt es genau eine Abbildung $f\colon N \to X$ mit $f(\alpha) = a$ und $f \circ \operatorname{suc} = t \circ f$.

(1.8) Korollar. Es seien Peanostrukturen N und P gegeben. Ferner sei $f\colon N \to P$ die eindeutige Abbildung mit $f(\alpha^N) = \alpha^P$ und $f \circ \operatorname{suc}^N = \operatorname{suc}^P \circ f$ und es sei $g\colon P \to N$ die eindeutige Abbildung mit $g(\alpha^P) = \alpha^N$ und $g \circ \operatorname{suc}^P = \operatorname{suc}^N \circ g$. Dann invertieren f und g sich gegenseitig.

Beweis. Es gilt

$$g(f(\alpha^N)) = g(\alpha^P) = \alpha^N,$$
$$g \circ f \circ \operatorname{suc}^N = g \circ \operatorname{suc}^P \circ f = \operatorname{suc}^N \circ g \circ f$$

sowie

$$f(g(\alpha^P)) = f(\alpha^N) = \alpha^P,$$
$$f \circ g \circ \operatorname{suc}^P = f \circ \operatorname{suc}^N \circ g = \operatorname{suc}^P \circ f \circ g.$$

Andererseits haben wir aber auch $\operatorname{id}_N(\alpha^N) = \alpha^N$ und $\operatorname{id}_N \circ \operatorname{suc}^N = \operatorname{suc}^N \circ \operatorname{id}_N$ sowie $\operatorname{id}_P(\alpha^P) = \alpha^P$ und $\operatorname{id}_P \circ \operatorname{suc}^P = \operatorname{suc}^P \circ \operatorname{id}_P$. Nach Korollar (1.7) folgt $g \circ f = \operatorname{id}_N$ sowie $f \circ g = \operatorname{id}_P$, d.h. f und g sind sich gegenseitig invertierende Abbildungen. □

Korollar (1.7) und Korollar (1.8) besagen zusammen insbesondere, dass alle Peanostrukturen *isomorph* sind, unter Verwendung eines geeigneten Isomorphiebegriffs: Es gibt sich gegenseitig invertierende Abbildungen, welche verträglich mit den Nachfolgerabbildungen und den Anfangselementen sind. Wir werden daher im Folgenden ausschließlich mit der Peanostruktur $\mathbb{N}_0$ arbeiten.

Algebraische Struktur

Als nächstes wollen wir die bekannte algebraische Struktur auf $\mathbb{N}_0$ herleiten, unter Verwendung der auf der Menge $\mathbb{N}_0$ definierten Peanostruktur.
Für die formale Einführung der Addition auf $\mathbb{N}_0$ wiederholen wir zunächst die notwendigen Konzepte aus der Algebra.
Ein *Monoid* besteht aus einer Menge M zusammen mit einer Verknüpfung $\cdot$ auf M, welche *Multiplikation* (oder *Monoidverknüpfung*) von M genannt wird, derart, dass die Multiplikation assoziativ ist und es ein neutrales Element bzgl. der Multiplikation, die *Eins* von M, gibt. Dieses neutrale Element ist eindeutig durch die Multiplikation bestimmt und wird als 1 notiert. Ein Monoid heißt *kommutativ*, falls seine Multiplikation kommutativ ist. Ein Monoid M erfüllt die *Kürzungseigenschaft*, falls für $x, y, z \in M$ aus $xz = yz$ oder $zx = zy$ stets $x = y$ folgt.
Ein *abelsches Monoid* ist ein kommutatives Monoid A, für welches wir jedoch eine andere Standardnotation verwenden: Die Monoidverknüpfung von A heißt *Addition* von A und wird als $+$ notiert. Das neutrale Element bzgl. der Addition heißt *Null* von A und wird als 0 notiert.
Um keinen Missbrauch zwischen den Notationen im abstrakten Kontext und den konkreten Elementen von $\mathbb{N}_0$ zu haben, verwenden wir vorerst noch die Notationen aus Definition (1.1) anstatt der Zahlen 0, 1, 2, usw.

(1.9) Proposition. Die Menge $\mathbb{N}_0$ wird ein abelsches Monoid, welches die Kürzungseigenschaft erfüllt, mit Addition rekursiv gegeben durch

$$m + n = \begin{cases} m, & \text{falls } n = \alpha, \\ \operatorname{suc}(m + \operatorname{prec} n), & \text{falls } n \neq \alpha. \end{cases}$$

für $m, n \in \mathbb{N}_0$. Die Null von $\mathbb{N}_0$ ist gegeben durch

$$0 = \alpha.$$

Ferner gilt

$$\operatorname{suc} n = n + \operatorname{suc} 0 = \operatorname{suc} 0 + n$$

für alle $n \in \mathbb{N}_0$.

Beweis. Wir definieren eine Verknüpfung a auf $\mathbb{N}_0$ durch $a(m, \alpha) := m$ für $m \in \mathbb{N}_0$ und $a(m, \operatorname{suc} n) := \operatorname{suc}(a(m, n))$ für $m, n \in \mathbb{N}_0$ (hier benutzen wir implizit Korollar (1.7)).
Um Assoziativität von a, d.h. $a(m, a(n, p)) = a(a(m, n), p)$ für $m, n, p \in \mathbb{N}_0$, zu zeigen, führen wir Induktion nach p. Für $p = \alpha$ gilt

$$a(m, a(n, \alpha)) = a(m, n) = a(a(m, n), \alpha).$$

Es sei also $p \in \mathbb{N}_0$ beliebig gegeben und gelte $a(m, a(n, p)) = a(a(m, n), p)$ für $m, n \in \mathbb{N}_0$. Dann folgt auch

$$a(m, a(n, \operatorname{suc} p)) = a(m, \operatorname{suc}(a(n, p))) = \operatorname{suc}(a(m, a(n, p))) = \operatorname{suc}(a(a(m, n), p)) = a(a(m, n), \operatorname{suc} p)$$

für $m, n \in \mathbb{N}_0$. Nach dem Induktionsprinzip gilt also $a(m, a(n, p)) = a(a(m, n), p)$ für alle $m, n, p \in \mathbb{N}_0$, d.h. a ist assoziativ.
Als nächstes wollen wir zeigen, dass α ein neutrales Element bzgl. a ist. In der Tat gilt $a(n, \alpha) = n$ für $n \in \mathbb{N}_0$ nach Definition von a, d.h. α ist ein rechtsneutrales Element bzgl. a. Um $a(\alpha, n) = n$ für $n \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach n. Für $n = \alpha$ gilt

$$a(\alpha, \alpha) = \alpha.$$

Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $a(\alpha, n) = n$. Dann folgt auch

$$a(\alpha, \operatorname{suc} n) = \operatorname{suc}(a(\alpha, n)) = \operatorname{suc} n.$$

Nach dem Induktionsprinzip gilt also auch $a(\alpha, n) = n$ für alle $n \in \mathbb{N}_0$, d.h. α ist ein linksneutrales Element bzgl. a. Insgesamt ist α ein neutrales Element bzgl. a.
Für $n \in \mathbb{N}_0$ gilt

$$\operatorname{suc} n = \operatorname{suc}(a(n, \alpha)) = a(n, \operatorname{suc} \alpha).$$

Um $\operatorname{suc} n = a(\operatorname{suc} \alpha, n)$ für $n \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach n. Für $n = \alpha$ gilt

$$\operatorname{suc} \alpha = a(\operatorname{suc} \alpha, \alpha).$$

Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $\operatorname{suc} n = a(\operatorname{suc} \alpha, n)$. Dann folgt auch

$$\operatorname{suc}(\operatorname{suc} n) = \operatorname{suc}(a(\operatorname{suc} \alpha, n)) = a(\operatorname{suc} \alpha, \operatorname{suc} n).$$

Nach dem Induktionsprinzip gilt also auch $\operatorname{suc} n = a(\operatorname{suc} \alpha, n)$ für alle $n \in \mathbb{N}_0$.
Um Kommutativität von a, d.h. $a(m, n) = a(n, m)$ für $m, n \in \mathbb{N}_0$, zu zeigen, führen wir Induktion nach n. Für $n = \alpha$ gilt

$$a(m, \alpha) = m = a(\alpha, m),$$

da α ein neutrales Element bzgl. a ist. Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $a(m, n) = a(n, m)$ für $m \in \mathbb{N}_0$. Unter Ausnutzung des Assoziativität von a folgt dann auch

$$a(m, \operatorname{suc} n) = \operatorname{suc}(a(m, n)) = \operatorname{suc}(a(n, m)) = a(n, \operatorname{suc} m) = a(n, a(\operatorname{suc} \alpha, m)) = a(a(n, \operatorname{suc} \alpha), m)$$

$$= a(\operatorname{suc} n, m)$$

für $m \in \mathbb{N}_0$. Nach dem Induktionsprinzip gilt also $a(m,n) = a(n,m)$ für alle $m, n \in \mathbb{N}_0$, d.h. a ist kommutativ. Um unter Ausnutzung der Kommutativität von a schließlich die Kürzungseigenschaft für a zu zeigen, müssen wir nachweisen, dass aus $a(m,p) = a(n,p)$ für $m, n, p \in \mathbb{N}_0$ stets $m = n$ folgt. Hierzu führen wir Induktion nach p. Es sei zunächst $p = \alpha$ und es seien $m, n \in \mathbb{N}_0$ mit $a(m,\alpha) = a(n,\alpha)$ gegeben. Dann gilt auch

$$m = a(m,\alpha) = a(n,\alpha) = n.$$

Es sei nun $p \in \mathbb{N}_0$ beliebig gegeben und es folge aus $a(m,p) = a(n,p)$ für $m, n \in \mathbb{N}_0$ stets $m = n$. Ferner seien $m, n \in \mathbb{N}_0$ mit $a(m, \operatorname{suc} p) = a(n, \operatorname{suc} p)$ gegeben. Dann folgt

$$\operatorname{suc}(a(m,p)) = a(m, \operatorname{suc} p) = a(n, \operatorname{suc} p) = \operatorname{suc}(a(n,p)),$$

wegen der Injektivität von suc also $a(m,p) = a(n,p)$ und damit $m = n$. Nach dem Induktionsprinzip folgt also aus $a(m,p) = a(n,p)$ für $m, n, p \in \mathbb{N}_0$ stets $m = n$, d.h. a erfüllt die Kürzungseigenschaft.
Insgesamt wird $\mathbb{N}_0$ ein abelsches Monoid, welches die Kürzungseigenschaft erfüllt, mit Addition gegeben durch $m + n = a(m,n)$ für $m, n \in \mathbb{N}_0$ und Null $0 = \alpha$. Ferner gilt $\operatorname{suc} n = n + \operatorname{suc} 0 = \operatorname{suc} 0 + n$ für alle $n \in \mathbb{N}_0$. □

(1.10) Konvention. Ab jetzt betrachten wir $\mathbb{N}_0$ als abelsches Monoid mit Addition gegeben wie in Proposition (1.9).

(1.11) Proposition. Das einzige negierbare Element von $\mathbb{N}_0$ ist 0.

Beweis. Wegen $0 + 0 = 0$ ist 0 negierbar in $\mathbb{N}_0$ mit $-0 = 0$. Für $n \neq 0$ gilt hingegen

$$m + n = m + \operatorname{suc}(\operatorname{prec} n) = \operatorname{suc}(m + \operatorname{prec} n) \neq 0$$

für alle $m \in \mathbb{N}_0$, da $0 = \alpha \notin \operatorname{Im} \operatorname{suc}$ ist. Dies bedeutet aber, dass jedes negierbare Element $n \in \mathbb{N}_0$ bereits gleich 0 sein muss. □

Ein *Halbring* besteht aus einem abelschen Monoid R zusammen mit einer Verknüpfung $\cdot$ auf R, welche *Multiplikation* von R genannt wird, derart, dass die unterliegende Menge von R zusammen mit der Multiplikation ein Monoid wird, und so, dass für alle $x \in R$ die Abbildungen $R \mapsto R$, $y \mapsto xy$ und $R \mapsto R$, $y \mapsto yx$ Homomorphismen abelscher Monoide sind. Ein Halbring heißt *kommutativ*, falls sein unterliegendes Monoid kommutativ ist, also falls seine Multiplikation kommutativ ist.
Ein *Halbbereich* ist ein Halbring R so, dass das unterliegende abelsche Monoid die Kürzungseigenschaft erfüllt, und so, dass für $x, y, z \in R$ aus $xz = yz$ oder $zx = zy$ stets $x = y$ oder $z = 0$ folgt.

(1.12) Satz. Die Menge $\mathbb{N}_0$ wird ein kommutativer Halbbereich mit Addition und Multiplikation rekursiv gegeben durch

$$m + n = \begin{cases} m, & \text{falls } n = \alpha, \\ \operatorname{suc}(m + \operatorname{prec} n), & \text{falls } n \neq \alpha, \end{cases}$$

$$m \cdot n = \begin{cases} \alpha, & \text{falls } n = \alpha, \\ (m \cdot (\operatorname{prec} n)) + m, & \text{falls } n \neq \alpha, \end{cases}$$

für $m, n \in \mathbb{N}_0$. Die Null und die Eins von $\mathbb{N}_0$ sind gegeben durch

$$0 = \alpha,$$
$$1 = \operatorname{suc} \alpha.$$

Ferner gilt

$$\operatorname{suc} n = n + 1 = 1 + n$$

für alle $n \in \mathbb{N}_0$.

Beweis. Nach Proposition (1.9) wird $\mathbb{N}_0$ ein abelsches Monoid, welches die Kürzungseigenschaft erfüllt, mit Addition gegeben durch

$$m + n = \begin{cases} m, & \text{falls } n = \alpha, \\ \operatorname{suc}(m + \operatorname{prec} n), & \text{falls } n \neq \alpha, \end{cases}$$

für $m, n \in \mathbb{N}_0$, und Null $0 = \alpha$. Wir definieren eine Verknüpfung b auf $\mathbb{N}_0$ durch $b(m, \alpha) := \alpha$ für $m \in \mathbb{N}_0$ und $b(m, \operatorname{suc} n) := b(m, n) + m$ für $m, n \in \mathbb{N}_0$ (hier benutzen wir implizit Korollar (1.7)).
Zuerst wollen wir zeigen, dass $b(-, p)\colon \mathbb{N}_0 \to \mathbb{N}_0$ für $p \in \mathbb{N}_0$ ein Homomorphismus abelscher Monoide ist, führen wir Induktion nach p. Für $p = \alpha$ gilt

$$b(m + n, \alpha) = \alpha = 0 = 0 + 0 = \alpha + \alpha = b(m, \alpha) + b(n, \alpha)$$

für $m, n \in \mathbb{N}_0$ sowie

$$b(0, \alpha) = \alpha = 0,$$

d.h. $b(-, \alpha)$ ist ein Homomorphismus abelscher Monoide. Es sei also $p \in \mathbb{N}_0$ beliebig gegeben und es sei $b(-, p)$ ein Homomorphismus abelscher Monoide. Dann folgt

$$\begin{aligned} b(m + n, \operatorname{suc} p) &= b(m + n, p) + (m + n) = (b(m, p) + b(n, p)) + (m + n) = (b(m, p) + m) + (b(n, p) + n) \\ &= b(m, \operatorname{suc} p) + b(n, \operatorname{suc} p) \end{aligned}$$

für $m, n \in \mathbb{N}_0$ sowie

$$b(0, \operatorname{suc} p) = b(0, p) + 0 = b(0, p) = 0,$$

d.h. auch $b(-, \operatorname{suc} p)$ ist ein Homomorphismus abelscher Monoide. Nach dem Induktionsprinzip ist also $b(-, p)$ für alle $p \in \mathbb{N}_0$ ein Homomorphismus abelscher Monoide.
Als nächstes wollen wir zeigen, dass $\operatorname{suc} \alpha$ ein neutrales Element bzgl. b ist. In der Tat gilt

$$b(n, \operatorname{suc} \alpha) = b(n, \alpha) + n = \alpha + n = 0 + n = n$$

für $n \in \mathbb{N}_0$, d.h. $\operatorname{suc} \alpha$ ist ein rechtsneutrales Element bzgl. b. Um $b(\operatorname{suc} \alpha, n) = n$ für $n \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach n. Für $n = \alpha$ gilt

$$b(\operatorname{suc} \alpha, \alpha) = \alpha.$$

Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $b(\operatorname{suc} \alpha, n) = n$. Dann folgt auch

$$b(\operatorname{suc} \alpha, \operatorname{suc} n) = b(\operatorname{suc} \alpha, n) + \operatorname{suc} \alpha = n + \operatorname{suc} \alpha = \operatorname{suc} n.$$

Nach dem Induktionsprinzip gilt also auch $b(\operatorname{suc} \alpha, n) = n$ für alle $n \in \mathbb{N}_0$, d.h. $\operatorname{suc} \alpha$ ist ein linksneutrales Element bzgl. b. Insgesamt ist $\operatorname{suc} \alpha$ ein neutrales Element bzgl. b.
Um Kommutativität von b, d.h. $b(m, n) = b(n, m)$ für $m, n \in \mathbb{N}_0$, zu zeigen, führen wir Induktion nach n. Für $n = \alpha$ gilt

$$b(m, \alpha) = \alpha = 0 = b(0, m) = b(\alpha, m)$$

für $m \in \mathbb{N}_0$, da $b(-, m)$ ein Homomorphismus abelscher Monoide ist. Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $b(m, n) = b(n, m)$ für $m \in \mathbb{N}_0$. Da $\operatorname{suc} \alpha$ ein linksneutrales Element bzgl. b und $b(-, m)$ für $m \in \mathbb{N}_0$ ein Homomorphismus abelscher Monoide ist, folgt dann auch

$$b(m, \operatorname{suc} n) = b(m, n) + m = b(n, m) + b(\operatorname{suc} \alpha, m) = b(n + \operatorname{suc} \alpha, m) = b(\operatorname{suc} n, m)$$

für $m \in \mathbb{N}_0$. Nach dem Induktionsprinzip gilt also $b(m, n) = b(n, m)$ für alle $m, n \in \mathbb{N}_0$, d.h. b ist kommutativ.
Aus der Kommutativität von b folgt, dass $b(p, -) = b(-, p)$ für alle $p \in \mathbb{N}_0$ ein Homomorphismus abelscher Monoide ist.

Um Assoziativität von b, d.h. $b(m, b(n,p)) = b(b(m,n),p)$ für $m,n,p \in \mathbb{N}_0$, zu zeigen, führen wir Induktion nach p. Für $p = \alpha$ gilt

$$b(m, b(n,\alpha)) = b(m,\alpha) = \alpha = b(b(m,n),\alpha).$$

Es sei also $p \in \mathbb{N}_0$ beliebig gegeben und gelte $b(m, b(n,p)) = b(b(m,n),p)$ für $m,n \in \mathbb{N}_0$. Da $b(m,-)$ für $m \in \mathbb{N}_0$ ein Homomorphismus abelscher Monoide ist, folgt dann auch

$$b(m, b(n, \operatorname{suc} p)) = b(m, b(n,p) + n) = b(m, b(n,p)) + b(m,n) = b(b(m,n),p) + b(m,n) = b(b(m,n), \operatorname{suc} p)$$

für $m,n \in \mathbb{N}_0$. Nach dem Induktionsprinzip gilt also $b(m, b(n,p)) = b(b(m,n),p)$ für alle $m,n,p \in \mathbb{N}_0$, d.h. b ist assoziativ.
Als nächstes wollen wir zeigen, dass aus $b(m,n) = 0$ für $m,n \in \mathbb{N}_0$ stets $m = 0$ oder $n = 0$ folgt. Hierzu führen wir Induktion nach n. Für $n = \alpha$ gilt $n = \alpha = 0$. Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und es folgt aus $b(m,n) = 0$ für $m \in \mathbb{N}_0$ stets $m = 0$. Ferner sei $m \in \mathbb{N}_0$ mit $b(m, \operatorname{suc} n) = 0$ gegeben. Es folgt $b(m,n) + m = b(m, \operatorname{suc} n) = 0$ und da b kommutativ ist, folgt die Negierbarkeit von m in $\mathbb{N}_0$. Nach Proposition (1.11) folgt $m = 0$.
Unter Ausnutzung der Kommutativität von b verbleibt zu zeigen, dass aus $b(m,n) = b(m,p)$ für $m,n,p \in \mathbb{N}_0$ stets $m = 0$ oder $n = p$ folgt. Hierzu führen wir Induktion nach n. Es sei zunächst $n = \alpha$ und es seien $m,p \in \mathbb{N}_0$ mit $b(m,\alpha) = b(m,p)$ gegeben. Dann folgt $b(m,p) = b(m,\alpha) = \alpha = 0$, also $m = 0$ oder $p = 0 = \alpha = n$. Es sei nun $n \in \mathbb{N}_0$ beliebig gegeben und es folge aus $b(m,n) = b(m,p)$ für $m,p \in \mathbb{N}_0$ stets $m = 0$ oder $n = p$. Ferner seien $m,p \in \mathbb{N}_0$ mit $b(m, \operatorname{suc} n) = b(m,p)$ gegeben und es gelte $m \neq 0$. Dann folgt $0 \neq b(m,n) + m = b(m, \operatorname{suc} n) = b(m,p)$, nach Proposition (1.11) also auch $p \neq 0$. Es folgt

$$b(m,n) + m = b(m,p) = b(m, \operatorname{suc}(\operatorname{prec} p)) = b(m, \operatorname{prec} p) + m.$$

Da die Addition von $\mathbb{N}_0$ jedoch die Kürzungseigenschaft erfüllt, impliziert dies bereits $b(m,n) = b(m, \operatorname{prec} p)$, also $n = \operatorname{prec} p$ und damit $\operatorname{suc} n = \operatorname{suc}(\operatorname{prec} p) = p$. Nach dem Induktionsprinzip folgt also aus $b(m,n) = b(m,p)$ für $m,n,p \in \mathbb{N}_0$ stets $m = 0$ oder $n = p$.
Insgesamt wird $\mathbb{N}_0$ ein kommutativer Halbbereich mit Multiplikation gegeben durch $m \cdot n = b(m,n)$ für $m,n \in \mathbb{N}_0$ und Eins $1 = \operatorname{suc} \alpha$. Ferner gilt $\operatorname{suc} n = n + 1 = 1 + n$ für alle $n \in \mathbb{N}_0$ nach Proposition (1.9). □

(1.13) Konvention. Ab jetzt betrachten wir $\mathbb{N}_0$ als kommutativen Halbbereich mit Addition und Multiplikation gegeben wie in Satz (1.12).

Da wir nun Addition und Multiplikation auf $\mathbb{N}_0$ hergeleitet haben, werden wir ab jetzt das Induktionsprinzip in der bekannten Form verwenden. Wir schreiben also 0 statt α sowie $n+1$ statt $\operatorname{suc} n$ sowie $n-1$ statt $\operatorname{prec} n$ für $n \in \mathbb{N}_0$.

Ordnungsstruktur

Es sei eine Menge X gegeben. Eine Relation r auf X heißt *transitiv*, falls für $x,y,z \in X$ aus $x\ r\ y$ und $y\ r\ z$ stets $x\ r\ z$ folgt; *reflexiv*, falls für $x \in X$ stets $x\ r\ x$ gilt; *antisymmetrisch*, falls für $x,y \in X$ aus $x\ r\ y$ und $y\ r\ x$ stets $x = y$ folgt; und *konnex*, falls für $x,y \in X$ stets $x\ r\ y$ oder $y\ r\ x$ oder $x = y$ gilt. Eine (*partielle*) *Ordnung* auf X ist eine Relation auf X, welche transitiv, reflexiv und antisymmetrisch ist. Eine *Totalordnung* auf X ist eine konnexe Ordnung auf X.
Eine *total geordnete Menge* ist eine Menge X zusammen mit einer Totalordnung $\leq$, welche *Totalordnung* von X genannt wird.
Es sei eine total geordnete Menge X gegeben. Für $x,y \in X$ schreiben wir $x < y$, falls $x \leq y$ und $x \neq y$ ist. Die Relation $<$ auf X ist transitiv und *irreflexiv*, d.h. für kein $x \in X$ gilt $x < x$.

(1.14) Proposition. Die Menge $\mathbb{N}_0$ wird eine total geordnete Menge, wobei die Totalordnung von $\mathbb{N}_0$ wie folgt gegeben ist. Für $m,n \in \mathbb{N}_0$ gilt genau dann $m \leq n$, wenn es ein $q \in \mathbb{N}_0$ mit $m + q = n$ gibt.

Beweis. Wir definieren eine Relation o auf $\mathbb{N}_0$ wie folgt: Für $m,n \in \mathbb{N}_0$ gelte $m\ o\ n$ genau dann, wenn es ein $q \in \mathbb{N}_0$ mit $m + q = n$ gibt. Wir wollen zeigen, dass o eine Totalordnung auf $\mathbb{N}_0$ ist.
Es seien $m,n,p \in \mathbb{N}_0$ mit $m\ o\ n$ und $n\ o\ p$ gegeben. Dann gibt es $q,r \in \mathbb{N}_0$ mit $m + q = n$ und $n + r = p$. Es folgt $m + q + r = n + r = p$, also $m\ o\ p$. Folglich ist o transitiv.
Für $n \in \mathbb{N}_0$ gilt stets $n + 0 = n$, also $n\ o\ n$. Folglich ist o reflexiv.

Es seien $m, n \in \mathbb{N}_0$ mit $m \; o \; n$ und $n \; o \; m$ gegeben. Dann gibt es $q, r \in \mathbb{N}_0$ mit $m + q = n$ und $n + r = m$. Es folgt $m + q + r = n + r = m$. Da $\mathbb{N}_0$ die Kürzungseigenschaft erfüllt, impliziert dies aber bereits $q + r = 0$. Auf Grund der Kommutativität der Addition erhalten wir $q = 0$ nach Proposition (1.11) und somit $m = n$. Folglich ist o antisymmetrisch.
Es sei $m \in \mathbb{N}_0$ gegeben. Um zu zeigen, dass für $n \in \mathbb{N}_0$ stets $m \; o \; n$ oder $n \; o \; m$ gilt, führen wir Induktion nach n. Für $n = 0$ gilt $0 + m = m$, also $n = 0 \; o \; m$. Es sei also $n \in \mathbb{N}_0$ beliebig gegeben und gelte $m \; o \; n$ oder $n \; o \; m$. Wir nehmen zunächst an, dass $m \; o \; n$ gilt, so dass es ein $q \in \mathbb{N}_0$ mit $m + q = n$ gibt. Es folgt $m + q + 1 = n + 1$, also auch $m \; o \; (n + 1)$. Nun nehmen wir an, dass $n \; o \; m$ gilt, so dass es ein $q \in \mathbb{N}_0$ mit $n + q = m$ gibt. Wegen der Reflexivität können wir ferner o.B.d.A. annehmen, dass $m \neq n$ ist. Dann folgt $q \neq 0$, also $(n + 1) + (q - 1) = n + q = m$ und damit $(n + 1) \; o \; m$. Nach dem Induktionsprinzip gilt für alle $n \in \mathbb{N}_0$ somit $m \; o \; n$ oder $n \; o \; m$. Folglich ist o konnex.
Insgesamt wird $\mathbb{N}_0$ eine total geordnete Menge mit Totalordnung $\leq = o$. □

(1.15) Konvention. Ab jetzt betrachten wir $\mathbb{N}_0$ auch als total geordnete Menge mit Totalordnung gegeben wie in Proposition (1.14).

(1.16) Bemerkung. Für $m, n \in \mathbb{N}_0$ gilt genau dann $m < n$, wenn es ein $p \in \mathbb{N}$ mit $m + p = n$ gibt.

Beweis. Es seien $m, n \in \mathbb{N}_0$ gegeben. Genau dann gilt $m < n$, wenn $m \leq n$ und $m \neq n$ gilt. Nun ist $m \leq n$ äquivalent dazu, dass es ein $p \in \mathbb{N}_0$ mit $m + p = n$ gibt. Auf Grund der Kürzungsregel ist dann jedoch $m \neq n = m + p$ äquivalent zu $p \neq 0$, d.h. zu $p \in \mathbb{N}$. Insgesamt gilt genau dann $m < n$, wenn es ein $p \in \mathbb{N}$ mit $m + p = n$ gibt. □

Wenn nichts anderes gesagt wird, fassen wir eine Teilmenge einer total geordneten Menge als total geordnete Menge bzgl. der *eingeschränkten Totalordnung* auf. So wird etwa $\{1, 3, 7\}$ eine *total geordnete Teilmenge* von $\mathbb{N}_0$ mit $1 < 3 < 7$.
Es sei eine partiell geordnete Menge X gegeben. Ein *kleinstes Element* von X ist ein Element $x \in X$ so, dass $x \leq y$ für alle $y \in X$ gilt. Ein *größtes Element* von X ist ein Element $x \in X$ so, dass $y \leq x$ für alle $y \in X$ gilt. Es lässt sich zeigen, dass kleinste und größte Elemente stets eindeutig bestimmt sind.

(1.17) Bemerkung.

(a) Es ist 0 das kleinste Element von $\mathbb{N}_0$. Es gibt kein größtes Element von $\mathbb{N}_0$.

(b) Es ist 1 das kleinste Element von $\mathbb{N}$. Es gibt kein größtes Element von $\mathbb{N}$.

(c) Für alle $n \in \mathbb{N}_0$ ist 0 das kleinste und n das größte Element von $\{m \in \mathbb{N}_0 \mid m \leq n\}$.

Beweis.

(a) Für alle $n \in \mathbb{N}_0$ ist $0 + n = n$ und damit $0 \leq n$. Folglich ist 0 das kleinste Element von $\mathbb{N}_0$.
Für jedes $n \in \mathbb{N}_0$ gilt ferner $n < n + 1$ und damit $n + 1 \not\leq n$. Folglich gibt es kein größtes Element von $\mathbb{N}_0$.

(b) Siehe Aufgabe 8(a).

(c) Es sei $n \in \mathbb{N}_0$ gegeben und es sei $U := \{m \in \mathbb{N}_0 \mid m \leq n\}$. Da 0 nach (a) kleinstes Element von $\mathbb{N}_0$ ist, folgt $0 \in U$ und $0 \leq m$ für alle $m \in U$, d.h. 0 ist das kleinste Element von U. Nach Definition von U gilt ferner $n \leq n$, also $n \in U$, sowie $m \leq n$ für alle $m \in U$, d.h. n ist das größte Element von U. □

(1.18) Proposition. Für alle $n \in \mathbb{N}_0$ besitzt jede nicht-leere Teilmenge von $\{m \in \mathbb{N}_0 \mid m \leq n\}$ ein kleinstes und ein größtes Element.

Beweis. Siehe Aufgabe 7(a). □

Eine *wohlgeordnete Menge* ist eine total geordnete Menge X so, dass jede Teilmenge (aufgefasst als total geordnete Teilmenge bzgl. der eingeschränkten Totalordnung) ein kleinstes Element besitzt.

(1.19) Korollar. Es ist $\mathbb{N}_0$ eine wohlgeordnete Menge.

Beweis. Siehe Aufgabe 7(b). □

(1.20) Proposition. Es seien $m, n, p \in \mathbb{N}_0$ gegeben.

(a) Genau dann gilt $p + m \leq p + n$, wenn $m \leq n$ ist.

(b) Genau dann gilt $pm \leq pn$, wenn $m \leq n$ oder $p = 0$ ist.

Beweis.

(a) Genau dann gilt $p+m \leq p+n$, wenn es ein $q \in \mathbb{N}_0$ mit $p+m+q = p+n$ gibt. Da $\mathbb{N}_0$ die Kürzungseigenschaft erfüllt, ist dies aber äquivalent dazu, dass es ein $q \in \mathbb{N}_0$ mit $m + q = n$ gibt, d.h. zu $m \leq n$.

(b) Da $\mathbb{N}_0$ ein Halbbereich ist, gilt genau dann $pm = pn$, wenn $m = n$ oder $p = 0$ ist.

Es gelte $p \neq 0$ und $m < n$, so dass es nach Bemerkung (1.16) ein $q \in \mathbb{N}$ mit $m + q = n$ gibt. Wir erhalten $pm + pq = p(m + q) = pn$, wobei wegen $p \neq 0$ und $q \neq 0$ auch $pq \neq 0$ ist. Folglich ist nach Bemerkung (1.16) auch $pm < pn$.

Wir haben also insbesondere: Wenn $m \leq n$ oder $p = 0$ ist, dann ist in jedem Fall $pm \leq pn$.

Andererseits, wenn $m \not\leq n$ und $p \neq 0$ ist, dann folgt aus der Konnexität von $<$, dass $n < m$ ist, also $pn < pm$ und damit $pm \not\leq pn$. Mittels Kontraposition schließen wir, dass $pm \leq pn$ stets $m \leq n$ oder $p = 0$ impliziert. □

(1.21) Korollar. Es ist

$$\mathbb{N}_0^\times = \{1\}.$$

Beweis. Siehe Aufgabe 8(b). □

Aufgaben

Aufgabe 1 (Peanostrukturen)**.** Es sei eine Peanostruktur N gegeben. Zeigen Sie:

(a) Es ist

$$N = \{\alpha\} \dot\cup \operatorname{Im} \operatorname{suc}.$$

(b) Die Einschränkung

$$\operatorname{suc}|^{N\setminus\{\alpha\}} \colon N \to N \setminus \{\alpha\}$$

ist eine Bijektion.

Aufgabe 2 (natürliche Zahlen)**.** Zeigen Sie, dass $\mathbb{N}$ zu einer Peanostruktur wird (mit einer geeignet zu definierenden Nachfolgerabbildung und einem geeignet zu definierenden Anfangselement).

Aufgabe 3 (Cantor-Diagonalisierung)**.** Es seien $p \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ und $s \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0$ definiert durch

$$p(m,n) := \sum_{i \in [1, m+n]} i + n,$$

$$s(m,n) := \begin{cases} (n+1, 0), & \text{falls } m = 0, \\ (m-1, n+1), & \text{falls } m \neq 0, \end{cases}$$

für $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$. Zeigen Sie:

(a) Es gilt $p(0, 0) = 0$ und $p(s(m, n)) = p(m, n) + 1$ für alle $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$.

(b) Die Menge $\mathbb{N}_0 \times \mathbb{N}_0$ wird eine Peanostruktur mit Nachfolgerabbildung $\operatorname{suc}^{\mathbb{N}_0 \times \mathbb{N}_0} = s$ und Anfangselement $\alpha^{\mathbb{N}_0 \times \mathbb{N}_0} = (0, 0)$.

(c) Es ist $p \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ eine Bijektion.

Aufgabe 4 (Potenzgesetze)**.** Für $n, k \in \mathbb{N}_0$ definieren wir rekursiv

$$n^k := \begin{cases} 1, & \text{falls } k = 0, \\ n^{k-1}\, n, & \text{falls } k \neq 0. \end{cases}$$

Zeigen Sie:

(a) Für $n, k, l \in \mathbb{N}_0$ gilt

$$n^k \, n^l = n^{k+l}.$$

(b) Für $n, k, l \in \mathbb{N}_0$ gilt

$$(n^k)^l = n^{kl}.$$

(c) Für $m, n, k \in \mathbb{N}_0$ gilt

$$m^k \, n^k = (mn)^k.$$

Aufgabe 5 (Zyklizität)**.** Es sei ein abelsches Untermonoid U von $\mathbb{N}_0$ mit $1 \in U$ gegeben. Zeigen Sie, dass dann bereits $U = \mathbb{N}_0$ ist.

Aufgabe 6 (Ordnung auf $\mathbb{N}_0$)**.** Es seien $m, n \in \mathbb{N}_0$ gegeben. Zeigen Sie: Genau dann gilt $m \leq n$, wenn es ein $p \in \mathbb{N}_0$ mit $n = \mathrm{suc}^p(m)$ gibt.

Aufgabe 7 (Wohlordnung auf $\mathbb{N}_0$)**.** Zeigen Sie:

(a) Für alle $n \in \mathbb{N}_0$ besitzt jede nicht-leere Teilmenge von $U_n = \{m \in \mathbb{N}_0 \mid m \leq n\}$ ein kleinstes und ein größtes Element.

Hinweis. Induktion nach n.

(b) Es ist $\mathbb{N}_0$ eine wohlgeordnete Menge.

Hinweis. Betrachten Sie für $U \subseteq \mathbb{N}_0$ und $n \in U$ die Teilmenge $V := \{m \in U \mid m \leq n\}$.

Aufgabe 8 (Einheiten von $\mathbb{N}_0$)**.** Zeigen Sie:

(a) Es ist 1 das kleinste Element von $\mathbb{N}$.

(b) Es ist $\mathbb{N}_0^\times = \{1\}$.

2 Die ganzen Zahlen

Formales Negieren

Es seien eine abelsche Gruppe Z und ein injektiver Homomorphismus abelscher Monoide $\iota\colon \mathbb{N}_0 \to Z$ gegeben. Wenn wir $\mathbb{N}_0$ mit $\mathrm{Im}\,\iota$ identifizieren, so können wir also Z als „Erweiterung“ von $\mathbb{N}_0$ auffassen, in welcher Negative stets existieren und in welcher sich die üblichen Rechenregeln bzgl. der Addition, wie Assoziativität und Kommutativität, fortsetzen.
In Z lassen sich also beliebige Differenzen $x - y$ von Elementen $x, y \in Z$ bilden. Insbesondere also von Elementen aus $\mathrm{Im}\,\iota$ oder, wenn wir direkt mit $\mathbb{N}_0$ arbeiten wollen, Differenzen der Form $\iota(m) - \iota(s)$ für $m, s \in \mathbb{N}_0$. Wir erhalten also die Abbildung

$$d\colon \mathbb{N}_0 \times \mathbb{N}_0 \to Z,\ (m, s) \mapsto \iota(m) - \iota(s).$$

Wir wollen nun der Frage nachgehen, welche Elemente aus $\mathbb{N}_0 \times \mathbb{N}_0$ via der Differenzbildung auf dasselbe Element in Z abgebildet werden (mit anderen Worten, welche Paare bildgleich bzgl. d sind). Es seien $(m, s), (n, t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gegeben. Nach Definition von d gilt genau dann $d(m, s) = d(n, t)$, wenn $\iota(m) - \iota(s) = \iota(n) - \iota(t)$ ist. Dies ist äquivalent zu $\iota(m) + \iota(t) = \iota(n) + \iota(s)$. Da ι als Homomorphismus verträglich mit den Additionen ist, gilt dies wiederum genau dann, wenn $\iota(m + t) = \iota(n + s)$ ist, und dies ist auf Grund der Injektivität von ι äquivalent zu $m + t = n + s$.
Unsere Analyse motiviert nun folgende Definition.

(1.22) Definition (Differenzgleichheit)**.** Die Relation $\equiv$ auf $\mathbb{N}_0 \times \mathbb{N}_0$ sei wie folgt definiert: Für $(m, s), (n, t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gelte genau dann $(m, s) \equiv (n, t)$, wenn

$$m + t = n + s$$

ist.
Haben wir $(m, s), (n, t) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $(m, s) \equiv (n, t)$ gegeben, so sagen wir, dass (m, s) und (n, t) *differenzgleich* sind.

Es sei eine Menge X gegeben. Eine Relation r auf X heißt *symmetrisch*, falls für $x, y \in X$ aus $x\ r\ y$ stets $y\ r\ x$ folgt. Eine *Äquivalenzrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und symmetrisch ist.
Es sei eine Äquivalenzrelation c auf X gegeben. Für $x \in X$ heißt $[x] = \{\tilde{x} \in X \mid \tilde{x}\ c\ x\}$ die *Äquivalenzklasse* von x bzgl. c. Die Menge aller Äquivalenzklassen $X/c = \{[x] \mid x \in X\}$ wird *Quotient* von X modulo c genannt.

(1.23) Bemerkung. Es ist $\equiv$ eine Äquivalenzrelation auf $\mathbb{N}_0 \times \mathbb{N}_0$.

Beweis. Es seien $(m,s),(n,t),(p,u) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $(m,s) \equiv (n,t)$ und $(n,t) \equiv (p,u)$ gegeben. Dann gilt $m+t = n+s$ und $n+u = p+t$, also

$$m+u+t = m+t+u = n+s+u = n+u+s = p+t+s = p+s+t.$$

Da das abelsche Monoid $\mathbb{N}_0$ die Kürzungseigenschaft erfüllt, folgt $m+u = s+p = p+s$, d.h. $(m,s) \equiv (p,u)$. Folglich ist $\equiv$ transitiv.
Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt $m+s = m+s$, also $(m,s) \equiv (m,s)$. Folglich ist $\equiv$ reflexiv.
Für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $(m,s) \equiv (n,t)$ gilt $m+t = n+s$, also auch $n+s = m+t$ und damit $(n,t) \equiv (m,s)$. Folglich ist $\equiv$ symmetrisch.
Insgesamt ist $\equiv$ eine Äquivalenzrelation. □

(1.24) Definition (Menge der ganzen Zahlen)**.** Die *Menge der ganzen Zahlen* ist definiert als

$$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0)/\equiv.$$

Ein Element von $\mathbb{Z}$ heißt *ganze Zahl*.
Die Äquivalenzklasse eines Paares $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ wird *Differenz* von (m,s) genannt und als

$$[m,s] := [(m,s)]_{\equiv}$$

notiert.

(1.25) Bemerkung. Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$, $k \in \mathbb{N}_0$ gilt

$$[m+k, s+k] = [m,s]$$

in $\mathbb{Z}$.

Beweis. Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$, $k \in \mathbb{N}_0$ gilt $m+k+s = m+s+k$, also $(m+k, s+k) \equiv (m,s)$ und damit $[m+k, s+k] = [m,s]$ in $\mathbb{Z}$. □

Als nächstes kommen wir zu ersten Aussagen hinsichtlich der algebraischen Struktur von $\mathbb{Z}$. Wir haben $\mathbb{Z}$ aus der Not heraus, nicht beliebige Differenzen bilden zu können, konstruiert. Daher sollte sich nun eine Addition auf $\mathbb{Z}$ ergeben, bei welcher jedes Element ein Negatives besitzt. Obwohl wir auf $\mathbb{N}_0$ eine Halbringstruktur und damit zwei Verknüpfungen definiert haben, betrachten wir zunächst nur die Addition, da bzgl. dieser Verknüpfung Negative konstruiert werden sollten. Die multiplikative Struktur sowie die Ordnung werden danach in Satz (1.32) betrachtet.
Eine *Gruppe* ist ein Monoid G in welchem jedes Element invertierbar ist. Das Inverse eines Elements $g \in G$ ist eindeutig bestimmt und wird als g^{-1} notiert.
Eine *abelsche Gruppe* ist eine kommutative Gruppe A, wobei wir die additive Notation eines abelschen Monoids verwenden. Das *Negative* (Inverse bzgl. der Addition) eines Elements $a \in A$ wird als $-a$ notiert.

(1.26) Satz. Die Menge $\mathbb{Z}$ wird eine abelsche Gruppe mit Addition gegeben durch

$$[m,s] +^{\mathbb{Z}} [n,t] = [m +^{\mathbb{N}_0} n, s +^{\mathbb{N}_0} t]$$

für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$. Die Null von $\mathbb{Z}$ ist gegeben durch

$$0^{\mathbb{Z}} = [0^{\mathbb{N}_0}, 0^{\mathbb{N}_0}].$$

Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ ist das Negative von $[m,s]$ in $\mathbb{Z}$ gegeben durch

$$-[m,s] = [s,m].$$

Beweis. Um zu zeigen, dass die beschriebene Addition wohldefiniert ist, seien $(m,s),(\tilde{m},\tilde{s}),(n,t),(\tilde{n},\tilde{t}) \in \mathbb{N}_0\times\mathbb{N}_0$ mit $(m,s) \equiv (\tilde{m},\tilde{s})$ und $(n,t) \equiv (\tilde{n},\tilde{t})$ gegeben. Dann gilt $m+\tilde{s} = \tilde{m}+s$ und $n+\tilde{t} = \tilde{n}+t$, also auch

$$m+n+\tilde{s}+\tilde{t} = m+\tilde{s}+n+\tilde{t} = \tilde{m}+s+\tilde{n}+t = \tilde{m}+\tilde{n}+s+t,$$

d.h. $(m+n,s+t) \equiv (\tilde{m}+\tilde{n},\tilde{s}+\tilde{t})$.
Somit erhalten wir eine wohldefinierte Verknüpfung

$$a\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z},\ ([m,s],[n,t]) \mapsto [m+n,s+t].$$

Wir wollen zeigen, dass $\mathbb{Z}$ eine abelsche Gruppe mit Addition a wird.
Für $(m,s),(n,t),(p,u) \in \mathbb{N}_0\times\mathbb{N}_0$ gilt

$$\begin{aligned} a([m,s],a([n,t],[p,u])) &= a([m,s],[n+p,t+u]) = [m+(n+p),s+(t+u)] = [(m+n)+p,(s+t)+u] \\ &= a([m+n,s+t],[p,u]) = a(a([m,s],[n,t]),[p,u]). \end{aligned}$$

Folglich ist a assoziativ.
Für $(m,s),(n,t) \in \mathbb{N}_0\times\mathbb{N}_0$ gilt

$$a([m,s],[n,t]) = [m+n,s+t] = [n+m,t+s] = a([n,t],[m,s]).$$

Folglich ist a kommutativ.
Für $(m,s) \in \mathbb{N}_0\times\mathbb{N}_0$ gilt

$$a([m,s],[0,0]) = [m+0,s+0] = [m,s].$$

Folglich ist $[0,0]$ ein neutrales Element bzgl. a.
Für $(m,s) \in \mathbb{N}_0\times\mathbb{N}_0$ gilt

$$a([m,s],[s,m]) = [m+s,s+m] = [0,0]$$

nach Bemerkung (1.25). Folglich ist $[s,m]$ ein inverses Element zu $[m,s]$ bzgl. a.
Insgesamt wird $\mathbb{Z}$ eine abelsche Gruppe mit Addition gegeben durch $[m,s]+[n,t] = a([m,s],[n,t])$ für $(m,s),(n,t) \in \mathbb{N}_0\times\mathbb{N}_0$, Null $0=[0,0]$ und Negativen $-[m,s]=[s,m]$ für $(m,s)\in\mathbb{N}_0\times\mathbb{N}_0$. □

(1.27) Konvention. Ab jetzt betrachten wir $\mathbb{Z}$ als abelsche Gruppe mit Addition gegeben wie in Satz (1.26).

Als nächstes wollen wir $\mathbb{N}_0$ in $\mathbb{Z}$ wiederfinden:

(1.28) Proposition. Die Abbildung

$$\iota\colon \mathbb{N}_0 \to \mathbb{Z},\ n \mapsto [n,0]$$

ist ein injektiver Homomorphismus abelscher Monoide.

Beweis. Für $m,n \in \mathbb{N}_0$ gilt

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

Da ferner auch

$$\iota(0) = [0,0] = 0$$

gilt, ist ι somit ein Homomorphismus abelscher Monoide. Für $m,n\in\mathbb{N}_0$ mit $\iota(m)=\iota(n)$ in $\mathbb{Z}$ gilt $[m,0]=[n,0]$, also $m = m+0 = n+0 = n$ in $\mathbb{N}_0$. Folglich ist ι injektiv. □

(1.29) Konvention. Von jetzt an identifizieren wir $\mathbb{N}_0$ mit dem Bild der injektiven Abbildung $\iota\colon \mathbb{N}_0 \to \mathbb{Z}$ aus Proposition (1.28). Das heißt, unter Missbrauch der Notationen schreiben wir $\mathbb{N}_0$ anstatt $\operatorname{Im}\iota$, und, für $n\in\mathbb{N}_0$, notieren wir das Bild $\iota(n)$ von n auch durch n. Ferner versehen wir $\operatorname{Im}\iota = \mathbb{N}_0$ via Strukturtransport entlang $\iota|^{\operatorname{Im}\iota}\colon \mathbb{N}_0 \to \operatorname{Im}\iota$ mit der bereits auf $\mathbb{N}_0$ definierten Struktur (Peanostruktur, Halbring, total geordnete Menge). Hierdurch wird das abelsche Monoid $\mathbb{N}_0 = \operatorname{Im}\iota$ ein abelsches Untermonoid von $\mathbb{Z}$.

Durch diese Konvention können wir nun eine neue Darstellung der Elemente in $\mathbb{Z}$ herleiten: Ganze Zahlen werden zu Differenzen (in $\mathbb{Z}$) von Elementen aus $\mathbb{N}_0$.

(1.30) Bemerkung. Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ ist

$$[m,s] = m - s.$$

Beweis. Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ ist

$$[m,s] = [m,0] + [0,s] = [m,0] - [s,0] = m - s. \qquad \square$$

(1.31) Bemerkung.

(a) Es ist

$$\mathbb{Z} = \{m - s \mid (m,s) \in \mathbb{N}_0 \times \mathbb{N}_0\}.$$

(b) Für $m,n,s,t \in \mathbb{N}_0$ gilt genau dann

$$m - s = n - t$$

in $\mathbb{Z}$, wenn

$$m + t = n + s$$

in $\mathbb{N}_0$ gilt.

Beweis.

(a) Nach Bemerkung (1.30) gilt

$$\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0)/{\equiv} = \{[m,s] \mid (m,s) \in \mathbb{N}_0 \times \mathbb{N}_0\} = \{m - s \mid (m,s) \in \mathbb{N}_0 \times \mathbb{N}_0\}. \qquad \square$$

Algebraische Struktur und Ordnungsstruktur

Da wir auf $\mathbb{N}_0$ neben der Struktur eines abelschen Monoids noch mehr Struktur definiert haben, stellt sich natürlich die Frage, ob sich diese Struktur irgendwie auf $\mathbb{Z}$ fortsetzen lässt. Eine positive Antwort liefert der nachfolgende Satz.
Ein *Ring* besteht aus einer abelschen Gruppe R zusammen mit einer Verknüpfung $\cdot$ auf R, welche *Multiplikation* von R genannt wird, derart, dass die unterliegende Menge von R zusammen mit der Multiplikation ein Monoid wird, und so, dass für alle $x \in R$ die Abbildungen $R \mapsto R$, $y \mapsto xy$ und $R \mapsto R$, $y \mapsto yx$ Homomorphismen abelscher Gruppen sind. Letztere Bedingung ist äquivalent dazu, dass die beiden Distributivgesetze erfüllt sind, also dass $x(y+z) = (xy) + (xz)$ und $(x+y)z = (xz) + (yz)$ für alle $x,y,z \in R$ gilt. Ein Ring heißt *kommutativ*, falls sein unterliegendes Monoid kommutativ ist, also falls seine Multiplikation kommutativ ist.
Ein *total geordneter Ring* ist ein Ring R zusammen mit einer Totalordnung $\leq$, welche Totalordnung von R genannt wird, so, dass für $x,y,z \in R$ aus $x \leq y$ stets $x + z \leq y + z$ folgt, und so, dass für $x,y \in R$ aus $0 \leq x$ und $0 \leq y$ stets $0 \leq xy$ folgt.
Es sei eine total geordnete Menge X gegeben. Eine *volle total geordnete Teilmenge* von X ist eine total geordnete Menge U so, dass die unterliegende Menge von U eine Teilmenge von X ist und so, dass für $x,y \in U$ genau dann $x \leq^U y$ gilt, wenn $x \leq^X y$ gilt.

