Teil III

Arithmetik

12

Die ganzen Zahlen

In diesem Kapitel wird die Arithmetik der ganzen Zahlen aus der Arithmetik der natürlichen Zahlen entwickelt. Es wird gezeigt, dass die Arithmetik der ganzen Zahlen die algebraische Struktur eines kommutativen Rings besitzt. Weitere Beispiele für Ringe werden behandelt und Ringhomomorphismen sowie Unterringe werden eingeführt. Abschließend wird kurz auf die Parallelisierung von Laufschleifen eingegangen.

12.1 Arithmetik der ganzen Zahlen

Konstruktion der ganzen Zahlen

Wir definieren eine Relation auf $\mathbb{N}_0 \times \mathbb{N}_0$ durch

$$(m,n) \simeq (u,v) \quad :\Longleftrightarrow \quad m+v = n+u. \tag{12.1}$$

Lemma 12.1. *Die Relation $\simeq$ ist eine Äquivalenz auf $\mathbb{N}_0 \times \mathbb{N}_0$ mit dem Vertretersystem*

$$\rho = \{(n,0) \mid n \in \mathbb{N}_0\} \cup \{(0,n) \mid n \in \mathbb{N}\}. \tag{12.2}$$

Beweis. Die erste Aussage ist leicht nachzurechen. Sei $(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0$. Ist $m = n$, so ist $(m,n) \simeq (0,0)$. Ist $m > n$, dann gibt es definitionsgemäß ein $l \in \mathbb{N}$ mit $m = n + l$, also $(m,n) \simeq (l,0)$. Ist $m < n$, dann existiert per definitionem ein $l \in \mathbb{N}_0$ mit $n = m + l$, mithin ist $(m,n) \simeq (0,l)$. Ferner sind je zwei Elemente von ρ inäquivalent. Also ist ρ ein Vertretersystem der Äquivalenz. □

Hier sind drei Äquivalenzklassen der obigen Äquivalenz

$$\begin{aligned}
\overline{(0,1)} &= \{(1,0),(2,1),(3,2),(4,3),\ldots\},\\
\overline{(0,0)} &= \{(0,0),(1,1),(2,2),(3,3),\ldots\},\\
\overline{(1,0)} &= \{(0,1),(1,2),(2,3),(3,4),\ldots\}.
\end{aligned}$$

Die Quotientenmenge von $\simeq$ heißt *Menge der ganzen Zahlen* und wird mit $\mathbb{Z}$ bezeichnet. Die Äquivalenzklasse $\overline{(m,n)}$ soll intuitiv die ganze Zahl "$m-n$" darstellen.

Addition und Multiplikation

Auf der Menge der ganzen Zahlen werden *Addition* und *Multiplikation* definiert

$$\overline{(m,n)} + \overline{(u,v)} := \overline{(m+u, n+v)} \tag{12.3}$$
$$\overline{(m,n)} \cdot \overline{(u,v)} := \overline{(mu+nv, mv+nu)}. \tag{12.4}$$

Beide Operationen sind anhand von Repräsentanten der Äquivalenzklassen definiert. Deshalb ist zu zeigen, dass die Operationen *wohldefiniert*, d. h., unabhängig von der Wahl der Repräsentanten, sind. Beispielsweise muss für die äquivalenten Paare $(1,2)$ und $(2,3)$ sowie $(3,0)$ und $(5,2)$ gelten

$$\overline{(1,2)} + \overline{(3,0)} = \overline{(2,3)} + \overline{(5,2)}$$
$$\overline{(1,2)} \cdot \overline{(3,0)} = \overline{(2,3)} \cdot \overline{(5,2)}.$$

Satz 12.2. *Die Addition und Multiplikation ganzer Zahlen sind wohldefiniert.*

Beweis. Wir zeigen, dass die Addition wohldefiniert ist. Seien $\overline{(m,n)} = \overline{(m',n')}$ und $\overline{(u,v)} = \overline{(u',v')}$, d. h., $m+n' = m'+n$ und $u+v' = u'+v$. Dann folgt $m+n'+u+v' = m'+n+u'+v$ und somit $\overline{(m+u,n+v)} = \overline{(m'+u',n'+v')}$, woraus sich definitionsgemäß $\overline{(m,n)} + \overline{(u,v)} = \overline{(m',n')} + \overline{(u',v')}$ ergibt. □

Die Menge der ganzen Zahlen wird unterteilt in die *positiven ganzen Zahlen*

$$n := \overline{(n,0)}, \quad n \in \mathbb{N}, \tag{12.5}$$

die Null $0 := (0,0)$ und die *negativen ganzen Zahlen*

$$-n := \overline{(0,n)}, \quad n \in \mathbb{N}. \tag{12.6}$$

Satz 12.3. *Für alle ganzen Zahlen a, b und c gelten folgende Rechenregeln*

- *Kommutativgesetz:*

$$a+b = b+a \tag{12.7}$$
$$a \cdot b = b \cdot a \tag{12.8}$$

- *Assoziativgesetz:*

$$a+(b+c) = (a+b)+c \tag{12.9}$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{12.10}$$

- *Gesetze für 0 und 1:*

$$a + 0 = a \tag{12.11}$$
$$a \cdot 1 = a, \quad \textit{falls } a \neq 0. \tag{12.12}$$

- *Distributivgesetz:*

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{12.13}$$
$$(a + b) \cdot c = a \cdot c + a \cdot c \tag{12.14}$$

- *Kürzungsregeln:*

$$a + b = a + c \Rightarrow b = c \tag{12.15}$$
$$a \cdot b = a \cdot c \Rightarrow b = c, \quad \textit{falls } a \neq 0. \tag{12.16}$$

Die aus der Schulmathematik bekannte Regel "Punkt- vor Strichrechnung" wird durch das Distributivgesetz beschrieben.