(1.32) Satz.

(a) Die Menge $\mathbb{Z}$ wird ein total geordneter kommutativer Ring mit Addition und Multiplikation gegeben durch

$$\begin{aligned}(m -^{\mathbb{Z}} s) +^{\mathbb{Z}} (n -^{\mathbb{Z}} t) &= (m +^{\mathbb{N}_0} n) -^{\mathbb{Z}} (s +^{\mathbb{N}_0} t),\\ (m -^{\mathbb{Z}} s) \cdot^{\mathbb{Z}} (n -^{\mathbb{Z}} t) &= (m \cdot^{\mathbb{N}_0} n +^{\mathbb{N}_0} s \cdot^{\mathbb{N}_0} t) -^{\mathbb{Z}} (m \cdot^{\mathbb{N}_0} t +^{\mathbb{N}_0} s \cdot^{\mathbb{N}_0} n),\end{aligned}$$

für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$. Die Null und die Eins von $\mathbb{Z}$ sind gegeben durch

$$0^{\mathbb{Z}} = 0^{\mathbb{N}_0},$$

$$1^{\mathbb{Z}} = 1^{\mathbb{N}_0}.$$

Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ ist das Negative von $m -^{\mathbb{Z}} s$ in $\mathbb{Z}$ gegeben durch

$$-(m -^{\mathbb{Z}} s) = s -^{\mathbb{Z}} m.$$

Die Totalordnung von $\mathbb{Z}$ ist wie folgt gegeben. Für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt genau dann $m -^{\mathbb{Z}} s \leq^{\mathbb{Z}} n -^{\mathbb{Z}} t$, wenn $m +^{\mathbb{N}_0} t \leq^{\mathbb{N}_0} n +^{\mathbb{N}_0} s$ ist.

(b) Der Halbring $\mathbb{N}_0$ wird bzgl. der Struktur aus (a) ein Unterhalbring von $\mathbb{Z}$. Die total geordnete Menge $\mathbb{N}_0$ ist eine volle total geordnete Teilmenge von $\mathbb{Z}$.

Beweis.

(a) Nach Satz (1.26) und Konvention (1.29) wird $\mathbb{Z}$ eine abelsche Gruppe, mit Addition gegeben durch

$$(m-s)+(n-t) = (m+n)-(s+t)$$

für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$. Ferner wird $\mathbb{N}_0$ ein abelsches Untermonoid von $\mathbb{Z}$.

Um zu zeigen, dass die beschriebene Multiplikation wohldefiniert ist, seien $(m,s),(\tilde{m},\tilde{s}),(n,t),(\tilde{n},\tilde{t}) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $m - s \equiv \tilde{m} - \tilde{s}$ und $n - t \equiv \tilde{n} - \tilde{t}$ in $\mathbb{Z}$ gegeben. Dann gilt $m + \tilde{s} = \tilde{m} + s$ und $n + \tilde{t} = \tilde{n} + t$ in $\mathbb{N}_0$, also auch

$$\begin{aligned}
mn + st + \tilde{m}\tilde{t} + \tilde{s}\tilde{n} + m\tilde{t} &= mn + m\tilde{t} + st + \tilde{m}\tilde{t} + \tilde{s}\tilde{n} = m(n+\tilde{t}) + st + \tilde{m}\tilde{t} + \tilde{s}\tilde{n} \\
&= m(\tilde{n}+t) + st + \tilde{m}\tilde{t} + \tilde{s}\tilde{n} = m\tilde{n} + ms + st + \tilde{m}\tilde{t} + \tilde{s}\tilde{n} \\
&= m\tilde{n} + \tilde{s}\tilde{n} + mt + st + \tilde{m}\tilde{t} = (m+\tilde{s})\tilde{n} + mt + st + \tilde{m}\tilde{t} \\
&= (\tilde{m}+s)\tilde{n} + mt + st + \tilde{m}\tilde{t} = \tilde{m}\tilde{n} + s\tilde{n} + mt + st + \tilde{m}\tilde{t} \\
&= \tilde{m}\tilde{n} + s\tilde{n} + st + mt + \tilde{m}\tilde{t} = \tilde{m}\tilde{n} + s(\tilde{n}+t) + mt + \tilde{m}\tilde{t} \\
&= \tilde{m}\tilde{n} + s(n+\tilde{t}) + mt + \tilde{m}\tilde{t} = \tilde{m}\tilde{n} + sn + s\tilde{t} + mt + \tilde{m}\tilde{t} \\
&= \tilde{m}\tilde{n} + sn + \tilde{m}\tilde{t} + s\tilde{t} + mt = \tilde{m}\tilde{n} + sn + (\tilde{m}+s)\tilde{t} + mt \\
&= \tilde{m}\tilde{n} + sn + (m+\tilde{s})\tilde{t} + mt = \tilde{m}\tilde{n} + sn + m\tilde{t} + \tilde{s}\tilde{t} + mt \\
&= \tilde{m}\tilde{n} + \tilde{s}\tilde{t} + mt + sn + m\tilde{t}
\end{aligned}$$

in $\mathbb{N}_0$. Da $\mathbb{N}_0$ jedoch die Kürzungsregel (bzgl. der Addtion) erfüllt, impliziert dies

$$(mn+st)+(\tilde{m}\tilde{t}+\tilde{s}\tilde{n}) = (\tilde{m}\tilde{n}+\tilde{s}\tilde{t})+(mt+sn)$$

in $\mathbb{N}_0$ und damit $(mn+st)-(mt+sn) = (\tilde{m}\tilde{n}+\tilde{s}\tilde{t})-(\tilde{m}\tilde{t}+\tilde{s}\tilde{n})$ in $\mathbb{Z}$.

Somit erhalten wir eine wohldefinierte Verknüpfung

$$b\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z},\ (m-s,n-t) \mapsto (mn+st)-(mt+sn).$$

Wir wollen zunächst zeigen, dass $\mathbb{Z}$ ein kommutativer Ring mit Multiplikation b wird.

Für $(m,s),(n,t),(p,u) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt

$$\begin{aligned}
b(m-s, b(n-t,p-u)) &= b(m-s,(np+tu)-(nu+tp)) \\
&= (m(np+tu)+s(nu+tp))-(m(nu+tp)+s(np+tu)) \\
&= (mnp+mtu+snu+stp)-(mnp+mtp+snp+stp) \\
&= (mnp+stp+mtu+snu)-(mnu+stp+mtp+snp) \\
&= ((mn+st)p+(mt+sn)u)-((mn+st)p+(mt+sn)p) \\
&= b((mn+st)-(mt+sn),p-u) = b(b(m-s,n-t),p-u)
\end{aligned}$$

Folglich ist b assoziativ.

Für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt

$$b(m-s,n-t) = (mn+st)-(mt+sn) = (nm+ts)-(ns+tm) = b(n-t,m-s).$$

Folglich ist b kommutativ.

Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt

$$b(m-s, 1^{\mathbb{N}_0}) = b(m-s, 1-0) = (m \cdot 1 + s \cdot 0) - (m \cdot 0 + s \cdot 1) = m - s.$$

Folglich ist $1^{\mathbb{N}_0}$ ein neutrales Element bzgl. b.

Für $(m,s),(n,t),(p,u) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt

$$\begin{aligned} b(m-s,(n-t)+(p-u)) &= b(m-s,(n+p)-(t+u)) \\ &= (m(n+p)+s(t+u)) - (m(t+u)+s(n+p)) \\ &= (mn+mp+st+su) - (mt+mu+sn+sp) \\ &= (mn+st+mp+su) - (mt+sn+mu+sp) \\ &= (mn+st) - (mt+sn) + (mp+su) - (mu+sp) \\ &= b(m-s,n-t) + b(m-s,p-u). \end{aligned}$$

Folglich gelten die Distributivgesetze.

Insgesamt wird $\mathbb{Z}$ ein kommutativer Ring mit Multiplikation gegeben durch $(m-s) \cdot^{\mathbb{Z}} (n-t) = b(m-s,n-t)$ für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ und Eins $1^{\mathbb{Z}} = 1^{\mathbb{N}_0}$.

Als nächstes kommen wir zur Ordnung auf $\mathbb{Z}$. Um zu zeigen, dass die beschriebene Totalordnung wohldefiniert ist, seien $(m,s),(\tilde{m},\tilde{s}),(n,t),(\tilde{n},\tilde{t}) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $m-s = \tilde{m}-\tilde{s}$ und $n-t = \tilde{n}-\tilde{t}$ in $\mathbb{Z}$ gegeben, so dass $m+\tilde{s} = \tilde{m}+s$ und $n+\tilde{t} = \tilde{n}+t$ in $\mathbb{N}_0$ gilt. Wenn $m+t \leq n+s$ in $\mathbb{N}_0$ gilt, dann folgt

$$\begin{aligned} \tilde{m}+\tilde{t}+s+t = \tilde{m}+s+\tilde{t}+t = m+\tilde{s}+\tilde{t}+t = m+t+\tilde{s}+\tilde{t} \leq n+s+\tilde{s}+\tilde{t} \\ = n+\tilde{t}+s+\tilde{s} = \tilde{n}+t+s+\tilde{s} = \tilde{n}+\tilde{s}+s+t \end{aligned}$$

und damit $\tilde{m}+\tilde{t} \leq \tilde{n}+\tilde{s}$ in $\mathbb{N}_0$ nach Proposition (1.20)(a).

Somit erhalten wir eine wohldefinierte Relation o auf $\mathbb{Z}$ gegeben durch $(m-s)\ o\ (n-t)$ für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ genau dann, wenn $m+t \leq n+s$ in $\mathbb{N}_0$ ist. Wir wollen zeigen, dass o eine Totalordnung auf $\mathbb{Z}$ ist.

Es seien $(m,s),(n,t),(p,u) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $(m-s)\ o\ (n-t)$ und $(n-t)\ o\ (p-u)$ gegeben. Dann gilt $m+t \leq n+s$ und $n+u \leq p+t$ in $\mathbb{N}_0$, also auch

$$m+u+t = m+t+u \leq n+s+u = n+u+s \leq p+t+s = p+s+t$$

und damit $m+u \leq p+s$ in $\mathbb{N}_0$ nach Proposition (1.20)(a), d.h. $(m-s)\ o\ (p-u)$. Folglich ist o transitiv.

Für $(m,s) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt stets $m+s \leq m+s$ in $\mathbb{N}_0$, also auch $(m-s)\ o\ (m-s)$ in $\mathbb{Z}$. Folglich ist o reflexiv.

Es seien $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $(m-s)\ o\ (n-t)$ und $(n-t)\ o\ (m-s)$ gegeben. Dann gilt $m+t \leq n+s$ und $n+s \leq m+t$ in $\mathbb{N}_0$, also $m+t = n+s$ in $\mathbb{N}_0$ und damit $m-s = n-t$ in $\mathbb{Z}$. Folglich ist o antisymmetrisch.

Für $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gilt $m+t \leq n+s$ oder $n+s \leq m+t$ in $\mathbb{N}_0$, also $(m-s)\ o\ (n-t)$ oder $(n-t)\ o\ (m-s)$ in $\mathbb{Z}$. Folglich ist o konnex.

Insgesamt wird $\mathbb{Z}$ eine total geordnete Menge mit Totalordnung $\leq^{\mathbb{Z}} = o$. Um zu zeigen, dass $\mathbb{Z}$ ein total geordneter Ring ist, verbleibt es, die Verträglichkeit von Addition und Multiplikation mit der Totalordnung zu zeigen.

Es seien $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $m-s \leq n-t$ in $\mathbb{Z}$ gegeben, so dass $m+t \leq n+s$ in $\mathbb{N}_0$ gilt. Für alle $(p,u) \in \mathbb{N}_0 \times \mathbb{N}_0$ folgt dann

$$m+p+t+u = m+t+p+u \leq n+s+p+u = n+p+s+u$$

in $\mathbb{N}_0$, also

$$(m-s)+(p-u) = (m+p)-(s+u) \leq (n+p)-(t+u) = (n-t)+(p-u)$$

in $\mathbb{Z}$.

Es seien $(m,s),(n,t) \in \mathbb{N}_0 \times \mathbb{N}_0$ mit $0 \leq m-s$ und $0 \leq n-t$ in $\mathbb{Z}$ gegeben, so dass $s \leq m$ und $t \leq n$ in $\mathbb{N}_0$ gilt. Wegen $s \leq m$ gibt es ein $q \in \mathbb{N}_0$ mit $m = s+q$. Nach Proposition (b) folgt aus $t \leq n$ nun $qt \leq qn$ und damit

$$\begin{aligned} mt + sn &= (s+q)t + sn = st + qt + sn = qt + st + sn \\ &\leq qn + st + sn = sn + qn + st = (s+q)n + st = mn + st \end{aligned}$$

in $\mathbb{N}_0$, also $0 \leq (mn+st) - (mt+sn) = (m-s) \cdot (n-t)$ in $\mathbb{Z}$.

Insgesamt wird $\mathbb{Z}$ ein total geordneter Ring.

(b) Wir betrachten $\mathbb{Z}$ mit der Struktur aus (a). Für $m,n \in \mathbb{N}_0$ gilt dann

$$m \cdot^{\mathbb{N}_0} n = (m \cdot^{\mathbb{N}_0} n + 0 \cdot^{\mathbb{N}_0} 0) - (m \cdot^{\mathbb{N}_0} 0 + 0 \cdot^{\mathbb{N}_0} n) = (m-0) \cdot^{\mathbb{Z}} (n-0) = m \cdot^{\mathbb{Z}} n.$$

Ferner ist $1^{\mathbb{N}_0} = 1^{\mathbb{Z}}$. Somit ist $\mathbb{N}_0$ ein Unterhalbring von $\mathbb{Z}$.

Für $m,n \in \mathbb{N}_0$ gilt ferner genau dann $m \leq^{\mathbb{N}_0} n$, wenn $(m-0) \leq^{\mathbb{Z}} (n-0)$ gilt, d.h. wenn $m \leq^{\mathbb{Z}} n$ gilt. Folglich ist $\mathbb{N}_0$ eine volle total geordnete Teilmenge von $\mathbb{N}_0$. □

(1.33) Konvention. Ab jetzt betrachten wir $\mathbb{Z}$ als total geordneten kommutativen Ring mit Addition, Multiplikation und Totalordnung gegeben wie in Satz (1.32).

Mit Hilfe der natürlichen Zahlen ergibt sich nun folgende Beschreibung von $\mathbb{Z}$.

(1.34) Satz.

(a) Es ist

$$\begin{aligned} \mathbb{N}_0 &= \{x \in \mathbb{Z} \mid x \geq 0\}, \\ \mathbb{N} &= \{x \in \mathbb{Z} \mid x > 0\}. \end{aligned}$$

(b) Es ist

$$\mathbb{Z} = \mathbb{N} \dot\cup \{0\} \dot\cup -\mathbb{N}.$$

Beweis.

(a) Da 0 nach Bemerkung (1.17)(a) das kleinste Element von $\mathbb{N}_0$ ist, gilt $x \geq 0$ für alle $x \in \mathbb{N}_0$. Es sei also umgekehrt ein $x \in \mathbb{Z}$ mit $x \geq 0$ gegeben. Nach Bemerkung (1.31)(a) gibt es $m,s \in \mathbb{N}_0$ mit $x = m-s$. Es folgt $m - s = x \geq 0$, also $m \geq s$. Dies bedeutet aber, dass es ein $p \in \mathbb{N}_0$ mit $m = s+p$ gibt, wir haben also $x = m - s = p \in \mathbb{N}_0$.

Insgesamt haben wir gezeigt, dass $\mathbb{N}_0 = \{x \in \mathbb{Z} \mid x \geq 0\}$ ist. Es folgt

$$\mathbb{N} = \mathbb{N}_0 \setminus \{0\} = \{x \in \mathbb{Z} \mid x \geq 0 \text{ und } x \neq 0\} = \{x \in \mathbb{Z} \mid x > 0\}.$$

(b) Es sei $x \in \mathbb{Z}$ gegeben. Da $<$ eine totale Striktordnung auf $\mathbb{Z}$ ist, gilt entweder $x > 0$ oder $x = 0$ oder $x < 0$. Nach (a) ist jedoch $x > 0$ äquivalent zu $x \in \mathbb{N}$, und es ist $x < 0$ äquivalent zu $-x > 0$, also zu $-x \in \mathbb{N}$ und damit zu $x \in -\mathbb{N}$. □

(1.35) Korollar. Es ist $\mathbb{Z}$ ein Bereich.

Beweis. Es ist $\mathbb{Z}$ ein total geordneter Ring.
Es seien $x,y \in \mathbb{Z}$ mit $x > 0$ und $y > 0$ gegeben. Nach Bemerkung (1.31)(a) gilt $x,y \in \mathbb{N}$, also $x,y \in \mathbb{N}_0$ mit $x \neq 0$ und $y \neq 0$. Da $\mathbb{N}_0$ ein kommutativer Halbbereich ist, folgt $xy \in \mathbb{N}_0$ und $xy \neq 0$, also $xy \in \mathbb{N}$ und damit $xy > 0$. □

(1.36) Korollar. Es ist

$$\mathbb{Z}^\times = \{1, -1\}.$$

Beweis. Siehe Aufgabe 11. □

Ein *archimedisch geordneter Ring* ist ein total geordneter Ring R so, dass für alle $x,y \in R$ mit $x > 0$ und $y \geq 0$ ein $n \in \mathbb{N}_0$ mit $x \cdot n \geq y$ existiert.

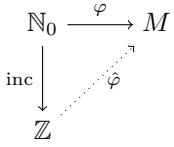
(1.37) Korollar. Es ist $\mathbb{Z}$ ein archimedisch geordneter Ring.

Beweis. Für $x,y \in \mathbb{Z}$ mit $x > 0$ und $y \geq 0$ gilt $xy \geq 1 \cdot y = y$ nach Satz (1.34)(a) und Bemerkung (1.17)(b). □

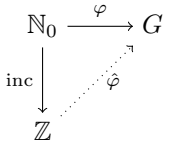
Aufgaben

Aufgabe 9 (universelle Eigenschaft der ganzen Zahlen)**.** Wir betrachten im Folgenden $\mathbb{N}_0$ als abelsches Monoid und $\mathbb{Z}$ als abelsche Gruppe. Zeigen Sie:

(a) Für jedes Monoid M und jeden Monoidhomomorphismus $\varphi\colon \mathbb{N}_0 \to M$ so, dass $\varphi(n)$ für alle $n \in \mathbb{N}_0$ invertierbar in M ist, gibt es genau einen Monoidhomomorphismus $\hat{\varphi}\colon \mathbb{Z} \to M$ mit $\varphi = \hat{\varphi}|_{\mathbb{N}_0}$.



(b) Für jede Gruppe G und jeden Monoidhomomorphismus $\varphi\colon \mathbb{N}_0 \to G$ gibt es genau einen Gruppenhomomorphismus $\hat{\varphi}\colon \mathbb{Z} \to G$ mit $\varphi = \hat{\varphi}|_{\mathbb{N}_0}$.



Aufgabe 10 (Differenzgleichheit auf abelscher Gruppe)**.** Es sei eine abelsche Gruppe A gegeben. Wir definieren eine Relation $\equiv$ auf $A \times A$ wie folgt: Für $(x, s), (y, t) \in A \times A$ gelte genau dann $(x, s) \equiv (y, t)$, wenn $x + t = y + s$ ist. Zeigen Sie:

(a) Es ist $\equiv$ eine Äquivalenzrelation auf $A \times A$.

(b) Auf $B := (A \times A)/\equiv$ gibt es eine Gruppenstruktur so, dass A und B als abelsche Gruppen isomorph werden.

Aufgabe 11 (Einheiten von $\mathbb{Z}$)**.** Zeigen Sie, dass

$$\mathbb{Z}^\times = \{1, -1\}$$

ist.

3 Die rationalen Zahlen

Formales Invertieren

Es seien ein kommutatives Monoid Q und ein injektiver Monoidhomomorphismus $\iota\colon \mathbb{Z} \to Q$ mit $\iota(x)$ invertierbar in Q für alle $x \in \mathbb{Z} \setminus \{0\}$ gegeben. Wenn wir $\mathbb{Z}$ mit $\operatorname{Im}\iota$ identifizieren, so können wir also Q als „Erweiterung“ auffassen, in welcher Inverse für alle Elemente ungleich der Null existieren und in welcher sich die üblichen Rechenregeln bzgl. der Multiplikation, wie Assoziativität und Kommutativität, fortsetzen.
Wir erhalten die Abbildung

$$f\colon \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to Q,\ (x, a) \mapsto \iota(x)\,\iota(a)^{-1}.$$

Wir wollen nun der Frage nachgehen, welche Elemente aus $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ via f auf dasselbe Element in Q abgebildet werden (mit anderen Worten, welche Paare bildgleich bzgl. f sind). Es seien $(x, a), (y, b) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ gegeben. Nach Definition von f gilt genau dann $f(x, a) = f(y, b)$, wenn $\iota(x)\,\iota(a)^{-1} = \iota(y)\,\iota(b)^{-1}$ ist. Dies ist äquivalent zu $\iota(x)\iota(b) = \iota(y)\iota(a)$. Da ι als Homomorphismus verträglich mit den Multiplikationen ist, gilt dies wiederum genau dann, wenn $\iota(xb) = \iota(ya)$ ist, und dies ist auf Grund der Injektivität von ι äquivalent zu $xb = ya$.
Diese Analyse motiviert nun folgende Definition.

(1.38) Definition (Bruchgleichheit)**.** Die Relation $\equiv$ auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ sei wie folgt definiert: Für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ gelte genau dann $(x, a) \equiv (y, b)$, wenn

$$xb = ya$$

ist.
Haben wir $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ mit $(x, a) \equiv (y, b)$ gegeben, so sagen wir, dass (x, a) und (y, b) *bruchgleich* sind.

(1.39) Bemerkung. Es ist $\equiv$ eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Beweis. Siehe Aufgabe 12(a). □

(1.40) Definition (Menge der rationalen Zahlen)**.** Die *Menge der rationalen Zahlen* ist definiert als

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\equiv.$$

Ein Element von $\mathbb{Q}$ heißt *rationale Zahl*.
Die Äquivalenzklasse eines $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ wird *Bruch* von (x, a) genannt und als

$$\frac{x}{a} := [(x, a)]_{\equiv}$$

notiert.

(1.41) Bemerkung. Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, $d \in \mathbb{Z} \setminus \{0\}$ gilt

$$\frac{xd}{ad} = \frac{x}{a}$$

in $\mathbb{Q}$.

Beweis. Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, $d \in \mathbb{Z} \setminus \{0\}$ gilt $xda = xad$, also $(xd, ad) \equiv (x, a)$ und damit $\frac{xd}{ad} = \frac{x}{a}$ in $\mathbb{Q}$. □

Analog zu Satz (1.26) können wir nun folgenden Satz herleiten, welcher zeigt, dass sich fast alle Elemente aus $\mathbb{Q}$ invertieren lassen.

(1.42) Satz. Die Menge $\mathbb{Q}$ wird ein kommutatives Monoid mit Multiplikation gegeben durch

$$\frac{x}{a} \cdot^{\mathbb{Q}} \frac{y}{b} = \frac{x \cdot^{\mathbb{Z}} y}{a \cdot^{\mathbb{Z}} b}$$

für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Die Eins von $\mathbb{Q}$ ist gegeben durch

$$1^{\mathbb{Q}} = \frac{1^{\mathbb{Z}}}{1^{\mathbb{Z}}}.$$

Für $(x, a) \in (\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \setminus \{0\})$ ist $\frac{x}{a}$ invertierbar in $\mathbb{Q}$ mit

$$((\frac{x}{a})^{-1})^{\mathbb{Q}} = \frac{a}{x}.$$

Beweis. Siehe Aufgabe 12(b). □

(1.43) Konvention. Ab jetzt betrachten wir $\mathbb{Q}$ als kommutatives Monoid mit Multiplikation gegeben wie in Satz (1.42).

Nun können wir $\mathbb{Z}$ in $\mathbb{Q}$ wiederfinden:

(1.44) Proposition. Die Abbildung

$$\iota \colon \mathbb{Z} \to \mathbb{Q},\ x \mapsto \frac{x}{1}$$

ist ein injektiver Homomorphismus kommutativer Monoide.

Beweis. Siehe Aufgabe 12(c). □

(1.45) Konvention. Von jetzt an identifizieren wir $\mathbb{Z}$ mit dem Bild der injektiven Abbildung $\iota\colon \mathbb{Z} \to \mathbb{Q}$ aus Proposition (1.44). Das heißt, unter Missbrauch der Notationen schreiben wir $\mathbb{Z}$ anstatt $\operatorname{Im}\iota$, und, für $x \in \mathbb{Z}$, notieren wir das Bild $\iota(x) = \frac{x}{1}$ von x auch durch x.

Analog zu Bemerkung (1.30) lässt sich durch diese Konvention eine neue Darstellung der Elemente in $\mathbb{Q}$ herleiten:

(1.46) Bemerkung. Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ist

$$\frac{x}{a} = xa^{-1}.$$

Beweis. Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ist

$$\frac{x}{a} = \frac{x}{1} \cdot \frac{1}{a} = \frac{x}{1} \cdot (\frac{a}{1})^{-1} = xa^{-1}.$$ □

(1.47) Bemerkung.

(a) Es ist

$$\mathbb{Q} = \{xa^{-1} \mid x \in \mathbb{Z},\, a \in \mathbb{Z} \setminus \{0\}\}.$$

(b) Für $x, y \in \mathbb{Z}$, $a, b \in \mathbb{Z} \setminus \{0\}$ gilt genau dann

$$xa^{-1} = yb^{-1}$$

in $\mathbb{Q}$, wenn

$$xb = ya$$

in $\mathbb{Z}$ gilt.

Beweis.

(a) Nach Bemerkung (1.46) gilt

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/{\equiv} = \{\frac{x}{a} \mid (x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\} = \{xa^{-1} \mid (x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}.$$ □

Da die Darstellung der Elemente von $\mathbb{Q}$ als Brüche, d.h. als Äquivalenzklassen von Elementen aus $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ durchaus üblich ist, werden wir, trotz Bemerkung (1.46) und Bemerkung (1.47), im Folgenden dieser kürzeren Darstellung meist den Vorzug geben.

Algebraische Struktur und Ordnungsstruktur

Nachdem wir die formale Inversion geklärt haben, setzen wir nun auch die Addition und die Totalordnung von $\mathbb{Z}$ auf $\mathbb{Q}$ fort.
Ein *Körper* ist ein kommutativer Ring K so, dass jedes Element von $K \setminus \{0\}$ invertierbar ist.
Ein *total geordneter Körper* ist ein total angeordneter Ring, dessen unterliegender Ring ein Körper ist.
In einem total geordneten Ring R ist das *Signum* eines Elements $x \in R$ gegeben durch

$$\operatorname{sgn} x = \begin{cases} 1, & \text{falls } x > 0, \\ 0, & \text{falls } x = 0, \\ -1, & \text{falls } x < 0, \end{cases}$$

und der *Absolutbetrag* von x durch

$$|x| = \begin{cases} x, & \text{falls } x \geq 0, \\ -x, & \text{falls } x \leq 0, \end{cases}$$

so dass $x = (\operatorname{sgn} x)\,|x|$ gilt.

(1.48) Satz.

(a) Die Menge $\mathbb{Q}$ wird ein total geordneter Körper mit Addition und Multiplikation gegeben durch

$$\frac{x}{a} +^{\mathbb{Q}} \frac{y}{b} = \frac{x \cdot^{\mathbb{Z}} b +^{\mathbb{Z}} a \cdot^{\mathbb{Z}} y}{a \cdot^{\mathbb{Z}} b},$$
$$\frac{x}{a} \cdot^{\mathbb{Q}} \frac{y}{b} = \frac{x \cdot^{\mathbb{Z}} y}{a \cdot^{\mathbb{Z}} b},$$

für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Die Null und die Eins von $\mathbb{Q}$ sind gegeben durch

$$0^{\mathbb{Q}} = \frac{0^{\mathbb{Z}}}{1^{\mathbb{Z}}},$$
$$1^{\mathbb{Q}} = \frac{1^{\mathbb{Z}}}{1^{\mathbb{Z}}}.$$

Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ist das Negative von $\frac{x}{a}$ in $\mathbb{Q}$ gegeben durch

$$(-\frac{x}{a})^{\mathbb{Q}} = \frac{(-x)^{\mathbb{Z}}}{a}.$$

Für $(x, a) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ mit $\frac{x}{a} \neq 0$ in $\mathbb{Q}$ ist das Inverse von $\frac{x}{a}$ gegeben durch

$$((\frac{x}{a})^{-1})^{\mathbb{Q}} = \frac{a}{x}.$$

Die Totalordnung von $\mathbb{Q}$ ist wie folgt gegeben. Für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ gilt genau dann $\frac{x}{a} \leq^{\mathbb{Q}} \frac{y}{b}$, wenn $(\operatorname{sgn} a)\, x|b| \leq^{\mathbb{Z}} (\operatorname{sgn} b)\, y|a|$ ist.

(b) Der total geordnete Ring $\mathbb{Z}$ wird bzgl. der Struktur aus (a) ein voller total geordneter Unterring von $\mathbb{Q}$.

Beweis.

(a) Siehe Aufgabe 12(b).

(b) Siehe Aufgabe 12(c). □

(1.49) Konvention. Ab jetzt betrachten wir $\mathbb{Q}$ als total geordneten Körper mit Addition, Multiplikation und Totalordnung gegeben wie in Satz (1.48).

Aufgaben

Aufgabe 12 (Konstruktion der rationalen Zahlen)**.** Zeigen Sie:

(a) Die Bruchgleichheitsrelation $\equiv$ auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ist eine Äquivalenzrelation.

(b) Die Menge $\mathbb{Q}$ wird ein total geordneter Körper mit Addition und Multiplikation gegeben durch

$$\frac{x}{a} +^{\mathbb{Q}} \frac{y}{b} = \frac{x \cdot^{\mathbb{Z}} b +^{\mathbb{Z}} a \cdot^{\mathbb{Z}} y}{a \cdot^{\mathbb{Z}} b},$$
$$\frac{x}{a} \cdot^{\mathbb{Q}} \frac{y}{b} = \frac{x \cdot^{\mathbb{Z}} y}{a \cdot^{\mathbb{Z}} b},$$

für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Die Totalordnung von $\mathbb{Q}$ ist wie folgt gegeben. Für $(x, a), (y, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ gilt genau dann $\frac{x}{a} \leq^{\mathbb{Q}} \frac{y}{b}$, wenn $(\operatorname{sgn} a) x|b| \leq^{\mathbb{Z}} (\operatorname{sgn} b) y|a|$ ist.

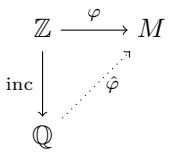
(c) Die Abbildung

$$\iota \colon \mathbb{Z} \to \mathbb{Q},\ x \mapsto \frac{x}{1}$$

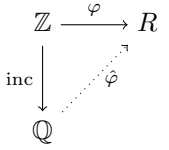
ist ein injektiver Ringhomomorphismus, welcher die Ordnungen erhält und reflektiert.

Aufgabe 13 (universelle Eigenschaft der rationalen Zahlen)**.** Wir betrachten im Folgenden $\mathbb{Z}$ und $\mathbb{Q}$ als kommutative Monoide bzw. als kommutative Ringe. Zeigen Sie:

(a) Für jedes Monoid M und jeden Monoidhomomorphismus $\varphi\colon \mathbb{Z} \to M$ so, dass $\varphi(x)$ für alle $x \in \mathbb{Z} \setminus \{0\}$ invertierbar in M ist, gibt es genau einen Monoidhomomorphismus $\hat{\varphi}\colon \mathbb{Q} \to M$ mit $\varphi = \hat{\varphi}|_{\mathbb{Z}}$.



(b) Für jeden Ring R und jeden Ringhomomorphismus $\varphi\colon \mathbb{Z} \to R$ so, dass $\varphi(x)$ für alle $x \in \mathbb{Z}\setminus\{0\}$ invertierbar in R ist, gibt es genau einen Ringhomomorphismus $\hat{\varphi}\colon \mathbb{Q} \to R$ mit $\varphi = \hat{\varphi}|_{\mathbb{Z}}$.



Kapitel II

Teilbarkeitslehre

1 Division mit Rest und die g-adische Darstellung

Division mit Rest

(2.1) Satz (Division mit Rest)**.** Für alle $x \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \{0\}$ gibt es eindeutige $q \in \mathbb{Z}$, $r \in [0, |n| - 1]$ mit

$$x = nq + r.$$

Beweis. Es sei $U := \{y \in \mathbb{N}_0 \mid \text{es gibt ein } p \in \mathbb{Z} \text{ mit } y = x - np\}$. Da $\mathbb{Z}$ nach Korollar (1.37) ein archimedischer Ring ist, gibt es ein $p \in \mathbb{N}_0$ mit $|n|p \geq |x|$. Wir erhalten

$$n(\operatorname{sgn} n)p = |n|p \geq |x| \geq -x$$

und damit

$$x - n(-(\operatorname{sgn} n)p) = x + n(\operatorname{sgn} n)p \geq 0.$$

Folglich ist $x - n(-(\operatorname{sgn} n)p) \in U$ und damit $U \neq \emptyset$. Da $\mathbb{N}_0$ nach Korollar (1.19) wohlgeordnet ist, besitzt U ein kleistes Element r. Es ist $r = x - nq$ bzw. $x = nq + r$ für ein $q \in \mathbb{Z}$ nach Definition von U. Ferner ist $U \subseteq \mathbb{N}_0$, also $r \geq 0$ nach Satz (1.34)(a). Wegen $r - |n| < r$ ist ferner $x - n(q + \operatorname{sgn} n) = x - nq - n \operatorname{sgn} n = r - |n| \notin U$. Dies bedeutet jedoch, dass $r - |n| \notin \mathbb{N}_0$, also $r - |n| < 0$ und damit $r < |n|$ gilt.
Für die Eindeutigkeit seien $q' \in \mathbb{Z}$, $r' \in [0, |n| - 1]$ mit $x = nq' + r'$ gegeben. O.B.d.A. gelte $r' \geq r$, so dass $r' - r \in [0, r] \subseteq [0, |n| - 1]$ ist. Dann gilt $nq + r = x = nq' + r'$, also

$$|n|(\operatorname{sgn} n)(q - q') = n(q - q') = nq - nq' = r' - r \in [0, |n| - 1].$$

Dies impliziert jedoch bereits $n(q - q') = r' - r = 0$ und damit $q - q' = 0$ wegen $n \neq 0$, also $r' = r$ und $q' = q$. □

(2.2) Definition (ganzzahliger Anteil, Rest)**.** Es seien $x \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \{0\}$ gegeben und es seien $q \in \mathbb{Z}$, $r \in [0, |n| - 1]$ die eindeutigen ganzen Zahlen mit $x = nq + r$. Dann heißt $x \operatorname{div} n := q$ der *ganzzahlige Anteil* und $x \bmod n := r$ der *Rest* bei der *Division mit Rest von x durch n.*

Die g-adische Darstellung

(2.3) Satz. Es seien $g \in \mathbb{N}$ mit $g \geq 2$ und $x \in \mathbb{N}_0$ gegeben. Ferner seien Folgen $(q_i)_{i \in \mathbb{N}_0}$ und $(r_i)_{i \in \mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$q_i := \begin{cases} x, & \text{falls } i = 0, \\ q_{i-1} \operatorname{div} g, & \text{falls } i \geq 1, \end{cases}$$
$$r_i := q_i \bmod g,$$

für $i \in \mathbb{N}_0$.

(a) Es existiert ein $n \in \mathbb{N}_0$ mit $r_n = q_n$ und $r_i = q_i = 0$ für $i > n$. Wenn $x \neq 0$ ist, dann kann $n \in \mathbb{N}_0$ so gewählt werden, dass zusätzlich $r_n = q_n \neq 0$ gilt.

(b) Es gilt

$$x = \sum_{i \in \mathbb{N}_0} g^i r_i.$$

Beweis. Nach Definition von $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ gilt

$$q_i = g(q_i \operatorname{div} g) + (q_i \bmod g) = gq_{i+1} + r_i$$

für alle $i \in \mathbb{N}_0$.

(a) Wegen $g \geq 2$ ist $q_i = q_{i-1} \operatorname{div} g < q_{i-1}$ für alle $i \in \mathbb{N}$, d.h. $(q_i)_{i\in\mathbb{N}_0}$ ist eine streng monoton fallende Folge. Es sei $n \in \mathbb{N}_0$ das kleinste Element mit $q_n < g$. Dann ist $q_n = g \cdot 0 + q_n$ und $q_n \in [0, g-1]$, also $q_{n+1} = q_n \operatorname{div} g = 0$ und $r_n = q_n \bmod g = q_n$. Durch Induktion folgt $q_i = 0$ und $r_i = 0$ für alle $i \in \mathbb{N}_0$ mit $i > n$. Im Fall $n = 0$ gilt ferner $r_0 = q_0 = x$ und damit $r_0 = q_0 \neq 1$, sofern $x \neq 0$. Im Fall $n \geq 1$ gilt $q_{n-1} \geq g$ auf Grund der Minimalität von n, also $r_n = q_n = q_{n-1} \operatorname{div} g \geq 1$ und damit $r_n = q_n \neq 0$. Somit gilt in jedem Fall $r_n = q_n$. Falls $x \neq 0$ ist, gilt ferner $r_n = q_n \neq 0$.

(b) Da $q_i = gq_{i+1} + r_i$ für alle $i \in \mathbb{N}_0$ gilt, folgt

$$\begin{aligned}\sum_{i\in\mathbb{N}_0} g^i r_i &= \sum_{i\in\mathbb{N}_0} g^i(q_i - gq_{i+1}) = \sum_{i\in\mathbb{N}_0} (g^i q_i - g^{i+1}q_{i+1}) = \sum_{i\in\mathbb{N}_0} g^i q_i - \sum_{i\in\mathbb{N}_0} g^{i+1}q_{i+1} \\ &= \sum_{i\in\mathbb{N}_0} g^i q_i - \sum_{i\in\mathbb{N}} g^i q_i = g^0 q_0 = x.\end{aligned}$$

□

Für eine Teilmenge X eines abelschen Monoids A bezeichne $X^{(\mathbb{N}_0)} = \{x \in X^{\mathbb{N}_0} \mid x_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$.

(2.4) Satz. Es sei $g \in \mathbb{N}$ mit $g \geq 2$ gegeben. Dann ist

$$[0, g-1]^{(\mathbb{N}_0)} \to \mathbb{N}_0,\ r \mapsto \sum_{i\in\mathbb{N}_0} g^i r_i$$

eine Bijektion.

Beweis. Wir setzen $\alpha\colon [0, g-1]^{(\mathbb{N}_0)} \to \mathbb{N}_0,\ r \mapsto \sum_{i\in\mathbb{N}_0} g^i r_i$. Nach Satz (2.3) gibt es für jedes $x \in \mathbb{N}_0$ ein $r \in [0, g-1]^{(\mathbb{N}_0)}$ mit $x = \alpha(r)$, d.h. α ist surjektiv.
Um zu zeigen, dass α auch injektiv ist, seien $r, s \in [0, g-1]^{(\mathbb{N}_0)}$ mit $\alpha(r) = \alpha(s)$ gegeben, so dass

$$\sum_{i\in\mathbb{N}_0} g^i(r_i - s_i) = \sum_{i\in\mathbb{N}_0} g^i r_i - \sum_{i\in\mathbb{N}_0} g^i s_i = \alpha_g(r) - \alpha_g(s) = 0$$

gilt. Ferner sei ein $n \in \mathbb{N}_0$ mit $r_i - s_i = 0$ für $i > n$ gegeben (wegen $r, s \in [0, g-1]^{(\mathbb{N}_0)}$ gibt es sogar ein $n \in \mathbb{N}_0$ mit $r_i = s_i = 0$ für $i > n$). Dann folgt

$$0 = \sum_{i\in\mathbb{N}_0} g^i(r_i - s_i) = \sum_{i\in[0,n]} g^i(r_i - s_i),$$

also

$$\begin{aligned}g^n\,|r_n - s_n| = |g^n(r_n - s_n)| &= |\sum_{i\in[0,n-1]} g^i(r_i - s_i)| \leq \sum_{i\in[0,n-1]} g^i\,|r_i - s_i| \leq \sum_{i\in[0,n-1]} g^i(g-1) \\ &= \sum_{i\in[0,n-1]} (g^{i+1} - g^i) = \sum_{i\in[0,n-1]} g^{i+1} - \sum_{i\in[0,n-1]} g^i = \sum_{i\in[1,n]} g^i - \sum_{i\in[0,n-1]} g^i = g^n - 1.\end{aligned}$$

Dies impliziert jedoch $|r_n - s_n| = 0$ und damit $r_n - s_n = 0$. Induktiv folgt $r_i - s_i = 0$ für alle $i \in \mathbb{N}_0$, d.h. $r = s$. Folglich ist α injektiv. □

Satz (2.4) besagt also gerade, dass es bei gegebenem $g \in \mathbb{N}$ mit $g \geq 2$ für jedes $x \in \mathbb{N}_0$ genau ein $r \in [0, g-1]^{(\mathbb{N}_0)}$ mit $x = \sum_{i \in \mathbb{N}_0} g^i r_i$ gibt.

(2.5) Definition (g-adische Darstellung)**.** Es seien $g \in \mathbb{N}$ mit $g \geq 2$ und $x \in \mathbb{N}_0$ gegeben. Das eindeutige $r \in [0, g-1]^{(\mathbb{N}_0)}$ mit $x = \sum_{i \in \mathbb{N}_0} g^i r_i$ heißt *g-adische Darstellung* von x.
Ist r die g-adische Darstellung von x und $n \in \mathbb{N}_0$ mit $r_i = 0$ für $i > n$, so schreiben wir

$$(r_n, \ldots, r_1, r_0)_g := x.$$

Satz (2.3) liefert eine Methode zur Berechnung der g-adischen Darstellung eines Elements aus $\mathbb{N}_0$:

(2.6) Algorithmus (g-adische Darstellung)**.**

(a) Rekursive Version:

- Eingabe: $g \in \mathbb{N}$ mit $g \geq 2$ und $x \in \mathbb{N}_0$
- Ausgabe: g-adische Darstellung von x
- Verfahren:

```
function gadic(x, g)
    if x = 0 then
        return ();
    end if;

    return gadic(x div g, g) ∪ (x mod g);
end function;
```

(b) Nicht-rekursive Version:

- Eingabe: $g \in \mathbb{N}$ mit $g \geq 2$ und $x \in \mathbb{N}_0$
- Ausgabe: g-adische Darstellung von x
- Verfahren:

```
function gadic(x, g)
    d := ();
    q := x;
    r := q mod g;

    while q ≠ 0 do
        d := (r) ∪ d;
        q := q div g;
        r := q mod g;
    end while;

    return d;
end function;
```

Aufgaben

Aufgabe 14 (Division mit Rest)**.** Entwerfen Sie einen Algorithmus zur Berechnung der Division mit Rest unter Einhaltung der nachfolgenden Vorgaben und implementieren Sie ihn in Magma.

- Eingabe: $(x, n) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$
- Ausgabe: $(q, r) \in \mathbb{Z} \times [0, |n| - 1]$ mit $x = nq + r$
- Verfahren: Das Programm soll wiederholt n von x abziehen bzw. zu x addieren (je nach Vorzeichen von x), bis der Rest erreicht ist.

Hinweis. Für $n < 0$ können Sie ausnutzen, dass $nq + r = (-n)(-q) + r$ ist.

Aufgabe 15 (g-adische Darstellung)**.** Implementieren Sie Algorithmus (2.6)(b) zur Berechnung der g-adischen Darstellung eines Elements aus $\mathbb{N}_0$ in Magma. Testen Sie Ihre Implementation, indem Sie die 26-adische Darstellung von

2386772756428542408

berechnen. Welches Wort erhalten Sie, wenn Sie 0 als `A`, 1 als `B`, usw. interpretieren?

2 Teilbarkeit und Ideale

Teilbarkeit

(2.7) Definition (Teilbarkeit)**.** Es seien $a, b \in \mathbb{Z}$ gegeben. Wir sagen a *teilt* b (oder dass a ein *Teiler* von b ist oder dass b ein *Vielfaches* von a ist), geschrieben $a \mid b$, falls ein $q \in \mathbb{Z}$ mit $b = aq$ existiert. Wenn a kein Teiler von b ist, so schreiben wir $a \nmid b$.

(2.8) Beispiel. Es gilt $3 \mid 6$ und $4 \nmid 6$.

(2.9) Bemerkung. Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Genau dann gilt $a \mid b$, wenn $b \bmod a = 0$ ist.

(2.10) Proposition.

(a) Für $a, b, c \in \mathbb{Z}$ folgt aus $a \mid b$ und $b \mid c$ stets $a \mid c$.

(b) Für $a \in \mathbb{Z}$ gilt $a \mid a$.

(c) Für $a, b \in \mathbb{Z}$ gilt genau dann $a \mid b$ und $b \mid a$, wenn $|a| = |b|$ ist.

Beweis.

(a) Es seien $a, b, c \in \mathbb{Z}$ mit $a \mid b$ und $b \mid c$ gegeben, d.h. es gebe $p, q \in \mathbb{Z}$ mit $b = ap$ und $c = bq$. Dann folgt

$$c = bq = (ap)q = a(pq),$$

also $a \mid c$.

(b) Für $a \in \mathbb{Z}$ gilt $a = a \cdot 1$, d.h. $a \mid a$.

(c) Es seien $a, b \in \mathbb{Z}$ gegeben. Zunächst gelte $a \mid b$ und $b \mid a$, d.h. es gebe $p, q \in \mathbb{Z}$ mit $b = ap$ und $a = bq$. Dann folgt

$$a = bq = (ap)q = a(pq).$$

Da $\mathbb{Z}$ ein Bereich ist, folgt $a = 0$ oder $pq = 1$. Wenn $a = 0$ ist, dann ist $b = ap = 0 = a$, also auch $|a| = |b|$. Wenn $pq = 1$ ist, dann ist $p \in \mathbb{Z}^\times = \{1, -1\}$, also auch in diesem Fall $|a| = |a|\,|p| = |ap| = |b|$.

Ist umgekehrt $|a| = |b|$, also $b = ua$ für ein $u \in \mathbb{Z}^\times$, so folgt $a = ub$ und damit $a \mid b$ und $b \mid a$. □

(2.11) Korollar.

(a) Die Teilbarkeitsrelation auf $\mathbb{Z}$ ist transitiv und reflexiv.

(b) Die Teilbarkeitsrelation auf $\mathbb{N}$ und auf $\mathbb{N}_0$ ist eine Ordnungsrelation.

(2.12) Proposition.

(a) Für $a, b, c \in \mathbb{Z}$ gilt: Wenn $a \mid b$ und $a \mid c$, dann auch $a \mid b + c$.

(b) Für $a \in \mathbb{Z}$ gilt $a \mid 0$.

(c) Für $a, b, c \in \mathbb{Z}$ gilt: Wenn $a \mid b$, dann auch $a \mid bc$.

Beweis.

(a) Es seien $a, b, c \in \mathbb{Z}$ mit $a \mid b$ und $a \mid c$ gegeben, d.h. es gebe $p, q \in \mathbb{Z}$ mit $b = ap$ und $c = aq$. Dann folgt

$$b + c = ap + aq = a(p + q),$$

also $a \mid b + c$.

(b) Für $a \in \mathbb{Z}$ gilt $0 = a \cdot 0$, also $a \mid 0$.

(c) Es seien $a, b, c \in \mathbb{Z}$ gegeben und es gelte $a \mid b$. Dann gibt es ein $q \in \mathbb{Z}$ mit $b = aq$. Es folgt

$$bc = (aq)c = a(qc),$$

also $a \mid bc$. □

(2.13) Korollar. Für $a, b \in \mathbb{Z}$ gilt genau dann $a \mid b$, wenn $a \mid -b$ gilt.

Beweis. Es seien $a, b \in \mathbb{Z}$ gegeben. Wenn $a \mid b$ gilt, so auch $a \mid b(-1) = -b$ nach Proposition (2.12)(c). Wenn $a \mid -b$ gilt, so auch $a \mid -(-b) = b$. □

(2.14) Bemerkung. Es seien $a, b, c \in \mathbb{Z}$ gegeben.

(a) Wenn $a \mid b$ gilt, dann auch $ca \mid cb$.

(b) Wenn $ca \mid cb$ und $c \neq 0$ gilt, dann auch $a \mid b$.

Beweis. Siehe Aufgabe 16(a). □

(2.15) Bemerkung. Für $a, b \in \mathbb{Z}$ gilt genau dann $a \mid b$, wenn $-a \mid b$ gilt.

Beweis. Siehe Aufgabe 16(b). □

(2.16) Bemerkung. Für $a \in \mathbb{Z}$ gilt $1 \mid a$ und $-1 \mid a$.

Beweis. Siehe Aufgabe 16(c). □

(2.17) Bemerkung. Für $a \in \mathbb{Z}$ gilt $0 \mid a$ genau dann, wenn $a = 0$ ist.

Beweis. Siehe Aufgabe 16(d). □

(2.18) Bemerkung. Es sei $a \in \mathbb{Z}$ gegeben. Genau dann gilt $a \mid 1$, wenn $a \in \mathbb{Z}^\times$ ist.

Beweis. Siehe Aufgabe 16(e). □

Ideale

Als nächstes wollen wir Teilbarkeit aus der Sichtweise der Algebra betrachten. Hierzu erinnern wir zunächst an den Begriff einer abelschen Untergruppe.
Es sei eine abelsche Gruppe A gegeben. Eine *abelsche Untergruppe* von A ist eine abelsche Gruppe U so, dass die unterliegende Menge von U eine Teilmenge von A ist und so, dass für $x, x' \in U$ stets $x +^U x' = x +^A x'$ gilt.
Es sei nun eine Teilmenge U von A gegeben. Da die Addition jeder Untergruppe von A vollständig durch die Addition von A bestimmt ist, gibt es höchstens eine Struktur einer abelschen Gruppe auf U so, dass U mit dieser Struktur eine abelsche Untergruppe von A wird. Wir sagen daher auch, dass U eine Untergruppe von A *ist*, falls so eine Gruppenstruktur auf U existiert. Genau dann ist U eine abelsche Untergruppe von A, wenn $U \neq \emptyset$ und für $x, x' \in U$ stets auch $x - x' \in U$ ist.

(2.19) Definition (Ideal)**.** Ein *Ideal* von $\mathbb{Z}$ ist eine abelsche Untergruppe I von $\mathbb{Z}$ so, dass für $x \in I$, $a \in \mathbb{Z}$ stets $xa \in I$ gilt. Die Abbildung

$$\mathbb{Z} \times I \to I,\ (a, x) \mapsto xa$$

wird *Skalarmultiplikation* von I genannt.
Ein Ideal I von $\mathbb{Z}$ heißt *echt* (oder *strikt*), falls $I \neq \mathbb{Z}$ gilt.
Ist I ein Ideal von $\mathbb{Z}$, so schreiben wir $I \trianglelefteq \mathbb{Z}$. Ist I kein Ideal von $\mathbb{Z}$, so schreiben wir $I \not\trianglelefteq \mathbb{Z}$. Ist I ein echtes Ideal von $\mathbb{Z}$, so schreiben wir $I \triangleleft \mathbb{Z}$.

Ein Ideal von $\mathbb{Z}$ ist also gerade ein $\mathbb{Z}$-Untermodul von $\mathbb{Z}$.

(2.20) Beispiel. Es ist

$$\{x \in \mathbb{Z} \mid x \text{ ist gerade}\}$$

ein Ideal von $\mathbb{Z}$.

(2.21) Lemma (Idealkriterium)**.** Es sei eine Teilmenge I von $\mathbb{Z}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist I ein Ideal von $\mathbb{Z}$.

(b) Es gilt:

- *Abgeschlossenheit unter Addition.* Für alle $x, y \in I$ ist
$$x + y \in I.$$
- *Abgeschlossenheit unter der Null.* Es ist
$$0 \in I.$$
- *Abgeschlossenheit unter Skalarmultiplikation.* Für alle $x \in I$, $a \in \mathbb{Z}$ ist
$$xa \in I.$$

(c) Es gilt:

- Es ist
$$I \neq \emptyset.$$
- Für alle $x, y \in I$, $a \in \mathbb{Z}$ ist
$$xa + y \in I.$$

(d) Es ist I eine abelsche Untergruppe von $\mathbb{Z}$.

Beweis. Zunächst gelte Bedingung (a), d.h. es sei I ein Ideal von $\mathbb{Z}$. Dann ist I insbesondere eine abelsche Untergruppe von $\mathbb{Z}$, nach dem Untergruppenkriterium ist für $x, y \in I$ also stets $x + y \in I$ und es ist $0 \in I$. Ferner ist nach Definition (2.19) für $x \in I$, $a \in \mathbb{Z}$ stets $xa \in I$. Insgesamt gilt also Bedingung (b).
Als nächstes gelte Bedingung (b), d.h. es sei I abgeschlossen unter Addition, unter der Null und unter Skalarmultiplikation. Wegen $0 \in I$ ist insbesondere $I \neq \emptyset$. Sind $x, y \in I$, $a \in \mathbb{Z}$ gegeben, so ist ferner $xa \in I$ und folglich $xa + y \in I$. Wir haben somit die Gültigkeit von Bedingung (c) gezeigt.
Nun gelte Bedingung (c), d.h. es sei $I \neq \emptyset$ und für $x, y \in I$, $a \in \mathbb{Z}$ sei stets $xa + y \in I$. Dann ist für $x, y \in I$ insbesondere $-x + y = x(-1) + y \in I$. Nach dem Untergruppenkriterium ist also I eine abelsche Untergruppe von $\mathbb{Z}$, d.h. es gilt Bedingung (d).
Schließlich gelte Bedingung (d), d.h. es sei I eine abelsche Untergruppe von $\mathbb{Z}$, und es seien $x \in I$, $a \in \mathbb{Z}$ gegeben. Wenn $a = 0$ ist, dann ist $xa = 0 \in I$. Wenn $a > 0$ ist, dann ist $xa = \sum_{i \in [1,a]} x \in I$, da I als abelsche Gruppe abgeschlossen unter Addition ist. Wenn $a < 0$ ist, dann ist $-a > 0$, also $x(-a) \in I$ und damit auch $xa = -(x(-a)) \in I$, da I als abelsche Gruppe abgeschlossen unter Negation ist. Somit ist also in jedem Fall $xa \in I$. Da $x \in I$, $a \in \mathbb{Z}$ beliebig gegeben waren, ist folglich I ein Ideal von $\mathbb{Z}$, d.h. es gilt Bedingung (a).
Insgesamt sind Bedingung (a), Bedingung (b), Bedingung (c) und Bedingung (d) äquivalent. □

(2.22) Bemerkung. Es seien Ideale I und J von $\mathbb{Z}$ gegeben. Dann gilt:

(a) Es ist $I \cap J$ ein Ideal von $\mathbb{Z}$.

(b) Es ist $I + J$ ein Ideal von $\mathbb{Z}$.

Beweis. Siehe Aufgabe 17. □

Als nächstes werden wir den Teilbarkeitsbegriff mit dem Idealbegriff in Verbindung bringen.

(2.23) Notation. Für $n \in \mathbb{Z}$ schreiben wir

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}.$$

(2.24) Bemerkung. Es seien $n, x \in \mathbb{Z}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es gilt $n \mid x$.

(b) Es ist $x \in n\mathbb{Z}$.

(c) Es gilt $x\mathbb{Z} \subseteq n\mathbb{Z}$.

Beweis. Wir zeigen zuerst die Äquivalenz von Bedingung (a) und Bedingung (b), danach die Äquivalenz von Bedingung (b) und Bedingung (c).
Genau dann gilt $n \mid x$, wenn es ein $q \in \mathbb{Z}$ gibt mit $x = nq$, d.h. genau dann, wenn $x \in n\mathbb{Z}$ ist. Folglich sind Bedingung (a) und Bedingung (b) äquivalent.
Als nächstes gelte Bedingung (b), d.h. es sei $x \in n\mathbb{Z}$. Dann gibt es ein $a \in \mathbb{Z}$ mit $x = na$. Für $b \in \mathbb{Z}$ folgt

$$xb = (na)b = n(ab) \in n\mathbb{Z}.$$

Somit ist $y \in n\mathbb{Z}$ für alle $y \in x\mathbb{Z}$, also $x\mathbb{Z} \subseteq n\mathbb{Z}$, d.h. es gilt Bedingung (c). Gilt umgekehrt Bedingung (c), d.h. ist $x\mathbb{Z} \subseteq n\mathbb{Z}$, so ist wegen $x = x \cdot 1 \in x\mathbb{Z}$ insbesondere $x \in n\mathbb{Z}$, d.h. es gilt auch Bedingung (b). Folglich sind Bedingung (b) und Bedingung (c) äquivalent. □

(2.25) Korollar. Für alle $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$.

Beweis. Für $x, y \in n\mathbb{Z}$ gilt $n \mid x$ und $n \mid y$ nach Bemerkung (2.24), also $n \mid x + y$ nach Proposition (2.12)(a) und damit $x + y \in n\mathbb{Z}$ nach Bemerkung (2.24). Weiter gilt $n \mid 0$ nach Proposition (2.12)(a) und damit $0 \in n\mathbb{Z}$ nach Bemerkung (2.24). Für $x \in n\mathbb{Z}$ gilt schließlich $n \mid x$ nach Bemerkung (2.24), für $a \in \mathbb{Z}$ ist also $n \mid xa$ nach Proposition (2.12)(c) und damit $xa \in n\mathbb{Z}$ nach Bemerkung (2.24). Nach dem Idealkriterium (2.21) ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$. □

(2.26) Korollar. Für $m, n \in \mathbb{Z}$ gilt genau dann $m\mathbb{Z} = n\mathbb{Z}$, wenn $|m| = |n|$ ist.

Beweis. Es seien $m, n \in \mathbb{Z}$ gegeben. Genau dann gilt $m\mathbb{Z} = n\mathbb{Z}$, wenn $m\mathbb{Z} \subseteq n\mathbb{Z}$ und $n\mathbb{Z} \subseteq m\mathbb{Z}$ ist. Nach Bemerkung (2.24) ist dies äquivalent zu $n \mid m$ und $m \mid n$, und dies ist wiederum äquivalent zu $|m| = |n|$ nach Proposition (2.10)(c). □

(2.27) Satz. Die Menge der Ideale von $\mathbb{Z}$ ist gegeben durch

$$\{n\mathbb{Z} \mid n \in \mathbb{N}_0\}.$$

Beweis. Nach Korollar (2.25) ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$ für alle $n \in \mathbb{N}_0$.
Es sei also umgekehrt ein beliebiges Ideal I von $\mathbb{Z}$ gegeben. Wenn $I = \{0\}$ ist, dann gilt $I = 0\mathbb{Z}$. Wir nehmen also im Folgenden an, dass $I \neq \{0\}$ ist. Dann ist $I \setminus \{0\} \neq \emptyset$ und da mit jedem $x \in I$ auch $-x \in I$ ist, folgt $I \cap \mathbb{N} \neq \emptyset$. Da $\mathbb{N}_0$ nach Korollar (1.19) wohlgeordnet ist, besitzt $I \cap \mathbb{N}$ ein kleistes Element n. Wir wollen zeigen, dass $I = n\mathbb{Z}$ ist. Zunächst ist wegen $n \in I$ auch $na \in I$ für alle $a \in \mathbb{Z}$, d.h. $n\mathbb{Z} \subseteq I$. Es sei also umgekehrt $x \in I$ gegeben. Nach dem Satz über die Division mit Rest (2.1) gibt es $q \in \mathbb{Z}$, $r \in [0, n-1]$ mit $x = nq + r$. Wegen $x \in I$ und $n \in I$ folgt $r = x - nq \in I$. Die Minimalität von n liefert nun $r = 0$ und damit $x = nq + r = nq \in n\mathbb{Z}$. Folglich ist auch $I \subseteq n\mathbb{Z}$ und damit insgesamt $I = n\mathbb{Z}$. □

Aufgaben

Aufgabe 16 (Teilbarkeit)**.** Zeigen Sie:

(a) Für $a, b, c \in \mathbb{Z}$ gilt: Wenn $a \mid b$ gilt, dann auch $ca \mid cb$. Wenn $ca \mid cb$ und $c \neq 0$ gilt, dann auch $a \mid b$.

(b) Für $a, b \in \mathbb{Z}$ gilt genau dann $a \mid b$, wenn $-a \mid b$ gilt.

(c) Für $a \in \mathbb{Z}$ gilt $1 \mid a$ und $-1 \mid a$.

(d) Für $a \in \mathbb{Z}$ gilt genau dann $0 \mid a$, wenn $a = 0$ ist.

(e) Für $a \in \mathbb{Z}$ gilt genau dann $a \mid 1$, wenn $a \in \mathbb{Z}^\times$ ist.

Aufgabe 17 (Schnitt und Summe von Idealen)**.** Es seien Ideale I und J von $\mathbb{Z}$ gegeben. Zeigen Sie:

(a) Es ist $I \cap J$ ein Ideal von $\mathbb{Z}$.

(b) Es ist $I + J$ ein Ideal von $\mathbb{Z}$.

Aufgabe 18 (Inklusion von Idealen)**.** Es seien Ideale I und J von $\mathbb{Z}$ gegeben. Zeigen Sie die Äquivalenz folgender Bedingungen.

(a) Es ist $I \subseteq J$

(b) Es ist $I \cap J = I$.

(c) Es ist $I + J = J$.

Aufgabe 19 (Idealprodukt)**.** Es seien Ideale I und J von $\mathbb{Z}$ gegeben. Das *Produkt* von I und J ist gegeben durch

$$IJ = I \cdot J := \{z \in \mathbb{Z} \mid \text{es gibt } n \in \mathbb{N}_0,\, x_k \in I,\, y_k \in J \text{ für } k \in [1,n] \text{ mit } z = \sum_{k\in[1,n]} x_k y_k\}.$$

Zeigen oder widerlegen Sie:

(a) Es ist IJ ein Ideal von $\mathbb{Z}$.

(b) Es ist $I \cap J \subseteq IJ$.

(c) Es ist $IJ \subseteq I \cap J$.

3 Größter gemeinsamer Teiler und euklidischer Algorithmus

Gemeinsame Teiler und gemeinsame Vielfache

(2.28) Definition (gemeinsamer Teiler, gemeinsames Vielfaches)**.** Es seien $a, b \in \mathbb{Z}$ gegeben.

(a) Ein *gemeinsamer Teiler* von a und b ist ein $d \in \mathbb{Z}$ so, dass $d \mid a$ und $d \mid b$ gilt.

(b) Ein *gemeinsames Vielfaches* von a und b ist ein $m \in \mathbb{Z}$ so, dass $a \mid m$ und $b \mid m$ gilt.

(2.29) Beispiel.

(a) Es sind 1, 2, -3 gemeinsame Teiler von 12 und 18.

(b) Es sind 12 und -24 gemeinsame Vielfache von 4 und 6.

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

(2.30) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.** Es seien $a, b \in \mathbb{Z}$ gegeben.

(a) Ein *größter gemeinsamer Teiler* von a und b ist ein gemeinsamer Teiler g von a und b derart, dass jeder gemeinsame Teiler d von a und b auch ein Teiler von g ist.

(b) Ein *kleinstes gemeinsames Vielfaches* von a und b ist ein gemeinsames Vielfaches l von a und b derart, dass jedes gemeinsame Vielfache m von a und b auch ein Vielfaches von l ist.

(2.31) Beispiel.

(a) Es ist 6 ein größter gemeinsamer Teiler von 12 und 18.

(b) Es ist -12 ein kleinstes gemeinsames Vielfaches von 4 und 6.

(2.32) Bemerkung. Es seien $a, b \in \mathbb{Z}$ mit $a \mid b$ gegeben.

(a) Es ist a ein größter gemeinsamer Teiler von a und b.

(b) Es ist b ein kleinstes gemeinsames Vielfaches von a und b.

Beweis.

(a) Es gilt $a \mid b$ und $a \mid a$ nach Proposition (2.10)(b), d.h. a ist ein gemeinsamer Teiler von a und b. Ferner ist jeder gemeinsame Teiler von a und b insbesondere ein Teiler von a. Folglich ist a ein größter gemeinsamer Teiler von a und b.

(b) Es gilt $a \mid b$ und $b \mid b$ nach Proposition (2.10)(b), d.h. b ist ein gemeinsames Vielfaches von a und b. Ferner ist jedes gemeinsame Vielfache von a und b insbesondere ein Vielfaches von b. Folglich ist b ein kleinstes gemeinsames Vielfaches von a und b. □

(2.33) Korollar. Es sei $a \in \mathbb{Z}$ gegeben.

(a) Es ist a ein größter gemeinsamer Teiler von 0 und a.

(b) Es ist 0 ein kleinstes gemeinsames Vielfaches von 0 und a.

Beweis.

(a) Nach Proposition (2.12)(b) gilt $a \mid 0$, es ist also a nach Bemerkung (2.32)(a) ein größter gemeinsamer Teiler von 0 und a.

(b) Dies lässt sich dual zu (a) beweisen. □

(2.34) Proposition. Es seien $a, b \in \mathbb{Z}$ gegeben.

(a) Es sei ein größter gemeinsamer Teiler g von a und b sowie $g' \in \mathbb{Z}$ gegeben. Genau dann ist g' ein größter gemeinsamer Teiler von a und b, wenn $|g| = |g'|$ ist.

(b) Es sei ein kleinstes gemeinsames Vielfaches l von a und b sowie $l' \in \mathbb{Z}$ gegeben. Genau dann ist l' ein kleinstes gemeinsames Vielfaches von a und b, wenn $|l| = |l'|$ ist.

Beweis.

(a) Zunächst sei g' ein größter gemeinsamer Teiler von a und b. Dann ist g' insbesondere ein gemeinsamer Teiler von a und b und g ein größter gemeinsamer Teiler von a und b, wir haben also $g' \mid g$. Andererseits ist aber auch g ein gemeinsamer Teiler von a und b und g' ein größter gemeinsamer Teiler von a und b, wir haben also auch $g \mid g'$. Mit Proposition (2.10)(c) folgt $|g| = |g'|$.

Ist umgekehrt $|g'| = |g|$, so gilt $g' = g$ oder $g' = -g$. Wenn $g' = g$ gilt, so ist g' ein größter gemeinsamer Teiler von a und b. Es gelte also schließlich $g' = -g$. Nach Bemerkung (2.15) ist dann mit g auch g' ein gemeinsamer Teiler von a und b. Ist ferner ein beliebiger gemeinsamer Teiler d von a und b gegeben, so ist d auch ein Teiler von g, da g ein größter gemeinsamer Teiler von a und b ist, und also auch ein Teiler von g' nach Proposition (2.12)(c).

(b) Dies lässt sich dual zu (a) beweisen. □

(2.35) Proposition. Es seien $a, b, a', b' \in \mathbb{Z}$ gegeben.

(a) Es sei ein größter gemeinsamer Teiler g von a und b gegeben. Genau dann ist g ein größter gemeinsamer Teiler von a' und b', wenn die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von a' und b' sind.

(b) Es sei ein kleinstes gemeinsames Vielfaches l von a und b gegeben. Genau dann ist l ein kleinstes gemeinsames Vielfaches von a' und b', wenn die gemeinsamen Vielfachen von a und b genau die gemeinsamen Vielfachen von a' und b' sind.

Beweis.

(a) Siehe Aufgabe 21.

(b) Dies lässt sich dual zu (a) beweisen. □

(2.36) Proposition. Es seien $a, b \in \mathbb{Z}$ und ein gemeinsamer Teiler $d \neq 0$ von a und b gegeben.

(a) Für jeden größten gemeinsamer Teiler g von a und b ist $\frac{g}{d}$ ein größter gemeinsamer Teiler von $\frac{a}{d}$ und $\frac{b}{d}$.

(b) Für jedes kleinste gemeinsame Vielfache l von a und b ist $\frac{l}{d}$ ein kleinstes gemeinsames Vielfaches von $\frac{a}{d}$ und $\frac{b}{d}$.

Beweis.

(a) Siehe Aufgabe 22.

(b) Dies lässt sich dual zu (a) beweisen. □

Idealtheoretische Interpretation

Nach Satz (2.27) gibt es für jedes Ideal I von $\mathbb{Z}$ ein $n \in \mathbb{N}_0$ mit $I = n\mathbb{Z}$. Andererseits sind für $a, b \in \mathbb{Z}$ auch die Summe $a\mathbb{Z} + b\mathbb{Z}$ und der Schnitt $a\mathbb{Z} \cap b\mathbb{Z}$ Ideale von $\mathbb{Z}$, siehe Bemerkung (2.22), es gibt also $m, n \in \mathbb{N}_0$ mit $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ und $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$. Nun drängt sich die Frage auf, welche Verbindung es zwischen m bzw. n sowie a und b gibt. Das Lemma von Bézout (2.38) wird hierauf eine Antwort geben: Es ist m ein größter gemeinsamer Teiler und n ein kleinstes gemeinsames Vielfaches von a und b.

(2.37) Bemerkung. Es seien $a, b \in \mathbb{Z}$ gegeben.

(a) Es sei $d \in \mathbb{Z}$ gegeben. Genau dann ist d ein gemeinsamer Teiler von a und b, wenn $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ gilt.

(b) Es sei $m \in \mathbb{Z}$ gegeben. Genau dann ist m ein gemeinsames Vielfaches von a und b, wenn $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$ gilt.

Beweis.

(a) Genau dann ist d ein gemeinsamer Teiler von a und b, wenn $d \mid a$ und $d \mid b$ gilt. Nach Bemerkung (2.24) ist dies äquivalent zu $a\mathbb{Z} \subseteq d\mathbb{Z}$ und $b\mathbb{Z} \subseteq d\mathbb{Z}$. Da $d\mathbb{Z}$ als abelsche Untergruppe von $\mathbb{Z}$ jedoch abgeschlossen unter der Addition und der Null ist, gilt genau dann $a\mathbb{Z} \subseteq d\mathbb{Z}$ und $b\mathbb{Z} \subseteq d\mathbb{Z}$, wenn $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ ist. Insgesamt ist d genau dann ein gemeinsamer Teiler von a und b, wenn $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ gilt.

(b) Genau dann ist m ein gemeinsames Vielfaches von a und b, wenn $a \mid m$ und $b \mid m$ gilt. Nach Bemerkung (2.24) ist dies äquivalent zu $m\mathbb{Z} \subseteq a\mathbb{Z}$ und $m\mathbb{Z} \subseteq b\mathbb{Z}$. Dies ist jedoch äquivalent zu $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$. Insgesamt ist m genau dann ein gemeinsames Vielfaches von a und b, wenn $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$ gilt. □

(2.38) Lemma (Lemma von Bézout, algebraische Version)**.** Es seien $a, b \in \mathbb{Z}$ gegeben.

(a) Es sei $g \in \mathbb{Z}$ gegeben. Genau dann ist g ein größter gemeinsamer Teiler von a und b, wenn

$$g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

gilt. Insbesondere gibt es stets einen größten gemeinsamen Teiler von a und b.

(b) Es sei $l \in \mathbb{Z}$ gegeben. Genau dann ist l ein kleinstes gemeinsames Vielfaches von a und b, wenn

$$l\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$$

gilt. Insbesondere gibt es stets ein kleinstes gemeinsames Vielfaches von a und b.

Beweis.

(a) Zunächst gelte $g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Dann ist insbesondere $a\mathbb{Z} + b\mathbb{Z} \subseteq g\mathbb{Z}$, d.h. g ist ein gemeinsamer Teiler von a und b nach Bemerkung (2.37)(a). Für jeden gemeinsamen Teiler d von a und b gilt ferner $g\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ nach Bemerkung (2.37)(a), also $d \mid g$ nach Bemerkung (2.24). Insgesamt ist g also ein größter gemeinsamer Teiler von a und b.

Nach Bemerkung (2.22)(b) ist $a\mathbb{Z} + b\mathbb{Z}$ ein Ideal von $\mathbb{Z}$. Folglich gibt es nach Satz (2.27) ein $g' \in \mathbb{Z}$ mit $a\mathbb{Z} + b\mathbb{Z} = g'\mathbb{Z}$. Wie wir gerade gesehen haben, ist dann g' ein größter gemeinsamer Teiler von a und b.

Schließlich sei umgekehrt g ein größter gemeinsamer Teiler von a und b. Wie wir gerade gesehen, gibt es einen größten gemeinsamen Teiler g' von a und b mit $a\mathbb{Z} + b\mathbb{Z} = g'\mathbb{Z}$. Dann ist aber bereits $|g| = |g'|$ nach Proposition (2.34)(a) und also $g\mathbb{Z} = g'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ nach Korollar (2.26).

(b) Dies lässt sich dual zu (a) beweisen. □

(2.39) Korollar (Lemma von Bézout, arithmetische Version)**.** Es seien $a, b \in \mathbb{Z}$ und ein größter gemeinsamer Teiler g von a und b gegeben. Dann gibt es $x, y \in \mathbb{Z}$ mit

$$g = ax + by.$$

Beweis. Nach dem Lemma von Bézout (2.38)(a) ist $g\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$. Insbesondere gilt also $g = g\cdot 1 \in g\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$, d.h. es gibt $x, y \in \mathbb{Z}$ mit $g = ax + by$. □

(2.40) Korollar. Es seien $a, b \in \mathbb{Z}$ und ein größter gemeinsamer Teiler g von a und b gegeben. Für $c \in \mathbb{Z}$ ist dann cg ein größter gemeinsamer Teiler von ca und cb.

Beweis. Es sei $c \in \mathbb{Z}$ gegeben. Da g ein gemeinsamer Teiler von a und b ist, gilt $g \mid a$ und $g \mid b$, also auch $cg \mid ca$ und $cg \mid cb$ nach Bemerkung (2.14)(a), d.h. cg ist ein gemeinsamer Teiler von ca und cb. Um zu zeigen, dass cg ein größter gemeinsamer Teiler von ca und cb ist, sei ein beliebiger gemeinsamer Teiler d von ca und cb gegeben. Nach dem Lemma von Bézout (2.39) gibt es $x, y \in \mathbb{Z}$ mit $g = ax + by$. Wegen $d \mid ca$ und $d \mid cb$ folgt

$$d \mid cax + cby = c(ax + by) = cg$$

nach Proposition (2.12)(a), (c). Insgesamt ist cg ein größter gemeinsamer Teiler von ca und cb. □

(2.41) Korollar. Es seien $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$ und ein größter gemeinsamer Teiler g von a und b gegeben. Für $c \in \mathbb{Z}$ gilt genau dann $a \mid bc$, wenn $\frac{a}{g} \mid c$ gilt.

Beweis. Es sei $c \in \mathbb{Z}$ gegeben. Zunächst gelte $a \mid bc$. Nach dem Lemma von Bézout (2.39) gibt es $x, y \in \mathbb{Z}$ mit $g = ax+by$. Es folgt $gc = acx+bcy$. Nun gilt $a \mid a$ nach Proposition (2.10)(b) und $a \mid bc$ nach Voraussetzung, also auch $a \mid acx + bcy = gc$ nach Proposition (2.12)(a), (c). Wegen $(a, b) \neq (0, 0)$ ist jedoch $g \neq 0$, es folgt also $\frac{a}{g} \mid c$ nach Bemerkung (2.14)(b).
Nun gelte umgekehrt $\frac{a}{g} \mid c$. Nach Bemerkung (2.14)(a) folgt $a \mid gc$ sowie $gc \mid bc$. Dies impliziert aber bereits $a \mid bc$ nach Proposition (2.10)(a). □

Nach Lemma (2.38)(a) gibt es für jedes Paar ganzer Zahlen einen größten gemeinsamen Teiler sowie ein kleinstes gemeinsames Vielfaches, und nach Proposition (2.34) sind diese eindeutig bis auf Vorzeichen.

(2.42) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.**

(a) Für $a, b \in \mathbb{Z}$ bezeichne $\gcd(a, b)$ den eindeutig bestimmten nicht-negativen größten gemeinsamen Teiler von a und b.

(b) Für $a, b \in \mathbb{Z}$ bezeichne $\operatorname{lcm}(a, b)$ das eindeutig bestimmte nicht-negative kleinste gemeinsame Vielfache von a und b.

Wir haben also wohldefinierte Abbildungen $\gcd\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}_0$ und $\operatorname{lcm}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}_0$ konstruiert.

Teilerfremdheit

(2.43) Definition (Teilerfremdheit)**.** Es seien $a, b \in \mathbb{Z}$ gegeben. Wir sagen, dass a und b *teilerfremd* (oder *relativ prim* oder *koprim*) sind, wenn $\gcd(a, b) = 1$ ist.

(2.44) Bemerkung. Für $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$ sind $\frac{a}{\gcd(a,b)}$ und $\frac{b}{\gcd(a,b)}$ teilerfremd.

Beweis. Für $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$ ist

$$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = \frac{\gcd(a, b)}{\gcd(a, b)} = 1$$

nach Proposition (2.36)(a), d.h. $\frac{a}{\gcd(a,b)}$ und $\frac{b}{\gcd(a,b)}$ sind teilerfremd. □

(2.45) Proposition. Es seien $a, b \in \mathbb{Z}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es sind a und b teilerfremd.

(b) Die Menge der größten gemeinsamen Teiler von a und b ist $\mathbb{Z}^\times$.

(c) Die Menge der gemeinsamen Teiler von a und b ist $\mathbb{Z}^\times$.

(d) Es ist $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

(e) Für alle $c \in \mathbb{Z}$ gibt es $x, y \in \mathbb{Z}$ mit $c = ax + by$.

(f) Es gibt $x, y \in \mathbb{Z}$ mit $1 = ax + by$.

Beweis. Wir zeigen zuerst die Äquivalent von Bedingung (a) und Bedingung (b), danach die Äquivalenz von Bedingung (b) und Bedingung (c), danach die Äquivalenz von Bedingung (a) und Bedingung (d), danach die Äquivalenz von Bedingung (a) und Bedingung (f), und schließlich die Äquivalenz von Bedingung (e) und Bedingung (f).
Es sind a und b genau dann teilerfremd, wenn $\gcd(a, b) = 1$ ist. Es sei g ein beliebiger größter gemeinsamer Teiler von a und b. Nach Proposition (2.34)(a) gilt $|g| = |\gcd(a, b)| = \gcd(a, b)$. Folglich sind a und b genau dann teilerfremd, wenn $|g| = 1$ ist, d.h. wenn $g \in \mathbb{Z}^\times$ ist. Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (b).
Wenn die Menge aller größten gemeinsamen Teiler gleich $\mathbb{Z}^\times$ ist, so auch die Menge aller gemeinsamen Teiler nach Bemerkung (2.18). Umgekehrt, wenn die Menge aller gemeinsamen Teiler gleich $\mathbb{Z}^\times$ ist, dann insbesondere auch die Menge aller größten gemeinsamen Teiler nach Bemerkung (2.16). Dies zeigt die Äquivalenz von Bedingung (b) und Bedingung (c).
Nach dem Lemma von Bézout (2.38)(a) ist 1 genau dann ein größter gemeinsamer Teiler von a und b, wenn $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ gilt. Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (d).
Die Teilerfremdheit von a und b impliziert nach dem Lemma von Bézout (2.39), dass es $x, y \in \mathbb{Z}$ mit $ax + by = \gcd(a, b) = 1$ gibt. Umgekehrt, wenn es $x, y \in \mathbb{Z}$ mit $ax + by = 1$ gibt, so haben wir $1 \in a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$ nach dem Lemma von Bézout (2.38)(a), also $\gcd(a, b) \mid 1$ nach Bemerkung (2.24) und damit $\gcd(a, b) = 1$ nach Bemerkung (2.18). Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (f).
Wenn es für $c \in \mathbb{Z}$ stets $x, y \in \mathbb{Z}$ mit $c = ax + by$, so auch insbesondere für $c = 1$. Umgekehrt, wenn es $x, y \in \mathbb{Z}$ mit $1 = ax + by$ gibt, so folgt $c = (ax + by)c = a(xc) + b(yc)$. Dies zeigt die Äquivalenz von Bedingung (e) und Bedingung (f).
Insgesamt sind Bedingung (a), Bedingung (b), Bedingung (d), Bedingung (e) und Bedingung (f) äquivalent. □

(2.46) Bemerkung. Es seien teilerfremde $a, b \in \mathbb{Z}$ gegeben. Für $c \in \mathbb{Z}$ gilt genau dann $a \mid bc$, wenn $a \mid c$ gilt.

Beweis. Dies folgt aus Korollar (2.41). □

(2.47) Korollar. Es seien $a, b, c \in \mathbb{Z}$ gegeben. Genau dann sind a und b sowie a und c jeweils teilerfremd, wenn a und bc teilerfremd sind.

Beweis. Zunächst seien a und b sowie a und c jeweils teilerfremd und es sei ein beliebiger gemeinsamer Teiler d von a und bc gegeben. Wegen der Teilerfremdheit von a und b sind auch d und b teilerfremd, so dass nach Bemerkung (2.46) auch $d \mid c$ gilt. Folglich ist d ein gemeinsamer Teiler von a und c. Nun sind aber auch a und c teilerfremd, es folgt also $d \in \mathbb{Z}^\times$ nach Proposition (2.45). Nach Bemerkung (2.16) ist also die Menge der gemeinsamen Teiler von a und bc gegeben durch $\mathbb{Z}^\times$, und also sind a und bc teilerfremd nach Proposition (2.45).
Wenn umgekehrt a und bc teilerfremd sind, dann sind auch a und b sowie a und c jeweils teilerfremd nach Proposition (2.12)(c). □

Beziehung zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen

(2.48) Satz. Es seien $a, b \in \mathbb{Z}$ gegeben. Dann ist

$$\gcd(a, b)\,\mathrm{lcm}(a, b) = |ab|.$$

Insbesondere sind a und b genau dann teilerfremd, wenn $\mathrm{lcm}(a, b) = |ab|$ ist.

Beweis. Zunächst seien a und b teilerfremd. Nach Proposition (2.45) gibt es dann $x, y \in \mathbb{Z}$ mit $1 = ax + by$. Da $\operatorname{lcm}(a, b)$ ein gemeinsames Vielfaches von a und b ist, gibt es ferner $p, q \in \mathbb{Z}$ mit $\operatorname{lcm}(a, b) = ap = bq$. Es folgt

$$ab(qx + py) = abqx + abpy = bqax + apby = \operatorname{lcm}(a, b)ax + \operatorname{lcm}(a, b)by = \operatorname{lcm}(a, b)(ax + by) = \operatorname{lcm}(a, b),$$

also $ab \mid \operatorname{lcm}(a, b)$. Andererseits ist aber auch ab ein gemeinsames Vielfaches von a und b, und da $\operatorname{lcm}(a, b)$ ein kleinstes gemeinsames Vielfaches von a und b ist, folgt $\operatorname{lcm}(a, b) \mid ab$. Proposition (2.10)(c) liefert

$$\operatorname{lcm}(a, b) = |\operatorname{lcm}(a, b)| = |ab|.$$

Im Folgenden seien a und b beliebig. Wenn $(a, b) = (0, 0)$ ist, so gilt

$$\gcd(a, b) \operatorname{lcm}(a, b) = 0 \cdot 0 = 0 = |0 \cdot 0| = |ab|.$$

Es sei also im Folgenden $(a, b) \neq (0, 0)$, so dass $\gcd(a, b) \neq 0$ ist. Nach Bemerkung (2.44) sind $\frac{a}{\gcd(a,b)}$ und $\frac{b}{\gcd(a,b)}$ teilerfremd. Der bereits bewiesene Spezialfall und Proposition (2.36) zeigen

$$\frac{\operatorname{lcm}(a, b)}{\gcd(a, b)} = \operatorname{lcm}\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = \left|\frac{a}{\gcd(a, b)} \cdot \frac{b}{\gcd(a, b)}\right| = \frac{|ab|}{\gcd(a, b)\ \gcd(a, b)},$$

also

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|.$$

Gilt schließlich $\operatorname{lcm}(a, b) = |ab|$, so folgt aus $\gcd(a, b) \operatorname{lcm}(a, b) = |ab|$ bereits $\gcd(a, b) = 1$, d.h. a und b sind teilerfremd. □

Der euklidische Algorithmus

Nach dem Lemma von Bézout (2.39) wissen wir, dass es für $a, b \in \mathbb{Z}$ stets $x, y \in \mathbb{Z}$ mit $\gcd(a, b) = ax + by$ gibt, d.h. dass sich $\gcd(a, b)$ als Linearkombination von a und b über $\mathbb{Z}$ schreiben lässt. Wir wollen nun einen Algorithmus herleiten, welcher zum einen $\gcd(a, b)$ und zum anderen eine solche Darstellung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ berechnet.

(2.49) Lemma. Für $a, b, q \in \mathbb{Z}$ gilt

$$\gcd(a, b) = \gcd(b, a - bq).$$

Beweis. Es seien $a, b, q \in \mathbb{Z}$ gegeben. Für $d \in \mathbb{Z}$ mit $d \mid b$ gilt nach Proposition (2.12)(a), (c) genau dann $d \mid a$, wenn $d \mid a - bq$ gilt. Somit sind die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von b und $a - bq$, also $\gcd(a, b) = \gcd(b, a - bq)$ nach Proposition (2.35)(a). □

(2.50) Korollar. Für $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ ist

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Beweis. Es seien $a, b \in \mathbb{Z}$ gegeben. Wir setzen $q := a \operatorname{div} b$ und $r := a \bmod b$. Dann ist $a = bq + r$, nach Lemma (2.49) also

$$\gcd(a, b) = \gcd(b, a \bmod b).$$ □

(2.51) Satz. Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Ferner sei eine Folge $(r_i)_{i \in \mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$r_i := \begin{cases} a, & \text{falls } i = 0, \\ b, & \text{falls } i = 1, \\ r_{i-2} \bmod r_{i-1}, & \text{falls } i \geq 2,\ r_{i-1} \neq 0, \\ 0, & \text{falls } i \geq 2,\ r_{i-1} = 0, \end{cases}$$

für $i \in \mathbb{N}_0$. Dann existiert ein $n \in \mathbb{N}$ mit $|r_n| = \gcd(a, b)$ und $r_i = 0$ für $i > n$.

Beweis. Wegen $r_i = r_{i-2} \bmod r_{i-1} \in [0, |r_{i-1}| - 1]$ gilt $|r_i| < |r_{i-1}|$ für $i \geq 2$. Somit ist $r_{|b|+1} = 0$. Wir setzen $n := \min\{i \in \mathbb{N} \mid r_i = 0\} - 1$. Dann ist $r_{n+1} = 0$, induktiv also $r_i = 0$ für alle $i \in \mathbb{N}_0$ mit $i > n$. Nach Korollar (2.50) gilt ferner

$$\gcd(r_{i-2}, r_{i-1}) = \gcd(r_{i-1}, r_{i-2} \bmod r_{i-1}) = \gcd(r_{i-1}, r_i)$$

für $i \in \mathbb{N}$, $i \geq 2$ mit $r_{i-1} \neq 0$. Induktiv erhalten wir

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0).$$

Nun ist aber $|r_n| = \gcd(r_n, 0) = \gcd(a, b)$ nach Korollar (2.33)(a). □

(2.52) Algorithmus (euklidischer Algorithmus)**.**

- Eingabe: $a, b \in \mathbb{Z}$.
- Ausgabe: $\gcd(a, b)$.
- Verfahren:

```
function ea(a, b)
    if b = 0 then
        return a;
    end if;

    r := a mod b;
    while r ≠ 0 do
        a := b;
        b := r;
        r := a mod b;
    end while;

    return |b|;
end function;
```

(2.53) Beispiel. Es ist $\gcd(2238, 168) = 6$.

Beweis. Wir berechnen den $\gcd(2238, 168)$ mittels euklidischem Algorithmus:

$$\begin{aligned} 2238 &= 168 \cdot 13 + 54, \\ 168 &= 54 \cdot 3 + 6, \\ 54 &= 6 \cdot 9 + 0. \end{aligned}$$

Somit ist $\gcd(2238, 168) = 6$. □

(2.54) Satz. Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Ferner seien Folgen $(r_i)_{i\in\mathbb{N}_0}$, $(x_i)_{i\in\mathbb{N}_0}$, $(y_i)_{i\in\mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$r_i := \begin{cases} a, & \text{falls } i = 0, \\ b, & \text{falls } i = 1, \\ r_{i-2} \bmod r_{i-1}, & \text{falls } i \geq 2,\ r_{i-1} \neq 0, \\ 0, & \text{falls } i \geq 2,\ r_{i-1} = 0, \end{cases}$$

$$x_i := \begin{cases} 1, & \text{falls } i = 0, \\ 0, & \text{falls } i = 1, \\ x_{i-2} - x_{i-1}(r_{i-2} \operatorname{div} r_{i-1}), & \text{falls } i \geq 2,\ r_{i-1} \neq 0, \\ 0, & \text{falls } i \geq 2,\ r_{i-1} = 0, \end{cases}$$

$$y_i := \begin{cases} 0, & \text{falls } i = 0, \\ 1, & \text{falls } i = 1, \\ y_{i-2} - y_{i-1}(r_{i-2} \operatorname{div} r_{i-1}), & \text{falls } i \geq 2,\ r_{i-1} \neq 0, \\ 0, & \text{falls } i \geq 2,\ r_{i-1} = 0, \end{cases}$$

für $i \in \mathbb{N}_0$.

(a) Für alle $i \in \mathbb{N}_0$ gilt

$$r_i = ax_i + by_i.$$

(b) Es existiert ein $n \in \mathbb{N}$ mit

$$|r_n| = |ax_n + by_n| = \gcd(a, b)$$

und $r_i = 0$ für $i > n$.

Beweis.

(a) Um $ax_i + by_i = r_i$ für alle $i \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach i. Zunächst gilt

$$\begin{aligned} ax_0 + by_0 &= a \cdot 1 + b \cdot 0 = a = r_0, \\ ax_1 + by_1 &= a \cdot 0 + b \cdot 1 = b = r_1, \end{aligned}$$

also $ax_i + by_i = r_i$ für $i \in \{0, 1\}$. Es sei also ein $i \in \mathbb{N}_0$ mit $i \geq 2$ gegeben und gelte $ax_{i-2} + by_{i-2} = r_{i-2}$ sowie $ax_{i-1} + by_{i-1} = r_{i-1}$. Wenn $r_{i-1} \neq 0$ ist, erhalten wir

$$\begin{aligned} ax_i + by_i &= a(x_{i-2} - x_{i-1}(r_{i-2} \operatorname{div} r_{i-1})) + b(y_{i-2} - y_{i-1}(r_{i-2} \operatorname{div} r_{i-1})) \\ &= ax_{i-2} - ax_{i-1}(r_{i-2} \operatorname{div} r_{i-1}) + by_{i-2} - by_{i-1}(r_{i-2} \operatorname{div} r_{i-1}) \\ &= ax_{i-2} + by_{i-2} - (ax_{i-1} + by_{i-1})(r_{i-2} \operatorname{div} r_{i-1}) = r_{i-2} - r_{i-1}(r_{i-2} \operatorname{div} r_{i-1}) = r_i. \end{aligned}$$

Wenn $r_{i-1} = 0$ ist, erhalten wir ebenfalls

$$ax_i + by_i = a \cdot 0 + b \cdot 0 = 0 = r_i.$$

Nach dem Induktionsprinzip gilt $ax_i + by_i = r_i$ für alle $i \in \mathbb{N}_0$.

(b) Nach Satz (2.51) gibt es ein $n \in \mathbb{N}$ mit $|r_n| = \gcd(a, b)$ und $r_i = 0$ für $i > n$. Wir erhalten

$$|ax_n + by_n| = |r_n| = \gcd(a, b)$$

nach (a). □

(2.55) Beispiel. Es ist $\gcd(2238, 168) = 6$ und

$$6 = 2238 \cdot (-3) + 168 \cdot 40.$$

Beweis. In Beispiel (2.53) haben wir $\gcd(2238, 168)$ mittels euklidischem Algorithmus berechnet:

$$\begin{aligned} 2238 &= 168 \cdot 13 + 54, \\ 168 &= 54 \cdot 3 + 6, \\ 54 &= 6 \cdot 9 + 0. \end{aligned}$$

Wir setzen

$$\begin{aligned} r_0 &:= 2238, & & \\ r_1 &:= 168, & q_1 &:= 13, \\ r_2 &:= 54, & q_2 &:= 3, \\ r_3 &:= 6, & q_3 &:= 9, \end{aligned}$$

und berechnen Koeffizienten $x_i, y_i \in \mathbb{Z}$ für $i \in [0,3]$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} x_0 &:= 1, & y_0 &:= 0, \\ x_1 &:= 0, & y_1 &:= 1, \\ x_2 &:= x_0 - x_1 q_1 = 1 - 0 \cdot 13 = 1, & y_2 &:= y_0 - y_1 q_1 = 0 - 1 \cdot 13 = -13, \\ x_3 &:= x_1 - x_2 q_2 = 0 - 1 \cdot 3 = -3, & y_3 &:= y_1 - y_2 q_2 = 1 - (-13) \cdot 3 = 40. \end{aligned}$$

Somit ist

$$6 = \gcd(2238, 168) = 2238 \cdot (-3) + 168 \cdot 40.$$ □

Aufgaben

Aufgabe 20 (größter gemeinsamer Teiler)**.** Es seien $a, b \in \mathbb{Z}$ für $i \in [1, n]$ gegeben.

(a) Definieren Sie die Begriffe eines gemeinsamen Teilers, eines gemeinsamen Vielfachen, eines größten gemeinsamen Teilers und eines kleinsten gemeinsamen Vielfachen von a_i für $i \in [1, n]$ analog zur Definition für $n = 2$.

(b) Es sei $n \geq 2$. Es seien ein größter gemeinsamer Teiler g von a_i für $i \in [1, n-1]$ und ein größter gemeinsamer Teiler h von g und a_n. Zeigen Sie, dass h ein größter gemeinsamer Teiler von a_i für $i \in [1, n]$ ist.

Aufgabe 21 (Charakterisierung von größter gemeinsamer Teilers)**.** Es seien $a, b, a', b' \in \mathbb{Z}$ und ein größter gemeinsamer Teiler g von a und b gegeben. Zeigen Sie: Genau dann ist g ein größter gemeinsamer Teiler von a' und b', wenn die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von a' und b' sind.

Aufgabe 22 (größter gemeinsamer Teiler der Kofaktoren)**.** Es seien $a, b \in \mathbb{Z}$ sowie ein gemeinsamer Teiler $d \neq 0$ und ein größter gemeinsamer Teiler g von a und b gegeben. Zeigen Sie, dass $\frac{g}{d}$ ein größter gemeinsamer Teiler von $\frac{a}{d}$ und $\frac{b}{d}$ ist.

Aufgabe 23 (lineare diophantische Gleichungen in 2 Unbekannten)**.** Es seien $a, b, c \in \mathbb{Z}$ gegeben.

(a) Zeigen Sie, dass es genau dann ein $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ mit $ax + by = c$ gibt, wenn $\gcd(a, b) \mid c$ gilt.

Nun gelte $\gcd(a, b) \mid c$ und es sei

$$S := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid ax + by = c\}.$$

Ferner sei ein $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ mit $ax_0 + by_0 = \gcd(a, b)$ gegeben.

(b) Beschreiben Sie S in Abhängigkeit von a, b, c, x_0, y_0.

(c) Wie erhält man aus a, b, c, x_0, y_0 ein $(x, y) \in S$ mit $|x|$ minimal?

(d) Wie erhält man aus a, b, c, x_0, y_0 ein $(x, y) \in S$ mit $x^2 + y^2$ minimal?

Aufgabe 24 (lineare diophantische Gleichungen)**.**

(a) Es seien $b_i \in \mathbb{Z}$ für $i \in [1, 3]$ gegeben durch

$$b_1 := 25,\ b_2 := 252,\ b_3 := 2520.$$

Bestimmen Sie die Menge aller $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ mit

$$1827x + 4158y = b_i$$

für $i \in [1, 3]$.

(b) Bestimmen Sie die Menge aller $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ mit

$$\begin{aligned} 1274x + 2156y - 415z &= 928, \\ 455x + 770y - 138z &= 331. \end{aligned}$$

(c) Bestimmen Sie die Menge aller $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ mit

$$\begin{aligned} 1274x + 2156y - 415z &= 928, \\ 455x + 770y - 138z &= 311. \end{aligned}$$

Aufgabe 25 ((erweiterter) euklidischer Algorithmus)**.**

(a) Implementieren Sie den euklidischen Algorithmus (2.54) für $\mathbb{Z}$ in Magma.

Bestimmen Sie als Anwendung für viele „zufällige“ $a, b \in \mathbb{N}$ mit $b < a$, wieviele Divisionsschritte der Algorithmus benötigt, bis der größte gemeinsame Teiler gefunden ist. Vergleichen sie diese Anzahl jeweils mit $\frac{12 \log 2}{\pi^2}(\log b)$.

Hinweis: Die Konstante $\frac{12 \log 2}{\pi^2}$ erhalten Sie in Magma durch `(12 * Log(2)) / (Pi(RealField())^2);`

(b) Implementieren Sie den erweiterten euklidischen Algorithmus für $\mathbb{Z}$ in Magma. Benutzen Sie nur sechs lokale Variablen in ihrer Funktion.

4 Primfaktoren

Irreduzibilität

Nach Bemerkung (2.16), Proposition (2.10)(b) und Proposition (2.12)(c) hat jedes $a \in \mathbb{Z}$ die Teiler $1, -1, a, -a$. Im Folgenden legen wir besonderes Augenmerk auf diejenigen $a \in \mathbb{Z}$, welche genau diese Teiler haben, also für welche aus $a = xy$ bereits $x, y \in \{1, -1, a, -a\}$ folgt. Da nach Proposition (2.12)(b) jede ganze Zahl ein Teiler von 0 ist und nach Bemerkung (2.18) die Teiler von 1 (und damit auch von -1) gerade die Einheiten von $\mathbb{Z}$ sind, werden wir hierbei die Sonderfälle $a \in \{0, 1, -1\}$ außen vorlassen.

(2.56) Definition ((ir)reduzibles Element)**.** Es sei $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ gegeben. Wir sagen, dass a *reduzibel* (oder *zerlegbar* oder *zusammengesetzt*) ist, falls es $x, y \in \mathbb{Z} \setminus \mathbb{Z}^\times$ mit $a = xy$ gibt. Falls a nicht reduzibel ist, so sagen wir, dass a *irreduzibel* (oder *unzerlegbar*) ist.

Eine Zahl $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ ist also genau dann irreduzibel, wenn aus $a = xy$ für $x, y \in \mathbb{Z}$ stets $x \in \mathbb{Z}^\times$ oder $y \in \mathbb{Z}^\times$ folgt.

(2.57) Bemerkung. Es sei $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ gegeben. Genau dann ist a irreduzibel, wenn für alle $d \in \mathbb{Z}$ mit $d \mid a$ stets $|d| = 1$ oder $|d| = |a|$ gilt.

Beweis. Es sei a irreduzibel. Ferner sei $d \in \mathbb{Z}$ mit $d \mid a$ gegeben, so dass also $a = dq$ für ein $q \in \mathbb{Z}$ gilt. Die Irreduzibilität von a impliziert $d \in \mathbb{Z}^\times$ oder $q \in \mathbb{Z}^\times$. Wenn $d \in \mathbb{Z}^\times$ gilt, so folgt $|d| = 1$, und wenn $q \in \mathbb{Z}^\times$ gilt, so folgt $|q| = 1$ und damit $|a| = |dq| = |d|\,|q| = |d|$.
Nun sei umgekehrt angenommen, dass für alle $d \in \mathbb{Z}$ mit $d \mid a$ stets $|d| = 1$ oder $|d| = |a|$ gilt. Um zu zeigen, dass a irreduzibel ist, seien $x, y \in \mathbb{Z}$ mit $a = xy$ gegeben. Dann gilt $x \mid a$ und $y \mid a$, nach Voraussetzung also $|x| = 1$ oder $|x| = |a|$. Im Fall $|x| = |a|$ erhalten wir $|a| = |xy| = |x|\,|y| = |a|\,|y|$ und damit $|y| = 1$. Somit gilt $|x| = 1$ oder $|y| = 1$, d.h. $x \in \mathbb{Z}^\times$ oder $y \in \mathbb{Z}^\times$. □

(2.58) Bemerkung. Es sei $p \in \mathbb{Z}$ gegeben. Genau dann ist p irreduzibel, wenn $-p$ irreduzibel ist.

Beweis. Zunächst sei p irreduzibel und es seien $x, y \in \mathbb{Z}$ mit $-p = xy$ gegeben. Dann folgt $p = -xy = (-x)y$, auf Grund der Irreduzibilität von p, also $-x \in \mathbb{Z}^\times$ oder $y \in \mathbb{Z}^\times$. Dann ist aber auch $x \in \mathbb{Z}^\times$ und damit $-p = xy$ irreduzibel.
Wenn umgekehrt $-p$ irreduzibel ist, dann ist auch $p = -(-p)$ irreduzibel. □

(2.59) Bemerkung. Es seien irreduzible $p, q \in \mathbb{Z}$ gegeben. Dann sind folgende Bedingungen äquivalent.

(a) Es gilt $|p| = |q|$.

(b) Es gilt $p \mid q$.

(c) Es gilt $q \mid p$.

Beweis. Wenn $|p| = |q|$ gilt, dann folgt $p \mid q$ nach Proposition (2.10)(c).
Es gelte also umgekehrt $p \mid q$. Da q irreduzibel ist, folgt $|p| = 1$ oder $|p| = |q|$ nach Bemerkung (2.57). Wegen der Irreduzibilität von p gilt aber $p \notin \mathbb{Z}^\times$, also $|p| \neq 1$ und damit $|p| = |q|$.
Folglich sind Bedingung (a) und Bedingung (b) äquivalent. Die Äquivalenz von Bedingung (a) und Bedingung (c) folgt aus Symmetriegründen. Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(2.60) Proposition. Es seien $a, p \in \mathbb{Z}$ gegeben und es sei p irreduzibel. Genau dann sind p und a teilerfremd, wenn $p \nmid a$ gilt.

Beweis. Zunächst gelte $p \nmid a$. Ferner sei ein gemeinsamer Teiler d von p und a gegeben. Wegen der Irreduzibilität von p gilt $|d| = 1$ oder $|d| = |p|$ nach Bemerkung (2.57). Nun gilt jedoch $p \nmid a$, also $|p| \neq |d|$ nach Bemerkung (2.15) und damit $|d| = 1$. Nach Proposition (2.45) sind p und a teilerfremd.
Sind umgekehrt p und a teilerfremd, so ist die Menge der gemeinsamen Teiler von p und a gleich $\mathbb{Z}^\times$ nach Proposition (2.45). Wegen p irreduzibel ist $p \notin \mathbb{Z}^\times$ und damit p kein gemeinsamer Teiler von p und a. Wegen $p \mid p$ nach Proposition (b) folgt $p \nmid a$. □

Primzahlen

Die Irreduzibilität von ganzen Zahlen lässt sich wie folgt charakterisieren:

(2.61) Lemma. Es sei $p \in \mathbb{Z} \setminus \{0, 1, -1\}$ gegeben. Genau dann ist p irreduzibel, wenn für $a, b \in \mathbb{Z}$ mit $p \mid ab$ stets auch $p \mid a$ oder $p \mid b$ gilt.

Beweis. Zunächst sei p irreduzibel und es seien $a, b \in \mathbb{Z}$ mit $p \mid ab$ gegeben. Es gelte ferner $p \nmid a$. Nach Proposition (2.60) sind p und a teilerfremd sowie p und ab nicht teilerfremd. Folglich sind p und b nicht teilerfremd nach Korollar (2.47), es gilt also $p \mid b$ nach Proposition (2.60).
Nun gelte umgekehrt für $a, b \in \mathbb{Z}$ mit $p \mid ab$ stets $p \mid a$ oder $p \mid b$. Ferner seien $x, y \in \mathbb{Z}$ mit $p = xy$ gegeben. Dann gilt insbesondere $p \mid p = xy$ nach Proposition (2.10)(b), also $p \mid x$ oder $p \mid y$. Da wegen $p = xy$ aber auch $x \mid p$ und $y \mid p$ gilt, folgt $|x| = |p|$ oder $|y| = |p|$ nach Proposition (2.10)(c). Da $|x| = |p|$ genau dann gilt, wenn $|y| = 1$ ist, also wenn $y \in \mathbb{Z}^\times$ ist, impliziert dies $y \in \mathbb{Z}^\times$ oder $x \in \mathbb{Z}^\times$ und damit die Irreduzibilität von p. □

In der Algebra nennt man Elemente eines kommutativen Rings *prim*, wenn sie die charakterisierende Eigenschaft aus Lemma (2.61) erfüllen. Im Allgemeinen sind dann irreduzible (in Analogie zu (2.56) definiert) und prime Elemente verschieden, d.h. die zu Lemma (2.61) analoge Aussage gilt nicht für jeden kommutativen Ring. Da in $\mathbb{Z}$ die beiden Begrifflichkeiten zusammenfallen, verzichten wir auf die formale Einführung von primen Elementen in $\mathbb{Z}$. Nichtsdestotrotz hat sich der folgende Begriff etabliert, auch unter Nicht-Mathematikern:

(2.62) Definition (Primzahl)**.** Eine *Primzahl* ist eine irreduzible natürliche Zahl.
Die Menge aller Primzahlen bezeichnen wir mit

$$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ irreduzibel}\}.$$

(2.63) Bemerkung. Es sei $p \in \mathbb{N} \setminus \{1\}$ gegeben. Genau dann ist p eine Primzahl, wenn für alle $d \in \mathbb{N}$ mit $d \mid p$ stets $d = 1$ oder $d = p$ gilt.

Beweis. Dies folgt aus Bemerkung (2.57). □

(2.64) Bemerkung. Es sei $p \in \mathbb{Z}$ gegeben. Genau dann ist p irreduzibel, wenn $|p|$ eine Primzahl ist.

Beweis. Nach Bemerkung (2.58) ist p genau dann irreduzibel, wenn $|p|$ irreduzibel ist, d.h. wenn $|p|$ eine Primzahl ist. □

Der Fundamentalsatz der Arithmetik

(2.65) Notation. Es sei eine Teilmenge S von $\mathbb{N}$ gegeben. Für $a \in \mathbb{N}_0^{(S)}$ setzen wir

$$\pi_S(a) := \prod_{s \in S} s^{a_s}.$$

(2.66) Bemerkung. Es sei eine Teilmenge S von $\mathbb{N}$ gegeben.

(a) Für $a, b \in \mathbb{N}_0^{(S)}$ ist

$$\pi_S(a+b) = \pi_S(a)\,\pi_S(b).$$

(b) Es ist

$$\pi_S(0) = 1.$$

(c) Für $c \in \mathbb{N}_0$, $a \in \mathbb{N}_0^{(S)}$ ist

$$\pi_S(ac) = \pi_S(a)^c.$$

Beweis.

(a) Für $a, b \in \mathbb{N}_0^{(S)}$ ist

$$\pi_S(a+b) = \prod_{s\in S} s^{(a+b)_s} = \prod_{s\in S} s^{a_s+b_s} = \prod_{s\in S}(s^{a_s}s^{b_s}) = (\prod_{s\in S} s^{a_s})(\prod_{s\in S} s^{b_s}) = \pi_S(a)\,\pi_S(b).$$

(b) Es ist

$$\pi_S(0) = \prod_{s\in S} s^{0_s} = \prod_{s\in S} s^0 = \prod_{s\in S} 1 = 1.$$

(c) Für $c \in \mathbb{N}_0$, $a \in \mathbb{N}_0^{(S)}$ ist

$$\pi_S(ac) = \prod_{s\in S} s^{(ac)_s} = \prod_{s\in S} s^{a_s c} = \prod_{s\in S}(s^{a_s})^c = (\prod_{s\in S} s^{a_s})^c = \pi_S(a)^c.$$ □

Es sei eine Teilmenge S von $\mathbb{N}$ gegeben. Wie in der linearen Algebra ist $\mathrm{e}_s \in \mathbb{N}_0^{(S)}$ für $s \in S$ gegeben durch

$$\mathrm{e}_s = (\delta_{s,t})_{t\in S}.$$

(2.67) Satz (Fundamentalsatz der Arithmetik)**.** Es ist

$$\pi_{\mathbb{P}} \colon \mathbb{N}_0^{(\mathbb{P})} \to \mathbb{N},\ a \mapsto \prod_{p\in\mathbb{P}} p^{a_p}$$

eine Bijektion.

Beweis. Um die Surjektivität von $\pi_{\mathbb{P}}$ zu beweisen, müssen wir zeigen, dass es für jedes $n \in \mathbb{N}$ ein $a \in \mathbb{N}_0^{(\mathbb{P})}$ mit $n = \pi_{\mathbb{P}}(v)$ gibt. Hierzu führen wir Induktion nach n. Für $n = 1$ gilt

$$n = 1 = \pi_{\mathbb{P}}(0)$$

nach Bemerkung (2.66)(b). Es sei also ein $n \in \mathbb{N}$ mit $n > 1$ beliebig gegeben und es sei angenommen, dass es für jedes $m \in \mathbb{N}$ mit $m < n$ ein $b \in \mathbb{N}_0^{(\mathbb{P})}$ mit $m = \pi_{\mathbb{P}}(b)$ gibt. Wenn n eine Primzahl ist, gilt

$$n = \prod_{p\in\mathbb{P}} p^{\delta_{p,n}} = \pi_{\mathbb{P}}(\mathrm{e}_n).$$

Andernfalls ist n reduzibel, es gilt also $l, m \in \mathbb{N} \setminus \{1\}$ mit $n = lm$. Wir haben $l < n$ und $m < n$ nach Bemerkung (2.57), so dass es nach Induktionsvoraussetzung $b, c \in \mathbb{N}_0^{(\mathbb{P})}$ mit $l = \pi_{\mathbb{P}}(b)$ und $m = \pi_{\mathbb{P}}(c)$ gibt. Nach Bemerkung (2.66)(a) impliziert dies jedoch

$$n = lm = \pi_{\mathbb{P}}(b)\,\pi_{\mathbb{P}}(c) = \pi_{\mathbb{P}}(b+c).$$

Nach dem Induktionsprinzip gibt es also für jedes $n \in \mathbb{N}$ ein $a \in \mathbb{N}_0^{(\mathbb{P})}$ mit $n = \pi_{\mathbb{P}}(a)$, d.h. $\pi_{\mathbb{P}}$ ist surjektiv.
Für die Injektivität seien $a, b \in \mathbb{N}_0^{(\mathbb{P})}$ mit $\pi_{\mathbb{P}}(a) = \pi_{\mathbb{P}}(b)$ gegeben. Ferner sei ein beliebiges $p \in \mathbb{P}$ gegeben. Nach Lemma (2.61) gilt genau dann $p \mid \pi_{\mathbb{P}}(a)$, wenn $a_p > 0$ ist. Entsprechend gilt genau dann $p \mid \pi_{\mathbb{P}}(b)$, wenn $b_p > 0$ ist. Wenn nun $a_p = 0$ ist, so folgt $p \nmid \pi_{\mathbb{P}}(a) = \pi_{\mathbb{P}}(b)$, also $b_p = 0 = a_p$. Es sei also im Folgenden $a_p > 0$, so dass $p \mid \pi_{\mathbb{P}}(a) = \pi_{\mathbb{P}}(b)$ und damit auch $b_p > 0$ folgt. Dies impliziert jedoch $a - \mathrm{e}_p \in \mathbb{N}_0^{(\mathbb{P})}$ und $b - \mathrm{e}_p \in \mathbb{N}_0^{(\mathbb{P})}$, und $\pi_{\mathbb{P}}(a) = \pi_{\mathbb{P}}(b)$ impliziert $\pi_{\mathbb{P}}(a - \mathrm{e}_p) = \pi_{\mathbb{P}}(b - \mathrm{e}_p)$. Induktiv können wir annehmen, dass $a - \mathrm{e}_p = b - \mathrm{e}_p$ ist, also auch $a = b$. Dies impliziert die Injektivität von $\pi_{\mathbb{P}}$. □

Der Fundamentalsatz der Arithmetik (2.67) besagt also gerade, dass es für jedes $n \in \mathbb{N}$ genau ein $a \in \mathbb{N}_0^{(\mathbb{P})}$ mit $n = \pi_{\mathbb{P}}(a) = \prod_{p\in\mathbb{P}} p^{a_p}$ gibt.
Algebraisch können wir dies so interpretieren: In Analogie zum Begriff eines Moduls über einem kommutativen Ring könnten wir den Begriff eines Moduls über einem kommutativen Halbring einführen, wobei wir als unterliegende Struktur lediglich ein abelsches (bzw. kommutatives) Monoid und keine abelsche Gruppe voraussetzten. Wie jedes kommutative Monoid würde dann $\mathbb{N}$ ein $\mathbb{N}_0$-Modul via $\mathbb{N}_0 \times \mathbb{N} \to \mathbb{N}$, $(c, x) \mapsto x^c$; dies ist im Wesentlichen die Aussage der Potenzgesetze. Der Fundamentalsatz der Arithmetik (2.67) (zusammen mit Bemerkung (2.66)) würde dann implizieren, dass $\pi_{\mathbb{P}} \colon \mathbb{N}_0^{(\mathbb{P})} \to \mathbb{N}$, $a \mapsto \prod_{p\in\mathbb{P}} p^{a_p}$ ein Isomorphismus von $\mathbb{N}_0$-Moduln ist. Dies wäre wiederum eine naheliegende Definition dafür, dass $\mathbb{P}$ eine Basis des $\mathbb{N}_0$-Moduls $\mathbb{N}$ ist.

(2.68) Definition (Primfaktorzerlegung)**.** Es sei $n \in \mathbb{N}$ gegeben. Das eindeutige $a \in \mathbb{N}_0^{(\mathbb{P})}$ mit $n = \prod_{p\in\mathbb{P}} p^{a_p}$ heißt *Primfaktorzerlegung* von n.

(2.69) Definition (Primfaktor)**.** Es sei $a \in \mathbb{Z} \setminus \{0\}$ gegeben. Ein *Primfaktor* (oder *Primteiler*) von a ist eine Primzahl p mit $p \mid a$.

p-adische Bewertung

(2.70) Definition (p-adische Bewertung)**.** Es sei $a \in \mathbb{Z} \setminus \{0\}$ gegeben.

(a) Ist $v \in \mathbb{N}_0^{(\mathbb{P})}$ die Primfaktorzerlegung von $|a|$, so schreiben wir

$$\mathrm{v}(a) := v.$$

(b) Für $p \in \mathbb{P}$ heißt

$$\mathrm{v}_p(a) := (\mathrm{v}(a))_p$$

die *p-adische Bewertung* von a.

(2.71) Bemerkung. Für $a \in \mathbb{Z} \setminus \{0\}$ ist

$$a = (\operatorname{sgn} a) \prod_{p\in\mathbb{P}} p^{\mathrm{v}_p(a)}.$$

Beweis. Für $a \in \mathbb{Z} \setminus \{0\}$ gilt $|a| = \pi_{\mathbb{P}}(\mathrm{v}(a))$ und damit

$$a = (\operatorname{sgn} a)\,|a| = (\operatorname{sgn} a)\,\pi_{\mathbb{P}}(\mathrm{v}(a)) = (\operatorname{sgn} a) \prod_{p\in\mathbb{P}} p^{\mathrm{v}_p(a)}. \qquad \square$$

(2.72) Bemerkung.

(a) Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}(ab) = \mathrm{v}(a) + \mathrm{v}(b).$$

(b) Es ist

$$\mathrm{v}(1) = 0.$$

(c) Für $c \in \mathbb{N}_0$, $a \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}(a^c) = \mathrm{v}(a)\, c.$$

Beweis.

(a) Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}(ab) = \mathrm{v}(|ab|) = \mathrm{v}(|a|\,|b|) = \mathrm{v}(\pi_{\mathbb{P}}(\mathrm{v}(a))\,\pi_{\mathbb{P}}(\mathrm{v}(b))) = \mathrm{v}(\pi_{\mathbb{P}}(\mathrm{v}(a) + \mathrm{v}(b))) = \mathrm{v}(a) + \mathrm{v}(b).$$

(b) Es ist

$$\mathrm{v}(1) = \mathrm{v}(\pi_{\mathbb{P}}(0)) = 0.$$

(c) Für $c \in \mathbb{N}_0$, $a \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}(a^c) = \mathrm{v}(|a^c|) = \mathrm{v}(|a|^c) = \mathrm{v}((\pi_{\mathbb{P}}(\mathrm{v}(a)))^c) = \mathrm{v}(\pi_{\mathbb{P}}(\mathrm{v}(a)\, c)) = \mathrm{v}(a)\, c. \qquad \square$$

(2.73) Korollar. Es sei $p \in \mathbb{P}$ gegeben.

(a) Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}_p(ab) = \mathrm{v}_p(a) + \mathrm{v}_p(b).$$

(b) Es ist

$$\mathrm{v}_p(1) = 0.$$

Beweis.

(a) Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist $\mathrm{v}(ab) = \mathrm{v}(a) + \mathrm{v}(b)$ nach Bemerkung (2.72)(a), also

$$\mathrm{v}_p(ab) = (\mathrm{v}(ab))_p = (\mathrm{v}(a) + \mathrm{v}(b))_p = \mathrm{v}_p(a) + \mathrm{v}_p(b).$$

für $p \in \mathbb{P}$.

(b) Nach Bemerkung (2.72)(b) ist $\mathrm{v}(1) = 0$, also

$$\mathrm{v}_p(1) = (\mathrm{v}(1))_p = 0_p = 0$$

für $p \in \mathbb{P}$. $\square$

(2.74) Proposition. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$ gegeben. Genau dann gilt

$$a \mid b,$$

wenn für alle $p \in \mathbb{P}$ stets

$$\mathrm{v}_p(a) \leq \mathrm{v}_p(b)$$

ist.

Beweis. Wenn $a \mid b$ gilt, so gibt es ein $q \in \mathbb{Z}$ mit $b = aq$ und es folgt

$$\mathrm{v}_p(b) = \mathrm{v}_p(aq) = \mathrm{v}_p(a) + \mathrm{v}_p(q) \geq \mathrm{v}_p(a)$$

für $p \in \mathbb{P}$ nach Korollar (2.73)(a).
Es gelte umgekehrt $\mathrm{v}_p(a) \leq \mathrm{v}_p(b)$ für alle $p \in \mathbb{P}$, so dass $d := \mathrm{v}(b) - \mathrm{v}(a) \in \mathbb{N}_0^{(\mathbb{P})}$ ist. Nach Bemerkung (2.66)(a) folgt

$$a\, \pi_{\mathbb{P}}(d) = \pi_{\mathbb{P}}(\mathrm{v}(a))\, \pi_{\mathbb{P}}(d) = \pi_{\mathbb{P}}(\mathrm{v}(a) + d) = \pi_{\mathbb{P}}(\mathrm{v}(b)) = b$$

und damit $a \mid b$. $\square$

(2.75) Korollar. Es seien $a \in \mathbb{Z} \setminus \{0\}$, $p \in \mathbb{P}$ gegeben. Genau dann ist p ein Primfaktor von a, wenn $\mathrm{v}_p(a) \geq 1$ ist.

Beweis. Wenn p ein Primfaktor von a ist, d.h. wenn $p \mid a$ gilt, dann ist $\mathrm{v}_p(a) \geq \mathrm{v}_p(p) = 1$ nach Proposition (2.74). Umgekehrt, wenn $\mathrm{v}_p(a) \geq 1$ gilt, dann ist

$$\mathrm{v}_q(p) = \delta_{q,p} \leq \mathrm{v}_q(a)$$

für alle $q \in \mathbb{P}$, es ist also p ein Primfaktor von a nach Proposition (2.74). $\square$

(2.76) Korollar. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$ gegeben.

(a) Es ist

$$\gcd(a,b) = \prod_{p \in \mathbb{P}} p^{\min(\mathrm{v}_p(a), \mathrm{v}_p(b))}.$$

(b) Es ist

$$\mathrm{lcm}(a,b) = \prod_{p \in \mathbb{P}} p^{\max(\mathrm{v}_p(a), \mathrm{v}_p(b))}.$$

Beweis.

(a) Wegen $\min(\mathrm{v}_p(a), \mathrm{v}_p(b)) \leq \mathrm{v}_p(a)$ und $\min(\mathrm{v}_p(a), \mathrm{v}_p(b)) \leq \mathrm{v}_p(b)$ ist $\prod_{p \in \mathbb{P}} p^{\min(\mathrm{v}_p(a), \mathrm{v}_p(b))}$ ein gemeinsamer Teiler von a und b nach Proposition (2.74). Für jeden gemeinsamen Teiler d von a und b gilt ferner $\mathrm{v}_p(d) \leq \mathrm{v}_p(a)$ und $\mathrm{v}_p(d) \leq \mathrm{v}_p(b)$ für alle $p \in \mathbb{P}$ nach Proposition (2.74), somit auch $\mathrm{v}_p(d) \leq \min(\mathrm{v}_p(a), \mathrm{v}_p(b))$ für alle $p \in \mathbb{P}$ und folglich $d \mid \prod_{p \in \mathbb{P}} p^{\min(\mathrm{v}_p(a), \mathrm{v}_p(b))}$ nach Proposition (2.74). Somit ist $\gcd(a,b) = \prod_{p \in \mathbb{P}} p^{\min(\mathrm{v}_p(a), \mathrm{v}_p(b))}$.

(b) Dies lässt sich dual zu (a) beweisen. □

(2.77) Korollar. Es sei $p \in \mathbb{P}$ gegeben. Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathrm{v}_p(a+b) \geq \min(\mathrm{v}_p(a), \mathrm{v}_p(b)).$$

Beweis. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$ gegeben. Dann ist $\gcd(a,b)$ ein gemeinsamer Teiler von a und b, also nach Proposition (2.12)(a) auch ein Teiler von $a+b$. Nach Korollar (2.76)(a) und Proposition (2.74) folgt

$$\mathrm{v}_p(a+b) \geq \mathrm{v}_p(\gcd(a,b)) = \min(\mathrm{v}_p(a), \mathrm{v}_p(b)).$$ □

Aufgaben

Aufgabe 26 (Reduzibilität)**.** Es sei ein reduzibles $n \in \mathbb{N}$ mit $n > 4$ gegeben. Zeigen Sie, dass

$$n \mid (n-1)!$$

gilt.

Aufgabe 27 (Primzahltest)**.** Es sei $n \in \mathbb{N} \setminus \{1\}$ gegeben. Zeigen Sie: Wenn für jede Primzahl p mit $p^2 \leq n$ stets $p \nmid n$ gilt, dann ist n selbst eine Primzahl.

Aufgabe 28 (reduzible Elemente)**.** Zeigen Sie, dass es zu jedem $n \in \mathbb{N}$ ein $R \in \mathbb{N}$ derart gibt, dass alle Elemente im ganzzahligen Intervall $[R+1, R+n]$ reduzibel sind.

Aufgabe 29 (konstante Eins als g-adische Darstellung)**.** Für $g \in \mathbb{N}$ mit $g \geq 2$ und $l \in \mathbb{N}$ sei $R_{g,l} = (1, \ldots, 1, 1)_g$ die Zahl, welche g-adisch durch l Einsen dargestellt wird. Zeigen oder widerlegen Sie:

(a) Für alle $g \in \mathbb{N}$ mit $g \geq 2$ gilt: Wenn l eine Primzahl ist, dann auch $R_{g,l}$.

(b) Für alle $g \in \mathbb{N}$ mit $g \geq 2$ gilt: Wenn $R_{g,l}$ eine Primzahl ist, dann auch l.

Aufgabe 30 (Fundamentalsatz der Arithmetik für $\mathbb{Q}_{>0}$)**.** Zeigen Sie, dass

$$\pi_{\mathbb{P}} \colon \mathbb{Z}^{(\mathbb{P})} \to \mathbb{Q}_{>0},\ a \mapsto \prod_{p \in \mathbb{P}} p^{a_p}$$

ein Gruppenisomorphismus ist.

Aufgabe 31 (Zerlegung in irreduzible Elemente)**.** Es sei $U := \{4n+1 \mid n \in \mathbb{N}_0\}$. Ein $a \in U$ heißt *U-reduzibel*, falls es $x, y \in U \setminus \{1\}$ mit $a = xy$ gibt, sonst *U-irreduzibel*.

(a) Zeigen Sie, dass U ein Untermonoid von $\mathbb{N}$ ist.

(b) Zeigen Sie, dass jedes Element aus U ein Produkt aus U-irreduziblen Elementen ist.

(c) Ist die Zerlegung in (b) eindeutig (bis auf Reihenfolge der Faktoren)?

Kapitel III

Arithmetische Funktionen

1 Die Dirichlet-Algebra

Definition arithmetischer Funktionen und Beispiele

(3.1) Definition (arithmetische Funktion)**.** Eine *arithmetische Funktion* (oder *zahlentheoretische Funktion*) ist eine Abbildung von $\mathbb{N}$ nach $\mathbb{C}$.

(3.2) Beispiel.

(a) Die Teilerfunktion $\tau\colon \mathbb{N} \to \mathbb{C}$ gegeben durch $\tau(n) = |\{d \in \mathbb{N} \mid d \text{ ist ein Teiler von } n\}|$ für $n \in \mathbb{N}$ ist eine arithmetische Funktion.

(b) Die Primteilerfunktion $\omega\colon \mathbb{N} \to \mathbb{C}$ gegeben durch $\omega(n) = |\{p \in \mathbb{P} \mid p \text{ ist ein Primteiler von } n\}|$ für $n \in \mathbb{N}$ ist eine arithmetische Funktion.

(c) Die p-adische Bewertung $\mathrm{v}_p\colon \mathbb{N} \to \mathbb{C}$ ist eine arithmetische Funktion.

Dirichlet-Faltung

Es ist $\mathrm{Map}(\mathbb{N}, \mathbb{C})$ ein $\mathbb{C}$-Vektorraum mit Addition gegeben durch

$$(f + g)(n) = f(n) + g(n)$$

für $n \in \mathbb{N}$, $f, g \in \mathrm{Map}(\mathbb{N}, \mathbb{C})$. Wir wollen nun eine Multiplikation auf $\mathrm{Map}(\mathbb{N}, \mathbb{C})$ definieren.

(3.3) Definition (Dirichlet-Faltung, Dirichlet-Eins)**.**

(a) Die Verknüpfung $*$ auf $\mathrm{Map}(\mathbb{N}, \mathbb{C})$ gegeben durch

$$(f * g)(n) = \sum_{\substack{a,b \in \mathbb{N} \\ ab = n}} f(a)g(b)$$

für $n \in \mathbb{N}$, $f, g \in \mathrm{Map}(\mathbb{N}, \mathbb{C})$ heißt *Dirichlet-Faltung*. Für $f, g \in \mathrm{Map}(\mathbb{N}, \mathbb{C})$ wird $f * g$ das *Dirichlet-Produkt* von f und g genannt.

(b) Die arithmetische Funktion ε gegeben durch

$$\varepsilon(n) = \delta_{n,1}$$

heißt *Dirichlet-Eins* (oder *Dirichlet-Identität*).

(3.4) Bemerkung. Es seien arithmetische Funktionen f und g gegeben. Für $n \in \mathbb{N}$ gilt

$$(f * g)(n) = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} f(d)g(\frac{n}{d}) = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} f(\frac{n}{d})g(d).$$

(3.5) Proposition. Der $\mathbb{C}$-Vektorraum $\mathrm{Map}(\mathbb{N},\mathbb{C})$ wird eine nullteilerfreie kommutative $\mathbb{C}$-Algebra mit Multiplikation gegeben durch die Dirichlet-Faltung $*$. Die Eins von $\mathrm{Map}(\mathbb{N},\mathbb{C})$ ist gegeben durch die Dirichlet-Eins ε.

Beweis. Wir verifizieren die Axiome einer $\mathbb{C}$-Algebra.
Für $f,g,h \in \mathrm{Map}(\mathbb{N},\mathbb{C})$ gilt

$$\begin{aligned}(f*(g*h))(n) &= \sum_{\substack{a,d\in\mathbb{N}\\ ad=n}} f(a)(g*h)(d) = \sum_{\substack{a,d\in\mathbb{N}\\ ad=n}} f(a)\Big(\sum_{\substack{b,c\in\mathbb{N}\\ bc=d}} g(b)h(c)\Big) = \sum_{\substack{a,d\in\mathbb{N}\\ ad=n}}\sum_{\substack{b,c\in\mathbb{N}\\ bc=d}} f(a)(g(b)h(c))\\ &= \sum_{\substack{a,b,c\in\mathbb{N}\\ abc=n}} f(a)g(b)h(c) = \sum_{\substack{d,c\in\mathbb{N}\\ dc=n}}\sum_{\substack{a,b\in\mathbb{N}\\ ab=d}} (f(a)g(b))h(c) = \sum_{\substack{d,c\in\mathbb{N}\\ dc=n}}\Big(\sum_{\substack{a,b\in\mathbb{N}\\ ab=d}} f(a)g(b)\Big)h(c)\\ &= \sum_{\substack{d,c\in\mathbb{N}\\ dc=n}} (f*g)(d)h(c) = ((f*g)*h)(n)\end{aligned}$$

für alle $n\in\mathbb{N}$ und damit $f*(g*h)=(f*g)*h$. Folglich ist $*$ assoziativ.
Für $f,g\in\mathrm{Map}(\mathbb{N},\mathbb{C})$ gilt

$$(f*g)(n) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b) = \sum_{\substack{b,a\in\mathbb{N}\\ ba=n}} g(b)f(a) = (g*f)(n)$$

für alle $n\in\mathbb{N}$ und damit $f*g=g*f$. Folglich ist $*$ kommutativ.
Für $f\in\mathrm{Map}(\mathbb{N},\mathbb{C})$ gilt

$$(f*\varepsilon)(n) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} f(\frac{n}{d})\varepsilon(d) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} f(\frac{n}{d})\delta_{d,1} = f(\frac{n}{1})\varepsilon(1) = f(n)$$

für alle $n\in\mathbb{N}$ und damit $f*\varepsilon=f$. Folglich ist ε ein neutrales Element bzgl. $*$.
Für $f,g,h\in\mathrm{Map}(\mathbb{N},\mathbb{C})$ gilt

$$\begin{aligned}(f*(g+h))(n) &= \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)(g+h)(b) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)(g(b)+h(b)) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} (f(a)g(b)+f(a)h(b))\\ &= \Big(\sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\Big) + \Big(\sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)h(b)\Big) = (f*g)(n)+(f*h)(n) = ((f*g)+(f*h))(n)\end{aligned}$$

für alle $n\in\mathbb{N}$ und damit $f*(g+h)=(f*g)+(f*h)$. Für $z\in\mathbb{C}$, $f,g\in\mathrm{Map}(\mathbb{N},\mathbb{C})$ gilt

$$\begin{aligned}(f*(zg))(n) &= \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)(zg)(b) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)(zg(b)) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} z(f(a)g(b)) = z\sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b) = z(f*g)(n)\\ &= (z(f*g))(n)\end{aligned}$$

für alle $n\in\mathbb{N}$ und damit $f*(zg)=z(f*g)$. Folglich gelten die Distributivgesetze.
Insgesamt wird $\mathrm{Map}(\mathbb{N},\mathbb{C})$ eine $\mathbb{C}$-Algebra mit Dirichlet-Faltung als Multiplikation und Dirichlet-Eins als Einselement. □

(3.6) Definition (Dirichlet-Algebra)**.** Die Menge der arithmetischen Funktionen $\mathrm{Map}(\mathbb{N},\mathbb{C})$ mit der $\mathbb{C}$-Algebrastruktur aus Proposition (3.5) heißt *Dirichlet-Algebra* und wird mit $\mathcal{A}$ bezeichnet.

(3.7) Bemerkung. Die Dirichlet-Algebra $\mathcal{A}$ ist nullteilerfrei.

Beweis. Um zu zeigen, dass $\mathcal{A}$ nullteilerfrei ist, seien $f,g\in\mathcal{A}\setminus\{0\}$ gegeben. Mit $m_0 := \min\{m\in\mathbb{N} \mid f(m)\neq 0\}$ und $n_0 := \min\{n\in\mathbb{N} \mid g(n)\neq 0\}$ gilt dann

$$(f*g)(m_0n_0) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=m_0n_0}} f(a)g(b) = f(m_0)g(n_0)\neq 0,$$

also insbesondere $f*g\neq 0$. □

(3.8) Definition (Dirichlet-Invertierbarkeit)**.** Eine arithmetische Funktion f heißt *Dirichlet-invertierbar*, falls f invertierbar im Ring $\mathcal{A}$ ist. Für eine Dirichlet-invertierbare arithmetische Funktion f wird $(f^{-1})^{\mathcal{A}}$ das *Dirichlet-Inverse* von f genannt.

(3.9) Proposition. Es ist

$$\mathcal{A}^\times = \{f \in \mathcal{A} \mid f(1) \neq 0\}.$$

Das Dirichlet-Inverse einer Dirichlet-invertierbaren arithmetischen Funktion f ist gegeben durch

$$(f^{-1})^{\mathcal{A}}(n) = \begin{cases} \frac{1}{f(1)}, & \text{falls } n = 1, \\ -\frac{1}{f(1)} \sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})\,(f^{-1})^{\mathcal{A}}(d), & \text{falls } n > 1, \end{cases}$$

für $n \in \mathbb{N}$.

Beweis. Es sei $f \in \mathcal{A}$ gegeben. Für $g \in \mathcal{A}$, $n \in \mathbb{N}$ erhalten wir

$$(f * g)(n) = \sum_{\substack{d\in\mathbb{N} \\ d|n}} f(\frac{n}{d})g(d) = \sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})g(d) + f(1)g(n)$$

oder äquivalent

$$f(1)g(n) = (f * g)(n) - \sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})g(d).$$

Ist $f \in \mathcal{A}^\times$, so folgt

$$f(1)f^{-1}(n) = \varepsilon(n) - \sum_{\substack{d\in\mathbb{N} \\ d|n\, d<n}} f(\frac{n}{d})f^{-1}(d) = \begin{cases} 1, & \text{falls } n = 1, \\ -\sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})f^{-1}(d), & \text{falls } n > 1, \end{cases}$$

also $f(1) \neq 0$ sowie

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)}, & \text{falls } n = 1, \\ -\frac{1}{f(1)} \sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})f^{-1}(d), & \text{falls } n > 1, \end{cases}$$

für $n \in \mathbb{N}$. Ist umgekehrt $f(1) \neq 0$, so definieren wir $g\colon \mathbb{N} \to \mathbb{C}$ rekursiv durch

$$g(n) := \begin{cases} \frac{1}{f(1)}, & \text{falls } n = 1, \\ -\frac{1}{f(1)} \sum_{\substack{d\in\mathbb{N} \\ d|n,\, d<n}} f(\frac{n}{d})\, g(d), & \text{falls } n > 1, \end{cases}$$

und erhalten $f * g = \varepsilon$, d.h. f ist invertierbar in $\mathcal{A}$ und $f^{-1} = g$. □

Multiplikativität

(3.10) Definition (Multiplikativität)**.** Eine arithmetische Funktion $f \neq 0$ heißt (*schwach*) *multiplikativ*, falls für teilerfremde $m, n \in \mathbb{N}$ stets

$$f(mn) = f(m)f(n)$$

gilt.
Die *Menge aller multiplikativen arithmetischen Funktionen* bezeichnen wir mit

$$\mathcal{A}_{\text{mul}} = \{f \in \mathcal{A} \mid f \text{ multiplikativ}\}.$$

(3.11) Bemerkung. Es sei eine multiplikative arithmetische Funktion f gegeben. Dann gilt

$$f(1) = 1.$$

Beweis. Da $f \neq 0$ ist, gibt es ein $n \in \mathbb{N}$ mit $f(n) \neq 0$. Die Teilerfremdheit von 1 und n impliziert

$$f(n) = f(1 \cdot n) = f(1)f(n)$$

und damit $f(1) = 1$. □

(3.12) Bemerkung. Eine arithmetische Funktion $f \neq 0$ ist genau dann multiplikativ, wenn für $n \in \mathbb{N}$ stets

$$f(n) = \prod_{p \in \mathbb{P}} f(p^{\mathrm{v}_p(n)})$$

gilt.

Beweis. Zunächst sei f multiplikativ. Für $p, q \in \mathbb{P}$ mit $p \neq q$ und $k, l \in \mathbb{N}_0$ sind p^k und q^l stets teilerfremd. Unter Beachtung von Bemerkung (3.11) impliziert die Multiplikativität von f induktiv $f(n) = \prod_{p \in \mathbb{P}} f(p^{\mathrm{v}_p(n)})$ für $n \in \mathbb{N}$.
Nun gelte umgekehrt $f(n) = \prod_{p \in \mathbb{P}} f(p^{\mathrm{v}_p(n)})$ für $n \in \mathbb{N}$. Um zu zeigen, dass f multiplikativ ist, seien teilerfremde $m, n \in \mathbb{N}$ gegeben. Dann sind die Mengen der Primfaktoren von m und n disjunkt, es gilt also

$$\begin{aligned} f(mn) &= f((\prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(m)})(\prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(n)})) = f((\prod_{\substack{p \in \mathbb{P} \\ p \mid m}} p^{\mathrm{v}_p(m)})(\prod_{\substack{p \in \mathbb{P} \\ p \mid n}} p^{\mathrm{v}_p(n)})) = (\prod_{\substack{p \in \mathbb{P} \\ p \mid m}} f(p^{\mathrm{v}_p(m)}))(\prod_{\substack{p \in \mathbb{P} \\ p \mid n}} f(p^{\mathrm{v}_p(n)})) \\ &= (\prod_{p \in \mathbb{P}} f(p^{\mathrm{v}_p(m)}))(\prod_{p \in \mathbb{P}} f(p^{\mathrm{v}_p(n)})) = f(m)f(n). \end{aligned}$$

□

(3.13) Beispiel. Die Teilerfunktion $\tau\colon \mathbb{N} \to \mathbb{C}$ ist multiplikativ.

Beweis. Es seien teilerfremde $m, n \in \mathbb{N}$ gegeben. Dann lässt sich jeder Teiler d von mn eindeutig als $d = ab$ mit $a \mid m$ und $b \mid n$ schreiben, d.h.

$$\{a \in \mathbb{N} \mid a \text{ teilt } m\} \times \{b \in \mathbb{N} \mid b \text{ teilt } n\} \to \{d \in \mathbb{N} \mid d \text{ teilt } mn\},\ (a, b) \mapsto ab$$

ist eine wohldefinierte Bijektion. Folglich gilt

$$\tau(mn) = |\{d \in \mathbb{N} \mid d \text{ teilt } mn\}| = |\{a \in \mathbb{N} \mid a \text{ teilt } m\}|\,|\{b \in \mathbb{N} \mid b \text{ teilt } n\}| = \tau(m)\tau(n).$$

Damit ist τ multiplikativ. □

(3.14) Proposition. Die Menge der multiplikativen arithmetischen Funktionen $\mathcal{A}_{\mathrm{mul}}$ ist eine Untergruppe von $\mathcal{A}^\times$.

Beweis. Für jede multiplikative arithmetische Funktion f gilt $f(1) = 1 \neq 0$ und damit $f \in \mathcal{A}^\times$ nach Proposition (3.9). Folglich ist $\mathcal{A}_{\mathrm{mul}} \subseteq \mathcal{A}^\times$. Um zu zeigen, dass $\mathcal{A}_{\mathrm{mul}}$ eine Untergruppe von $\mathcal{A}^\times$ ist, verwenden wir das Untergruppenkriterium.
Es seien $f, g \in \mathcal{A}_{\mathrm{mul}}$ gegeben. Um zu zeigen, dass $f * g \in \mathcal{A}_{\mathrm{mul}}$ ist, seien ferner teilerfremde $m, n \in \mathbb{N}$ gegeben. Dann ist

$$\{a \in \mathbb{N} \mid a \text{ teilt } m\} \times \{b \in \mathbb{N} \mid b \text{ teilt } n\} \to \{d \in \mathbb{N} \mid d \text{ teilt } mn\},\ (a, b) \mapsto ab$$

eine Bijektion. Folglich gilt

$$\begin{aligned} (f * g)(mn) &= \sum_{\substack{d \in \mathbb{N} \\ d \mid mn}} f(d)g(\frac{mn}{d}) = \sum_{\substack{(a,b) \in \mathbb{N} \times \mathbb{N} \\ a \mid m,\, b \mid n}} f(ab)g(\frac{mn}{ab}) = \sum_{\substack{a \in \mathbb{N} \\ a \mid m}} \sum_{\substack{b \in \mathbb{N} \\ b \mid n}} f(ab)g(\frac{m}{a}\frac{n}{b}) \\ &= \sum_{\substack{a \in \mathbb{N} \\ a \mid m}} \sum_{\substack{b \in \mathbb{N} \\ b \mid n}} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b}) = \sum_{\substack{a \in \mathbb{N} \\ a \mid m}} f(a)g(\frac{m}{a}) \sum_{\substack{b \in \mathbb{N} \\ b \mid n}} f(b)g(\frac{n}{b}) = (f * g)(m)(f * g)(n). \end{aligned}$$

Somit ist $f * g \in \mathcal{A}_{\mathrm{mul}}$.
Für $m, n \in \mathbb{N}$ gilt genau dann $mn = 1$, wenn $m = n = 1$ ist. Folglich haben wir

$$\varepsilon(mn) = \delta_{mn,1} = \delta_{m,1}\delta_{n,1} = \varepsilon(m)\varepsilon(n)$$

für $m, n \in \mathbb{N}$. Insbesondere ist $\varepsilon \in \mathcal{A}_{\mathrm{mul}}$.
Schließlich sei $f \in \mathcal{A}_{\mathrm{mul}}$ gegeben. Wir definieren eine arithmetische Funktion g durch

$$g(n) := \prod_{p \in \mathbb{P}} f^{-1}(p^{\mathrm{v}_p(n)}).$$

Für $p \in \mathbb{P}$, $k \in \mathbb{N}_0$ gilt dann

$$(f * g)(p^k) = \sum_{\substack{a,b \in \mathbb{N} \\ ab = p^k}} f(a)g(b) = \sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} f(p^i)g(p^j) = \sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} f(p^i)f^{-1}(p^j) = \sum_{\substack{a,b \in \mathbb{N} \\ ab = p^k}} f(a)f^{-1}(b) = \varepsilon(p^k).$$

Andererseits ist $g \in \mathcal{A}_{\mathrm{mul}}$, also auch $f*g \in \mathcal{A}_{\mathrm{mul}}$ und damit $f*g = \varepsilon$ nach Bemerkung (3.12). Folglich ist $g = f^{-1}$ und somit f^{-1} multiplikativ.
Nach dem Untergruppenkriterium ist $\mathcal{A}_{\mathrm{mul}}$ eine Untergruppe von $\mathcal{A}^\times$. □

Aufgaben

Aufgabe 32 (invertierbare arithmetische Funktionen)**.** Für $l \in \mathbb{N}$, $j \in [1, l]$ setzen wir

$$\mathrm{Part}(l, j) := \{\alpha \in \mathbb{N}^j \mid \sum_{i \in [1,j]} \alpha_i = l\}.$$

Zeigen Sie:

(a) Für $l \in \mathbb{N}$, $j \in [1, l]$ ist

$$\mathrm{Part}(l, j) = \dot{\bigcup_{k \in [j-1, l-1]}} (\mathrm{Part}(k, j-1) \times \{l - k\}).$$

(b) Für $f \in \mathcal{A}^\times$, $p \in \mathbb{P}$, $l \in \mathbb{N}$ gilt

$$(f^{-1})^{\mathcal{A}}(p^l) = \sum_{j \in [1,l]} \frac{(-1)^j}{f(1)^{j+1}} \sum_{\alpha \in \mathrm{Part}(l,j)} \prod_{i \in [1,j]} f(p^{\alpha_i}).$$

(c) Für $f \in \mathcal{A}_{\mathrm{mul}}$, $n \in \mathbb{N}$ mit $n > 1$ gilt

$$(f^{-1})^{\mathcal{A}}(n) = \prod_{p \in \mathbb{P}} \Big(\sum_{j \in [1, \mathrm{v}_p(n)]} (-1)^j \sum_{\alpha \in \mathrm{Part}(\mathrm{v}_p(n), j)} \prod_{i \in [1,j]} f(p^{\alpha_i}) \Big).$$

2 Summatorfunktion

Punktweise Einsfunktion und Möbius-Funktion

(3.15) Definition (punktweise Eins)**.** Die arithmetische Funktion

$$\iota \colon \mathbb{N} \to \mathbb{C},\ n \mapsto 1$$

heißt *punktweise Eins* (oder *punktweise Einsfunktion*).

(3.16) Bemerkung. Die punktweise Eins ι ist eine multiplikative arithmetische Funktion.

Nach Proposition (3.14) ist ι insbesondere Dirichlet-invertierbar. Das Dirichlet-Inverse von ι, also das Inverse von ι im Ring der arithmetischen Funktion $\mathcal{A}$, hat einen eigenen Namen:

(3.17) Definition (Möbius-Funktion)**.** Die arithmetische Funktion

$$\mu := (\iota^{-1})^{\mathcal{A}}$$

heißt *Möbius-Funktion* (oder *Möbiussche Funktion* oder *Möbiussche My-Funktion*).

(3.18) Bemerkung. Die Möbius-Funktion μ ist eine multiplikative arithmetische Funktion.

Beweis. Dies folgt aus Proposition (3.14). □

(3.19) Proposition. Für $n \in \mathbb{N}$ ist

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{falls } n \text{ quadratfrei ist,} \\ 0, & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Beweis. Für $n \in \mathbb{N}$ gilt

$$\mu(n) = \iota^{-1}(n) = \left\{ \begin{array}{ll} \frac{1}{\iota(1)}, & \text{falls } n = 1, \\ -\frac{1}{\iota(1)} \sum_{\substack{d \in \mathbb{N} \\ d|n,\, d<n}} \iota(\frac{n}{d})\, \iota^{-1}(d), & \text{falls } n > 1 \end{array} \right\} = \begin{cases} 1, & \text{falls } n = 1, \\ -\sum_{\substack{d \in \mathbb{N} \\ d|n,\, d<n}} \mu(d), & \text{falls } n > 1, \end{cases}$$

nach Proposition (3.9). Insbesondere erhalten wir

$$\mu(p^k) = -\sum_{\substack{d \in \mathbb{N} \\ d|p^k,\, d<p^k}} \mu(d) = -\sum_{j \in [0,k-1]} \mu(p^j)$$

für $p \in \mathbb{P}$, $k \in \mathbb{N}$. Es ergibt sich

$$\mu(p) = -\mu(1) = -1$$

für $p \in \mathbb{P}$. Dies impliziert für $p \in \mathbb{P}$, $k \in \mathbb{N}$ mit $k \geq 2$ jedoch

$$\mu(p^k) = -\sum_{j \in [0,k-1]} \mu(p^j) = -\sum_{j \in [2,k-1]} \mu(p^j),$$

woraus sich induktiv $\mu(p^k) = 0$ ergibt. Da μ multiplikativ ist, erhalten wir

$$\mu(n) = \prod_{p \in \mathbb{P}} \mu(p^{\mathrm{v}_p(n)}) = \Big(\prod_{\substack{p \in \mathbb{P} \\ \mathrm{v}_p(n)=0}} 1\Big)\Big(\prod_{\substack{p \in \mathbb{P} \\ \mathrm{v}_p(n)=1}} (-1)\Big)\Big(\prod_{\substack{p \in \mathbb{P} \\ \mathrm{v}_p(n) \geq 2}} 0\Big) = \begin{cases} (-1)^{\omega(n)}, & \text{falls } n \text{ quadratfrei ist,} \\ 0, & \text{falls } n \text{ nicht quadratfrei ist,} \end{cases}$$

für $n \in \mathbb{N}$. □

Summator

(3.20) Definition (Summatorfunktion)**.** Die Abbildung

$$\mathrm{T}\colon \mathcal{A} \to \mathcal{A},\ f \mapsto f * \iota$$

heißt *Summator* (oder *Summationsoperator*) auf $\mathcal{A}$. Für $f \in \mathcal{A}$ wird $\mathrm{T}f$ die *Summatorfunktion* (oder *summatorische Funktion*) von f genannt.

(3.21) Beispiel. Es ist

$$\mathrm{T}\mu = \varepsilon.$$

Beweis. Da $\mu = (\iota^{-1})^{\mathcal{A}}$ ist, gilt

$$\mathrm{T}\mu = \mu * \iota = \varepsilon.$$

□

(3.22) Bemerkung. Es sei eine arithmetische Funktion f gegeben. Für $n \in \mathbb{N}$ ist

$$(\mathrm{T}f)(n) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} f(d).$$

Beweis. Für $n \in \mathbb{N}$ gilt

$$(\mathrm{T}f)(n) = (f * \iota)(n) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} f(d)\iota(\frac{n}{d}) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} f(d). \qquad \square$$

(3.23) Korollar. Es sei eine arithmetische Funktion f gegeben. Genau dann ist f Dirichlet-invertierbar, wenn $\mathrm{T}f$ Dirichlet-invertierbar ist.

Beweis. Nach Bemerkung (3.22) ist $(\mathrm{T}f)(1) = f(1)$. Folglich gilt genau dann $f(1) \neq 0$, wenn $(\mathrm{T}f)(1) \neq 0$ ist. Nach Proposition (3.9) ist also f genau dann Dirichlet-invertierbar, wenn $\mathrm{T}f$ Dirichlet-invertierbar ist. $\square$

(3.24) Bemerkung. Für $f, g \in \mathcal{A}$ gilt

$$\mathrm{T}(f * g) = \mathrm{T}f * g = f * \mathrm{T}g.$$

Beweis. Da $\mathcal{A}$ assoziativ und kommutativ ist, gilt

$$\mathrm{T}(f * g) = (f * g) * \iota = (f * \iota) * g = \mathrm{T}f * g,$$
$$\mathrm{T}(f * g) = (f * g) * \iota = f * (g * \iota) = f * \mathrm{T}g$$

für $f, g \in \mathcal{A}$. $\square$

Möbiussche Umkehrformel

(3.25) Bemerkung. Der Summator $\mathrm{T}\colon \mathcal{A} \to \mathcal{A}$ ist ein $\mathbb{C}$-Vektorraumautomorphismus. Der zu T inverse $\mathbb{C}$-Vektorraumautomorphismus $\mathrm{T}^{-1}\colon \mathcal{A} \to \mathcal{A}$ ist gegeben durch

$$\mathrm{T}^{-1}g = g * \mu$$

für $g \in \mathcal{A}$.

Beweis. Zunächst ist $\mathrm{T}\colon \mathcal{A} \to \mathcal{A}$, $f \mapsto f * \iota$ ein Vektorraumhomomorphismus, da $\mathcal{A}$ eine Algebra über $\mathbb{C}$ ist. Wegen $\iota * \mu = \mu * \iota = \varepsilon$ ist jedoch T auch invertierbar mit $\mathrm{T}^{-1}\colon \mathcal{A} \to \mathcal{A}$ gegeben durch $\mathrm{T}^{-1}g = g * \mu$ für $g \in \mathcal{A}$. Dies impliziert aber bereits, dass T ein Vektorraumautomorphismus ist. $\square$

(3.26) Korollar (Möbiussche Umkehrformel)**.** Es sei eine arithmetische Funktion f gegeben. Für $n \in \mathbb{N}$ ist

$$f(n) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} \mu(a)\,(\mathrm{T}f)(b).$$

Beweis. Es ist $f = \mathrm{T}^{-1}(\mathrm{T}f) = \mu * \mathrm{T}f$ und damit

$$f(n) = (\mu * \mathrm{T}f)(n) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} \mu(a)\,(\mathrm{T}f)(b)$$

für $n \in \mathbb{N}$. $\square$

(3.27) Korollar. Es sei eine arithmetische Funktion f gegeben. Genau dann ist f multiplikativ, wenn $\mathrm{T}f$ multiplikativ ist.

Beweis. Nach Bemerkung (3.16) und Bemerkung (3.18) sind ι und μ multiplikativ. Da $\mathcal{A}_{\mathrm{mul}}$ nach Proposition (3.14) eine Untergruppe von $\mathcal{A}^\times$ ist, gilt: Wenn f multiplikativ ist, dann ist auch $\mathrm{T}f = f * \iota$ multiplikativ; und wenn $\mathrm{T}f$ multiplikativ ist, dann ist nach Bemerkung (3.25) auch $f = \mathrm{T}^{-1}(\mathrm{T}f) = \mathrm{T}f * \mu$ multiplikativ. $\square$

Aufgaben

Aufgabe 33 (Primteilerfunktion)**.** Berechnen Sie $\omega * \mu$.

Aufgabe 34 (Liouville-Funktion)**.** Die *Liouville-Funktion* ist definiert als

$$\lambda\colon \mathbb{N} \to \mathbb{C},\ n \mapsto (-1)^{\Omega(n)},$$

wobei $\Omega(n) := \sum_{p\in\mathbb{P}} \mathrm{v}_p(n)$ für $n \in \mathbb{N}$.

(a) Die Liouville-Funktion λ ist multiplikativ.

(b) Das Dirichlet-Inverse von λ ist gegeben durch

$$\lambda^{-1}(n) = |\mu(n)|$$

für $n \in \mathbb{N}$.

(c) Für $n \in \mathbb{N}$ gilt

$$\sum_{\substack{d\in\mathbb{N}\\ d|n}} \lambda(d) = \begin{cases} 1, & \text{falls } n \text{ ein Quadrat ist,} \\ 0, & \text{falls } n \text{ kein Quadrat ist.} \end{cases}$$

(d) Für $n \in \mathbb{N}$ gilt

$$\lambda(n) = \sum_{\substack{d\in\mathbb{N}\\ d^2|n}} \mu\left(\frac{n}{d^2}\right).$$

3 Teilersummen und vollkommene Zahlen

Teilersummenfunktion

(3.28) Definition (Teilersummenfunktion)**.** Die Summatorfunktion $\sigma := \mathrm{T}\,\mathrm{inc}$ der Inklusion $\mathrm{inc}\colon \mathbb{N} \to \mathbb{C}$, $n \mapsto n$ heißt *Teilersummenfunktion.*

(3.29) Bemerkung. Für $n \in \mathbb{N}$ ist

$$\sigma(n) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} d$$

Beweis. Nach Bemerkung (3.22) gilt

$$\sigma(n) = (\mathrm{T}\,\mathrm{inc})(n) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \mathrm{inc}(d) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} d$$

für $n \in \mathbb{N}$. □

(3.30) Bemerkung. Die Teilersummenfunktion σ ist eine multiplikative arithmetische Funktion.

Beweis. Da die Inklusion $\mathrm{inc}\colon \mathbb{N} \to \mathbb{C}$ eine multiplikative arithmetische Funktion ist, gilt dies nach Korollar (3.27) auch für deren Summatorfunktion $\mathrm{T}\,\mathrm{inc} = \sigma$. □

(3.31) Proposition. Für $n \in \mathbb{N}$ gilt

$$\sigma(n) = \prod_{p\in\mathbb{P}} \frac{p^{\mathrm{v}_p(n)+1} - 1}{p-1} = \prod_{\substack{p\in\mathbb{P}\\ p|n}} \frac{p^{\mathrm{v}_p(n)+1} - 1}{p-1}.$$

Beweis. Für $p \in \mathbb{P}$, $k \in \mathbb{N}$ gilt

$$\sigma(p^k) = \sum_{\substack{d \in \mathbb{N} \\ d | p^k}} d = \sum_{i \in [0,k]} p^i = \frac{p^{k+1} - 1}{p - 1}$$

nach der geometrischen Summenformel. Da σ nach Bemerkung (3.30) multiplikativ ist, folgt

$$\sigma(n) = \prod_{\substack{p \in \mathbb{P} \\ p | n}} \sigma(p^{\mathrm{v}_p(n)}) = \prod_{\substack{p \in \mathbb{P} \\ p | n}} \frac{p^{\mathrm{v}_p(n)+1} - 1}{p - 1} = \prod_{p \in \mathbb{P}} \frac{p^{\mathrm{v}_p(n)+1} - 1}{p - 1}$$

für $n \in \mathbb{N}$ nach Bemerkung (3.12). □

Mersenne-Zahlen und Mersenne-Primzahlen

(3.32) Definition (Mersenne-Zahl)**.** Für $n \in \mathbb{N}$ heißt

$$\mathrm{M}_n := 2^n - 1$$

die *n-te Mersenne-Zahl* (oder *n-te Mersennesche Zahl*).

(3.33) Beispiel. Es ist

$\mathrm{M}_1 = 1$,
$\mathrm{M}_2 = 3$,
$\mathrm{M}_3 = 7$,
$\mathrm{M}_4 = 15$,
$\mathrm{M}_5 = 31$.

(3.34) Proposition. Es sei $n \in \mathbb{N}$ gegeben. Wenn die n-te Mersenne-Zahl M_n eine Primzahl ist, dann ist auch n eine Primzahl.

Beweis. Es sei n reduzibel, etwa $n = lm$ mit $l, m \in \mathbb{N}$ und $l > 1$, $m > 1$. Dann ist auch $2^l - 1 > 1$ und $\sum_{i \in [0,m-1]} (2^l)^i > 1$ und damit

$$\mathrm{M}_n = \mathrm{M}_{lm} = 2^{lm} - 1 = (2^l - 1)(\sum_{i \in [0,m-1]} (2^l)^i)$$

reduzibel.
Im Umkehrschluss folgt: Wenn M_n eine Primzahl ist, dann ist auch n eine Primzahl. □

(3.35) Definition (Mersenne-Primzahl)**.** Die Primzahlen der Form M_p für $p \in \mathbb{P}$ heißen *Mersenne-Primzahlen* (oder *Mersennesche Primzahlen*).

Die Umkehrung von Proposition (3.34) gilt nicht, wie folgendes Beispiel zeigt.

(3.36) Beispiel. Es ist

$$\mathrm{M}_{11} = 23 \cdot 89.$$

Es ist unbekannt, ob es unendlich viele Mersenne-Primzahlen gibt. Am 25. Januar 2013 wurde die 48. bekannte Mersenne-Primzahl von Cooper, Woltman und Kurowski im Rahmen des Projekts GIMPS (Great Internet Mersenne Prime Search) gefunden, sie lautet $2^{57885161} - 1$ und hat 17 425 170 Dezimalstellen.

(3.37) Bemerkung. Es sei $p \in \mathbb{P}$ so gegeben, dass M_p eine Mersennesche Primzahl ist. Dann gilt

$$\sigma(\mathrm{M}_p) = 2^p.$$

Beweis. Da M_p eine Primzahl ist, gilt

$$\sigma(\mathrm{M}_p) = \sum_{\substack{d\in\mathbb{N}\\ d\mid \mathrm{M}_p}} d = 1 + \mathrm{M}_p = 1 + 2^p - 1 = 2^p. \qquad \square$$

(3.38) Bemerkung. Für $n \in \mathbb{N}$ gilt

$$\mathrm{M}_n = \sigma(2^{n-1}).$$

Beweis. Nach Proposition (3.31) gilt für $n \in \mathbb{N}$ stets

$$\sigma(2^{n-1}) = \frac{2^n - 1}{2 - 1} = \mathrm{M}_n. \qquad \square$$

Vollkommene Zahlen

(3.39) Definition (vollkommene Zahl)**.** Eine *vollkommene Zahl* (oder *perfekte Zahl*) ist eine natürliche Zahl$n$ mit

$$n = \sum_{\substack{d\in\mathbb{N}\\ d\mid n,\, d<n}} d.$$

Die ersten vier vollkommene Zahlen waren schon in der Antike bekannt:

(3.40) Beispiel. Die ersten fünf vollkommenen Zahlen sind

6, 28, 496, 8128, 33550336.

Es ist unbekannt, ob es unendlich viele vollkommene Zahlen gibt. Ferner sind alle bekannten vollkommenen Zahlen gerade – es ist nicht bekannt, ob es ungerade vollkommene Zahlen gibt.
Zum Studium von vollkommenen Zahlen eignet sich die Teilersummenfunktion, wie folgende Bemerkung zeigt.

(3.41) Bemerkung. Es sei $n \in \mathbb{N}$ gegeben. Genau dann ist n vollkommen, wenn $\sigma(n) = 2n$ ist.

Beweis. Nach Definition (3.39) ist n genau dann vollkommen, wenn $\sum_{\substack{d\in\mathbb{N}\\ d\mid n,\, d<n}} d = n$ ist. Wegen

$$\sigma(n) = \sum_{\substack{d\in\mathbb{N}\\ d\mid n}} d = \sum_{\substack{d\in\mathbb{N}\\ d\mid n,\, d<n}} d + n$$

ist dies aber zu $\sigma(n) = 2n$ äquivalent. $\square$

Charakterisierung vollkommener Zahlen durch Mersenne-Primzahlen

(3.42) Satz (Euklid, Euler)**.** Es sei eine gerade natürliche Zahl n gegeben. Genau dann ist n vollkommen, wenn

$$n = 2^{\mathrm{v}_2(n)}\mathrm{M}_{\mathrm{v}_2(n)+1}$$

gilt und $\mathrm{M}_{\mathrm{v}_2(n)+1}$ eine Mersennesche Primzahl ist.

Beweis. Es gelte zunächst $n = 2^{\mathrm{v}_2(n)}\mathrm{M}_{\mathrm{v}_2(n)+1}$ und es sei $\mathrm{M}_{\mathrm{v}_2(n)+1} \in \mathbb{P}$. Nach Bemerkung (3.37) gilt $\sigma(\mathrm{M}_{\mathrm{v}_2(n)+1}) = 2^{\mathrm{v}_2(n)+1}$ und nach Bemerkung (3.38) gilt $\sigma(2^{\mathrm{v}_2(n)}) = \mathrm{M}_{\mathrm{v}_2(n)+1}$. Da $\mathrm{M}_{\mathrm{v}_2(n)+1}$ ungerade und damit teilerfremd zu $2^{\mathrm{v}_2(n)}$ ist und da σ nach Bemerkung (3.30) eine multiplikative arithmetische Funktion ist, erhalten wir

$$\sigma(n) = \sigma(2^{\mathrm{v}_2(n)}\mathrm{M}_{\mathrm{v}_2(n)+1}) = \sigma(2^{\mathrm{v}_2(n)})\sigma(\mathrm{M}_{\mathrm{v}_2(n)+1}) = \mathrm{M}_{\mathrm{v}_2(n)+1}2^{\mathrm{v}_2(n)+1} = 2n.$$

Nach Bemerkung (3.41) ist n vollkommen.

Nun sei umgekehrt n vollkommen und es sei $m := \frac{n}{2^{\mathrm{v}_2(n)}}$, so dass $n = 2^{\mathrm{v}_2(n)}m$ gilt. Nach Bemerkung (3.41) und Bemerkung (3.38) erhalten wir

$$2^{\mathrm{v}_2(n)+1}m = 2n = \sigma(n) = \sigma(2^{\mathrm{v}_2(n)}m) = \sigma(2^{\mathrm{v}_2(n)})\sigma(m) = \mathrm{M}_{\mathrm{v}_2(n)+1}\sigma(m)$$

und damit $\mathrm{M}_{\mathrm{v}_2(n)+1} \mid 2^{\mathrm{v}_2(n)+1}m$. Da $\mathrm{M}_{\mathrm{v}_2(n)+1}$ ungerade ist, folgt $\mathrm{M}_{\mathrm{v}_2(n)+1} \mid m$, d.h. es ist $m = \mathrm{M}_{\mathrm{v}_2(n)+1}q$ für ein $q \in \mathbb{N}$. Wegen $n = 2^{\mathrm{v}_2(n)}m = 2^{\mathrm{v}_2(n)}\mathrm{M}_{\mathrm{v}_2(n)+1}q$ und $\mathrm{v}_2(n) > 0$ ist q ein echter Teiler von n. Da aber

$$\sigma(m) = 2^{\mathrm{v}_2(n)+1}\frac{m}{\mathrm{M}_{\mathrm{v}_2(n)+1}} = 2^{\mathrm{v}_2(n)+1}q = (1+\mathrm{M}_{\mathrm{v}_2(n)+1})q = q + \mathrm{M}_{\mathrm{v}_2(n)+1}q = q + m$$

gilt, sind folglich q und m die einzigen Teiler von m. Dann muss aber bereits $q = 1$ und $m = \mathrm{M}_{\mathrm{v}_2(n)+1}$ eine Primzahl sein. □

Aufgaben

Aufgabe 35 (vollkommene Zahlen)**.** Es sei $n \in \mathbb{N}$ gegeben. Zeigen Sie, dass n genau dann vollkommen ist, wenn

$$\sum_{\substack{d\in\mathbb{N}\\ d\mid n}} \frac{1}{d} = 2$$

ist.

Aufgabe 36 (Unvollkommenheit von Primzahlpotenzen)**.** Es seien $p \in \mathbb{P}$ und $k \in \mathbb{N}$ gegeben. Zeigen Sie, dass p^k nicht vollkommen ist.

4 Derivation von arithmetischen Funktionen

Derivationsoperator

(3.43) Definition (derivierte arithmetische Funktion)**.** Die Abbildung $\mathrm{D}\colon \mathcal{A} \to \mathcal{A}$ gegeben durch

$$(\mathrm{D}f)(n) = f(n)\ln(n)$$

für $n \in \mathbb{N}$, $f \in \mathcal{A}$, heißt *Derivationsoperator* (oder *Ableitungsoperator*) auf $\mathcal{A}$. Für $f \in \mathcal{A}$ wird $\mathrm{D}f$ die *derivierte arithmetische Funktion* (oder *arithmetische Ableitung*) von f genannt.

(3.44) Bemerkung (Leibniz-Regel)**.** Für $f, g \in \mathcal{A}$ gilt

$$\mathrm{D}(f * g) = \mathrm{D}f * g + f * \mathrm{D}g.$$

Beweis. Für $f, g \in \mathcal{A}$, $n \in \mathbb{N}$ gilt

$$\begin{aligned}
(\mathrm{D}(f*g))(n) &= (f*g)(n)\ln(n) = \Big(\sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\Big)\ln(n) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\ln(n) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\ln(ab)\\
&= \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)(\ln(a)+\ln(b)) = \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\ln(a) + \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\ln(b)\\
&= \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} (\mathrm{D}f)(a)g(b) + \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)(\mathrm{D}g)(b) = (\mathrm{D}f*g)(n) + (f*\mathrm{D}g)(n)\\
&= (\mathrm{D}f*g + f*\mathrm{D}g)(n)
\end{aligned}$$

und damit $\mathrm{D}(f*g) = \mathrm{D}f*g + f*\mathrm{D}g$. □

(3.45) Proposition. Der Derivationsoperator $\mathrm{D}\colon \mathcal{A} \to \mathcal{A}$ ist ein $\mathbb{C}$-Vektorraumendomorphismus mit

$$\begin{aligned}
\operatorname{Ker}\mathrm{D} &= \mathbb{C}\varepsilon,\\
\operatorname{Im}\mathrm{D} &= \mathcal{A}\setminus\mathcal{A}^\times.
\end{aligned}$$

Beweis. Für $f, g \in \mathcal{A}$, $n \in \mathbb{N}$ gilt

$$\begin{aligned}(\mathrm{D}(f+g))(n) &= (f+g)(n)\ln(n) = (f(n)+g(n))\ln(n) = f(n)\ln(n) + g(n)\ln(n) = (\mathrm{D}f)(n) + (\mathrm{D}g)(n)\\ &= (\mathrm{D}f + \mathrm{D}g)(n)\end{aligned}$$

und damit $\mathrm{D}(f+g) = \mathrm{D}f + \mathrm{D}g$. Ferner gilt für $z \in \mathbb{C}$, $f \in \mathcal{A}$, $n \in \mathbb{N}$ stets

$$(\mathrm{D}(zf))(n) = (zf)(n)\ln(n) = (zf(n))\ln(n) = z(f(n)\ln(n)) = z(\mathrm{D}f)(n) = (z(\mathrm{D}f))(n)$$

und damit $\mathrm{D}(zf) = z(\mathrm{D}f)$. Somit ist D ein $\mathbb{C}$-Vektorraumendomorphismus.
Da $\ln(1) = 0$ ist, gilt für $f \in \mathcal{A}$ stets

$$(\mathrm{D}f)(1) = f(1)\ln(1) = f(1)\cdot 0 = 0.$$

Wegen $\ln(n) \neq 0$ für $n \in \mathbb{N}$ mit $n \neq 1$ ist der Kern von D somit gegeben durch

$$\begin{aligned}\operatorname{Ker}\mathrm{D} &= \{f \in \mathcal{A} \mid \mathrm{D}f = 0\} = \{f \in \mathcal{A} \mid (\mathrm{D}f)(n) = 0 \text{ für alle } n \in \mathbb{N}\}\\ &= \{f \in \mathcal{A} \mid (\mathrm{D}f)(n) = 0 \text{ für alle } n \in \mathbb{N} \text{ mit } n \neq 1\}\\ &= \{f \in \mathcal{A} \mid f(n)\ln(n) = 0 \text{ für alle } n \in \mathbb{N} \text{ mit } n \neq 1\}\\ &= \{f \in \mathcal{A} \mid f(n) = 0 \text{ für alle } n \in \mathbb{N} \text{ mit } n \neq 1\} = \mathbb{C}\varepsilon.\end{aligned}$$

Da nach Proposition (3.9) außerdem

$$\mathcal{A} \setminus \mathcal{A}^\times = \{f \in \mathcal{A} \mid f(1) = 0\}$$

ist, gilt ferner $\mathrm{D}f \in \mathcal{A} \setminus \mathcal{A}^\times$ für $f \in \mathcal{A}$ und damit $\operatorname{Im}\mathrm{D} \subseteq \mathcal{A} \setminus \mathcal{A}^\times$. Es sei umgekehrt $g \in \mathcal{A} \setminus \mathcal{A}^\times$ gegeben, so dass $g(1) = 0$ gilt. Für $f \in \mathcal{A}$ gegeben durch

$$f(n) = \begin{cases} 0, & \text{falls } n = 1,\\ g(n)\frac{1}{\ln(n)}, & \text{falls } n \neq 1,\end{cases}$$

für $n \in \mathbb{N}$ erhalten wir

$$(\mathrm{D}f)(n) = f(n)\ln(n) = \left.\begin{cases} 0, & \text{falls } n = 1,\\ g(n), & \text{falls } n \neq 1\end{cases}\right\} = g(n)$$

für $n \in \mathbb{N}$ und damit $\mathrm{D}f = g$. Folglich ist $g \in \operatorname{Im}\mathrm{D}$. Insgesamt gilt

$$\operatorname{Im}\mathrm{D} = \mathcal{A} \setminus \mathcal{A}^\times.$$ □

Derivation und Summator

(3.46) Bemerkung. Für $f \in \mathcal{A}$ gilt

$$\mathrm{T}\mathrm{D}f - \mathrm{T}\mathrm{D}f = f * \mathrm{D}\iota.$$

Beweis. Nach Bemerkung (3.44) gilt

$$\mathrm{T}\mathrm{D}f = \mathrm{D}(f * \iota) = \mathrm{D}f * \iota + f * \mathrm{D}\iota = \mathrm{T}\mathrm{D}f + f * \mathrm{D}\iota.$$

und damit $\mathrm{T}\mathrm{D}f - \mathrm{T}\mathrm{D}f = f * \mathrm{D}\iota$ für $f \in \mathcal{A}$. □

(3.47) Korollar. Für $f \in \mathcal{A}$ gilt

$$\mathrm{T}\mathrm{D}^2 f = \mathrm{D}\mathrm{T}\mathrm{D}f - \mathrm{D}f * \mathrm{D}\iota.$$

Beweis. Nach Bemerkung (3.46) gilt

$$\mathrm{D}\mathrm{T}\mathrm{D}f - \mathrm{T}\mathrm{D}^2 f = \mathrm{D}\mathrm{T}\mathrm{D}f - \mathrm{T}\mathrm{D}\mathrm{D}f = \mathrm{D}f * \mathrm{D}\iota$$

und damit $\mathrm{T}\mathrm{D}^2 f = \mathrm{D}\mathrm{T}\mathrm{D}f - \mathrm{D}f * \mathrm{D}\iota$ für $f \in \mathcal{A}$. □

von-Mangoldt-Funktion

(3.48) Definition (von-Mangoldt-Funktion)**.** Die arithmetische Funktion

$$\Lambda := \mathrm{T}^{-1}\mathrm{D}\iota$$

heißt *von-Mangoldt-Funktion.*

(3.49) Bemerkung. Die von-Mangoldt-Funktion Λ ist nicht Dirichlet-invertierbar.

Beweis. Nach Proposition (3.45) ist $\mathrm{D}\iota$ nicht Dirichlet-invertierbar. Folglich ist $\Lambda = \mathrm{T}^{-1}\mathrm{D}\iota$ nach Korollar (3.23) ebenfalls nicht Dirichlet-invertierbar. □

Nach Proposition (3.14) ist Λ insbesondere nicht multiplikativ.

(3.50) Proposition. Für $n \in \mathbb{N}$ ist

$$\Lambda(n) = \begin{cases} \ln p, & \text{falls } n = p^k \text{ für } p \in \mathbb{P},\ k \in \mathbb{N}, \\ 0, & \text{sonst.} \end{cases}$$

Beweis. Wir definieren eine arithmetische Funktion f durch

$$f(n) := \begin{cases} \ln p, & \text{falls } n = p^k \text{ für } p \in \mathbb{P},\ k \in \mathbb{N}, \\ 0, & \text{sonst.} \end{cases}$$

Für $n \in \mathbb{N}$ gilt dann

$$\begin{aligned}(\mathrm{T}f)(n) &= \sum_{\substack{d\in\mathbb{N}\\ d\mid n}} f(d) = \sum_{\substack{p\in\mathbb{P}\\ p\mid n}} \sum_{j\in[1,\mathrm{v}_p(n)]} f(p^j) = \sum_{\substack{p\in\mathbb{P}\\ p\mid n}} \sum_{j\in[1,\mathrm{v}_p(n)]} \ln p = \sum_{\substack{p\in\mathbb{P}\\ p\mid n}} \mathrm{v}_p(n)\ln p = \ln\Big(\prod_{\substack{p\in\mathbb{P}\\ p\mid n}} p^{\mathrm{v}_p(n)}\Big) = \ln n \\ &= \iota(n)\ln(n) = (\mathrm{D}\iota)(n),\end{aligned}$$

also $\mathrm{T}f = \mathrm{D}\iota$ und damit $\Lambda = \mathrm{T}^{-1}\mathrm{D}\iota = f$. □

(3.51) Bemerkung. Es ist

$$\Lambda = -\mathrm{TD}\mu.$$

Beweis. Nach Bemerkung (3.25), Bemerkung (3.46) und Proposition (3.45) gilt

$$\Lambda = \mathrm{T}^{-1}\mathrm{D}\iota = \mu * \mathrm{D}\iota = \mathrm{DT}\mu - \mathrm{TD}\mu = \mathrm{D}\varepsilon - \mathrm{TD}\mu = -\mathrm{TD}\mu.$$ □

(3.52) Proposition. Für $f \in \mathcal{A}$ gilt

$$f * \Lambda = \mathrm{T}^{-1}\mathrm{DT}f - \mathrm{D}f = \mathrm{D}f - \mathrm{TDT}^{-1}f.$$

Beweis. Nach Bemerkung (3.46) und Bemerkung (3.24) gilt

$$\mathrm{DT}f - \mathrm{TD}f = f * \mathrm{D}\iota = f * \mathrm{T}\Lambda = \mathrm{T}(f * \Lambda)$$

und nach Bemerkung (3.25) somit

$$f * \Lambda = \mathrm{T}^{-1}(\mathrm{DT}f - \mathrm{TD}f) = \mathrm{T}^{-1}\mathrm{DT}f - \mathrm{T}^{-1}\mathrm{TD}f = \mathrm{T}^{-1}\mathrm{DT}f - \mathrm{D}f$$

für $f \in \mathcal{A}$. Ferner liefert Bemerkung (3.24) auch

$$f * \Lambda = \mathrm{TT}^{-1}f * \Lambda = \mathrm{T}(\mathrm{T}^{-1}f * \Lambda) = \mathrm{DTT}^{-1}f - \mathrm{TDT}^{-1}f = \mathrm{D}f - \mathrm{TDT}^{-1}f$$

für $f \in \mathcal{A}$. □

(3.53) Korollar (Selberg-Identität)**.** Es gilt

$$\begin{aligned}\mathrm{T}^{-1}\mathrm{D}^2\iota &= \mathrm{D}\Lambda + \Lambda * \Lambda, \\ \mathrm{TD}^2\mu &= -\mathrm{D}\Lambda + \Lambda * \Lambda.\end{aligned}$$

Beweis. Nach Proposition (3.52), Bemerkung (3.25), Proposition (3.45) und Bemerkung (3.51) gilt

$$\Lambda * \Lambda = \mathrm{T}^{-1}\mathrm{D}\mathrm{T}\Lambda - \mathrm{D}\Lambda = \mathrm{T}^{-1}\mathrm{D}^2\iota - \mathrm{D}\Lambda,$$
$$\Lambda * \Lambda = \mathrm{D}\Lambda - \mathrm{T}\mathrm{D}\mathrm{T}^{-1}\Lambda = \mathrm{D}\Lambda + \mathrm{T}\mathrm{D}(-\mathrm{T}^{-1}\Lambda) = \mathrm{D}\Lambda + \mathrm{T}\mathrm{D}\mathrm{D}\mu = \mathrm{D}\Lambda + \mathrm{T}\mathrm{D}^2\mu,$$

also $\mathrm{T}^{-1}\mathrm{D}^2\iota = \mathrm{D}\Lambda + \Lambda * \Lambda$ und $\mathrm{T}\mathrm{D}^2\mu = -\mathrm{D}\Lambda + \Lambda * \Lambda$. □

Die in Korollar (3.53) hergeleiteten Formeln finden im Beweis des *Primzahlsatzes* Anwendung: Die Abbildung $\pi\colon \mathbb{R} \to \mathbb{R}$ gegeben durch

$$\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$$

für $x \in \mathbb{R}$ heißt *Primzahlfunktion*. Der Primzahlsatz besagt, dass π asymptotisch gleich der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto \frac{x}{\ln x}$ ist:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Aufgaben

Aufgabe 37 (Quotientenregel)**.** Zeigen Sie: Für $f, g \in \mathcal{A}$ gilt

$$\mathrm{D}(f * g^{-1}) = (\mathrm{D}f * g - f * \mathrm{D}g) * g^{-2}.$$

Kapitel IV

Modulare Arithmetik

1 Kongruenzen und Restklassenringe

Kongruenzen ganzer Zahlen

(4.1) Definition (Kongruenz ganzer Zahlen)**.** Es sei $n \in \mathbb{Z}$ gegeben. Für $a, b \in \mathbb{Z}$ sagen wir, dass a *kongruent* b *modulo* n ist, geschrieben $a \equiv_n b$, wenn $n \mid a - b$ gilt, und sonst, dass a *inkongruent* b *modulo* n ist, geschrieben $a \not\equiv_n b$.

(4.2) Bemerkung. Es sei $n \in \mathbb{Z}$ geben. Für $a \in \mathbb{Z}$ gilt genau dann $a \equiv_n 0$, wenn $n \mid a$ gilt.

(4.3) Beispiel. Es ist $1 \equiv_7 8$, $3 \equiv_7 10$, $2 \equiv_7 9$, $2 \equiv_7 16$, $2 \equiv_7 -5$, $16 \equiv_7 -5$.

(4.4) Bemerkung. Es seien $n, a, b \in \mathbb{Z}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es gilt $a \equiv_n b$.

(b) Es gibt ein $q \in \mathbb{Z}$ mit $a = nq + b$.

(c) Es ist $a - b \in n\mathbb{Z}$.

Beweis. Genau dann gilt $a \equiv_n b$, d.h. $n \mid a-b$, wenn es ein $q \in \mathbb{Z}$ mit $a = nq+b$ gibt. Somit sind Bedingung (a) und Bedingung (b) äquivalent.
Ferner gilt nach Bemerkung (2.24) genau dann $a \equiv_n b$, d.h. $n \mid a - b$, wenn $a - b \in n\mathbb{Z}$ ist. Folglich sind auch Bedingung (a) und Bedingung (c) äquivalent.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(4.5) Bemerkung. Für alle $n \in \mathbb{Z}$ ist

$$\equiv_n = \equiv_{-n}.$$

Beweis. Es seien $n \in \mathbb{Z}$ und $a, b \in \mathbb{Z}$ gegeben. Es ist $a \equiv_n b$ äquivalent zu $n \mid a-b$, und es ist $a \equiv_{-n} b$ äquivalent zu $-n \mid a - b$. Nach Bemerkung (2.15) gilt jedoch genau dann $n \mid a - b$, wenn $-n \mid a - b$ gilt, d.h. $a \equiv_n b$ ist äquivalent zu $a \equiv_{-n} b$.
Folglich ist $\equiv_n = \equiv_{-n}$. □

Eigenschaften von Kongruenzen

(4.6) Proposition. Für alle $n \in \mathbb{Z}$ ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. Es sei $n \in \mathbb{Z}$ gegeben.
Es seien $a, b, c \in \mathbb{Z}$ mit $a \equiv_n b$ und $b \equiv_n c$ gegeben, so dass $n \mid a - b$ und $n \mid b - c$ gilt. Dann gilt jedoch auch $n \mid (a - b) + (b - c) = a - c$ nach Proposition (2.12)(a), d.h. $a \equiv_n c$. Folglich ist $\equiv_n$ transitiv.
Für alle $a \in \mathbb{Z}$ gilt $n \mid 0 = a - a$ nach Proposition (2.12)(b), also $a \equiv_n a$. Folglich ist $\equiv_n$ reflexiv.
Es seien $a, b \in \mathbb{Z}$ mit $a \equiv_n b$ gegeben, so dass $n \mid a - b$ gilt. Dann gilt auch $n \mid b - a$ nach Korollar (2.13), d.h. $b \equiv_n a$. Folglich ist $\equiv_n$ symmetrisch.
Insgesamt ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$. □

(4.7) Proposition. Es sei $n \in \mathbb{Z}$ gegeben.

(a) Für $a, \tilde{a}, b, \tilde{b} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ und $b \equiv_n \tilde{b}$ gilt auch $a + b \equiv_n \tilde{a} + \tilde{b}$.

(b) Für $a, \tilde{a} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ gilt auch $-a \equiv_n -\tilde{a}$.

(c) Für $a, \tilde{a}, b, \tilde{b} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ und $b \equiv_n \tilde{b}$ gilt auch $ab \equiv_n \tilde{a}\tilde{b}$.

Beweis.

(a) Es seien $a, \tilde{a}, b, \tilde{b} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ und $b \equiv_n \tilde{b}$ gegeben, so dass $n \mid a - \tilde{a}$ und $n \mid b - \tilde{b}$ gilt. Nach Proposition (2.12)(a) gilt dann auch $n \mid (a - \tilde{a}) + (b - \tilde{b}) = (a + b) - (\tilde{a} + \tilde{b})$, d.h. $a + b \equiv_n \tilde{a} + \tilde{b}$.

(b) Es seien $a, \tilde{a} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ gegeben, so dass $n \mid a - \tilde{a}$ gilt. Nach Korollar (2.13) folgt $n \mid \tilde{a} - a = -a - (-\tilde{a})$, d.h. $-a \equiv_n -\tilde{a}$.

(c) Es seien $a, \tilde{a}, b, \tilde{b} \in \mathbb{Z}$ mit $a \equiv_n \tilde{a}$ und $b \equiv_n \tilde{b}$ gegeben, so dass $n \mid a - \tilde{a}$ und $b - \tilde{b}$ gilt. Nach Proposition (2.12)(a), (c) gilt dann auch

$$n \mid (a - \tilde{a})b + \tilde{a}(b - \tilde{b}) = ab - \tilde{a}b + \tilde{a}b - \tilde{a}\tilde{b} = ab - \tilde{a}\tilde{b},$$

d.h. $ab \equiv_n \tilde{a}\tilde{b}$. □

(4.8) Bemerkung. Es seien $n, d, a, b \in \mathbb{Z}$ mit $d \mid n$ gegeben. Wenn $a \equiv_n b$ ist, dann auch $a \equiv_d b$.

Beweis. Wegen $a \equiv_n b$ gilt, d.h. $n \mid a - b$, dann gilt wegen $d \mid n$ auch $d \mid a - b$ nach Proposition (2.10)(a) und damit $a \equiv_d b$. □

(4.9) Bemerkung. Es seien $m \in \mathbb{N}$ und $n_i \in \mathbb{Z}$ für $i \in [1, m]$ gegeben. Für $a, b \in \mathbb{Z}$ gilt genau dann

$$a \equiv_{n_i} b$$

für alle $i \in [1, m]$, wenn

$$a \equiv_{\operatorname{lcm}(n_i)_{i \in [1,m]}} b$$

gilt.

Beweis. Es seien $a, b \in \mathbb{Z}$ gegeben. Für $i \in [1, m]$ gilt genau dann $a \equiv_{n_i} b$, wenn $n_i \mid a - b$ gilt, und es gilt genau dann $a \equiv_{\operatorname{lcm}(n_i)_{i \in [1,m]}} b$, wenn $\operatorname{lcm}(n_i)_{i \in [1,m]} \mid a - b$ gilt. Nach Definition eines kleinsten gemeinsamen Vielfachen ist die Bedingung $n_i \mid a - b$ für alle $i \in [1, m]$ jedoch äquivalent zur Bedingung $\operatorname{lcm}(n_i)_{i \in [1,m]} \mid a - b$. Folglich gilt genau dann $a \equiv_{n_i} b$ für alle $i \in [1, m]$, wenn $a \equiv_{\operatorname{lcm}(n_i)_{i \in [1,m]}} b$ gilt. □

Konstruktion der Restklassenringe

(4.10) Proposition. Es sei $n \in \mathbb{Z}$ gegeben. Die Menge $\mathbb{Z}/\equiv_n$ wird ein kommutativer Ring mit Addition und Multiplikation gegeben durch

$$[x] +^{\mathbb{Z}/\equiv_n} [y] = [x +^{\mathbb{Z}} y],$$
$$[x] \cdot^{\mathbb{Z}/\equiv_n} [y] = [x \cdot^{\mathbb{Z}} y]$$

für $x, y \in \mathbb{Z}$. Die Null und die Eins von $\mathbb{Z}/\equiv_n$ sind gegeben durch

$$0^{\mathbb{Z}/\equiv_n} = [0^{\mathbb{Z}}],$$
$$1^{\mathbb{Z}/\equiv_n} = [1^{\mathbb{Z}}].$$

Für $x \in \mathbb{Z}$ ist das Negative von $[x]$ in $\mathbb{Z}/\equiv_n$ gegeben durch

$$(-[x])^{\mathbb{Z}/\equiv_n} = [(-x)^{\mathbb{Z}}].$$

Beweis. Um zu zeigen, dass die beschriebene Addition und die beschriebene Multiplikation wohldefiniert sind, seien $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ mit $[x] = [\tilde{x}]$ und $[y] = [\tilde{y}]$ gegeben. Dann gilt $x \equiv_n \tilde{x}$ und $y \equiv_n \tilde{y}$, also auch $x + y \equiv_n \tilde{x} + \tilde{y}$ und $xy \equiv_n \tilde{x}\tilde{y}$ nach Proprosition (4.7)(a), (c) und damit $[x + y] = [\tilde{x} + \tilde{y}]$ und $[xy] = [\tilde{x}\tilde{y}]$ in $\mathbb{Z}/\equiv_n$.
Somit erhalten wir eine wohldefinierte Verknüpfungen

$$a\colon \mathbb{Z}/\equiv_n \times \mathbb{Z}/\equiv_n \to \mathbb{Z}/\equiv_n,\ ([x],[y]) \mapsto [x+y],$$
$$m\colon \mathbb{Z}/\equiv_n \times \mathbb{Z}/\equiv_n \to \mathbb{Z}/\equiv_n,\ ([x],[y]) \mapsto [xy].$$

Wir wollen zeigen, dass $\mathbb{Z}/\equiv_n$ ein kommutativer Ring mit Addition a und Multiplikation m wird.
Für $x, y, z \in \mathbb{Z}$ gilt

$$a([x], a([y],[z])) = a([x],[y+z]) = [x + (y+z)] = [(x+y)+z] = a([x+y],[z]) = a(a([x],[y]),[z]).$$

Folglich ist a assoziativ.
Für alle $x, y \in \mathbb{Z}$ gilt

$$a([x],[y]) = [x+y] = [y+x] = a([y],[x]).$$

Folglich ist $+$ kommutativ.
Für $x \in \mathbb{Z}$ gilt

$$a([0],[x]) = [0+x] = [x].$$

Folglich ist $[0]$ ein neutrales Element bzgl. a.
Für $x \in \mathbb{Z}$ gilt

$$a([-x],[x]) = [(-x)+x] = [0].$$

Folglich ist $[-x]$ ein zu $[x]$ inverses Element bzgl. a.
Analog zeigt man, dass m assoziativ und kommutativ und dass $[1]$ ein neutrales Element bzgl. m ist.
Für $x, y, z \in \mathbb{Z}$ gilt

$$m([x], a([y],[z])) = m([x],[y+z]) = [x(y+z)] = [xy+xz] = a([xy],[xz]) = a(m([x],[y]), m([x],[z])).$$

Folglich gelten die Distributivgesetze.
Insgesamt wird $\mathbb{Z}/\equiv_n$ ein kommutativer Ring mit Addition und Multiplikation gegeben durch $[x]+[y] = a([x],[y])$ und $[x] \cdot [y] = m([x],[y])$ für $x, y \in \mathbb{Z}$, Null $0 = [0]$, Eins $1 = [1]$ und Negativen $-[x] = [-x]$ für $x \in \mathbb{Z}$. □

(4.11) Definition (Restklassenring)**.** Es sei $n \in \mathbb{Z}$ gegeben. Der kommutative Ring $\mathbb{Z}/n := \mathbb{Z}/\equiv_n$ mit Addition und Multiplikation gegeben wie in Proposition (4.10) heißt *Restklassenring* von $\mathbb{Z}$ modulo n. Für $x \in \mathbb{Z}$ heißt die Äquivalenzklasse $[x]_n := [x]_{\equiv_n}$ auch die *Restklasse* von x modulo n.

Der Restklassenring $\mathbb{Z}/n$ wird in der Literatur oft auch als $\mathbb{Z}/n\mathbb{Z}$ bezeichnet und über das Ideal $n\mathbb{Z}$ konstruiert, vgl. Bemerkung (4.4).

(4.12) Bemerkung. Für alle $n \in \mathbb{Z}$ ist

$$\mathbb{Z}/n = \mathbb{Z}/(-n).$$

Beweis. Für $n \in \mathbb{Z}$ gilt nach Bemerkung (4.5) stets $\equiv_n = \equiv_{-n}$, also

$$\mathbb{Z}/n = \mathbb{Z}/\equiv_n = \mathbb{Z}/\equiv_{-n} = \mathbb{Z}/(-n)$$

als Mengen und nach Definition von Addition und Multiplikation auch als Ringe. □

(4.13) Bemerkung. Es sei $n \in \mathbb{Z}$ gegeben. Für $a \in \mathbb{Z}$ ist

$$[a]_n = a + n\mathbb{Z}.$$

Beweis. Für $a \in \mathbb{Z}$ gilt nach Bemerkung (4.4) stets

$$[a] = \{\tilde{a} \in \mathbb{Z} \mid \tilde{a} \equiv_n a\} = \{\tilde{a} \in \mathbb{Z} \mid \tilde{a} - a \in n\mathbb{Z}\} = \{\tilde{a} \in \mathbb{Z} \mid \tilde{a} \in a + n\mathbb{Z}\} = a + n\mathbb{Z}.$$ □

(4.14) Konvention. Es sei $n \in \mathbb{Z}$ gegeben. Für $a \in \mathbb{Z}$ schreiben wir unter Missbrauch der Notation meistens kurz a anstatt $[a]_n$ für die Restklasse von a modulo n, und sagen dann immer dazu, sobald a als Element von $\mathbb{Z}/n$ anzusehen ist.

Mit Konvention (4.14) gilt für $x, y \in \mathbb{Z}$ also $x = y$ in genau dann $\mathbb{Z}/n$, wenn $x \equiv_n y$ in $\mathbb{Z}$.

(4.15) Beispiel. In $\mathbb{Z}/7$ ist $1 = 8 = -6$, $3 = 10 = -4$, $2 = -5$. Es gilt $5 + 4 = 9 = 2$, $3 \cdot 4 = 12 = 5$, $13 \cdot 13 = (-1) \cdot (-1) = 1$.

Kongruenzen und Division mit Rest

Die Bezeichnung Restklasse bzw. Restklassenring kommt daher, dass jedes Element in $\mathbb{Z}/n$ für $n \in \mathbb{N}$, also jede Restklasse modulo n, durch den Rest eines beliebigen Repräsentanten bei Division mit Rest durch n repräsentiert wird, wie wir nun sehen werden.

(4.16) Proposition. Es sei $n \in \mathbb{Z} \setminus \{0\}$ gegeben.

(a) Für $a \in \mathbb{Z}$ ist $a \equiv_n a \bmod n$.

(b) Für $a, b \in \mathbb{Z}$ gilt genau dann $a \equiv_n b$, wenn $a \bmod n = b \bmod n$ ist.

Beweis.

(a) Für alle $a \in \mathbb{Z}$ gilt $a = n\,(a \operatorname{div} n) + (a \bmod n)$ nach dem Satz über die Division mit Rest (2.1), also $a \equiv_n a \bmod n$ nach Bemerkung (4.4).

(b) Es seien $a, b \in \mathbb{Z}$ gegeben. Nach (a) gilt $a \equiv_n a \bmod n$ und $b \equiv_n b \bmod n$. Folglich gilt genau dann $a \equiv_n b$, wenn $a \bmod n \equiv_n b \bmod n$ ist. Dies widerum ist äquivalent zu $n \mid (a \bmod n) - (b \bmod n)$. Da jedoch $a \bmod n \in [0, |n| - 1]$ und $b \bmod n \in [0, |n| - 1]$ gilt, ist $n \mid (a \bmod n) - (b \bmod n)$ gleichbedeutend mit $(a \bmod n) - (b \bmod n) = 0$, d.h. mit $a \bmod n = b \bmod n$. □

(4.17) Korollar. Es sei $n \in \mathbb{Z} \setminus \{0\}$ gegeben.

(a) Für $a \in \mathbb{Z}$ ist $a = a \bmod n$ in $\mathbb{Z}/n$.

(b) Für $a, b \in \mathbb{Z}$ gilt genau dann $a = b$ in $\mathbb{Z}/n$, wenn $a \bmod n = b \bmod n$ in $\mathbb{Z}$ ist.

Beweis.

(a) Für $a \in \mathbb{Z}$ gilt $a \equiv_n a \bmod n$ in $\mathbb{Z}$ nach Proposition (4.16)(a), also $a = a \bmod n$ in $\mathbb{Z}/n$.

(b) Es seien $a, b \in \mathbb{Z}$ gegeben. Genau dann gilt $a = b$ in $\mathbb{Z}/n$, wenn $a \equiv_n b$ in $\mathbb{Z}$ ist. Nach Proposition (4.16)(b) ist dies jedoch äquivalent zu $a \bmod n = b \bmod n$ in $\mathbb{Z}$. □

(4.18) Korollar. Für $n \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathbb{Z}/n = \{0, \ldots, |n| - 1\}.$$

Beweis. Für $n \in \mathbb{Z} \setminus \{0\}$, $x \in \mathbb{Z}$ ist $x \bmod n \in [0, |n| - 1]$. □

(4.19) Definition (Standardtransversale)**.** Für $n \in \mathbb{Z} \setminus \{0\}$ heißt $[0, |n| - 1]$ die *Standardtransversale* (oder das *Standardrepräsentantensystem*) von $\mathbb{Z}$ bzgl. $\equiv_n$.

Nullteiler im Restklassenring

(4.20) Bemerkung. Es sei $p \in \mathbb{Z} \setminus \{0, 1, -1\}$ gegeben. Genau dann ist p irreduzibel, wenn für $a, b \in \mathbb{Z}$ mit $ab \equiv_p 0$ stets auch $a \equiv_p 0$ oder $b \equiv_p 0$ gilt.

Beweis. Nach Lemma (2.61) ist p genau dann irreduzibel, wenn für $a, b \in \mathbb{Z}$ mit $p \mid ab$ stets auch $p \mid a$ oder $p \mid b$ gilt, d.h. wenn aus $ab \equiv_p 0$ stets $a \equiv_p 0$ oder $b \equiv_p 0$ folgt. □

(4.21) Proposition. Es sei $n \in \mathbb{Z}$ gegeben. Genau dann ist $\mathbb{Z}/n$ ein Bereich, wenn $n = 0$ oder n irreduzibel ist.

Beweis. Wenn $n = 0$ ist, so ist $\mathbb{Z}/n = \mathbb{Z}/0 \cong \mathbb{Z}$ ein Bereich. Wenn $n \in \mathbb{Z}^\times = \{1, -1\}$ ist, so ist $\mathbb{Z}/n = \mathbb{Z}/1 = \{0\}$ kein Bereich. Wenn $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ ist, so ist $\mathbb{Z}/n$ nach Bemerkung (4.20) genau dann ein Bereich, wenn n irreduzibel ist. □

In Abschnitt 3 werden wir sehen, dass $\mathbb{Z}/n$ für n irreduzibel sogar ein Körper ist.

Aufgaben

Aufgabe 38 (Rechnen in $\mathbb{Z}/n$)**.**

(a) Berechnen Sie $17 + 23 + 40 - 8$ und $2 \cdot (-3) \cdot 15$ und $6^{1000000}$ in $\mathbb{Z}/7$.

(b) Berechnen Sie $(-8) + 13 - 2 + 5$ und $4 \cdot 3 \cdot 5$ und 9^{14} in $\mathbb{Z}/8$.

(c) Ist $3^{2016} = 3^{2012}$ in $\mathbb{Z}/80$?

Aufgabe 39 (chinesischer Restsatz)**.** Zeigen Sie: Wir haben einen wohldefinierten bijektiven Ringhomomorphismus $\mathbb{Z}/6 \to \mathbb{Z}/2 \times \mathbb{Z}/3$, $[x]_6 \mapsto ([x]_2, [x]_3)$.

Aufgabe 40 (Inverse in $\mathbb{Z}/n$)**.**

(a) Bestimmen Sie die Inversen der invertierbaren Elemente in $\mathbb{Z}/11$.

(b) Es sei $a \in \mathbb{Z}$ so, dass a^2 in $\mathbb{Z}/12$ invertierbar ist. Ist dann auch a invertierbar?

Aufgabe 41 (abelsche Untergruppen von $\mathbb{Z}/n$)**.** Es sei $n \in \mathbb{Z}$ gegeben. Bestimmen Sie alle abelschen Untergruppen von $\mathbb{Z}/n$.

2 Lineare Kongruenzgleichungen und der chinesische Restsatz

Lineare Kongruenzgleichungen in einer Unbekannten

(4.22) Bemerkung. Es seien $n, a, b \in \mathbb{Z}$ gegeben. Für $x \in \mathbb{Z}$ gilt genau dann

$$ax \equiv_n b,$$

wenn es ein $y \in \mathbb{Z}$ mit

$$ax + ny = b$$

gibt.

Beweis. Für $x \in \mathbb{Z}$ gilt nach Proposition (4.4) (und Proposition (4.6)) genau dann $ax \equiv_n b$, wenn es ein $y \in \mathbb{Z}$ mit $ax + ny = b$ gibt. □

(4.23) Korollar. Es seien $n, a, b \in \mathbb{Z}$ gegeben. Genau dann gibt es ein $x \in \mathbb{Z}$ mit

$$ax \equiv_n b,$$

wenn

$$\gcd(a, n) \mid b$$

gilt.

Beweis. Nach Bemerkung (4.22) gibt es genau dann ein $x \in \mathbb{Z}$ mit $ax \equiv_n b$, wenn es $x, y \in \mathbb{Z}$ mit $ax + ny = b$ gibt. Dies ist nach Aufgabe 23(a) äquivalent dazu, dass $\gcd(a, n) \mid b$ gilt. □

(4.24) Korollar. Es sei $n \in \mathbb{Z}$ gegeben. Für $a \in \mathbb{Z}$ gibt es genau dann ein $x \in \mathbb{Z}$ mit

$$ax \equiv_n 1,$$

wenn a und n teilerfremd sind.

Beweis. Es sei $a \in \mathbb{Z}$ gegeben. Nach Korollar (4.23) gibt es genau dann ein $x \in \mathbb{Z}$ mit $ax \equiv_n 1$, wenn $\gcd(a, x) \mid 1$ gilt. Dies ist nach Bemerkung (2.18) äquivalent zu $\gcd(a, n) = 1$, d.h. zur Teilerfremdheit von a und n. □

(4.25) Proposition. Es seien $n, a, b \in \mathbb{Z}$ mit $(a, n) \neq (0, 0)$ und $\gcd(a, n) \mid b$ gegeben. Ferner sei $x_0 \in \mathbb{Z}$ mit

$$\frac{a}{\gcd(a,n)} x_0 \equiv_{\frac{n}{\gcd(a,n)}} 1$$

gegeben. Für $x \in \mathbb{Z}$ gilt genau dann

$$ax \equiv_n b,$$

wenn

$$x \equiv_{\frac{n}{\gcd(a,n)}} x_0 \frac{b}{\gcd(a,n)}$$

ist.

Beweis. Es sei $x \in \mathbb{Z}$ gegeben. Wegen $\frac{a}{\gcd(a,n)} x_0 \equiv_{\frac{n}{\gcd(a,n)}} 1$ gibt es nach Bemerkung (4.22) ein $y_0 \in \mathbb{Z}$ mit

$$\frac{a}{\gcd(a,n)} x_0 + \frac{n}{\gcd(a,n)} y_0 = 1$$

und also mit

$$ax_0 + ny_0 = \gcd(a, n).$$

Für $y \in \mathbb{Z}$ gilt nach Aufgabe 23(b) genau dann $ax + ny = b$, wenn

$$(x, y) \in (x_0, y_0) \frac{b}{\gcd(a,n)} + (\frac{n}{\gcd(a,n)}, -\frac{a}{\gcd(a,n)})\mathbb{Z}$$

ist. Nach Bemerkung (4.22) bedeutet dies aber, dass $ax \equiv_n b$ genau dann gilt, wenn

$$x \in x_0 \frac{b}{\gcd(a,n)} + \frac{n}{\gcd(a,n)} \mathbb{Z} = [x_0 \frac{b}{\gcd(a,n)}]_{\frac{n}{\gcd(a,n)}}$$

ist, d.h. wenn

$$x \equiv_{\frac{n}{\gcd(a,n)}} x_0 \frac{b}{\gcd(a,n)}$$

gilt. □

(4.26) Beispiel.

(a) Es gibt kein $x \in \mathbb{Z}$ mit $18x \equiv_{30} 20$.

(b) Für $x \in \mathbb{Z}$ gilt genau dann $18x \equiv_{30} 12$, wenn $x \equiv_5 -1$ ist.

(c) Für $x \in \mathbb{Z}$ gilt genau dann $18x \equiv_{30} 24$, wenn $x \equiv_5 -2$ ist.

Beweis.

(a) Da $\gcd(18, 30) = 6$ ist und $6 \nmid 20$ gilt, gibt es nach Korollar (4.23) kein $x \in \mathbb{Z}$ mit $18x \equiv_{30} 20$.

(b) Es ist $\frac{18}{6} \cdot 2 = 3 \cdot 2 = 6 \equiv_5 1$. Für $x \in \mathbb{Z}$ ist $18x \equiv_3 12$ nach Proposition (4.25) äquivalent zu

$$x \equiv_5 2 \cdot \frac{12}{6} = 4 \equiv_5 -1.$$

(c) Für $x \in \mathbb{Z}$ ist $18x \equiv_3 24$ nach Proposition (4.25) äquivalent zu

$$x \equiv_5 2 \cdot \frac{24}{6} = 8 \equiv_5 -2.$$

□

(4.27) Korollar. Es seien $n, a, x, y \in \mathbb{Z}$ mit $(a, n) \neq (0, 0)$ gegeben. Genau dann gilt

$$ax \equiv_n ay,$$

wenn

$$x \equiv_{\frac{n}{\gcd(a,n)}} y$$

ist.

Beweis. Nach Bemerkung (2.44) sind $\frac{a}{\gcd(a,n)}$ und $\frac{n}{\gcd(a,n)}$ teilerfremd, so dass es nach Korollar (4.24) ein $x_0 \in \mathbb{Z}$ mit $\frac{a}{\gcd(a,n)} x_0 \equiv_{\frac{n}{\gcd(a,n)}} 1$ gibt. Ferner folgt aus Proposition (4.25), dass $ax \equiv_n ay$ genau dann gilt, wenn $x \equiv_{\frac{n}{\gcd(a,n)}} x_0 \frac{ay}{\gcd(a,n)}$ ist. Nun impliziert $\frac{a}{\gcd(a,n)} x_0 \equiv_{\frac{n}{\gcd(a,n)}} 1$ jedoch $\frac{a}{\gcd(a,n)} x_0 y \equiv_{\frac{n}{\gcd(a,n)}} y$ nach Proposition (4.7)(c), so dass also die Bedingung $ax \equiv_n ay$ äquivalent zur Bedingung $x \equiv_{\frac{n}{\gcd(a,n)}} y$ ist. □

Alternativer Beweis von Korollar (4.27). Es ist $ax \equiv_n ay$ äquivalent zu $n \mid ax - ay = a(x - y)$, und es ist $x \equiv_{\frac{n}{\gcd(a,n)}} y$ äquivalent zu $\frac{n}{\gcd(a,n)} \mid x - y$. Nach Korollar (2.41) gilt jedoch genau dann $n \mid a(x - y)$, wenn $\frac{n}{\gcd(a,n)} \mid x - y$ gilt. Folglich ist $ax \equiv_n ay$ äquivalent zu $x \equiv_{\frac{n}{\gcd(a,n)}} y$. □

Alternativer Beweis von Beispiel (4.26)(b), (c).

(b) Es sei $x \in \mathbb{Z}$ gegeben. Wegen $\gcd(6, 30) = 6$ gilt nach Korollar (4.27) genau dann $18x \equiv_{30} 12$, wenn $3x \equiv_5 2$ ist. Wegen $2 \cdot 3 = 6 \equiv_5 1$ ist dies aber widerum äquivalent zu $x \equiv_5 2 \cdot 2 = 4 \equiv_5 -1$.

(c) Es sei $x \in \mathbb{Z}$ gegeben. Wegen $\gcd(6, 30) = 6$ gilt nach Korollar (4.27) genau dann $18x \equiv_{30} 24$, wenn $3x \equiv_5 4$ ist. Wegen $2 \cdot 3 = 6 \equiv_5 1$ ist dies aber widerum äquivalent zu $x \equiv_5 2 \cdot 4 = 8 \equiv_5 -2$. □

(4.28) Korollar. Es seien $n, a, x, y \in \mathbb{Z}$ so gegeben, dass a und n teilerfremd sind. Genau dann gilt $ax \equiv_n ay$, wenn $x \equiv_n y$ gilt.

(4.29) Korollar. Es seien $p \in \mathbb{P}$, $a, x, y \in \mathbb{Z}$ mit $p \nmid a$ gegeben. Genau dann gilt $ax \equiv_p ay$, wenn $x \equiv_p y$ gilt.

Beweis. Nach Proposition (2.60) folgt aus $p \nmid a$, dass a und p teilerfremd sind. Somit folgt aus Korollar (4.28), dass die Bedingungen $ax \equiv_p ay$ und $x \equiv_p y$ äquivalent sind. □

Simultane Kongruenzen: Der chinesische Restsatz

(4.30) Bemerkung. Es seien $m \in \mathbb{N}$, $n_i \in \mathbb{Z}$ für $i \in [1, m]$ und ein gemeinsames Vielfaches $n \in \mathbb{Z}$ von $(n_i)_{i\in[1,m]}$ gegeben. Dann ist

$$\mathbb{Z}/n \to \prod_{i\in[1,m]} \mathbb{Z}/n_i,\ [x]_n \mapsto ([x]_{n_i})_{i\in[1,m]}$$

ein wohldefinierter Ringhomomorphismus.

Beweis. Es seien $x, \tilde{x} \in \mathbb{Z}$ mit $[x]_n = [\tilde{x}]_n$ in $\mathbb{Z}/n$ gegeben, so dass $x \equiv_n \tilde{x}$ in $\mathbb{Z}$ gilt. Da n ein gemeinsames Vielfaches von $(n_i)_{i\in[1,m]}$ ist, folgt $x \equiv_{n_i} \tilde{x}$ für alle $i \in [1, m]$ nach Bemerkung (4.8). Somit gilt auch $[x]_{n_i} = [\tilde{x}]_{n_i}$ in $\mathbb{Z}/n_i$ für alle $i \in [1, m]$ und damit $([x]_{n_i})_{i\in[1,m]} = ([\tilde{x}]_{n_i})_{i\in[1,m]}$ in $\prod_{i\in[1,m]} \mathbb{Z}/n_i$. Folglich erhalten wir eine wohldefinierte Abbildung

$$\pi\colon \mathbb{Z}/n \to \prod_{i\in[1,m]} \mathbb{Z}/n_i,\ [x]_n \mapsto ([x]_{n_i})_{i\in[1,m]}.$$

Für $x, y \in \mathbb{Z}$ gilt

$$\begin{aligned}
\pi([x]_n + [y]_n) &= \pi([x + y]_n) = ([x + y]_{n_i})_{i\in[1,m]} = ([x]_{n_i} + [y]_{n_i})_{i\in[1,m]} = ([x]_{n_i})_{i\in[1,m]} + ([y]_{n_i})_{i\in[1,m]} \\
&= \pi([x]_n) + \pi([y]_n), \\
\pi([x]_n\,[y]_n) &= \pi([xy]_n) = ([xy]_{n_i})_{i\in[1,m]} = ([x]_{n_i}\,[y]_{n_i})_{i\in[1,m]} = ([x]_{n_i})_{i\in[1,m]}\,([y]_{n_i})_{i\in[1,m]} \\
&= \pi([x]_n)\,\pi([y]_n)
\end{aligned}$$

und es ist

$$\pi(1) = \pi([1]_n) = ([1]_{n_i})_{i\in[1,m]} = (1)_{i\in[1,m]} = 1.$$

Somit ist π ein Ringhomomorphismus. □

(4.31) Proposition. Es seien $m \in \mathbb{N}$, $n_i \in \mathbb{Z}$ für $i \in [1,m]$ und ein gemeinsames Vielfaches $n \in \mathbb{Z}$ von $(n_i)_{i\in[1,m]}$ gegeben. Genau dann ist

$$\mathbb{Z}/n \to \prod_{i\in[1,m]} \mathbb{Z}/n_i,\ [x]_n \mapsto ([x]_{n_i})_{i\in[1,m]}$$

injektiv, wenn $|n| = \operatorname{lcm}(n_i)_{i\in[1,m]}$ ist.

Beweis. Es sei $\pi\colon \mathbb{Z}/n \to \prod_{i\in[1,m]} \mathbb{Z}/n_i$, $[x]_n \mapsto ([x]_{n_i})_{i\in[1,m]}$.
Zunächst sei π injektiv. Wegen $n_i \mid \operatorname{lcm}(n_j)_{j\in[1,m]}$ für $i \in [1,m]$ gilt

$$\pi([\operatorname{lcm}(n_j)_{j\in[1,m]}]_n) = ([\operatorname{lcm}(n_j)_{j\in[1,m]}]_{n_i})_{i\in[1,m]} = 0.$$

Die Injektivität von π impliziert $[\operatorname{lcm}(n_j)_{j\in[1,m]}]_n = 0$ in $\mathbb{Z}/n$, es gilt also $n \mid \operatorname{lcm}(n_j)_{j\in[1,m]}$ in $\mathbb{Z}$. Andererseits ist n ein gemeinsames Vielfaches und $\operatorname{lcm}(n_j)_{j\in[1,m]}$ ein kleinstes gemeinsames Vielfaches von $(n_i)_{i\in[1,m]}$. Daher gilt auch $\operatorname{lcm}(n_j)_{j\in[1,m]} \mid n$. Nach Proposition (2.10)(c) gilt daher $|n| = \operatorname{lcm}(n_j)_{j\in[1,m]}$.
Nun gelte umgekehrt $|n| = \operatorname{lcm}(n_i)_{i\in[1,m]}$. Es sei $x \in \mathbb{Z}$ mit $([x]_{n_i})_{i\in[1,m]} = 0$ in $\prod_{i\in[1,m]} \mathbb{Z}/n_i$ gegeben. Dann gilt $[x]_{n_i} = 0$ in $\mathbb{Z}/n_i$ und damit $x \equiv_{n_i} 0$ in $\mathbb{Z}$ für alle $i \in [1,m]$. Nach Bemerkung (4.9) folgt $x \equiv_{\operatorname{lcm}(n_i)_{i\in[1,m]}} 0$, wegen $n = \operatorname{lcm}(n_i)_{i\in[1,m]}$ also $x \equiv_n 0$ in $\mathbb{Z}$ und damit $[x]_n = 0$ in $\mathbb{Z}/n$. Folglich ist $\operatorname{Ker}\pi = \{0\}$ und damit π injektiv. □

(4.32) Lemma (chinesischer Restsatz, arithmetische Version)**.** Es seien $m \in \mathbb{N}$ und paarweise teilerfremde $n_i \in \mathbb{Z}$ für $i \in [1,m]$ gegeben. Ferner seien $a_i \in \mathbb{Z}$ für $i \in [1,m]$ gegeben. Für $i \in [1,m]$ sei $y_i \in \mathbb{Z}$ mit

$$(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i \equiv_{n_i} 1$$

gegeben.
Für $x \in \mathbb{Z}$ gilt genau dann

$$x \equiv_{n_i} a_i$$

für alle $i \in [1,m]$, wenn

$$x \equiv_{\prod_{k\in[1,m]} n_k} \sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i$$

ist.

Beweis. Wenn

$$x \equiv_{\prod_{k\in[1,m]} n_k} \sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i$$

gilt, dann nach Bemerkung (4.8) auch

$$x \equiv_{n_k} \sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i \equiv_{n_k} a_k(\prod_{j\in[1,m]\setminus\{k\}} n_j)y_k \equiv_{n_k} a_k \cdot 1 = a_k$$

für $k \in [1,m]$.
Es gelte umgekehrt $x \equiv_{n_i} a_i$ für alle $i \in [1,m]$. Nach Bemerkung (4.30) ist

$$\pi\colon \mathbb{Z}/\prod_{i\in[1,m]} n_i \to \prod_{i\in[1,m]} \mathbb{Z}/n_i,\ [x]_{\prod_{i\in[1,m]} n_i} \mapsto ([x]_{n_i})_{i\in[1,m]}$$

ein wohldefinierter Ringhomomorphismus. Wegen der paarweise Teilerfremdheit von $(n_i)_{i\in[1,m]}$ ist

$$\prod_{i\in[1,m]} n_i = \operatorname{lcm}(n_i)_{i\in[1,m]}$$

und damit π injektiv nach Proposition (4.31). Wie wir gerade gesehen haben gilt jedoch

$$x \equiv_{n_k} a_k \equiv_{n_k} \sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i$$

für alle $k \in [1,m]$, also

$$\begin{aligned}\pi([x]_{\prod_{k\in[1,m]} n_k}) = ([x]_{n_k})_{k\in[1,m]} &= ([\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i]_{n_k})_{k\in[1,m]} \\ &= \pi([\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i]_{\prod_{k\in[1,m]} n_k})\end{aligned}$$

und auf Grund der Injektivität von π somit

$$[x]_{\prod_{k\in[1,m]} n_k} = [\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i]_{\prod_{k\in[1,m]} n_k}.$$

Dies bedeutet aber gerade

$$x \equiv_{\prod_{k\in[1,m]} n_k} \sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i.$$ □

(4.33) Beispiel. Für $x \in \mathbb{Z}$ gilt genau dann

$$x \equiv_5 3,$$
$$x \equiv_7 5,$$
$$x \equiv_9 7,$$

wenn

$$x \equiv_{315} -2$$

ist.

Beweis. Es ist

$$\begin{aligned}&7\cdot 9\cdot 2 = 63\cdot 2 \equiv_5 3\cdot 2 = 6 \equiv_5 1,\\ &5\cdot 9\cdot(-2) = 45\cdot(-2) \equiv_7 3\cdot(-2) = -6 \equiv_7 1,\\ &5\cdot 7\cdot(-1) = 35\cdot(-1) \equiv_9 (-1)\cdot(-1) = 1.\end{aligned}$$

Nach dem chinesischen Restsatz gilt also genau dann $x \equiv_5 3$ und $x \equiv_7 5$ und $x \equiv_9 7$, wenn

$$x \equiv_{315} 3\cdot 7\cdot 9\cdot 2 + 5\cdot 5\cdot 9\cdot(-2) + 7\cdot 5\cdot 7\cdot(-1) = -317 \equiv_{315} -2$$

ist. □

(4.34) Satz (chinesischer Restsatz, algebraische Version)**.** Es seien $m \in \mathbb{N}$ und paarweise teilerfremde $n_i \in \mathbb{Z}$ für $i \in [1,m]$ gegeben. Dann ist

$$\mathbb{Z}/(\prod_{i\in[1,m]} n_i) \to \prod_{i\in[1,m]} \mathbb{Z}/n_i,\ [x]_{\prod_{i\in[1,m]} n_i} \mapsto ([x]_{n_i})_{i\in[1,m]}$$

ein Ringisomorphismus.

Beweis. Nach Bemerkung (4.30) ist $\pi\colon \mathbb{Z}/(\prod_{i\in[1,m]} n_i) \to \prod_{i\in[1,m]} \mathbb{Z}/n_i$, $[x]_{\prod_{i\in[1,m]} n_i} \mapsto ([x]_{n_i})_{i\in[1,m]}$ ein Ringhomomorphismus.
Wegen der paarweise Teilerfremdheit von $(n_i)_{i\in[1,m]}$ ist

$$\prod_{i\in[1,m]} n_i = \operatorname{lcm}(n_i)_{i\in[1,m]}$$

und damit π injektiv nach Proposition (4.31).
Um die Surjektivität von π zu zeigen, seien $a_i \in \mathbb{Z}$ für $i \in [1,m]$ gegeben. Da $(n_i)_{i\in[1,m]}$ paarweise teilerfremd ist, sind $(\prod_{j\in[1,m]\setminus\{i\}} n_j)$ und n_i für alle $i \in [1,m]$ teilerfremd. Nach Korollar (4.24) gibt es daher für alle $i \in [1,m]$ ein $y_i \in \mathbb{Z}$ mit

$$(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i \equiv_{n_i} 1.$$

Nun folgt

$$\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i \equiv_{n_k} a_k$$

nach Lemma (4.32) für $k \in [1,m]$ und damit

$$\pi([\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i]_{\prod_{k\in[1,m]} n_k}) = ([\sum_{i\in[1,m]} a_i(\prod_{j\in[1,m]\setminus\{i\}} n_j)y_i]_{n_k})_{k\in[1,m]} = ([a_k]_{n_k})_{k\in[1,m]}.$$

Somit ist π in der Tat surjektiv. □

Da $\mathbb{Z}/1 = \{0\}$ ist, ergibt sich aus dem Fundamentalsatz für Arithmetik:

(4.35) Korollar. Für alle $n \in \mathbb{Z} \setminus \{0\}$ ist

$$\mathbb{Z}/n \to \prod_{p\in\mathbb{P}} \mathbb{Z}/p^{\mathrm{v}_p(n)},\ [x]_n \mapsto ([x]_{p^{\mathrm{v}_p(n)}})_{p\in\mathbb{P}}$$

ein Ringisomorphismus.

Aufgaben

Aufgabe 42 (zwei simultane Kongruenzen)**.** Es seien $m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ gegeben. Zeigen Sie: Genau dann gibt es ein $x \in \mathbb{Z}$ mit $x \equiv_m a$ und $x \equiv_n b$, wenn $a \equiv_{\gcd(m,n)} b$ ist.

Aufgabe 43 (simultane lineare Kongruenzgleichungen)**.** Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$\begin{aligned} 6x &\equiv_{16} 8,\\ 15x &\equiv_{27} 3,\\ 14x &\equiv_{49} 35. \end{aligned}$$

3 Die prime Restklassengruppe

Prime Restklassen

(4.36) Definition (prime Restklasse)**.** Es sei $n \in \mathbb{Z}$ gegeben. Die Einheitengruppe $(\mathbb{Z}/n)^\times$ wird *prime Restklassengruppe* genannt, ihre Elemente *prime Restklassen.*

(4.37) Bemerkung. Für alle $n \in \mathbb{Z} \setminus \{0\}$ ist

$$(\mathbb{Z}/n)^\times \to \bigtimes_{p\in\mathbb{P}} (\mathbb{Z}/p^{\mathrm{v}_p(n)})^\times,\ [x]_n \mapsto ([x]_{p^{\mathrm{v}_p(n)}})_{p\in\mathbb{P}}$$

ein Gruppenisomorphismus.

Beweis. Dies folgt aus Korollar (4.35). □

Um die primen Restklassengruppen $(\mathbb{Z}/n)^\times$ für $n \in \mathbb{Z} \setminus \{0\}$ zu verstehen, genügt es also, die primen Restklassengruppen $(\mathbb{Z}/p^k)^\times$ für $p \in \mathbb{P}$, $k \in \mathbb{N}_0$ zu verstehen.

Modulare Einheiten

(4.38) Definition (modulare Einheit)**.** Es seien $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ gegeben. Wir sagen, dass a *invertierbar modulo* n (oder eine *Einheit modulo* n) ist, falls a invertierbar in $\mathbb{Z}/n$ ist.

(4.39) Bemerkung. Es seien $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist a eine Einheit modulo n.

(b) Es existiert ein $x \in \mathbb{Z}$ mit $ax \equiv_n 1$.

(c) Es ist a teilerfremd zu n.

Beweis. Die Äquivalenz von Bedingung (a) und Bedingung (b) gilt nach Definition von $\mathbb{Z}/n$. Die Äquivalenz von Bedingung (b) und Bedingung (c) gilt nach Korollar (4.24). □

(4.40) Korollar. Für $n \in \mathbb{Z}$ ist

$$(\mathbb{Z}/n)^\times = \{[x] \mid x \in \mathbb{Z} \text{ so, dass } x \text{ teilerfremd zu } n \text{ ist}\}.$$

Endliche Primkörper

Mit Korollar (4.40) können wir eine Antwort auf die Frage geben, wann ein Restklassenring von $\mathbb{Z}$ ein Körper ist.

(4.41) Satz. Für $n \in \mathbb{Z}$ ist $\mathbb{Z}/n$ genau dann ein Körper, wenn n irreduzibel ist.

Beweis. Es sei $n \in \mathbb{N}_0$ gegeben. Dann ist $\mathbb{Z}/n = \mathbb{Z}/(-n)$ stets ein kommutativer Ring. Wenn $n = 0$ ist, so ist $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ kein Körper. Wenn $n = 1$ ist, so ist $\mathbb{Z}/\{1\} = \{0\}$ ebenfalls kein Körper.
Im Folgenden sei also $n > 1$. Wir betrachten die Standardtransversale $[0, n-1]$ von $\mathbb{Z}$ bzgl. $\equiv_n$. Wegen $n > 1$ gilt stets $0 \neq 1$ in $\mathbb{Z}/n$. Somit ist $\mathbb{Z}/n$ genau dann ein Körper, wenn jedes $x \in [1, n-1]$ invertierbar in $\mathbb{Z}/n$ ist. Nach Korollar (4.40) gilt dies aber genau dann, wenn jedes $x \in [1, n-1]$ teilfremd zu n ist. Wegen $n > 1$ ist dies äquivalent dazu, dass n eine Primzahl ist. □

(4.42) Definition (endliche Primkörper)**.** Für $p \in \mathbb{P}$ heißt $\mathbb{F}_p := \mathbb{Z}/p$ der *Primkörper* zur Primzahl p.

Euler-Funktion

(4.43) Definition (Euler-Funktion)**.** Die *Euler-Funktion* (oder *Eulersche Funktion* oder *Eulersche Phi-Funktion*) ist definiert als

$$\varphi\colon \mathbb{N} \to \mathbb{C},\ n \mapsto |\{x \in [1,n] \mid x \text{ ist teilerfremd zu } n\}|.$$

(4.44) Bemerkung. Für alle $n \in \mathbb{N}$ ist

$$\varphi(n) = |(\mathbb{Z}/n)^\times|.$$

Beweis. Es sei $n \in \mathbb{N}$ gegeben. Wir betrachten die Transversale $[1, n]$ von $\mathbb{Z}$ bzgl. $\equiv_n$. Nach Korollar (4.40) ist

$$(\mathbb{Z}/n)^\times = \{[x] \mid x \in \mathbb{Z} \text{ mit } \gcd(x,n) = 1\} = \{[x] \mid x \in [1,n] \text{ mit } \gcd(x,n) = 1\}$$

und damit

$$|(\mathbb{Z}/n)^\times| = |\{[x] \mid x \in [1,n] \text{ mit } \gcd(x,n) = 1\}| = |\{x \in [1,n] \mid \gcd(x,n) = 1\}| = \varphi(n).$$ □

(4.45) Korollar. Für alle $p \in \mathbb{P}$ ist

$$\varphi(p) = p - 1.$$

Beweis. Für $p \in \mathbb{P}$ ist $\mathbb{Z}/p = \mathbb{F}_p$ ein Körper nach Satz (4.41) und damit

$$\varphi(p) = |(\mathbb{Z}/p)^\times| = |\mathbb{F}_p^\times| = |\mathbb{F}_p \setminus \{0\}| = |\mathbb{F}_p| - 1 = p - 1$$

nach Bemerkung (4.44). □

(4.46) Korollar. Die Euler-Funktion φ ist eine multiplikative arithmetische Funktion.

Beweis. Für $n \in \mathbb{N}$ gilt

$$(\mathbb{Z}/n)^\times \cong \bigtimes_{p\in\mathbb{P}} (\mathbb{Z}/p^{\mathrm{v}_p(n)})^\times$$

nach Bemerkung (4.37) und somit

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\bigtimes_{p\in\mathbb{P}} (\mathbb{Z}/p^{\mathrm{v}_p(n)})^\times| = \prod_{p\in\mathbb{P}} |(\mathbb{Z}/p^{\mathrm{v}_p(n)})^\times| = \prod_{p\in\mathbb{P}} \varphi(p^{\mathrm{v}_p(n)})$$

nach Bemerkung (4.44). Die Multiplikativität von φ folgt nun aus Bemerkung (3.12). □

(4.47) Proposition. Für $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \prod_{\substack{p\in\mathbb{P}\\ p|n}} (1 - \frac{1}{p})$$

Beweis. Siehe Aufgabe 44(a). □

(4.48) Proposition. Die Summatorfunktion der Euler-Funktion φ ist

$$\mathrm{T}\varphi = \mathrm{inc}\colon \mathbb{N} \to \mathbb{C},\ n \mapsto n.$$

Für $n \in \mathbb{N}$ gilt

$$\sum_{\substack{d\in\mathbb{N}\\ d|n}} \varphi(d) = n.$$

Beweis. Siehe Aufgabe 45(a). □

(4.49) Korollar. Für $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \sum_{\substack{d\in\mathbb{N}\\ d|n}} \frac{\mu(d)}{d}.$$

Beweis. Siehe Aufgabe 45(b). □

Der Satz von Lagrange

(4.50) Definition (Äquivalenz modulo Untergruppe)**.** Es seien $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Für $\alpha, \beta \in (\mathbb{Z}/n)^\times$ sagen wir, dass α *äquivalent* β *modulo* U ist, geschrieben $\alpha \sim_U \beta$, wenn $\beta^{-1}\alpha \in U$ gilt.

(4.51) Proposition. Es sei $n \in \mathbb{Z}$ gegeben. Für jede Untergruppe U von $(\mathbb{Z}/n)^\times$ ist $\sim_U$ eine Äquivalenzrelation auf $(\mathbb{Z}/n)^\times$.

Beweis. Es sei eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben.
Es seien $\alpha, \beta, \gamma \in (\mathbb{Z}/n)^\times$ mit $\alpha \sim_U \beta$ und $\beta \sim_U \gamma$ gegeben, so dass $\beta^{-1}\alpha \in U$ und $\gamma^{-1}\beta \in U$ gilt. Dann gilt jedoch auch $\gamma^{-1}\alpha = (\gamma^{-1}\beta)(\beta^{-1}\alpha) \in U$, d.h. $\alpha \sim_U \gamma$. Folglich ist $\sim_U$ transitiv.
Für alle $\alpha \in (\mathbb{Z}/n)^\times$ gilt $\alpha^{-1}\alpha = 1 \in U$, also $\alpha \sim_U \alpha$. Folglich ist $\equiv_n$ reflexiv.
Es seien $\alpha, \beta \in (\mathbb{Z}/n)^\times$ mit $\alpha \sim_U \beta$ gegeben, so dass $\beta^{-1}\alpha \in U$ gilt. Dann gilt auch $\alpha^{-1}\beta = (\beta^{-1}\alpha)^{-1} \in U$, d.h. $\beta \sim_U \alpha$. Folglich ist $\sim_U$ symmetrisch.
Insgesamt ist $\sim_U$ eine Äquivalenzrelation auf $(\mathbb{Z}/n)^\times$. □

(4.52) Definition (Nebenklasse)**.** Es seien $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Für $\alpha \in \mathbb{Z}$ heißt die Äquivalenzklasse $[\alpha]_U := [\alpha]_{\sim_U}$ auch die *Nebenklasse* von α modulo U. Die *Menge der Nebenklassen* modulo U wird mit

$$(\mathbb{Z}/n)^\times/U := (\mathbb{Z}/n)^\times/\sim_U$$

bezeichnet.

Für $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ lässt sich auf der Quotientenmenge $(\mathbb{Z}/n)^\times/U$ eine Gruppenstruktur definieren, ähnlich zur Konstruktion der Struktur der unterliegenden abelschen Gruppe auf $\mathbb{Z}/n$. Auf diese Struktur kommt es uns jedoch nicht an, weswegen wir sie an dieser Stelle nicht studieren werden.
Der Bezeichnung Nebenklasse erklärt sich wie folgt:

(4.53) Bemerkung. Es seien $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ ist

$$[\alpha]_U = \alpha U.$$

Beweis. Für $\alpha \in (\mathbb{Z}/n)^\times$ gilt

$$[\alpha] = \{\tilde{\alpha} \in (\mathbb{Z}/n)^\times \mid \tilde{\alpha} \sim_U \alpha\} = \{\tilde{\alpha} \in (\mathbb{Z}/n)^\times \mid \alpha^{-1}\tilde{\alpha} \in U\} = \{\tilde{\alpha} \in (\mathbb{Z}/n)^\times \mid \tilde{\alpha} \in \alpha U\} = \alpha U. \qquad \square$$

(4.54) Bemerkung. Es seien $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Dann ist

$$U \to \alpha U,\ \xi \mapsto \alpha\xi$$

eine wohldefinierte Bijektion.

Beweis. Da $(\mathbb{Z}/n)^\times$ eine Gruppe ist, haben wir eine wohldefinierte Bijektion

$$(\mathbb{Z}/n)^\times \mapsto \alpha(\mathbb{Z}/n)^\times,\ \xi \mapsto \alpha\xi,$$

welche nach Definition von αU zu einer Bijektion

$$U \mapsto \alpha U,\ \xi \mapsto \alpha\xi$$

einschränkt. $\square$

(4.55) Definition (Nebenklassenindex)**.** Es seien $n \in \mathbb{Z}$ und eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Der *Nebenklassenindex* von U in $(\mathbb{Z}/n)^\times$ ist definiert als

$$[(\mathbb{Z}/n)^\times : U] := |(\mathbb{Z}/n)^\times/U|.$$

(4.56) Lemma (Satz von Lagrange)**.** Es sei $n \in \mathbb{N}$ gegeben. Für jede Untergruppe U von $(\mathbb{Z}/n)^\times$ gilt

$$\varphi(n) = |U| \cdot [(\mathbb{Z}/n)^\times : U].$$

Beweis. Es sei eine Untergruppe U von $(\mathbb{Z}/n)^\times$ gegeben. Dann ist $(\mathbb{Z}/n)^\times/U = (\mathbb{Z}/n)^\times/\sim_U$ eine Partition von U, so dass

$$(\mathbb{Z}/n)^\times = \dot{\bigcup_{X \in (\mathbb{Z}/n)^\times/U}} X$$

gilt. Nach Bemerkung (4.53) gilt $|X| = |U|$ für alle $X \in (\mathbb{Z}/n)^\times/U$ und damit

$$\begin{aligned}\varphi(n) = |(\mathbb{Z}/n)^\times| &= |\dot{\bigcup_{X \in (\mathbb{Z}/n)^\times/U}} X| = \sum_{X \in (\mathbb{Z}/n)^\times/U} |X| = \sum_{X \in (\mathbb{Z}/n)^\times/U} |U| = |U| \cdot |(\mathbb{Z}/n)^\times/U| \\ &= |U| \cdot [(\mathbb{Z}/n)^\times : U]\end{aligned}$$

nach Bemerkung (4.44). $\square$

Zyklische Untergruppen

(4.57) Definition (von einem Element erzeugte Untergruppe)**.** Es sei $n \in \mathbb{Z}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ heißt

$$\langle \alpha \rangle = \langle \alpha \rangle_{\mathbf{Grp}} := \bigcap \{U \mid U \text{ ist eine Untergruppe von } (\mathbb{Z}/n)^\times \text{ mit } \alpha \in U\}$$

von $(\mathbb{Z}/n)^\times$ die *von α erzeugte Untergruppe* von $(\mathbb{Z}/n)^\times$.

(4.58) Bemerkung. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Dann ist $\langle \alpha \rangle$ die bzgl. Inklusion kleinste Untergruppe von $(\mathbb{Z}/n)^\times$, welche α als Element enthält.

Beweis. Es sei $\mathcal{U} := \{U \mid U \text{ ist eine Untergruppe von } (\mathbb{Z}/n)^\times \text{ mit } \alpha \in U\}$, so dass

$$\langle \alpha \rangle = \bigcap \mathcal{U} = \bigcap_{U \in \mathcal{U}} U$$

gilt. Dann ist $\alpha \in U$ für alle $U \in \mathcal{U}$, also auch

$$\alpha \in \bigcap_{U \in \mathcal{U}} U = \langle \alpha \rangle.$$

Für eine beliebige Untergruppe U von $(\mathbb{Z}/n)^\times$ mit $g \in U$ gilt hingegen $U \in \mathcal{U}$, also

$$\langle \alpha \rangle = \bigcap_{U' \in \mathcal{U}} U' \subseteq U. \qquad \square$$

(4.59) Notation. Es sei $n \in \mathbb{Z}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ schreiben wir

$$\alpha^{\mathbb{Z}} = \{\alpha^k \mid k \in \mathbb{Z}\}.$$

(4.60) Definition (diskrete Exponentiation)**.** Es sei $n \in \mathbb{Z}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ heißt

$$\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times,\ k \mapsto \alpha^k$$

die *diskrete Exponentiation* zur Basis α.

(4.61) Bemerkung. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Die diskrete Exponentiation

$$\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times,\ k \mapsto \alpha^k$$

ist ein Gruppenhomomorphismus mit

$$\operatorname{Im} \exp_\alpha = \alpha^{\mathbb{Z}}.$$

Beweis. Für $k, l \in \mathbb{Z}$ ist

$$\exp_\alpha(k + l) = \alpha^{k+l} = \alpha^k \, \alpha^l = \exp_\alpha(k) \, \exp_\alpha(l).$$

Folglich ist $\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times,\ k \mapsto \alpha^k$ ein Gruppenhomomorphismus. Ferner gilt

$$\operatorname{Im} \exp_\alpha = \{\exp_\alpha(k) \mid k \in \mathbb{Z}\} = \{\alpha^k \mid k \in \mathbb{Z}\} = \alpha^{\mathbb{Z}}. \qquad \square$$

Wir werden nun sehen, dass das Erzeugnis einer primen Restklasse gerade gleich der Menge aller Potenzen dieser Restklasse ist.

(4.62) Lemma. Es sei $n \in \mathbb{Z}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ ist

$$\langle \alpha \rangle = \alpha^{\mathbb{Z}}.$$

Beweis. Es sei ein $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Dann ist $\alpha = \alpha^1 \in \alpha^{\mathbb{Z}}$ und es ist $\alpha^{\mathbb{Z}}$ eine Untergruppe von $(\mathbb{Z}/n)^\times$ nach Bemerkung (4.61). Da $\langle \alpha \rangle$ nach Bemerkung (4.58) aber die bzgl. Inklusion kleinste Untergruppe von $(\mathbb{Z}/n)^\times$ ist, welche α enthält, impliziert dies bereits $\langle \alpha \rangle \subseteq \alpha^{\mathbb{Z}}$. Umgekehrt ist insbesondere $\alpha \in \langle \alpha \rangle$ nach Bemerkung (4.58), also auch $\alpha^k \in \langle \alpha \rangle$ nach dem Untergruppenkriterium, d.h. es ist $\alpha^{\mathbb{Z}} \subseteq \langle \alpha \rangle$. Insgesamt haben wir $\langle \alpha \rangle = \alpha^{\mathbb{Z}}$. $\square$

(4.63) Definition (Ordnung)**.** Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Die *Ordnung* von α ist definiert als

$$\operatorname{ord} \alpha := |\langle \alpha \rangle|.$$

(4.64) Bemerkung. Es sei $n \in \mathbb{N}$ gegeben. Für alle $\alpha \in (\mathbb{Z}/n)^\times$ gilt

$$\operatorname{ord} \alpha \mid \varphi(n).$$

Beweis. Da $\langle \alpha \rangle$ eine Untergruppe von $(\mathbb{Z}/n)^\times$ ist, gilt

$$\operatorname{ord} \alpha = |\langle \alpha \rangle| \mid \varphi(n)$$

für alle $\alpha \in (\mathbb{Z}/n)^\times$ nach dem Satz von Lagrange (4.56). □

(4.65) Satz. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Dann ist

$$\mathbb{Z}/(\operatorname{ord} \alpha) \to \langle \alpha \rangle,\ [k] \mapsto \alpha^k$$

ein wohldefinierter Gruppenisomorphismus. Insbesondere ist

$$\operatorname{ord} \alpha = \min \{k \in \mathbb{N} \mid \alpha^k = 1\}$$

und

$$\langle \alpha \rangle = \{\alpha^k \mid k \in [0, \operatorname{ord} \alpha - 1]\}.$$

Beweis. Nach Bemerkung (4.61) und Lemma (4.62) ist $\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times$, $k \mapsto \alpha^k$ ein Gruppenhomomorphismus mit $\operatorname{Im} \exp_\alpha = \alpha^{\mathbb{Z}} = \langle \alpha \rangle$. Insbesondere ist $\operatorname{Ker} \exp_\alpha$ eine abelsche Untergruppe von $\mathbb{Z}$, d.h. es existiert nach Lemma (2.21) und Satz (2.27) ein $m \in \mathbb{N}_0$ mit $\operatorname{Ker} \exp_\alpha = m\mathbb{Z}$. Da $(\mathbb{Z}/n)^\times$ eine endliche Gruppe ist, kann $\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times$ nicht injektiv sein. Folglich ist $m\mathbb{Z} = \operatorname{Ker} \exp_\alpha \neq \{0\}$ und damit $m > 0$. Genauer gilt

$$m = \min(\mathbb{N} \cap m\mathbb{Z}) = \min(\mathbb{N} \cap \operatorname{Ker} \exp_\alpha) = \min \{k \in \mathbb{N} \mid \exp_\alpha(k) = 1\} = \min \{k \in \mathbb{N} \mid \alpha^k = 1\}.$$

Es seien $k, l \in \mathbb{Z}$ gegeben. Genau dann gilt $\alpha^k = \alpha^l$ in $(\mathbb{Z}/n)^\times$, wenn $\alpha^{k-l} = 1$ ist, d.h. wenn $k - l \in \operatorname{Ker} \exp_\alpha = m\mathbb{Z}$ gilt. Dies ist nach Bemerkung (4.4) äquivalent zu $k \equiv_m l$ in $\mathbb{Z}$, d.h. zu $k = l$ in $\mathbb{Z}/m$. Folglich haben wir eine wohldefinierte injektive Abbildung

$$\varepsilon \colon \mathbb{Z}/m \to \langle \alpha \rangle,\ [k] \mapsto \alpha^k.$$

Wegen $\varepsilon([k]) = \alpha^k = \exp_\alpha(k)$ für $k \in \mathbb{Z}$ ist

$$\operatorname{Im} \varepsilon = \operatorname{Im} \exp_\alpha = \alpha^{\mathbb{Z}} = \langle \alpha \rangle$$

nach Bemerkung (4.61) und Lemma (4.62), d.h. ε ist auch surjektiv. Ferner gilt

$$\varepsilon([k] + [l]) = \varepsilon([k + l]) = \exp_\alpha(k + l) = \exp_\alpha(k) \exp_\alpha(l) = \varepsilon([k])\, \varepsilon([l])$$

für $k, l \in \mathbb{Z}$ nach Bemerkung (4.61), d.h. ε ist ein Gruppenhomomorphismus. Auf Grund der Bijektivität ist ε also sogar ein Gruppenisomorphismus.
Insbesondere folgt

$$\operatorname{ord} \alpha = |\langle \alpha \rangle| = |\operatorname{Im} \varepsilon| = |\mathbb{Z}/m| = m = \min \{k \in \mathbb{N} \mid \alpha^k = 1\}$$

sowie

$$\langle \alpha \rangle = \operatorname{Im} \varepsilon = \{\varepsilon([k]) \mid k \in [0, m-1]\} = \{\alpha^k \mid k \in [0, m-1]\} = \{\alpha^k \mid k \in [0, \operatorname{ord} \alpha - 1]\}$$

nach Korollar (4.18). □

(4.66) Korollar. Es seien $n \in \mathbb{Z}$, $m \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Genau dann gilt

$$\alpha^m = 1$$

in $(\mathbb{Z}/n)^\times$, wenn

$$\operatorname{ord}\alpha \mid m$$

gilt.

Beweis. Nach Satz (4.65) ist

$$\mathbb{Z}/(\operatorname{ord}\alpha) \to \langle\alpha\rangle,\ [k] \mapsto \alpha^k$$

ein wohldefinierter Gruppenisomorphismus. Folglich gilt genau dann $\alpha^m = 1$, wenn $m = 0$ in $\mathbb{Z}/(\operatorname{ord}\alpha)$ ist, d.h. wenn $\operatorname{ord}\alpha \mid m$ gilt. □

(4.67) Korollar. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Für alle $k \in \mathbb{Z}$ gilt

$$\operatorname{ord}\alpha^k = \frac{\operatorname{ord}\alpha}{\gcd(k, \operatorname{ord}\alpha)}.$$

Beweis. Nach Satz (4.65), Korollar (4.66) und Korollar (2.41) gilt

$$\begin{aligned}\operatorname{ord}\alpha^k &= \min\{l \in \mathbb{N} \mid (\alpha^k)^l = 1\} = \min\{l \in \mathbb{N} \mid \alpha^{kl} = 1\} = \min\{l \in \mathbb{N} \mid \operatorname{ord}\alpha \mid kl\} \\ &= \min\{l \in \mathbb{N} \mid \frac{\operatorname{ord}\alpha}{\gcd(k, \operatorname{ord}\alpha)} \mid l\} = \frac{\operatorname{ord}\alpha}{\gcd(k, \operatorname{ord}\alpha)}.\end{aligned}$$

□

(4.68) Korollar. Es seien $n, k \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist $\langle\alpha^k\rangle = \langle\alpha\rangle$.

(b) Es ist $\operatorname{ord}\alpha^k = \operatorname{ord}\alpha$.

(c) Es sind k und $\operatorname{ord}\alpha$ teilerfremd.

Beweis. Wegen $\alpha^k \in \langle\alpha\rangle$ gilt $\langle\alpha^k\rangle \subseteq \langle\alpha\rangle$ nach Bemerkung (4.58). Somit haben wir genau dann $\langle\alpha^k\rangle = \langle\alpha\rangle$, wenn $|\langle\alpha^k\rangle| = |\langle\alpha\rangle|$ gilt, d.h. genau dann, wenn $\operatorname{ord}\alpha^k = \operatorname{ord}\alpha$ ist. Folglich sind Bedingung (a) und Bedingung (b) äquivalent.
Nach Korollar (4.67) gilt ferner $\operatorname{ord}\alpha = (\operatorname{ord}\alpha^k)\gcd(k, \operatorname{ord}\alpha)$. Somit ist die Bedingung $\operatorname{ord}\alpha^k = \operatorname{ord}\alpha$ äquivalent zur Bedingung $\gcd(k, \operatorname{ord}\alpha) = 1$, d.h. zur Teilerfremdheit von k und $\operatorname{ord}\alpha$. Wir haben also auch die Äquivalenz von Bedingung (b) und Bedingung (c) gezeigt.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(4.69) Korollar. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$. Die Anzahl aller $\beta \in (\mathbb{Z}/n)^\times$ mit $\langle\alpha\rangle = \langle\beta\rangle$ ist durch $\varphi(\operatorname{ord}\alpha)$ gegeben.

Beweis. Nach Satz (4.65) gilt

$$\langle\alpha\rangle = \{\alpha^k \mid k \in [0, \operatorname{ord}\alpha - 1]\} = \{\alpha^k \mid k \in [1, \operatorname{ord}\alpha]\}.$$

Somit gilt für $\beta \in (\mathbb{Z}/n)^\times$ mit $\langle\alpha\rangle = \langle\beta\rangle$ stets $\beta = \alpha^k$ für ein $k \in [1, \operatorname{ord}\alpha]$. Aus Korollar (4.68) folgt nun

$$\begin{aligned}|\{\beta \in (\mathbb{Z}/n)^\times \mid \langle\alpha\rangle = \langle\beta\rangle\}| &= |\{k \in [1, \operatorname{ord}\alpha] \mid \langle\alpha\rangle = \langle\alpha^k\rangle\}| = |\{k \in [1, \operatorname{ord}\alpha] \mid k \text{ teilerfremd zu } \operatorname{ord}\alpha\}| \\ &= \varphi(\operatorname{ord}\alpha).\end{aligned}$$

□

(4.70) Beispiel. In $(\mathbb{Z}/7)^\times$ ist

$$\begin{aligned}\langle[1]\rangle &= \{1\}, \\ \langle[2]\rangle &= \{1, 2, 4\}, \\ \langle[3]\rangle &= \{1, 2, 3, 4, 5, 6\}, \\ \langle[4]\rangle &= \{1, 2, 4\}, \\ \langle[5]\rangle &= \{1, 2, 3, 4, 5, 6\}, \\ \langle[6]\rangle &= \{1, 6\}.\end{aligned}$$

Insbesondere ist $\operatorname{ord}[1] = 1$, $\operatorname{ord}[2] = 3$, $\operatorname{ord}[3] = 6$, $\operatorname{ord}[4] = 3$, $\operatorname{ord}[5] = 6$, $\operatorname{ord}[6] = 2$.

(4.71) Proposition. Es seien $n \in \mathbb{Z}$ und $\alpha, \beta \in (\mathbb{Z}/n)^\times$ gegeben. Wenn $\operatorname{ord}\alpha$ teilerfremd zu $\operatorname{ord}\beta$ ist, dann gilt

$$\operatorname{ord}(\alpha\beta) = (\operatorname{ord}\alpha)(\operatorname{ord}\beta).$$

Beweis. Es sei $\operatorname{ord}\alpha$ teilerfremd zu $\operatorname{ord}\beta$. Nach Proposition (2.45) gibt es $x, y \in \mathbb{Z}$ mit $1 = (\operatorname{ord}\alpha)x + (\operatorname{ord}\beta)y$. Da $(\mathbb{Z}/n)^\times$ kommutativ ist, ergibt sich

$$\alpha = \alpha^{(\operatorname{ord}\alpha)x+(\operatorname{ord}\beta)y} = \alpha^{(\operatorname{ord}\alpha)x}\,\alpha^{(\operatorname{ord}\beta)\,y} = \alpha^{(\operatorname{ord}\beta)\,y} = \alpha^{(\operatorname{ord}\beta)\,y}\,\beta^{(\operatorname{ord}\beta)\,y} = (\alpha\beta)^{(\operatorname{ord}\beta)y}$$

und damit

$$\alpha^{\operatorname{ord}(\alpha\beta)} = (\alpha\beta)^{(\operatorname{ord}\beta)y\operatorname{ord}(\alpha\beta)} = 1.$$

Nach Korollar (4.66) gilt also $\operatorname{ord}\alpha \mid \operatorname{ord}(\alpha\beta)$. Analog zeigt man, dass $\operatorname{ord}\beta \mid \operatorname{ord}(\alpha\beta)$ gilt. Somit ist $\operatorname{ord}(\alpha\beta)$ ein gemeinsames Vielfaches von $\operatorname{ord}\alpha$ und $\operatorname{ord}\beta$ und daher $\operatorname{lcm}(\operatorname{ord}\alpha, \operatorname{ord}\beta) \mid \operatorname{ord}(\alpha\beta)$. Da jedoch $\operatorname{ord}\alpha$ teilerfremd zu $\operatorname{ord}\beta$ ist, gilt $\operatorname{lcm}(\operatorname{ord}\alpha, \operatorname{ord}\beta) = (\operatorname{ord}\alpha)(\operatorname{ord}\beta)$ nach Satz (2.48) und damit $(\operatorname{ord}\alpha)(\operatorname{ord}\beta) \mid \operatorname{ord}(\alpha\beta)$. Ferner liefert die Kommutativität von $(\mathbb{Z}/n)^\times$ auch

$$(\alpha\beta)^{(\operatorname{ord}\alpha)(\operatorname{ord}\beta)} = \alpha^{(\operatorname{ord}\alpha)(\operatorname{ord}\beta)}\,\beta^{(\operatorname{ord}\alpha)(\operatorname{ord}\beta)} = 1$$

und damit $\operatorname{ord}(\alpha\beta) \mid (\operatorname{ord}\alpha)(\operatorname{ord}\beta)$ nach Korollar (4.66). Es folgt $\operatorname{ord}(\alpha\beta) = (\operatorname{ord}\alpha)(\operatorname{ord}\beta)$ nach Proposition (2.10)(c). □

Der Satz von Euler

(4.72) Satz (Satz von Euler)**.** Es seien teilerfremde $n \in \mathbb{N}$, $a \in \mathbb{Z}$ gegeben. Dann gilt

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

Beweis. Da a und n teilerfremd sind, ist a nach Bemerkung (4.39) eine Einheit modulo n, d.h. es ist $[a] \in (\mathbb{Z}/n)^\times$. Nach Bemerkung (4.64) gilt ferner $\operatorname{ord}[a] \mid \varphi(n)$ und nach Korollar (4.66) somit

$$[a^{\varphi(n)}] = [a]^{\varphi(n)} = 1$$

in $\mathbb{Z}/n$. Dies bedeutet aber gerade

$$a^{\varphi(n)} \equiv_n 1.$$ □

Alternativer Beweis des Satzes von Euler (4.72). Da a und n teilerfremd sind, ist a nach Bemerkung (4.39) eine Einheit modulo n, d.h. es ist $[a] \in (\mathbb{Z}/n)^\times$. Folglich ist

$$(\mathbb{Z}/n)^\times \to (\mathbb{Z}/n)^\times,\ \xi \mapsto [a]\,\xi$$

eine wohldefinierte Bijektion. Auf Grund der Kommutativität von $(\mathbb{Z}/n)^\times$ erhalten wir

$$\prod_{\xi\in(\mathbb{Z}/n)^\times} \xi = \prod_{\xi\in(\mathbb{Z}/n)^\times} ([a]\,\xi) = \Big(\prod_{\xi\in(\mathbb{Z}/n)^\times} [a]\Big)\Big(\prod_{\xi\in(\mathbb{Z}/n)^\times} \xi\Big),$$

also

$$1 = \prod_{\xi\in(\mathbb{Z}/n)^\times} [a] = [a]^{|(\mathbb{Z}/n)^\times|} = [a]^{\varphi(n)} = [a^{\varphi(n)}]$$

in $\mathbb{Z}/n$ und damit $a^{\varphi(n)} \equiv_n 1$ in $\mathbb{Z}$. □

(4.73) Korollar. Es seien $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $p \nmid a$ gegeben. Dann gilt

$$a^{p-1} \equiv_p 1.$$

Beweis. Nach Korollar (4.45) ist $\varphi(p) = p - 1$, so dass aus dem Satz von Euler (4.72) bereits

$$a^{p-1} = a^{\varphi(p)} \equiv_p 1$$

folgt. □

(4.74) Korollar (kleiner Satz von Fermat)**.** Es sei $p \in \mathbb{P}$ gegeben. Für alle $a \in \mathbb{Z}$ gilt

$$a^p \equiv_p a.$$

Beweis. Es sei $a \in \mathbb{Z}$ gegeben. Wenn $p \nmid a$ gilt, dann ist $a^{p-1} \equiv_p 1$ nach Korollar (4.73) und damit auch $a^p \equiv_p a$ nach Proposition (4.7)(c). Wenn hingegen $p \mid a$ gilt, so haben wir $a^p \equiv_p 0^p = 0 \equiv_p a$ nach Proposition (4.7)(c). Folglich gilt in jedem Fall $a^p \equiv_p a$. □

(4.75) Korollar (Satz von Wilson)**.** Es sei $n \in \mathbb{N}$ mit $n > 1$ gegeben. Genau dann ist n eine Primzahl, wenn

$$(n-1)! \equiv_n -1$$

gilt.

Beweis. Es sei zunächst n eine Primzahl. Für jedes $a \in [1, n-1]$ gilt $a^{n-1} \equiv_n 1$ nach Korollar (4.73) und somit $a^{n-1} - 1 = 0$ in $\mathbb{F}_n$. Da $\mathbb{F}_n$ ein Körper ist, hat das Polynom $x^{n-1} - 1$ über $\mathbb{F}_n$ jedoch höchstens $n - 1$ Nullstellen. Folglich gilt

$$x^{n-1} - 1 = \prod_{a \in [1,n-1]} (x - a)$$

über $\mathbb{F}_n$. Es folgt

$$-1 = 0^{n-1} - 1 = \prod_{a \in [1,n-1]} (0 - a) = \prod_{a \in [1,n-1]} (-a) = (-1)^{n-1} \prod_{a \in [1,n-1]} a = (n-1)!$$

in $\mathbb{F}_n$, d.h. es gilt $(n-1)! \equiv_n -1$ in $\mathbb{Z}$.
Für die Umkehrung siehe Aufgabe 46. □

Alternativer Beweis des Satzes von Wilson (4.75). Für $\alpha \in \mathbb{F}_n^\times$ gilt genau dann $\alpha^{-1} = \alpha$, wenn $(\alpha - 1)(\alpha + 1) = \alpha^2 - 1 = 0$ ist. Nun ist $\mathbb{F}_n$ nach Satz (4.41) ein Körper und damit insbesondere ein Bereich. Folglich gilt für $\alpha \in \mathbb{F}_n^\times$ genau dann $\alpha^{-1} = \alpha$, wenn $\alpha - 1 = 0$ oder $\alpha + 1 = 0$ ist, d.h. wenn $\alpha \in \{1, -1\}$ ist. Somit ist für jedes $\alpha \in \mathbb{F}_n^\times \setminus \{1, -1\}$ das Inverse α^{-1} ein Element von $\mathbb{F}_n^\times \setminus \{1, -1, \alpha\}$. Es folgt

$$[(n-1)!] = \prod_{a \in [1,n-1]} [a] = \prod_{\alpha \in \mathbb{F}_n^\times} \alpha = 1 \cdot (-1) \cdot \prod_{\alpha \in \mathbb{F}_n^\times \setminus \{1,-1\}} \alpha = -1 = [-1]$$

in $\mathbb{F}_n$ und damit

$$(n-1)! \equiv_n -1.$$ □

Für die Umkehrung siehe Aufgabe 46.

(4.76) Korollar. Für jede ungerade Primzahl p gilt

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv_p (-1)^{\frac{p+1}{2}}.$$

Beweis. Siehe Aufgabe 47. □

Anwendung: Ein symmetrisches Kryptosystem

Im Folgenden wollen wir als Anwendung ein einfaches Verfahren zu Ver- und Entschlüsseln von Nachrichten kennenlernen. Die Ausgangssituation ist wie folgt: Ein Sender verschlüsselt einen gegebenen Text und sendet das Chiffrat danach über einen unsicheren Kanal an einen Empfänger, welcher den Geheimtext anschließend wieder entschlüsselt und so den ursprünglichen Text erhält.
Wir betrachten zunächst ein sogenanntes *symmetrisches Kryptosystem*, bestehend aus einer Menge von *Klartexten* $\mathcal{P}$, einer Menge von *Geheimtexten* (oder *Chiffraten*) $\mathcal{C}$ und einem *Schlüssel* K, welcher seinerseits zwei Abbildungen $e\colon \mathcal{P} \to \mathcal{C}$, die *Verschlüsselungsfunktion*, und eine Abbildung $d\colon \mathcal{C} \to \mathcal{P}$, die *Entschlüsselungsfunktion*, mit

$$d \circ e = \mathrm{id}_{\mathcal{P}}$$

bedingt. Der Schlüssel wird sowohl zum Verschlüsseln als auch zum Entschlüsseln benutzt und sollte daher sowohl dem Sender als auch dem Empfänger vorliegen und ansonsten geheim sein.
Im Folgenden wird die Menge der Klartexte $\mathcal{P}$ immer eine endliche Menge sein, meistens von der Form $[0, n-1]$ für ein hinreichend großes $n \in \mathbb{N}$. In der Praxis muss ein zu verschlüsselnder Text also zunächst in ein Element oder eine Folge von Elementen aus $\mathcal{P}$ umgewandelt werden. Diesen Prozess werden wir hier nicht näher thematisieren.

(4.77) Anwendung.

- Initialisierung:
  - Wähle geeignete große natürliche Zahl n (mit $\varphi(n)$ groß, etwa eine Primzahl).
  - Wähle eine Einheit a modulo n.
  - Berechne $b \in [1, n-1]$ mit b invers zu a modulo n.
  - Halte den Schlüssel $K := (n, a, b)$ geheim.
  - Die Menge der Klartexte ist $\mathcal{P} := [0, n-1]$. Die Menge der Geheimtexte ist $\mathcal{C} := [0, n-1]$.
- Verschlüsselung eines Klartexts $x \in \mathcal{P}$:
  - Berechne
    $$e(x) = ax \bmod n.$$
- Entschlüsselung eines Geheimtexts $y \in \mathcal{C}$:
  - Berechne
    $$d(y) = by \bmod n.$$
- Beispiel:
  - Wir wählen $n = 101$, $a = 26$. Dann ist $26 \cdot 35 = 910 \equiv_{101} 1$, also $b = 35$. Der Schlüssel ist
    $$K = (n, a, b) = (101, 26, 35).$$
    Die Menge der Klartexte und der Geheimtexte ist
    $$\mathcal{P} = \mathcal{C} = [0, n-1] = [0, 100].$$
  - Die Verschlüsselung des Klartexts $x = 50$ ergibt
    $$e(x) = ax \bmod n = 26 \cdot 50 \bmod 101 = 1300 \bmod 101 = 88.$$
  - Die Entschlüsselung des Geheimtexts $y = 88$ ergibt
    $$d(y) = by \bmod n = 35 \cdot 88 \bmod 101 = 3080 \bmod 101 = 50.$$

Der wesentliche Bestandteil des Schlüssels $K = (n, a, b)$ aus Anwendung (4.77) ist natürlich a, da n nach hinreichend oftmaliger Anwendung bekannt ist und b aus n und a berechnet werden kann.
Das Kryptosystem in (4.77) besitzt darüberhinaus einige offensichtliche Nachteile: Es ist vergleichsweise unsicher, sofern n im Vergleich zur Gesamtgröße der übertragenen Daten nicht sehr groß ist. Insbesondere ist es also für eine häufige Anwendung ungeeignet. Ferner ist es zwingend notwendig, dass sich Sender und Empfänger vor der Nachrichtenübermittlung auf einen gemeinsamen geheimen Schlüssel geeinigt haben. Dies kann etwa über einen sicheren Kanal passieren, welcher jedoch in der Praxis nicht immer gegeben ist (wären sichere Kanäle stets gegeben, so würde man keine Verschlüsselungstechniken benötigen). Wir werden in Anwendung (4.104) ein Verfahren kennenlernen, welches einem einen Schlüsselaustausch über einen unsicheren Kanal gestattet.

Anwendung: RSA-Kryptosystem

Als nächstes werden wir ein Verschlüsselungsverfahren kennenlernen, bei welchem das Problem des gemeinsamen Schlüssels nicht auftaucht, da es keinen gemeinsamen Schlüssel gibt. Es handelt sich hierbei um ein sogenanntes *Public-Key-Kryptosystem*, bei welchem im Vergleich zu einem symmetrischen Kryptosystem der gemeinsame Schlüssel K durch zwei Schlüssel ersetzt wird, einem *öffentlichen Schlüssel* K_{open} und einem *privaten Schlüssel* K_{priv}. Der öffentliche Schlüssel wird zum Versenden von Nachrichten benutzt und wird nicht geheimgelten, sondern öffentlich publiziert, etwa auf der persönlichen Homepage des Empfängers. Entsprechend darf die Verschlüsselungsfunktion $e\colon \mathcal{P} \to \mathcal{C}$ eines Public-Key-Kryptosystems nur vom öffentlichen Schlüssel abhängen.
Die Ausgangssituation ist also nun wie folgt: Ein Sender ermittelt den öffentlichen Schlüssel des Empfängers, verschlüsselt mit dessen Hilfe einen gegebenen Text und sendet danach das Chiffrat über einen unsicheren Kanal an den Empfänger. Dieser entschlüsselt anschließend den Geheimtext mit Hilfe des privaten Schlüssels und erhält so den ursprünglichen Text.
Bevor wir in Anwendung (4.80) ein konkretes Verfahren vorstellen, wollen wir zunächst die dahinterstehende Theorie herleiten.

(4.78) Proposition. Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ gegeben. Ferner seien sich modulo $\varphi(pq)$ gegenseitig invertierbare $a, b \in \mathbb{Z}$ gegeben. Für alle $x \in \mathbb{Z}$ gilt dann

$$x^{ab} \equiv_{pq} x.$$

Beweis. Es sei $x \in \mathbb{Z}$ gegeben.
Zunächst sei p kein Primfaktor von x. Nach Korollar (4.73) gilt dann $x^{p-1} \equiv_p 1$. Nun ist nach Korollar (4.46) und Korollar (4.45) jedoch $\varphi(pq) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$, es gilt also auch $x^{\varphi(pq)} = (x^{p-1})^{q-1} \equiv_p 1$. Wegen $ab \equiv_{\varphi(pq)} 1$ impliziert dies $x^{ab} \equiv_p x$. Ist hingegen p ein Primfaktor von x, so haben wir $x \equiv_p 0$ und somit auch in diesem Fall $x^{ab} \equiv_p 0 \equiv_p x$.
Es gilt also in jedem Fall $x^{ab} \equiv_p x$. Analog ist auch $x^{ab} \equiv_q x$ und damit $x^{ab} \equiv_{\operatorname{lcm}(p,q)} x$ nach Bemerkung (4.9). Wegen $p \neq q$ sind p und q teilerfremd, es ist also $\operatorname{lcm}(p, q) = pq$ nach Satz (2.48) und damit $x^{ab} \equiv_{pq} x$. □

(4.79) Korollar. Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ und sich modulo $\varphi(pq)$ gegenseitig invertierbare $a, b \in \mathbb{Z}$ gegeben. Dann sind

$$\mathbb{Z}/(pq) \to \mathbb{Z}/(pq),\ [x] \mapsto [x]^a,$$
$$\mathbb{Z}/(pq) \to \mathbb{Z}/(pq),\ [y] \mapsto [y]^b$$

sich gegenseitig invertierbare Monoidisomorphismen.

Das vorangegangene Korollar ist Grundlage des nachfolgenden Verschlüsselungsverfahrens.

(4.80) Anwendung (RSA-Kryptosystem; Rivest, Shamir, Adleman; 1977)**.**

- Initialisierung:
  - Wähle geeignete große Primzahlen p und q mit $p \neq q$ (ungefähr 250 Stellen).
  - Berechne $n := pq$ und $\varphi(n) = (p-1)(q-1)$.
  - Wähle geeignetes $a \in [1, \varphi(n)]$ mit $\gcd(a, \varphi(n)) = 1$.
  - Berechne $b \in [1, \varphi(n)]$ mit b invers zu a modulo $\varphi(n)$.

  - Publiziere den öffentlichen Schlüssel $K_{\text{open}} := (n, a)$ (zum Beispiel auf persönlicher Homepage).
  - Halte den privaten Schlüssel $K_{\text{priv}} := b$ geheim.
  - Die Menge der Klartexte ist $\mathcal{P} := [0, n-1]$. Die Menge der Geheimtexte ist $\mathcal{C} := [0, n-1]$.

- Verschlüsselung eines Klartexts $x \in \mathcal{P}$:
  - Berechne
$$e(x) = x^a \bmod n.$$

- Entschlüsselung eines Geheimtexts $y \in \mathcal{C}$:
  - Berechne
$$d(y) = y^b \bmod n.$$

- Beispiel:
  - Wir wählen $p = 3$, $q = 11$. Dann ist $n = pq = 3 \cdot 11 = 33$ und $\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$. Wir wählen $a = 3$. Dann ist $3 \cdot 7 = 21 \equiv_{20} 1$, also $b = 7$. Der öffentliche Schlüssel ist
$$K_{\text{open}} = (n, a) = (33, 3).$$
    Der private Schlüssel ist
$$K_{\text{priv}} = b = 7.$$
  - Die Verschlüsselung des Klartexts $x = 13$ ergibt
$$e(x) = x^a \bmod n = 13^3 \bmod 33 = (13 \cdot 169) \bmod 33 = (13 \cdot 4) \bmod 33 = 52 \bmod 33 = 19.$$
  - Die Entschlüsselung des Geheimtexts $y = 19$ ergibt
$$\begin{aligned} d(y) &= y^b \bmod n = 19^7 \bmod 33 = (-14)^7 \bmod 33 = (196^3(-14)) \bmod 33 \\ &= ((-2)^3(-14)) \bmod 33 = (8 \cdot 14) \bmod 33 = 112 \bmod 33 = 13. \end{aligned}$$

Die Sicherheit des RSA-Kryptosystems beruht auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Könnte ein Angreifer aus der Kenntnis des öffentlichen Schlüssels $K_{\text{open}} := (n, a)$ in Anwendung (4.80) die Primfaktoren von n ermitteln, so könnte er auch $\varphi(n)$ und damit mit Hilfe des erweiterten euklidischen Algorithmus' den privaten Schlüssel berechnen. Umgekehrt kann man auch zeigen, dass sich mit Hilfe des privaten Schlüssels die Primfaktoren von n ermitteln lassen.

Aufgaben

Aufgabe 44 (Eulersche Phi-Funktion)**.** Zeigen Sie:

(a) Für $n \in \mathbb{N}$ gilt
$$\varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} (1 - \frac{1}{p})$$

(b) Die Abbildung $f\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n\varphi(n)$ ist injektiv.

Aufgabe 45 (Summatorfunktion der Euler-Funktion)**.** Zeigen Sie:

(a) Die Summatorfunktion der Euler-Funktion ist gegeben durch
$$\mathrm{T}\varphi = \mathrm{inc}\colon \mathbb{N} \to \mathbb{C}.$$

(b) Für $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \sum_{\substack{d \in \mathbb{N} \\ d|n}} \frac{\mu(d)}{d}.$$

Aufgabe 46 (Satz von Wilson)**.** Es sei $n \in \mathbb{N}$ mit $n > 1$ gegeben. Zeigen Sie: Wenn

$$(n-1)! \equiv_n -1$$

gilt, dann ist n eine Primzahl.

Aufgabe 47 (Satz von Wilson für ungerade Primzahlen)**.** Zeigen Sie: Für jede ungerade Primzahl p gilt

$$(\frac{p-1}{2}!)^2 \equiv_p (-1)^{\frac{p+1}{2}}.$$

Aufgabe 48 (Satz von Wilson für Primzahlzwillinge)**.** Es sei $n \in \mathbb{N}$ mit $n > 1$ gegeben. Zeigen Sie: Genau dann sind n und $n+2$ Primzahlen, wenn

$$4(n-1)! \equiv_{n(n+2)} -(n+4)$$

ist.

Aufgabe 49 (Struktur der primen Restklassengruppe $(\mathbb{Z}/2^k)^\times$)**.** Zeigen Sie:

(a) Für $l \in \mathbb{N}_0$, $a \in \mathbb{Z}$ gilt

$$(1+4a)^{2^l} \equiv_{2^{l+3}} 1 + 2^{l+2}a.$$

(b) Für $k \in \mathbb{N}$ mit $k \geq 2$ ist 5 invertierbar modulo 2^k und die Ordnung von $[5]$ in $(\mathbb{Z}/2^k)^\times$ ist gegeben durch

$$\operatorname{ord}[5] = 2^{k-2}.$$

(c) Für $k \in \mathbb{N}$ ist

$$(\mathbb{Z}/2^k)^\times \cong \begin{cases} \mathbb{Z}/1, & \text{für } k = 1, \\ \mathbb{Z}/2, & \text{für } k = 2, \\ \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2}, & \text{für } k \geq 3. \end{cases}$$

4 Primitivwurzeln und Indexarithmetik

Diskrete Exponentiation und diskreter Logarithmus

Es seien $n \in \mathbb{Z}$, $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Nach Definition (4.60) und Bemerkung (4.61) haben wir einen Gruppenhomomorphismus

$$\exp_\alpha \colon \mathbb{Z} \to (\mathbb{Z}/n)^\times,\ k \mapsto \alpha^k,$$

die *diskrete Exponentiation* zur Basis α. Ferner induziert diese nach Satz (4.65) den Gruppenisomorphismus

$$\mathbb{Z}/(\operatorname{ord}\alpha) \to \langle\alpha\rangle,\ [k] \mapsto \alpha^k.$$

Wir werden im Folgenden diesen Gruppenisomorphismus wieder aufgreifen.

(4.81) Definition (diskrete Exponentiation, diskreter Logarithmus)**.** Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben.

(a) Unter Missbrauch der Terminologie unter der Notation bezeichnen wir den Gruppenisomorphismus

$$\exp_\alpha \colon \mathbb{Z}/(\operatorname{ord}\alpha) \to \langle\alpha\rangle,\ [k] \mapsto \alpha^k$$

als *diskrete Exponentiation* zur Basis α.

(b) Der zur diskreten Exponentiation $\exp_\alpha\colon \mathbb{Z}/(\operatorname{ord}\alpha) \to \langle\alpha\rangle$ inverse Gruppenhomomorphismus

$$\log_\alpha\colon \langle\alpha\rangle \to \mathbb{Z}/(\operatorname{ord}\alpha)$$

heißt *diskreter Logarithmus* zur Basis α.

(4.82) Beispiel.

(a) Die diskrete Exponentiation zur Basis 2 in $\mathbb{F}_{11}$ ist wie folgt gegeben:

k	0	1	2	3	4	5	6	7	8	9	10
$\exp_2(k)$	1	2	4	8	5	10	9	7	3	6	1

Insbesondere ist $\operatorname{ord} 2 = 10$ in $\mathbb{F}_{11}^\times$ und $\langle 2\rangle = \mathbb{F}_{11}$. Der diskrete Logarithmus zur Basis 2 in $\mathbb{F}_{11}$ ist wie folgt gegeben:

α	1	2	3	4	5	6	7	8	9	10
$\log_2(\alpha)$	0	1	8	2	4	9	7	3	6	5

(b) Die diskrete Exponentiation zur Basis 2 in $\mathbb{F}_7$ ist wie folgt gegeben:

k	0	1	2	3
$\exp_2(k)$	1	2	4	1

Insbesondere ist $\operatorname{ord} 2 = 3$ in $\mathbb{F}_7^\times$ und $\langle 2\rangle = \{1, 2, 4\}$. Der diskrete Logarithmus zur Basis 2 in $\mathbb{F}_7$ ist wie folgt gegeben:

α	1	2	4
$\log_2(\alpha)$	0	1	2

(c) Die diskrete Exponentiation zur Basis 2 in $\mathbb{Z}/21$ ist wie folgt gegeben:

k	0	1	2	3	4	5	6
$\exp_2(k)$	1	2	4	8	16	11	1

Insbesondere ist $\operatorname{ord} 2 = 6$ in $(\mathbb{Z}/21)^\times$ und $\langle 2\rangle = \{1, 2, 4, 8, 11, 16\}$. Der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}/21$ ist wie folgt gegeben:

α	1	2	4	8	11	16
$\log_2(\alpha)$	0	1	2	3	5	4

Im Allgemeinen ist es ein schwieriges Problem, diskrete Logarithmen zu berechnen.

(4.83) Bemerkung. Es seien $n \in \mathbb{Z}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben.

(a) Für $\beta, \gamma \in \langle\alpha\rangle$ ist

$$\log_\alpha(\beta\gamma) = \log_\alpha(\beta) + \log_\alpha(\gamma).$$

(b) Es ist

$$\log_\alpha(1) = 0.$$

(c) Für $k \in \mathbb{Z}$, $\beta \in \langle\alpha\rangle$ ist

$$\log_\alpha(\beta^k) = \log_\alpha(\beta)k.$$

Beweis. Diese Eigenschaften gelten, da $\log_\alpha\colon \langle\alpha\rangle \to \mathbb{Z}/(\operatorname{ord}\alpha)$ ein Gruppenhomomorphismus ist. □

(4.84) Korollar. Es sei $n \in \mathbb{Z}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$, $\beta \in \langle\alpha\rangle$, $\gamma \in \langle\beta\rangle$ gilt $\gamma \in \langle\alpha\rangle$ und

$$\log_\alpha(\gamma) = \log_\alpha(\beta)\,\log_\beta(\gamma).$$

Beweis. Es seien $\alpha \in (\mathbb{Z}/n)^\times$, $\beta \in \langle\alpha\rangle$, $\gamma \in \langle\beta\rangle$ sowie $k \in \mathbb{Z}$ mit $\log_\beta(\gamma) = [k]$ gegeben. Wegen $\beta \in \langle\alpha\rangle$ ist dann auch $\gamma = \beta^k \in \langle\alpha\rangle$ und nach Bemerkung (4.83)(c) gilt

$$\log_\alpha(\gamma) = \log_\alpha(\beta^k) = \log_\alpha(\beta)\,k = \log_\alpha(\beta)\,[k] = \log_\alpha(\beta)\,\log_\beta(\gamma).$$ □

Primitivwurzeln

(4.85) Definition (Primitivwurzel)**.** Es sei $n \in \mathbb{Z}$ gegeben. Eine *Primitivwurzel* modulo n ist ein $r \in \mathbb{Z}$ so, dass r invertierbar modulo n ist und $(\mathbb{Z}/n)^\times = \langle [r] \rangle$ gilt.

(4.86) Beispiel.

(a) Es ist 2 eine Primitivwurzel modulo 11.

(b) Es ist 2 keine Primitivwurzel modulo 7.

(c) Es ist 2 keine Primitivwurzel modulo 21.

Beweis.

(a) Dies folgt aus Beispiel (4.82)(a).

(b) Dies folgt aus Beispiel (4.82)(b).

(c) Dies folgt aus Beispiel (4.82)(c). □

(4.87) Bemerkung. Es seien $n \in \mathbb{N}$, $r \in \mathbb{Z}$ so gegeben, dass r invertierbar modulo n ist. Genau dann ist r eine Primitivwurzel modulo n, wenn

$$\operatorname{ord}[r] = \varphi(n)$$

ist.

Beweis. Da stets $\langle [r] \rangle \subseteq (\mathbb{Z}/n)^\times$ gilt, ist r genau dann eine Primitivwurzel modulo n, wenn $|\langle [r] \rangle| = |(\mathbb{Z}/n)^\times|$ ist. Nach Bemerkung (4.44) und Definition (4.63) gilt dies jedoch genau dann, wenn $\operatorname{ord}[r] = \varphi(n)$ ist. □

(4.88) Korollar. Es seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und eine Primitivwurzel r modulo n gegeben. Genau dann ist r^k eine Primitivwurzel modulo n, wenn k und $\varphi(n)$ teilerfremd sind.

Beweis. Da r eine Primitivwurzel modulo n ist, gilt $\operatorname{ord}[r] = \varphi(n)$ nach Bemerkung (4.87). Ferner ist r^k genau dann eine Primitivwurzel modulo n, wenn $\operatorname{ord}[r^k] = \varphi(n)$ gilt, d.h. wenn $\operatorname{ord}[r]^k = \operatorname{ord}[r]$ ist. Nach Korollar (4.68) ist dies jedoch äquivalent zur Teilerfremdheit von k und $\operatorname{ord}[r] = \varphi(n)$. □

(4.89) Korollar. Es sei $n \in \mathbb{N}$ gegeben. Wenn es eine Primitivwurzel modulo n gibt, dann ist die Anzahl aller inkongruenten Primitivwurzeln modulo n durch $\varphi(\varphi(n))$ gegeben.

Beweis. Es sei eine Primitivwurzel r modulo n gegeben, so dass $(\mathbb{Z}/n)^\times = \langle [a] \rangle$ gilt. Nach Korollar (4.69) und Bemerkung (4.87) ist die Anzahl aller Primitivwurzeln modulo n gegeben durch

$$\begin{aligned}&|\{s \in [1, n-1] \mid s \text{ ist Primitivwurzel modulo } n\}| = |\{s \in [1, n-1] \mid (\mathbb{Z}/n)^\times = \langle [s] \rangle\}| \\ &= |\{\sigma \in (\mathbb{Z}/n)^\times \mid (\mathbb{Z}/n)^\times = \langle \sigma \rangle\}| = |\{\sigma \in (\mathbb{Z}/n)^\times \mid \langle [r] \rangle = \langle \sigma \rangle\}| = \varphi(\operatorname{ord}[r]) = \varphi(\varphi(n)).\end{aligned}$$ □

Als nächstes wollen wir zeigen, dass es modulo Primzahlen stets Primitivwurzeln gibt.

(4.90) Proposition. Für alle $n \in \mathbb{Z}$ existiert ein $\alpha \in (\mathbb{Z}/n)^\times$ mit

$$\operatorname{ord}\alpha = \operatorname{lcm}(\operatorname{ord}\beta)_{\beta \in (\mathbb{Z}/n)^\times}.$$

Beweis. Wir setzen $l := \operatorname{lcm}(\operatorname{ord}\beta)_{\beta \in (\mathbb{Z}/n)^\times}$. Für $p \in \mathbb{P}$ ist $\mathrm{v}_p(l) = \max\{\mathrm{v}_p(\operatorname{ord}\beta) \mid \beta \in (\mathbb{Z}/n)^\times\}$ nach Korollar (2.76)(b). Folglich gibt es für jedes $p \in \mathbb{P}$ ein $\beta_p \in (\mathbb{Z}/n)^\times$ so, dass $\mathrm{v}_p(l) = \mathrm{v}_p(\operatorname{ord}\beta_p)$ ist. Für $p \in \mathbb{P}$ gilt also $p^{\mathrm{v}_p(l)} \mid \operatorname{ord}\beta_p$ und nach Korollar (4.67) folgt

$$\operatorname{ord}\beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}} = \frac{\operatorname{ord}\beta_p}{\gcd(\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}, \operatorname{ord}\beta_p)} = \frac{\operatorname{ord}\beta_p}{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}} = p^{\mathrm{v}_p(l)}.$$

Insbesondere ist $(\beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}})_{p \in \mathbb{P}}$ paarweise teilerfremd. Da $\mathrm{v}_p(l) = 0$ für fast alle $p \in \mathbb{P}$ gilt, ist $\operatorname{ord}\beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}} = 1$ und damit auch $\beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}} = 1$ für fast alle $p \in \mathbb{P}$. Wir setzen $\alpha := \prod_{p \in \mathbb{P}} \beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}}$ und erhalten

$$\operatorname{ord}\alpha = \operatorname{ord}(\prod_{p \in \mathbb{P}} \beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}}) = \prod_{p \in \mathbb{P}} \operatorname{ord}\beta_p^{\frac{\operatorname{ord}\beta_p}{p^{\mathrm{v}_p(l)}}} = \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(l)} = l = \operatorname{lcm}(\operatorname{ord}\beta)_{\beta \in (\mathbb{Z}/n)^\times}$$

nach Proposition (4.71). □

(4.91) Korollar. Für alle $p \in \mathbb{P}$ existiert eine Primitivwurzel modulo p.

Beweis. Wir setzen $l := \operatorname{lcm}(\operatorname{ord}\beta)_{\beta\in\mathbb{F}_p^\times}$. Dann ist $\beta^l = 1$ und somit $\beta^l - 1 = 0$ für alle $\beta \in \mathbb{F}_p^\times$. Da das Polynom $x^l - 1$ über $\mathbb{F}_p$ höchstens l Nullstellen hat, gilt nach Bemerkung (4.44) folglich $\varphi(p) = |\mathbb{F}_p^\times| \leq l$. Andererseits gilt nach Bemerkung (4.64) stets $\operatorname{ord}\beta \mid \varphi(p)$ für alle $\beta \in \mathbb{F}_p^\times$ und damit $l = \operatorname{lcm}(\operatorname{ord}\beta)_{\beta\in\mathbb{F}_p^\times} \mid \varphi(p)$. Insgesamt haben wir

$$\varphi(p) = l = \operatorname{lcm}(\operatorname{ord}\beta)_{\beta\in\mathbb{F}_p^\times}.$$

Nach Proposition (4.90) gibt es jedoch eine Einheit r modulo p mit $\operatorname{ord}[r] = \operatorname{lcm}(\operatorname{ord}\beta)_{\beta\in(\mathbb{Z}/n)^\times} = \varphi(p)$, so dass r nach Bemerkung (4.87) eine Primitivwurzel modulo p ist. □

Es ist bekannt, modulo welchen natürlichen Zahlen es Primitivwurzeln gibt. Wir werden diese Charakterisierung im Folgenden angeben, jedoch im Rahmen der Vorlesung nicht beweisen:

(4.92) Satz (Gauss)**.** Es sei $n \in \mathbb{N}$ gegeben. Genau dann existiert eine Primitivwurzel modulo n, wenn

$$n \in \{2, 4\} \dot\cup \{p^k \mid p \in \mathbb{P} \setminus \{2\},\, k \in \mathbb{N}\} \dot\cup \{2p^k \mid p \in \mathbb{P} \setminus \{2\},\, k \in \mathbb{N}\}$$

ist.

Ohne Beweis. □

Index

Es seien $n \in \mathbb{Z}$, $\rho \in (\mathbb{Z}/n)^\times$, $\alpha \in \langle\rho\rangle$ gegeben. Nach Definition (4.81)(b) des diskreten Logarithmus

$$\log_\rho\colon \langle\rho\rangle \to \mathbb{Z}/(\operatorname{ord}\rho)$$

gilt für $k \in \mathbb{Z}$ genau dann $\rho^k = \alpha$, wenn $\log_\rho(\alpha) = [k]$ ist. Jede Restklasse in $\mathbb{Z}/(\operatorname{ord}\rho)$ besitzt einen eindeutigen Vertreter in der Standardtransversalen $[0, (\operatorname{ord}\rho) - 1]$.
Wir wollen nun eine Abbildung einführen, welche jeder Einheit modulo n, also jedem Vertreter einer primen Restklasse, den eindeutigen Standardvertreter des diskreten Logarithmus zu einer gegebenen Basis ρ zuordnet. Damit wir dies auch wirklich für jede Einheit modulo n machen können, muss $(\mathbb{Z}/n)^\times = \langle\rho\rangle$ gelten, d.h. ρ muss von einer Primitivwurzel modulo n repräsentiert werden. Der Standardvertreter des diskreten Logarithmus ist dann ein Element von $[0, (\operatorname{ord}\rho) - 1] = [0, \varphi(n) - 1]$

(4.93) Definition (Index)**.** Es seien $n \in \mathbb{Z}$ und eine Primitivwurzel r modulo n gegeben. Für $a \in \mathbb{Z}$ teilerfremd zu n heißt das eindeutige $k \in [0, \varphi(n)-1]$ mit $a \equiv_n r^k$ der *Index* (oder der *diskrete Logarithmus*) von a modulo n zur Basis r, geschrieben

$$\operatorname{ind}_r(a) = k.$$

(4.94) Bemerkung. Es seien $n \in \mathbb{Z}$ und eine Primitivwurzel r modulo n gegeben. Für $a \in \mathbb{Z}$ teilerfremd zu n gilt

$$\log_{[r]}([a]) = [\operatorname{ind}_r(a)].$$

(4.95) Korollar. Es seien $n \in \mathbb{Z}$ und eine Primitivwurzel r modulo n gegeben. Für $a \in \mathbb{Z}$ teilerfremd zu n und für $k \in \mathbb{N}_0$ gilt genau dann

$$r^k \equiv_n a,$$

wenn

$$k \equiv_{\varphi(n)} \operatorname{ind}_r(a)$$

gilt.

(4.96) Beispiel. Es ist 2 eine Primitivwurzel modulo 11. Der Index modulo 11 zur Basis 2 ist wie folgt gegeben:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2(a)$	0	1	8	2	4	9	7	3	6	5

Beweis. Dies folgt aus Beispiel (4.82)(a). □

Wie bei allgemeinen diskretes Logarithmen ist es in der Regel vergleichsweise schwierig, Indizes zu gegebenen Primitivwurzeln als Basen zu berechnen.

(4.97) Bemerkung. Es seien $n \in \mathbb{Z}$ und eine Primitivwurzel r modulo n gegeben.

(a) Für $a, b \in \mathbb{Z}$ teilerfremd zu n ist

$$\operatorname{ind}_r(ab) = (\operatorname{ind}_r(a) + \operatorname{ind}_r(b)) \bmod \varphi(n).$$

(b) Es ist

$$\operatorname{ind}_r(1) = 0.$$

(c) Für $k \in \mathbb{N}_0$ und $a \in \mathbb{Z}$ teilerfremd zu n ist

$$\operatorname{ind}_r(a^k) = (\operatorname{ind}_r(a)\, k) \bmod \varphi(n).$$

Beweis.

(a) Dies folgt aus Bemerkung (4.83)(a).

(b) Dies folgt aus Bemerkung (4.83)(b).

(c) Dies folgt aus Bemerkung (4.83)(c). □

(4.98) Bemerkung. Es seien $n \in \mathbb{Z}$ und Primitivwurzeln r und s modulo n gegeben. Für $a \in \mathbb{Z}$ teilerfremd zu n gilt

$$\operatorname{ind}_s(a) = (\operatorname{ind}_s(r) \operatorname{ind}_r(a)) \bmod \varphi(n).$$

Beweis. Dies folgt aus Korollar (4.84). □

Spezielle monomiale Kongruenzgleichungen in einer Unbekannten

(4.99) Bemerkung. Es seien $n \in \mathbb{Z}$, eine Primitivwurzel r modulo n, ein $k \in \mathbb{N}_0$ und ein $a \in \mathbb{Z}$ teilerfremd zu n gegeben. Für $x \in \mathbb{Z}$ gilt genau dann

$$x^k \equiv_n a,$$

wenn x teilerfremd zu n und

$$\operatorname{ind}_r(x)\, k \equiv_{\varphi(n)} \operatorname{ind}_r(a)$$

ist.

Beweis. Es sei $x \in \mathbb{Z}$ gegeben. Zunächst gelte $x^k \equiv_n a$, so dass $x^k = a$ in $\mathbb{Z}/n$. Nach Bemerkung (4.39) ist a wegen der Teilerfremdheit zu n eine Einheit modulo n, also auch x eine Einheit modulo n und damit x teilerfremd zu n. Nach Bemerkung (4.97)(c) folgt aus $x^k \equiv_n a$ ferner

$$\operatorname{ind}_r(x)\, k \equiv_{\varphi(n)} \operatorname{ind}_r(x^k) = \operatorname{ind}_r(a).$$

Ist umgekehrt x teilerfremd zu n und $\operatorname{ind}_r(x)\, k \equiv_{\varphi(n)} \operatorname{ind}_r(a)$, so folgt

$$x^k \equiv_n \left(r^{\operatorname{ind}_r(x)}\right)^k = r^{\operatorname{ind}_r(x)\, k} \equiv_n r^{\operatorname{ind}_r(a)} \equiv_n a.$$ □

(4.100) Proposition. Es seien $n, k \in \mathbb{N}_0$, $a \in \mathbb{Z}$ so gegeben, dass a teilerfremd zu n ist und eine Primitivwurzel modulo n existiert. Die folgenden Bedingungen sind äquivalent.

(a) Es existiert ein $x \in \mathbb{Z}$ mit

$$x^k \equiv_n a.$$

(b) Für jede Primitivwurzel r modulo n gibt es ein $y \in \mathbb{Z}$ mit

$$ky \equiv_{\varphi(n)} \operatorname{ind}_r(a).$$

(c) Für jede Primitivwurzel r modulo n gilt

$$\gcd(k, \varphi(n)) \mid \operatorname{ind}_r(a).$$

(d) Es gilt

$$a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv_n 1.$$

Beweis. Es sei eine Primitivwurzel r modulo n gegeben.
Wenn es ein $x \in \mathbb{Z}$ mit $x^k \equiv_n a$ gibt, so gilt auch

$$k \operatorname{ind}_r(x) = \operatorname{ind}_r(x)\, k \equiv_{\varphi(n)} \operatorname{ind}_r(a)$$

nach Bemerkung (4.99). Umgekehrt, wenn es ein $y \in \mathbb{Z}$ mit $ky \equiv_{\varphi(n)} \operatorname{ind}_r(a)$ gibt, so gilt auch

$$(r^k)^y = r^{ky} \equiv_n r^{\operatorname{ind}_r(a)} \equiv_n a.$$

Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (b).
Nach Korollar (4.23) gibt es genau dann ein $y \in \mathbb{Z}$ mit $ky \equiv_{\varphi(n)} \operatorname{ind}_r(a)$, wenn $\gcd(k, \varphi(n)) \mid \operatorname{ind}_r(a)$. Folglich sind auch Bedingung (b) und Bedingung (c) äquivalent.
Schließlich gilt nach Bemerkung (4.99) und Bemerkung (4.97)(b) genau dann

$$a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv_n 1,$$

wenn

$$\operatorname{ind}_r(a)\, \frac{\varphi(n)}{\gcd(k, \varphi(n))} \equiv_{\varphi(n)} 0$$

ist. Nach Bemerkung (4.27) ist diese Bedingung wegen $\frac{\varphi(n)}{\gcd(\frac{\varphi(n)}{\gcd(k,\varphi(n))}, \varphi(n))} = \gcd(k, \varphi(n))$ jedoch äquivalent zu

$$\operatorname{ind}_r(a) \equiv_{\gcd(k,\varphi(n))} 0,$$

d.h. zu $\gcd(k, \varphi(n)) \mid \operatorname{ind}_r(a)$. Dies zeigt die Äquivalenz von Bedingung (d) und Bedingung (c).
Insgesamt sind Bedingung (a), Bedingung (b), Bedingung (c) und Bedingung (d) äquivalent. □

(4.101) Proposition. Es seien $n, k \in \mathbb{N}_0$, eine Primitivwurzel r modulo n sowie $a \in \mathbb{Z}$ mit $a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv_n 1$ gegeben. Ferner sei $y_0 \in \mathbb{Z}$ mit

$$\frac{k}{\gcd(k, \varphi(n))} y_0 \equiv_{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} 1$$

gegeben. Für $x \in \mathbb{Z}$ gilt genau dann

$$x^k \equiv_n a,$$

wenn

$$\operatorname{ind}_r(x) \equiv_{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} y_0 \frac{\operatorname{ind}_r(a)}{\gcd(k, \varphi(n))}$$

ist.

Beweis. Da $a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv_n 1$ gilt, ist insbesondere a eine Einheit modulo n und nach Proposition (c) gilt

$$\gcd(k, \varphi(n)) \mid \operatorname{ind}_r(a).$$

Es sei $x \in \mathbb{Z}$ gegeben. Nach Bemerkung (4.99) gilt genau dann

$$x^k \equiv_n a,$$

wenn x teilerfremd zu n und

$$k \operatorname{ind}_r(x) \equiv_{\varphi(n)} \operatorname{ind}_r(a)$$

ist. Wegen $\frac{k}{\gcd(k,\varphi(n))} y_0 \equiv_{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} 1$ ist dies nach Proposition (4.25) jedoch genau dann der Fall, wenn

$$\operatorname{ind}_r(x) \equiv_{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} y_0 \frac{\operatorname{ind}_r(a)}{\gcd(k, \varphi(n))}$$

gilt. □

(4.102) Beispiel.

(a) Es gibt kein $x \in \mathbb{Z}$ mit $x^4 \equiv_{11} 6$.

(b) Für $x \in \mathbb{Z}$ gilt genau dann $x^4 \equiv_{11} 3$, wenn $x \equiv_{11} 4$ oder $x \equiv_{11} -4$ ist.

Beweis.

(a) Nach Beispiel (4.96) ist 2 eine Primitivwurzel modulo 11 und es ist $\operatorname{ind}_2(6) = 9$. Da $\gcd(4, \varphi(11)) = \gcd(4, 10) = 2$ ist und $2 \nmid 9$ gilt, gibt es nach Proposition (4.100) kein $x \in \mathbb{Z}$ mit $x^4 \equiv_{11} 6$.

(b) Es sei $x \in \mathbb{Z}$ gegeben. Nach Bemerkung (4.99) gilt genau dann $x^4 \equiv_{11} 3$, wenn $4 \operatorname{ind}_2(x) \equiv_{10} \operatorname{ind}_2(3)$ ist. Es ist $\operatorname{ind}_2(3) = 8$ nach Beispiel (4.96). Wegen $\gcd(4, 10) = 2$ ist die Bedingung $4 \operatorname{ind}_2(x) \equiv_{10} 8$ nach Korollar (4.27) äquivalent zur Bedingung $\operatorname{ind}_2(x) \equiv_5 2$. Wegen $\operatorname{ind}_2(x) \in [0, 10]$ gilt dies genau dann der Fall, wenn $\operatorname{ind}_2(x) \in \{2, 7\}$ ist, d.h. genau dann, wenn $x \equiv_{11} 2^2 = 4$ oder $x \equiv_{11} 2^7 \equiv_{11} 7 \equiv_{11} -4$ ist. □

(4.103) Beispiel. Für $x \in \mathbb{Z}$ gilt genau dann $3x^4 + x^3 - 4x^2 + x + 5 \equiv_{11} 0$, wenn $x \equiv_{11} 3$ oder $x \equiv_{11} -5$ ist.

Beweis. Es sei $x \in \mathbb{Z}$ gegeben. Wegen $3 \cdot 4 \equiv_{11} 1$ ist

$$\begin{aligned} 3x^4 + x^3 - 4x^2 + x + 5 &\equiv_{11} 3(x^4 + 4x^3 - 4 \cdot 4x^2 + 4x + 4 \cdot 5) \equiv_{11} 3(x^4 + 4x^3 + 6x^2 + 4x + 9) \\ &= 3(x^4 + 4x^3 + 6x^2 + 4x + 1 + 8) = 3((x+1)^4 + 8) \equiv_{11} 3((x+1)^4 - 3). \end{aligned}$$

Somit gilt genau dann $3x^4 + x^3 - 4x^2 + x + 5 \equiv_{11} 0$, wenn $(x+1)^4 \equiv_{11} 3$ ist. Nach Beispiel (b) ist dies jedoch äquivalent zu $x + 1 \equiv_{11} 4$ oder $x + 1 \equiv_{11} -4$, d.h. zu $x \equiv_{11} 3$ oder $x \equiv_{11} -5$. □

Anwendung: Diffie-Hellman-Schlüsselaustausch

Es seien $p \in \mathbb{P}$, eine Primitivwurzel r modulo p und ein $a \in [1, p-1]$ gegeben. Eine naive Methode, um den Index $\operatorname{ind}_r(a)$ zu berechnen, ist die Berechnung aller Potenzen r^k für $k \in [1, p-1]$. Wenn p groß genug ist, dauert dies zu lange, man spricht vom *DL-Problem* (diskreter Logarithmus) für p.
Im Allgemeinen ist kein wesentlich effizienterer Algorithmus zur Berechnung der Indizes bekannt, d.h. das DL-Problem kann für eine sorgfältig ausgewählte Primzahl p nicht in vertretbarer Zeit gelöst werden. Auf dieser Problematik beruht ein Verfahren aus der Kryptographie, welches wir im Folgenden diskutieren wollen. Das Verfahren dient zur Konstruktion eines gemeinsamen Schlüssels zur Verwendung in einem symmetrischen Kryptosystem, wie etwa das in Anwendung (4.77).

(4.104) Anwendung (Diffie-Hellman-Schlüsselaustausch; Diffie, Hellman, Merkle; 1976)**.**

- Initialisierung:
  - Wähle geeignete große Primzahl p (so, dass das DL-Problem für p nicht lösbar ist) und eine Primitivwurzel $r \in [1, p-1]$ modulo p.

- Austausch von Informationen:
  - Benutzer A wählt $k \in [0, p-2]$, berechnet $a := r^k \bmod p$ und sendet a an Benutzer B.
  - Benutzer B wählt $l \in [0, p-2]$, berechnet $b := r^l \bmod p$ und sendet b an Benutzer A.
- Generierung des Schlüssels $K := r^{kl} \bmod p$:
  - Benutzer A berechnet $b^k \bmod p = K$.
  - Benutzer B berechnet $a^l \bmod p = K$.
- Beispiel:
  - Wir wählen $p = 11$ und $r = 2$.
  - Benutzer A wählt $k = 5$ und sendet $a = r^k \bmod p = 2^5 \bmod 11 = 10$ an Benutzer B. Dieser wählt $l = 7$ und sendet $b = r^l \bmod p = 2^7 \bmod 11 = 7$ an Benutzer A.
  - Benutzer A berechnet

$$K = b^k \bmod p = 7^5 \bmod 11 = ((7^2)^2 \cdot 7) \bmod 11 = (49^2 \cdot 7) \bmod 11 = (5^2 \cdot 7) \bmod 11$$
$$= (25 \cdot 7) \bmod 11 = (3 \cdot 7) \bmod 11 = 21 \bmod 11 = 10.$$

    Benutzer B berechnet

$$K = a^l \bmod p = 10^7 \bmod 11 = (-1)^7 \bmod 11 = (-1) \bmod 11 = 10.$$

Anwendung: Elgamal-Kryptosystem

Die Idee des Diffie-Hellman-Schlüsselaustauschs (4.104) lässt sich auch im Public-Key-Kryptosystem in Anwendung (4.106) wiederfinden, welches auf folgender Beobachtung beruht:

(4.105) Bemerkung. Es seien $p \in \mathbb{P}$, eine Primitivwurzel r modulo p und ein $k \in \mathbb{N}_0$ gegeben. Für $l \in \mathbb{N}_0$ und

$$e_l \colon \mathbb{F}_p \to \mathbb{F}_p \times \mathbb{F}_p,\ [x] \mapsto ([r^l], [(r^k)^l][x]),$$
$$d \colon \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p,\ ([y_1], [y_2]) \mapsto [y_1]^{-k}\,[y_2]$$

gilt

$$d \circ e_l = \mathrm{id}_{\mathbb{F}_p}.$$

Beweis. Es sei $l \in \mathbb{N}_0$ gegeben. Für $x \in \mathbb{Z}$ gilt dann

$$d(e_l([x])) = d([r^l], [(r^k)^l][x]) = d([r^l], [(r^k)^l\, x]) = [r^l]^{-k}\,[(r^k)^l\, x] = [x].$$

Somit ist $d \circ e_l = \mathrm{id}_{\mathbb{F}_p}$. □

(4.106) Anwendung (Elgamal-Kryptosystem)**.**

- Initialisierung:
  - Wähle geeignete große Primzahl p (so, dass das DL-Problem für p nicht lösbar ist), eine Primitivwurzel $r \in [1, p-1]$ modulo p und ein $k \in [0, p-2]$.
  - Berechne $a := r^k \bmod p$.
  - Publiziere den öffentlichen Schlüssel $K_{\text{open}} := (p, r, a)$ (zum Beispiel auf persönlicher Homepage).
  - Halte den privaten Schlüssel $K_{\text{priv}} := k$ geheim.
  - Die Menge der Klartexte ist $\mathcal{P} := [0, p-1]$. Die Menge der Geheimtexte ist $\mathcal{C} := [0, p-1] \times [0, p-1]$.
- Verschlüsselung eines Klartexts $x \in \mathcal{P}$:
  - Wähle zufällig $l \in [0, p-2]$.

  - Berechne

$$e_l(x) = (r^l \bmod p, a^l\, x \bmod p).$$

- Entschlüsselung eines Geheimtexts $(y_1, y_2) \in \mathcal{C}$:
  - Berechne $z \in \mathbb{Z}$ mit z invers zu y_1^k modulo p.
  - Berechne

$$d(y_1, y_2) = zy_2 \bmod p.$$

- Beispiel:
  - Wir wählen $p = 2579$, $r = 2$, $k = 765$. Dann ist $a = r^k \bmod p = 2^{765} \bmod 2579 = 949$. Der öffentliche Schlüssel ist

$$K_{\text{open}} = (p, r, a) = (2579, 2, 949).$$

    Der private Schlüssel ist

$$K_{\text{priv}} = k = 765.$$

    Die Menge der Klartexte ist

$$\mathcal{P} = [0, p-1] = [0, 2578].$$

    Die Menge der Geheimtexte ist

$$\mathcal{C} = [0, p-1] \times [0, p-1] = [0, 2578] \times [0, 2578].$$

  - Die Verschlüsselung des Klartexts $x = 1299$ für $l = 853$ ergibt

$$e_l(x) = (r^l \bmod p, a^l\, x \bmod p) = (2^{853} \bmod 2579, 949^{853} \cdot 1299 \bmod 2579) = (435, 2396).$$

  - Die Entschlüsselung des Geheimtexts $(y_1, y_2) = (435, 2396)$ ergibt sich wie folgt: Es ist

$$435^{765} \cdot 1980 \equiv_{2579} 1,$$

    also $z = 1980$. Wir erhalten

$$d(y_1, y_2) = zy_2 \bmod p = 1980 \cdot 2396 \bmod 2579 = 1299.$$

Aufgaben

Aufgabe 50 (schnelle modulare Exponentiation)**.** Entwerfen Sie einen praktikablen Algorithmus zur Berechnung der diskreten Exponentiation unter Einhaltung der nachfolgenden Vorgaben und implementieren Sie diesen in Magma.

- Eingabe: $(a, k, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$
- Ausgabe: $b \in [0, n-1]$ mit $b \equiv_n \exp_{[a]}(k)$
- Verfahren: Das Programm soll $\exp_{[a]}(k)$ aus $\exp_{[a]}(2^i)$ für geignete $i \in \mathbb{N}_0$ und der Binärdarstellung von k berechnen.

Hinweis. Benutzen Sie zur Berechnung der Binärdarstellung zum Beispiel Ihr Programm aus Aufgabe 15.

Aufgabe 51 (Indexberechnung)**.** Entwerfen Sie einen Algorithmus zur Berechnung der Indizes bezüglich einer Primitivwurzel unter Einhaltung der nachfolgenden Vorgaben und implementieren Sie diesen in Magma.

- Eingabe: $(r, p) \in \mathbb{N} \times \mathbb{P}$ mit $r < p - 1$

- Ausgabe: $(\mathrm{ind}_r(a))_{a\in[1,p-1]}$ oder `false`
- Verfahren: Das Programm soll nacheinander alle möglichen Exponenten k betrachten und hierfür die zugehörige Potenz $a := r^k \bmod p$ berechnen. Sofern sich herausstellt, dass r keine Primitivwurzel modulo p ist, soll `false` ausgegeben werden. Andernfalls soll das Programm k an die Stelle a einer Liste schreiben und diese am Ende ausgeben.

Aufgabe 52 (monomiale Kongruenzgleichungen)**.**

(a) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$16x^{12} \equiv_{19} 55.$$

(b) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$2x^{8} \equiv_{23} 11.$$

(c) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$x^4 \equiv_7 4,$$
$$x^7 \equiv_{11} 3.$$

(d) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$x^7 \equiv_{10403} 20.$$

Hinweis. Für Potenz- und Indexberechnungen dürfen Sie Ihre Programme aus Aufgabe 50 benutzen.

Aufgabe 53 (Angriff auf RSA)**.** Es seien $n \in \mathbb{N}$ mit $n \geq 2$ sowie $x, y \in \mathbb{N}$ mit $x^2 \equiv_n y^2$, $x \not\equiv_n y$, $x \not\equiv_n -y$ gegeben. Zeigen Sie, dass $\gcd(x+y, n), \gcd(x-y, n) \in [2, n-1]$ gilt.

Aufgabe 54 (Elgamal-Kryptosysteme)**.** In einem Elgamal-Kryptosystem sei der öffentliche Schlüssel durch $K_{\text{open}} = (p, r, a) = (53, 2, 30)$ gegeben. Wie lautet der Klartext zum Geheimtext $(y_1, y_2) = (24, 37)$?

5 Modulare Quadrate und quadratische Reziprozität

Modulare Quadrate

(4.107) Definition ((invertierbares) modulares Quadrat)**.** Es seien $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ gegeben.

(a) Wir sagen, dass a ein *Quadrat modulo* n ist, falls a ein Quadrat in $\mathbb{Z}/n$ ist.

(b) Wir sagen, dass a ein *invertierbares Quadrat modulo* n ist, falls a ein Quadrat in $(\mathbb{Z}/n)^\times$ ist.

(4.108) Bemerkung. Es seien $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ gegeben.

(a) Genau dann ist a ein Quadrat modulo n, wenn ein $x \in \mathbb{Z}$ mit $a \equiv_n x^2$ existiert.

(b) Genau dann ist a ein invertierbares Quadrat modulo n, wenn ein modulo n invertierbares $x \in \mathbb{Z}$ mit $a \equiv_n x^2$ existiert.

Beweis.

(b) Es sei zunächst a ein invertierbares Quadrat modulo n. Dann ist a ein Quadrat in $(\mathbb{Z}/n)^\times$, d.h. es ist a eine Einheit modulo n und es existiert ein $x \in \mathbb{Z}$ mit $a \equiv_n x^2$. Es folgt $[a] = [x^2] = [x]^2$ und somit $[x]\,[x]\,[a]^{-1} = 1$ in $\mathbb{Z}/n$. Folglich ist $[x]$ invertierbar in $\mathbb{Z}/n$ mit $[x]^{-1} = [x]\,[a]^{-1}$ und damit x eine Einheit modulo n.

Ist umgekehrt $a \equiv_n x^2$ für eine Einheit x modulo n, so ist a ein Quadrat modulo n und eine Einheit modulo n, also ein invertierbares Quadrat modulo n. □

Eine Operation auf den absolut kleinsten Repräsentanten

Für ungerades $n \in \mathbb{N}$ betrachten wir im Folgenden die Transversale $[-\frac{n-1}{2}, \frac{n-1}{2}]$ von $\mathbb{Z}/n$.

(4.109) Notation. Es sei ein ungerades $n \in \mathbb{N}$ gegeben. Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$ und $\alpha \in (\mathbb{Z}/n)^\times$ bezeichnen wir mit $i\alpha$ das eindeutige $j \in [-\frac{n-1}{2}, \frac{n-1}{2}]$ mit $[i]\alpha = [j]$.

(4.110) Bemerkung. Es sei ein ungerades $n \in \mathbb{N}$ gegeben.

(a) Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$, $\alpha, \beta \in (\mathbb{Z}/n)^\times$ gilt

$$i(\alpha\beta) = (i\alpha)\beta.$$

(b) Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$ gilt

$$i1^{(\mathbb{Z}/n)^\times} = i.$$

(c) Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$, $\alpha \in (\mathbb{Z}/n)^\times$ gilt

$$(-i)\alpha = -(i\alpha).$$

(4.111) Proposition. Es seien ein ungerades $n \in \mathbb{N}$ und eine Einheit a modulo n gegeben. Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$ gilt

$$i[a]_n = ia - n\lfloor \frac{ia}{n} + \frac{1}{2} \rfloor.$$

Beweis. Für $i \in [-\frac{n-1}{2}, \frac{n-1}{2}]$ gilt $ia = n(ia \operatorname{div} n) + (ia \bmod n)$ und damit

$$\begin{aligned} i[a]_n &= \left.\begin{cases} ia \bmod n, & \text{falls } ia \bmod n \le \frac{n-1}{2}, \\ (ia \bmod n) - n, & \text{falls } ia \bmod n \ge \frac{n+1}{2} \end{cases}\right\} = \left\{\begin{array}{ll} ia - n(ia \operatorname{div} n), & \text{falls } ia \bmod n \le \frac{n-1}{2}, \\ ia - n(ia \operatorname{div} n) - n, & \text{falls } ia \bmod n \ge \frac{n+1}{2} \end{array}\right\} \\ &= \left.\begin{cases} ia - n(ia \operatorname{div} n), & \text{falls } ia \bmod n \le \frac{n-1}{2}, \\ ia - n((ia \operatorname{div} n) + 1), & \text{falls } ia \bmod n \ge \frac{n+1}{2} \end{cases}\right\} = ia - n\lfloor ia \operatorname{div} n + \frac{ia \bmod n}{n} + \frac{1}{2} \rfloor \\ &= ia - n\lfloor \frac{ia}{n} + \frac{1}{2} \rfloor. \end{aligned}$$

□

Kronecker-Signum

(4.112) Definition (Fehlstand)**.** Es seien ein ungerades $n \in \mathbb{N}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Ein $i \in [1, \frac{n-1}{2}]$ heißt *Fehlstand* (oder *Inversionsrest*) von α, falls $i\alpha \in [-\frac{n-1}{2}, -1]$ ist.
Die *Menge aller Fehlstände* von α bezeichnen wir mit

$$\operatorname{Inv}(\alpha) = \operatorname{Inv}_n(\alpha) := \{i \in [1, \frac{n-1}{2}] \mid i\alpha \in [-\frac{n-1}{2}, -1]\}.$$

(4.113) Beispiel. Es ist

$$\begin{aligned} &\operatorname{Inv}_7([1]) = \emptyset, \\ &\operatorname{Inv}_7([2]) = \{2, 3\}, \\ &\operatorname{Inv}_7([3]) = \{2\}, \\ &\operatorname{Inv}_7([4]) = \{1, 3\}, \\ &\operatorname{Inv}_7([5]) = \{1\}, \\ &\operatorname{Inv}_7([6]) = \{1, 2, 3\}. \end{aligned}$$

(4.114) Definition (Kronecker-Signum)**.** Es seien ein ungerades $n \in \mathbb{N}$ und $\alpha \in (\mathbb{Z}/n)^\times$ gegeben. Das *Kronecker-Signum* (oder *Signum*) von α modulo n ist definiert als

$$\varepsilon(\alpha) = \varepsilon_n(\alpha) := (-1)^{|\operatorname{Inv}_n(\alpha)|}.$$

(4.115) Beispiel. Es ist

$$\varepsilon_7([1]) = \varepsilon_7([2]) = \varepsilon_7([4]) = 1,$$
$$\varepsilon_7([3]) = \varepsilon_7([5]) = \varepsilon_7([6]) = -1.$$

Beweis. Nach Beispiel (4.113) ist

$$\varepsilon([1]) = (-1)^{|\mathrm{Inv}([1])|} = (-1)^0 = 1,$$
$$\varepsilon([2]) = (-1)^{|\mathrm{Inv}([2])|} = (-1)^2 = 1,$$
$$\varepsilon([3]) = (-1)^{|\mathrm{Inv}([3])|} = (-1)^1 = -1,$$
$$\varepsilon([4]) = (-1)^{|\mathrm{Inv}([4])|} = (-1)^2 = 1,$$
$$\varepsilon([5]) = (-1)^{|\mathrm{Inv}([5])|} = (-1)^1 = -1,$$
$$\varepsilon([6]) = (-1)^{|\mathrm{Inv}([6])|} = (-1)^3 = -1. \qquad \square$$

(4.116) Bemerkung. Es sei ein ungerades $n \in \mathbb{N}$ gegeben. Für $\alpha \in (\mathbb{Z}/n)^\times$ ist

$$\varepsilon_n(\alpha) = \prod_{i \in [1, \frac{n-1}{2}]} (-1)^{\chi_{\mathrm{Inv}_n(\alpha)}(i)} = \prod_{i \in [1, \frac{n-1}{2}]} \mathrm{sgn}(i\alpha).$$

Beweis. Wegen $\alpha \in (\mathbb{Z}/n)^\times$ ist $i\alpha \neq 0$ für alle $i \in [1, \frac{n-1}{2}]$. Es folgt

$$\chi_{\mathrm{Inv}(\alpha)}(i) = \left.\begin{cases} 1 & \text{falls } i \in \mathrm{Inv}(\alpha), \\ 0 & \text{falls } i \notin \mathrm{Inv}(\alpha) \end{cases}\right\} = \begin{cases} 1 & \text{falls } i\alpha \in [-\frac{n-1}{2}, -1], \\ 0 & \text{falls } i\alpha \in [1, \frac{n-1}{2}] \end{cases}$$

und damit

$$(-1)^{\chi_{\mathrm{Inv}(\alpha)}(i)} = \left.\begin{cases} (-1)^1 & \text{falls } i\alpha \in [-\frac{n-1}{2}, -1], \\ (-1)^0 & \text{falls } i\alpha \in [1, \frac{n-1}{2}] \end{cases}\right\} = \left.\begin{cases} -1 & \text{falls } i\alpha \in [-\frac{n-1}{2}, -1], \\ 1 & \text{falls } i\alpha \in [1, \frac{n-1}{2}] \end{cases}\right\} = \mathrm{sgn}(i\alpha)$$

für $i \in [1, \frac{n-1}{2}]$. Wir erhalten

$$\prod_{i \in [1, \frac{n-1}{2}]} \mathrm{sgn}(i\alpha) = \prod_{i \in [1, \frac{n-1}{2}]} (-1)^{\chi_{\mathrm{Inv}(\alpha)}(i)} = \prod_{\substack{i \in [1, \frac{n-1}{2}] \\ i\alpha \in [1, \frac{n-1}{2}]}} (-1)^{\chi_{\mathrm{Inv}(\alpha)}(i)} \prod_{\substack{i \in [1, \frac{n-1}{2}] \\ i\alpha \in [-\frac{n-1}{2}, -1]}} (-1)^{\chi_{\mathrm{Inv}(\alpha)}(i)}$$
$$= \prod_{\substack{i \in [1, \frac{n-1}{2}] \\ i\alpha \in [1, \frac{n-1}{2}]}} (-1)^0 \prod_{\substack{i \in [1, \frac{n-1}{2}] \\ i\alpha \in [-\frac{n-1}{2}, -1]}} (-1)^1 = \prod_{i \in \mathrm{Inv}(\alpha)} (-1) = (-1)^{|\mathrm{Inv}(\alpha)|}. \qquad \square$$

(4.117) Korollar. Es seien ein ungerades $n \in \mathbb{N}$ und eine Einheit a modulo n gegeben. Dann gilt

$$\varepsilon_n([a]_n) = \prod_{j \in [1, \frac{n-1}{2}]} \mathrm{sgn}(a\frac{j}{n} - \lfloor a\frac{j}{n} + \frac{1}{2} \rfloor).$$

Beweis. Nach Bemerkung (4.116) und Proposition (4.111) gilt

$$\varepsilon_n([a]) = \prod_{j \in [1, \frac{n-1}{2}]} \mathrm{sgn}(j[a]) = \prod_{j \in [1, \frac{n-1}{2}]} \mathrm{sgn}(ja - n\lfloor \frac{ja}{n} + \frac{1}{2} \rfloor) = \prod_{j \in [1, \frac{n-1}{2}]} \mathrm{sgn}(a\frac{j}{n} - \lfloor a\frac{j}{n} + \frac{1}{2} \rfloor). \qquad \square$$

Für theoretische Zwecke sind die Formeln für das Signum aus Definition (4.114) und Bemerkung (4.116) etwas schwerfällig, weswegen wir nun eine geeignetere Darstellung herleiten wollen.

(4.118) Proposition. Es sei ein ungerades $n \in \mathbb{N}$ gegeben und es sei

$$X := \{i \in [-\frac{n-1}{2}, \frac{n-1}{2}] \mid i \neq 0\}.$$

Für $i, i' \in X$ gelte genau dann $i \; c \; i'$, wenn $|i| = |i'|$ ist.

(a) Es ist c eine Äquivalenzrelation auf X.

(b) Für $i \in X$ ist

$$[i]_c = \{i, -i\}.$$

(c) Es ist

$$[1, \frac{n-1}{2}]$$

eine Transversale von X bzgl. c.

(d) Es seien Transversalen T und T' von X bzgl. c und ein kommutatives Monoid M gegeben. Für jede Abbildung $f\colon X \to M$ mit $f(i) = f(-i)$ für alle $i \in X$ gilt

$$\prod_{i \in T} f(i) = \prod_{i' \in T'} f(i').$$

Nun sei ferner $\alpha \in (\mathbb{Z}/n)^\times$ und eine Transversale T von X bzgl. c gegeben.

(e) Es ist

$$\{i\alpha \mid i \in T\}$$

eine Transversale von X bzgl. c.

(f) Es sei $T_0 := [1, \frac{n-1}{2}]$. Dann gilt

$$\varepsilon_n(\alpha) = \prod_{i \in T} (-1)^{\chi_{T_0}(i) + \chi_{T_0}(i\alpha)}.$$

(g) Es ist

$$\varepsilon_n(\alpha) = \prod_{i \in T} (-1)^{1 - \chi_T(i\alpha)}.$$

Beweis. Es sei $a\colon X \to \mathbb{N}$, $i \mapsto |i|$.

(a) Es ist c die Bildgleichheitsrelation bzgl. a und damit eine Äquivalenzrelation.

(b) Für $i \in X$ ist

$$[i]_c = a^{-1}(\{a(i)\}) = a^{-1}(\{|i|\}) = \{i, -i\}.$$

(c) Es sei $T_0 := [1, \frac{n-1}{2}]$. Da für alle $i \in X$ entweder $i > 0$ oder $i < 0$ gilt, ist $\mathrm{quo}|_{T_0}\colon T_0 \to X/c$ nach (b) eine Bijektion und damit T_0 eine Transversale von X bzgl. c.

(d) Es sei eine Abbildung $f\colon X \to M$ mit $f(i) = f(-i)$ für alle $i \in X$ gegeben. Nach (b) gibt es eine eindeutige Abbildung $\bar{f}\colon X/c \to M$ mit $f = \bar{f} \circ \mathrm{quo}$, gegeben durch $\bar{f}([i]) = f(i)$ für $i \in X$. Insbesondere haben wir also

$$\prod_{i \in T} f(i) = \prod_{i \in T} \bar{f}([i]) = \prod_{K \in X/c} \bar{f}(K) = \prod_{i' \in T'} \bar{f}([i']) = \prod_{i' \in T'} f(s').$$

(e) Es sei $T' := \{i\alpha \mid i \in T\}$. Ferner sei $i \in X$ beliebig gegeben. Dann ist $[i\alpha^{-1}] = \{i\alpha^{-1}, -(i\alpha^{-1})\}$ nach (b). Da T Transversale ist, gilt entweder $i\alpha^{-1} \in T$ oder $(-i)\alpha^{-1} = -(i\alpha^{-1}) \in T$. Im ersten Fall ist dann aber $i \in T'$, im zweiten ist $-i \in T'$. Folglich ist entweder $i \in T'$ oder $-i \in T'$. Da $i \in X$ beliebig war und $[i] = \{i, -i\}$ für alle $i \in X$ gilt, ist T' somit eine Transversale von X bzgl. c.

(f) Es sei $T_0 := [1, \frac{n-1}{2}]$. Ein Vertreter $i \in T_0$ ist genau dann ein Fehlstand von α, wenn $i\alpha \notin T_0$ ist. Nach Bemerkung (4.116) erhalten wir somit

$$\varepsilon(\alpha) = \prod_{i \in [1, \frac{n-1}{2}]} (-1)^{\chi_{\mathrm{Inv}_n(\alpha)}(i)} = \prod_{i \in T_0} (-1)^{1-\chi_{T_0}(i\alpha)} = \prod_{i \in T_0} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)}.$$

Wegen

$$(-1)^{\chi_{T_0}(-i)+\chi_{T_0}((-i)\alpha)} = (-1)^{\chi_{T_0}(-i)+\chi_{T_0}(-(i\alpha))} = (-1)^{1-\chi_{T_0}(i)+1-\chi_{T_0}(i\alpha)} = (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)}$$

für $i \in X$ folgt

$$\varepsilon(\alpha) = \prod_{i \in T_0} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)} = \prod_{i \in T} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)}.$$

nach (d).

(g) Es sei $T_0 := [1, \frac{n-1}{2}]$ und $T' := \{i\alpha \mid i \in T\}$. Dann ist T_0 eine Transversale von X bzgl. c nach (c) und T' eine Transversale von X bzgl. c nach (e).

Wegen

$$(-1)^{\chi_{T_0}(-i)+\chi_T(-i)} = (-1)^{1-\chi_{T_0}(i)+1-\chi_T(i)} = (-1)^{\chi_{T_0}(i)+\chi_T(i)}$$

für $i \in X$ folgt

$$\prod_{i \in T} (-1)^{\chi_{T_0}(i)+\chi_T(i)} = \prod_{i' \in T'} (-1)^{\chi_{T_0}(i')+\chi_T(i')} = \prod_{i \in T} (-1)^{\chi_{T_0}(i\alpha)+\chi_T(i\alpha)}$$

nach (d) und damit

$$\varepsilon_n(\alpha) = \prod_{i \in T} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)} = \prod_{i \in T} (-1)^{\chi_T(i)+\chi_T(i\alpha)} = \prod_{i \in T} (-1)^{1-\chi_T(i\alpha)}$$

nach (f). □

Proposition (4.111) liefert uns eine Formel für das Kronecker-Signum, welche jedoch nicht für explizite Rechnungen geeignet ist.

(4.119) Korollar. Für alle ungeraden $n \in \mathbb{N}$ ist

$$\varepsilon_n \colon (\mathbb{Z}/n)^\times \to \mathbb{Z}^\times$$

ein Gruppenhomomorphismus.

Beweis. Es seien ein ungerades $n \in \mathbb{N}$ und $\alpha, \beta \in (\mathbb{Z}/n)^\times$ gegeben. Wir setzen $X := \{i \in [-\frac{n-1}{2}, \frac{n-1}{2}] \mid i \neq 0\}$. Für $i, i' \in X$ gelte genau dann $i \; c \; i'$, wenn $|i| = |i'|$ ist. Nach Proposition (4.118)(a) ist c eine Äquivalenzrelation auf X. Ferner ist $T_0 := [1, \frac{n-1}{2}]$ nach Proposition (4.118)(c) eine Transversale von X bzgl. c, und nach Proposition (4.118)(e) ist $T_0' := \{i\alpha \mid i \in T_0\}$ eine Transversale von X bzgl. c. Mit Proposition (4.118)(f) folgt

$$\begin{aligned}
\varepsilon(\alpha \circ \beta) &= \prod_{i \in T_0} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha\beta)} = \prod_{i \in T_0} ((-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)} (-1)^{\chi_{T_0}(i\alpha)+\chi_{T_0}(i\alpha\beta)}) \\
&= (\prod_{i \in T_0} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)}) (\prod_{i \in T_0} (-1)^{\chi_{T_0}(i\alpha)+\chi_{T_0}(i\alpha\beta)}) \\
&= (\prod_{i \in T_0} (-1)^{\chi_{T_0}(i)+\chi_{T_0}(i\alpha)}) (\prod_{i' \in T_0'} (-1)^{\chi_{T_0}(i')+\chi_{T_0}(i'\beta)}) = \varepsilon(\alpha)\, \varepsilon(\beta).
\end{aligned}$$

Folglich ist $\varepsilon \colon (\mathbb{Z}/n)^\times \to \mathbb{Z}^\times$ ein Gruppenhomomorphismus. □

Wir studieren das Kronecker-Signum modulo einer ungeraden Primzahl:

(4.120) Proposition. Es sei eine ungerade Primzahl p gegeben.

(a) Es sei eine Primitivwurzel r modulo p gegeben. Für $i \in \mathbb{Z}$ ist

$$\varepsilon_p([r]^i) = (-1)^i.$$

(b) Es ist $\varepsilon_p \colon \mathbb{F}_p^\times \to \mathbb{Z}^\times$ ein surjektiver Gruppenhomomorphismus.

(c) Es sei ein surjektiver Gruppenhomomorphismus $\varphi \colon \mathbb{F}_p^\times \to \mathbb{Z}^\times$ gegeben. Dann ist $\varphi = \varepsilon_p$.

(d) Es ist

$$\operatorname{Ker} \varepsilon_p = \{\alpha^2 \mid \alpha \in \mathbb{F}_p^\times\}.$$

Beweis.

(a) Wir setzen $X := \{i \in [-\frac{n-1}{2}, \frac{n-1}{2}] \mid i \neq 0\}$. Für $i, i' \in X$ gelte genau dann $i \; c \; i'$, wenn $|i| = |i'|$ ist. Nach Proposition (4.118)(a) ist c eine Äquivalenzrelation auf X. Da $\operatorname{ord}[r] = \varphi(p) = p - 1$ in $\mathbb{F}_p^\times$ ist, haben wir $r^{\frac{p-1}{2}} \equiv_p -1$. Folglich ist $T := \{1[r]^i \mid i \in [1, \frac{p-1}{2}]\}$ eine Transversale von X bzgl. c. Nach Proposition (4.118)(g) erhalten wir

$$\varepsilon([r]) = \prod_{j \in T} (-1)^{1-\chi_T(j[r])} = \prod_{i \in [1, \frac{p-1}{2}]} (-1)^{1-\chi_T((1[r]^i)[r])} = \prod_{i \in [1, \frac{p-1}{2}]} (-1)^{1-\chi_T(1[r]^{i+1})}$$

$$= (-1)^{1-\chi_T(1[r]^{\frac{p-1}{2}+1})} = -1.$$

Da $\varepsilon \colon \mathbb{F}_p^\times \to \mathbb{Z}^\times$ nach Korollar (4.119) ein Gruppenhomomorphismus ist, folgt $\varepsilon([r]^i) = (-1)^i$ für $i \in \mathbb{Z}$.

Nach Korollar (4.91) gibt es eine Primitivwurzel r modulo p, so dass $\mathbb{F}_p^\times = \langle [r] \rangle$ ist.

(b) Nach (a) gilt $\varepsilon([r]^i) = (-1)^i$ für $i \in \mathbb{Z}$. Insbesondere ist $\operatorname{Im} \varepsilon = \mathbb{Z}^\times$, also ε surjektiv.

(c) Wegen der Surjektivität von φ ist $\operatorname{Im} \varphi = \mathbb{Z}^\times = \{1, -1\}$ und $\varphi([r]) \neq 1$. Folglich muss $\varphi([r]) = -1$ gelten. Dies impliziert aber bereits

$$\varphi([r]^i) = \varphi([r])^i = (-1)^i = \varepsilon([r]^i)$$

für $i \in \mathbb{Z}$ nach (a) und somit $\varphi = \varepsilon$.

(d) Es ist

$$\operatorname{Ker} \varepsilon = \{\beta \in \mathbb{F}_p^\times \mid \varepsilon(\beta) = 1\} = \{[r]^j \mid j \in \mathbb{Z} \text{ mit } \varepsilon([r]^j) = 1\} = \{[r]^j \mid j \in \mathbb{Z} \text{ mit } (-1)^j = 1\}$$
$$= \{[r]^{2i} \mid i \in \mathbb{Z}\} = \{\alpha^2 \mid \alpha \in \mathbb{F}_p^\times\}.$$ □

Legendre-Jacobi-Symbol

(4.121) Definition (Legendre-Jacobi-Symbol)**.** Es seien ein ungerades $n \in \mathbb{N}$ und ein $a \in \mathbb{Z}$ gegeben. Das *Legendre-Jacobi-Symbol* ([1]) von a und n, gesprochen a über n, ist definiert als

$$\left(\frac{a}{n}\right) := \begin{cases} \varepsilon_n([a]_n), & \text{falls } a \text{ teilerfremd zu } n, \\ 0, & \text{falls } a \text{ nicht teilerfremd zu } n. \end{cases}$$

(4.122) Beispiel. Es ist

$$\left(\frac{0}{7}\right) = 0,$$
$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,$$
$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

[1] In der Literatur wird das Legendre-Jacobi-Symbol für (allgemeines) ungerades $n \in \mathbb{N}$ meistens als *Jacobi-Symbol* bezeichnet. Ist n sogar eine ungerade Primzahl, so spricht man vom *Legendre-Symbol*. Mit dieser Terminologie ist das Legendre-Symbol also ein Spezialfall des Jacobi-Symbols.

Beweis. Dies folgt aus Beispiel (4.115). □

(4.123) Bemerkung. Es sei ein ungerades $n \in \mathbb{N}$ gegeben. Dann ist

$$\left(\frac{-}{n}\right) : \mathbb{Z} \to \mathbb{Z}$$

ein Monoidhomomorphismus (bzgl. der gewöhnlichen Multiplikation auf $\mathbb{Z}$).

Beweis. Da $\varepsilon\colon (\mathbb{Z}/n)^\times \to \mathbb{Z}^\times$ nach Korollar (4.119) ein Gruppenhomomorphismus ist, gilt

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \left\{\begin{matrix}\varepsilon([ab]), & \text{falls } ab \text{ teilerfremd zu } n,\\ 0, & \text{sonst}\end{matrix}\right\} = \left\{\begin{matrix}\varepsilon([a])\,\varepsilon([b]), & \text{falls } a \text{ und } b \text{ teilerfremd zu } n,\\ 0, & \text{sonst}\end{matrix}\right\}\\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

für $a, b \in \mathbb{Z}$ sowie

$$\left(\frac{1}{n}\right) = \varepsilon([1]) = \varepsilon(1) = 1.$$

Folglich ist $\left(\frac{-}{n}\right) : \mathbb{Z} \to \mathbb{Z}$ ein Monoidhomomorphismus. □

(4.124) Bemerkung. Es seien ein ungerades $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ gegeben. Wenn $a \equiv_n b$ ist, so gilt

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

Beweis. Nach Korollar (2.50) ist a genau dann teilerfremd zu n, wenn b teilerfremd zu n ist. Folglich gilt

$$\left(\frac{a}{n}\right) = \left\{\begin{matrix}\varepsilon([a]), & \text{falls } a \text{ teilerfremd zu } n,\\ 0, & \text{falls } a \text{ nicht teilerfremd zu } n\end{matrix}\right\} = \left\{\begin{matrix}\varepsilon([b]), & \text{falls } b \text{ teilerfremd zu } n,\\ 0, & \text{falls } b \text{ nicht teilerfremd zu } n\end{matrix}\right\} = \left(\frac{b}{n}\right)$$

nach Korollar (4.17)(b). □

(4.125) Proposition. Es seien ein ungerades $p \in \mathbb{P}$ und ein $a \in \mathbb{Z}$ gegeben. Genau dann ist a ein invertierbares Quadrat modulo p, wenn

$$\left(\frac{a}{p}\right) = 1$$

ist.

Beweis. Nach Proposition (4.120)(d) ist $\operatorname{Ker}\varepsilon_p = \{\alpha^2 \mid \alpha \in \mathbb{F}_p^\times\}$. Somit ist a genau dann ein invertierbares Quadrat modulo p, wenn $[a] \in \operatorname{Ker}\varepsilon$ ist. Nach Definition (4.121) ist dies aber genau dann der Fall, wenn

$$\left(\frac{a}{p}\right) = 1$$

gilt. □

(4.126) Beispiel. Es sind 1, 2 und 4 invertierbare Quadrate modulo 7. Es sind 3, 5 und 6 keine Quadrate modulo 7.

Beweis. Dies folgt aus Beispiel (4.122). □

(4.127) Proposition (Euler-Kriterium)**.** Es sei ein ungerades $p \in \mathbb{P}$ gegeben. Für $a \in \mathbb{Z}$ gilt

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}.$$

Beweis. Es sei $a \in \mathbb{Z}$ gegeben. Wenn p ein Teiler von a ist, so gilt

$$\left(\frac{a}{p}\right) = 0 \equiv_p a^{\frac{p-1}{2}}.$$

Es gelte also im Folgenden $p \nmid a$, so dass a eine Einheit modulo p ist. Nach Korollar (4.91) gibt es eine Primitivwurzel r modulo p. Für diese gilt $\operatorname{ord}[r] = \varphi(p) = p-1$, also $[r^{\frac{p-1}{2}}] = [r]^{\frac{p-1}{2}} = [-1]$ in $\mathbb{F}_p^\times$ und damit $r^{\frac{p-1}{2}} \equiv_p -1$. Nach Bemerkung (4.124) und Proposition (4.120)(a) folgt

$$\left(\frac{a}{p}\right) = \varepsilon([a]) = \varepsilon([r^{\operatorname{ind}_r(a)}]) = \varepsilon([r]^{\operatorname{ind}_r(a)}) = (-1)^{\operatorname{ind}_r(a)} \equiv_p (r^{\frac{p-1}{2}})^{\operatorname{ind}_r(a)} = (r^{\operatorname{ind}_r(a)})^{\frac{p-1}{2}} \equiv_p a^{\frac{p-1}{2}}. \qquad \square$$

Kroneckers Formel und das quadratische Reziprozitätsgesetz

(4.128) Proposition (KRONECKER)**.** Es sei $R\colon \mathbb{R} \to \mathbb{R}$ definiert durch

$$R(x) := \begin{cases} x - \lfloor x + \frac{1}{2} \rfloor, & \text{falls } x \notin \frac{1}{2} + \mathbb{Z}, \\ 0, & \text{falls } x \in \frac{1}{2} + \mathbb{Z}, \end{cases}$$

für $x \in \mathbb{R}$.

(a) Für $x \in \mathbb{R}$ gilt

$$\operatorname{sgn} R(x) = \prod_{i \in \mathbb{Z}} \operatorname{sgn}((x-i)(x-i+\frac{1}{2})).$$

(b) Für ein ungerades $m \in \mathbb{N}$ mit $m > 1$ und $x \in (0, \frac{1}{2})_{\mathbb{R}}$ gilt

$$\operatorname{sgn} R(mx) = \prod_{i \in [1, \frac{m-1}{2}]} \operatorname{sgn}((x - \frac{i}{m})(x + \frac{i}{m} - \frac{1}{2})).$$

Beweis.

(a) Es sei $x \in \mathbb{R}$ gegeben. Für $i \in \mathbb{Z}$ gilt genau dann $(x-i)(x-i+\frac{1}{2}) \le 0$, wenn $x \le i$ und $x \ge i - \frac{1}{2}$ ist, d.h. wenn $i \in [x, x+\frac{1}{2}]_{\mathbb{R}}$ ist. Somit gilt für $i \in \mathbb{Z} \setminus \{\lfloor x + \frac{1}{2} \rfloor\}$ stets $(x-i)(x-i+\frac{1}{2}) > 0$ und damit

$$\operatorname{sgn}((x-i)(x-i+\frac{1}{2})) = 1.$$

Für $i = \lfloor x + \frac{1}{2} \rfloor$, $i > x + \frac{1}{2}$ gilt ferner $(x-i)(x-i+\frac{1}{2}) \le 0$ genau dann, wenn $\lfloor x + \frac{1}{2} \rfloor = i \ge x$ ist, d.h. wenn $R(x) = x - \lfloor x + \frac{1}{2} \rfloor \le 0$ gilt. Für $i = x + \frac{1}{2}$ gilt schließlich $(x-i)(x-i+\frac{1}{2}) = 0 = R(x)$. Somit haben wir

$$\operatorname{sgn} R(x) = \operatorname{sgn}((x - \lfloor x + \frac{1}{2} \rfloor)(x - \lfloor x + \frac{1}{2} \rfloor + \frac{1}{2})) = \prod_{i \in \mathbb{Z}} \operatorname{sgn}((x-i)(x-i+\frac{1}{2})).$$

(b) Es seien ein ungerades $m \in \mathbb{N}$ mit $m > 1$ und $x \in (0, \frac{1}{2})_{\mathbb{R}}$ gegeben. Für $i \in \mathbb{Z}$ folgt aus $(mx-i)(mx-i+\frac{1}{2}) \le 0$ bereits $mx \le i$ und $mx \ge i - \frac{1}{2}$, also

$$i \ge mx > 0,$$
$$i \le mx + \frac{1}{2} < m\frac{1}{2} + \frac{1}{2} = \frac{m+1}{2}$$

und damit $i \in [1, \frac{m+1}{2}]$. Nach (a) folgt

$$\operatorname{sgn} R(mx) = \prod_{i \in [1, \frac{m-1}{2}]} \operatorname{sgn}((mx-i)(mx-i+\frac{1}{2})) = \prod_{i \in [1, \frac{m-1}{2}]} \operatorname{sgn}((x - \frac{i}{m})(x - \frac{i}{m} + \frac{1}{2m}))$$

$$
\begin{aligned}
&= \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{i}{m}) \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{i}{m}+\frac{1}{2m}) \\
&= \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{i}{m}) \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{\frac{m+1}{2}-i}{m}+\frac{1}{2m}) \\
&= \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{i}{m}) \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{m+1}{2m}+\frac{i}{m}+\frac{1}{2m}) \\
&= \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x-\frac{i}{m}) \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}(x+\frac{i}{m}-\frac{1}{2}) \\
&= \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}((x-\frac{i}{m})(x+\frac{i}{m}-\frac{1}{2})). \qquad \square
\end{aligned}
$$

(4.129) Satz. Für ungerade $m, n \in \mathbb{N}$ gilt

$$\left(\frac{m}{n}\right) = \prod_{j\in[1,\frac{n-1}{2}]} \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}((\frac{j}{n}-\frac{i}{m})(\frac{j}{n}+\frac{i}{m}-\frac{1}{2})).$$

Beweis. Es sei $R\colon \mathbb{R} \to \mathbb{R}$ definiert durch

$$R(x) := \begin{cases} x - \lfloor x+\frac{1}{2}\rfloor, & \text{falls } x \notin \frac{1}{2}+\mathbb{Z}, \\ 0, & \text{falls } x \in \frac{1}{2}+\mathbb{Z}, \end{cases}$$

für $x \in \mathbb{R}$.
Ist m teilerfremd zu n, so gilt

$$\left(\frac{m}{n}\right) = \varepsilon_n([m]) = \prod_{j\in[1,\frac{n-1}{2}]} \operatorname{sgn}(m\frac{j}{n} - \lfloor m\frac{j}{n}+\frac{1}{2}\rfloor) = \prod_{j\in[1,\frac{n-1}{2}]} \operatorname{sgn} R(m\frac{j}{n}).$$

nach Korollar (4.117)
Es sei also m nicht teilerfremd zu n. Dann ist $\gcd(m,n) \geq 3$ und damit $\frac{n}{\gcd(m,n)} \leq \frac{n}{3} \leq \frac{n-1}{2}$. Es folgt

$$R(m\frac{\frac{n}{\gcd(m,n)}}{n}) = R(m\gcd(m,n)) = 0$$

und damit

$$\left(\frac{m}{n}\right) = 0 = \prod_{j\in[1,\frac{n-1}{2}]} \operatorname{sgn} R(m\frac{j}{n}).$$

Nach Proposition (4.128)(b) gilt in jedem Fall

$$\left(\frac{m}{n}\right) = \prod_{j\in[1,\frac{n-1}{2}]} \operatorname{sgn} R(m\frac{j}{n}) = \prod_{j\in[1,\frac{n-1}{2}]} \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}((\frac{j}{n}-\frac{i}{m})(\frac{j}{n}+\frac{i}{m}-\frac{1}{2})). \qquad \square$$

(4.130) Korollar (quadratisches Reziprozitätsgesetz)**.** Für ungerade $m, n \in \mathbb{N}$ gilt

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}} \left(\frac{n}{m}\right) = \begin{cases} \left(\frac{n}{m}\right), & \text{falls } m \equiv_4 1 \text{ oder } n \equiv_4 1, \\ -\left(\frac{n}{m}\right), & \text{falls } m \equiv_4 -1 \text{ und } n \equiv_4 -1. \end{cases}$$

Beweis. Es seien ungerade $m, n \in \mathbb{N}$ gegeben. Nach Satz (4.129) gilt

$$\left(\frac{m}{n}\right) = \prod_{j\in[1,\frac{n-1}{2}]} \prod_{i\in[1,\frac{m-1}{2}]} \operatorname{sgn}((\frac{j}{n}-\frac{i}{m})(\frac{j}{n}+\frac{i}{m}-\frac{1}{2}))$$

$$= (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \prod_{i\in[1,\frac{m-1}{2}]} \prod_{j\in[1,\frac{n-1}{2}]} \operatorname{sgn}((\frac{i}{m} - \frac{j}{n})(\frac{i}{m} + \frac{j}{n} - \frac{1}{2})) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).$$

Wenn $m \equiv_4 1$ ist, so gilt $4 \mid m-1$ nach Bemerkung (4.4) und damit

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right) = ((-1)^{n-1})^{\frac{m-1}{4}} \left(\frac{n}{m}\right) = \left(\frac{n}{m}\right).$$

Wenn $n \equiv_4 1$ ist, so erhalten wir $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ auf analoge Weise. Ist hingegen $m \equiv_4 -1$ und $n \equiv_4 -1$, so gilt $\frac{m-1}{2} \equiv_2 1$ und $\frac{n-1}{2} \equiv_2 1$, also auch $\frac{m-1}{2}\frac{n-1}{2} \equiv_2 1$ und damit

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right) = -\left(\frac{n}{m}\right). \qquad \square$$

(4.131) Korollar. Es seien ungerade $p, q \in \mathbb{P}$ gegeben.

(a) Es sei $p \equiv_4 1$ oder $q \equiv_4 1$. Genau dann ist p ein invertierbares Quadrat modulo q, wenn q ein invertierbares Quadrat modulo p ist.

(b) Es sei $p \equiv_4 q \equiv_4 -1$. Genau dann ist p ein invertierbares Quadrat modulo q, wenn q kein invertierbares Quadrat modulo p ist.

Beweis. Dies folgt aus dem quadratischen Reziprozitätsgesetz (4.130) und Proposition (4.125). $\square$

(4.132) Korollar. Es sei $a \in \mathbb{Z}$ gegeben. Dann ist

$$\left(\frac{a}{-}\right) : \{n \in \mathbb{N} \mid n \text{ ungerade}\} \to \mathbb{Z}$$

ein Monoidhomomorphismus (bzgl. der gewöhnlichen Multiplikation auf $\{n \in \mathbb{N} \mid n \text{ ungerade}\}$ und $\mathbb{Z}$).

Beweis. Es seien ungerade $n_1, n_2 \in \mathbb{N}$ gegeben. Da dann auch $n_1 n_2$ ungerade ist, existiert ein ungerades $b \in \mathbb{N}$ mit $a \equiv_{n_1 n_2} b$. Nach Bemerkung (4.8) gilt insbesondere $a \equiv_{n_1} b$ und $a \equiv_{n_2} b$. Mit Bemerkung (4.124), dem quadratischen Reziprozitätsgesetz (4.130) und Bemerkung (4.123) folgt

$$\begin{aligned}
\left(\frac{a}{n_1 n_2}\right) &= \left(\frac{b}{n_1 n_2}\right) = (-1)^{\frac{b-1}{2}\frac{n_1 n_2 - 1}{2}} \left(\frac{n_1 n_2}{b}\right) = (-1)^{\frac{b-1}{2}\frac{n_1 n_2 - 1}{2}} \left(\frac{n_1}{b}\right)\left(\frac{n_2}{b}\right) \\
&= (-1)^{\frac{b-1}{2}\frac{n_1 n_2 - 1}{2}} (-1)^{\frac{n_1-1}{2}\frac{b-1}{2}} \left(\frac{b}{n_1}\right) (-1)^{\frac{n_2-1}{2}\frac{b-1}{2}} \left(\frac{b}{n_2}\right) \\
&= (-1)^{\frac{n_1 n_2 - 1}{2}\frac{b-1}{2} + \frac{n_1-1}{2}\frac{b-1}{2} + \frac{n_2-1}{2}\frac{b-1}{2}} \left(\frac{b}{n_1}\right)\left(\frac{b}{n_2}\right) = (-1)^{\frac{n_1 n_2 + n_1 + n_2 - 3}{2}\frac{b-1}{2}} \left(\frac{b}{n_1}\right)\left(\frac{b}{n_2}\right) \\
&= ((-1)^{\frac{(n_1+1)(n_2+1)-4}{2}})^{\frac{b-1}{2}} \left(\frac{b}{n_1}\right)\left(\frac{b}{n_2}\right) = \left(\frac{b}{n_1}\right)\left(\frac{b}{n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right).
\end{aligned}$$

Wegen $a \equiv_1 1$ gilt nach Bemerkung (4.124) und Bemerkung (4.123) ferner

$$\left(\frac{a}{1}\right) = \left(\frac{1}{1}\right) = 1.$$

Insgesamt ist ein $\left(\frac{a}{-}\right) : \{n \in \mathbb{N} \mid n \text{ ungerade}\} \to \mathbb{Z}$ ein Monoidhomomorphismus. $\square$

Die Ergänzungssätze zum quadratischen Reziprozitätsgesetz

(4.133) Proposition (erster und zweiter Ergänzungssatz zum quadratischen Reziprozitätsgesetz)**.** Es sei ein ungerades $n \in \mathbb{N}$ gegeben.

(a) Es gilt

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1, & \text{falls } n \equiv_4 1, \\ -1, & \text{falls } n \equiv_4 -1. \end{cases}$$

(b) Es gilt

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1, & \text{falls } n \equiv_8 1 \text{ oder } n \equiv_8 -1, \\ -1, & \text{falls } n \equiv_8 3 \text{ oder } n \equiv_8 -3. \end{cases}$$

Beweis.

(a) Siehe Aufgabe 55(b).

(b) Siehe Aufgabe 55(c). □

(4.134) Korollar. Es seien ungerade $p, q \in \mathbb{P}$ gegeben.

(a) Es sei $q \equiv_4 1$. Genau dann ist p ein invertierbares Quadrat modulo q, wenn q ein invertierbares Quadrat modulo p ist.

(b) Es sei $q \equiv_4 -1$. Genau dann ist p ein invertierbares Quadrat modulo q, wenn $-q$ ein invertierbares Quadrat modulo p ist.

Beweis.

(a) Dies folgt aus Korollar (4.131)(a).

(b) Nach Bemerkung (4.123), dem ersten Ergänzungssatz (4.133)(a) und dem quadratischen Reziprozitätsgesetz (4.130) gilt

$$\begin{aligned}\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}+\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q+1}{2}}\left(\frac{p}{q}\right) \\ &= ((-1)^{\frac{q+1}{2}})^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right).\end{aligned}$$

Somit ist p nach Proposition (4.125) genau dann ein invertierbares Quadrat modulo q, wenn $-q$ ein invertierbares Quadrat modulo p ist. □

(4.135) Beispiel. Es ist

$$\left(\frac{1711}{997}\right) = -1.$$

Beweis. Mit Hilfe von Bemerkung (4.123), Bemerkung (4.124), dem quadratischen Reziprozitätsgesetz (4.130) und den Ergänzungssätzen (4.133) berechnen wir

$$\begin{aligned}\left(\frac{1711}{997}\right) &= \left(\frac{-283}{997}\right) = \left(\frac{-1}{997}\right)\left(\frac{283}{997}\right) = (-1)^{\frac{997-1}{2}}\left(\frac{283}{997}\right) = \left(\frac{283}{997}\right) = (-1)^{\frac{283-1}{2}\cdot\frac{997-1}{2}}\left(\frac{997}{283}\right) \\ &= \left(\frac{997}{283}\right) = \left(\frac{-135}{283}\right) = \left(\frac{-1}{283}\right)\left(\frac{135}{283}\right) = (-1)^{\frac{283-1}{2}}\left(\frac{135}{283}\right) = -\left(\frac{135}{283}\right) \\ &= -(-1)^{\frac{135-1}{2}\cdot\frac{283-1}{2}}\left(\frac{283}{135}\right) = \left(\frac{283}{135}\right) = \left(\frac{13}{135}\right) = (-1)^{\frac{13-1}{2}\cdot\frac{135-1}{2}}\left(\frac{135}{13}\right) = \left(\frac{5}{13}\right) \\ &= (-1)^{\frac{5-1}{2}\cdot\frac{13-1}{2}}\left(\frac{13}{5}\right) = \left(\frac{13}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = (-1)^{\frac{5-1}{2}}(-1)^{\frac{5^2-1}{8}} = -1.\end{aligned}$$ □

Aufgaben

Aufgabe 55 (Ergänzungssätze zum quadratischen Reziprozitätsgesetz)**.** Es sei ein ungerades $n \in \mathbb{N}$ gegeben.

(a) Bestimmen Sie $\mathrm{Inv}_n([-1]_n)$ und $\mathrm{Inv}_n([2]_n)$.

(b) Zeigen Sie, dass $\left(\frac{-1}{n}\right) = \varepsilon_n([-1]_n) = (-1)^{\frac{n-1}{2}}$ ist.

(c) Zeigen Sie, dass $\left(\frac{2}{n}\right) = \varepsilon_n([2]_n) = (-1)^{\frac{n^2-1}{8}}$ ist.

Aufgabe 56 (Legendre-Jacobi-Symbole und invertierbare modulare Quadrate)**.**

(a) Berechnen Sie $\left(\frac{23}{71}\right)$ und $\left(\frac{6}{23}\right)$.

(b) Ist 256 ein invertierbares Quadrat modulo 601?

Aufgabe 57 (6 als modulares Quadrat)**.** Charakterisieren Sie alle $p \in \mathbb{P}$, für welche 6 ein Quadrat modulo p ist.

Aufgabe 58 (quadratische Kongruenzgleichungen)**.** Es sei $n \in \mathbb{Z}$ gegeben.

(a) Es sei n ungerade und es seien $a, b, c \in \mathbb{Z}$ mit a teilerfremd zu n gegeben. Zeigen Sie: Genau dann gibt es ein $x \in \mathbb{Z}$ mit

$$ax^2 + bx + c \equiv_n 0,$$

wenn $b^2 - 4ac$ ein Quadrat modulo $4an$ ist.

(b) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ mit $b^2 \mid \gcd(a, n)$ gegeben. Zeigen Sie: Für $x \in \mathbb{Z}$ gilt genau dann

$$x^2 \equiv_n a,$$

wenn $b \mid x$ und

$$(\frac{x}{b})^2 \equiv_{\frac{n}{b^2}} \frac{a}{b^2}$$

gilt.

(c) Es sei ein Quadrat a modulo n mit $(a, n) \neq (0, 0)$ gegeben. Zeigen Sie: Für jeden gemeinsamen Primfaktor p von $\gcd(a, n)$ und $\frac{n}{\gcd(a,n)}$ gilt

$$p^2 \mid \gcd(a, n).$$

Insbesondere gilt: Wenn $\gcd(a, n)$ quadratfrei ist, dann sind $\gcd(a, n)$ und $\frac{n}{\gcd(a,n)}$ teilerfremd.

(d) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ mit $(a, n) \neq (0, 0)$, $b^2 \mid \gcd(a, n)$ und $\frac{\gcd(a,n)}{b^2}$ quadratfrei gegeben. Zeigen Sie: Genau dann ist a ein Quadrat modulo n, wenn $\frac{a}{b^2}$ ein invertierbares Quadrat modulo $\frac{n}{\gcd(a,n)}$ ist.

Aufgabe 59 (quadratische Kongruenzgleichungen)**.**

(a) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$

$$4x^2 \equiv_{39} 63x - 4.$$

(b) Bestimmen Sie die Menge aller $x \in \mathbb{Z}$ mit

$$x^2 + 47x + 58 \equiv_{137} 0.$$