Lineare Ordnung

Die lineare Ordnung $\leq$ auf der Menge der natürlichen Zahlen lässt sich fortsetzen auf die Menge der ganzen Zahlen

$$a \leq b \quad :\Longleftrightarrow \quad b - a \in \mathbb{N}_0 \quad \text{für alle } a, b \in \mathbb{Z}. \tag{12.17}$$

Es handelt sich wirklich eine Fortsetzung, denn für alle natürlichen Zahlen a und b gilt

$$a \leq b \text{ in } \mathbb{N}_0 \quad \Longleftrightarrow \quad b - a \in \mathbb{N}_0 \quad \Longleftrightarrow \quad a \leq b \text{ in } \mathbb{Z}. \tag{12.18}$$

12.2 Ringe

Wir stellen die wichtigsten Grundeigenschaften von Ringen zusammen.

Definition von Ringen

Ein *Ring* ist ein Quintupel $(R, +, \cdot, 0, 1)$, bestehend aus einer nichtleeren Menge R, einer *Addition* $+ : R \times R \to R : (a, b) \mapsto a + b$, einer *Multiplikation* $\cdot : R \times R \to R : (a, b) \mapsto a \cdot b$ und zwei Elementen $0, 1 \in R$, wobei folgende Rechenregeln gelten:

- Die Addition ist kommutativ, d. h., $a + b = b + a$ für alle $a, b \in R$.
- Die Addition ist assoziativ, d. h., $(a+b)+c = a+(b+c)$ für alle $a, b, c \in R$.
- Das Element 0 is additiv *neutral*, d. h., $a + 0 = a$ für alle $a \in R$.

- Zu jedem Element $a \in R$ gibt es ein $b \in R$ mit $a + b = 0$ für alle $a, b \in R$. Ein solches Element b wird *(additives) Inverses* von a genannt.
- Die Multiplikation ist assoziativ, d. h., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$.
- Das Element 1 is multiplikativ *neutral*, d. h., $a \cdot 1 = a = 1 \cdot a$ für alle $a \in R$.
- Die Multiplikation ist distributiv über der Addition, d. h., $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in R$.

Das Element 0 heißt *Null* und das Element 1 *Eins* in R. Wenn keine Verwechslungen zu befürchten sind, wird ein Ring $(R, +, \cdot, 0, 1)$ mit $(R, +, \cdot)$ oder noch kürzer mit R bezeichnet. Das Produkt $a \cdot b$ wird auch ab geschrieben. Ein Ring R heißt *kommutativ*, wenn seine Multiplikation kommutativ ist.

Aus dem Satz 12.3 erhalten wir sofort den folgenden

Satz 12.4. *Die Menge der ganzen Zahlen bildet zusammen mit der Addition (12.3) und der Multiplikation (12.4) einen kommutativen Ring.*

Lemma 12.5. *Sei R ein Ring.*

- *Die Null und die Eins in R sind eindeutig bestimmt.*
- *Jedes Element $a \in R$ hat ein eindeutig bestimmtes additives Inverses, es wird mit $-a$ bezeichnet.*
- *Für alle Elemente $a, b \in R$ gilt*

$$a0 = 0 = 0a,\ -(-a) = a,\ (-a)b = a(-b) = -ab,\ (-a)(-b) = ab.$$

Beweis. Seien 0 und $0'$ Nullen in R. Dann gilt $0' = 0 + 0'$, weil 0 neutral ist, und $0 + 0' = 0$, weil $0'$ neutral ist. Der Beweis für die Eins erfolgt analog.

Für additive Inverse b und c von $a \in R$ gilt definitionsgemäß $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$.

Aus $0 = 0 + 0$ folgt mit dem Distributivgesetz $a0 = a(0 + 0) = a0 + a0$. Da 0 neutral ist, ergibt sich $a0 + 0 = a0 + a0$. Wird auf beiden Seiten $-(a0)$ addiert, erhellt sich $a0 = 0$. Analog wird $0a = 0$ gezeigt.

Nach Definition ist $-(-a)$ das additive Inverse von $-a$, d. h. $(-a) + (-(-a)) = 0$. Wird auf beiden Seiten a addiert, folgt $-(-a) = a$.

Es gilt $ab + (-a)b = (a + (-a))b = 0b = 0$. Also folgt $-ab = (-a)b$. Analog wird $-(ab) = a(-b)$ bewiesen.

Mit den letzten beiden Aussagen ergibt sich $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$. □

Die Summe $a + (-b)$ wird im Folgenden auch als *Differenz* $a - b$ geschrieben.

Vielfache und Potenzen von Ringelementen

Sei R ein Ring. Die *nichtnegativen Vielfachen* von $a \in R$ werden induktiv definiert:

- $0a = 0$,
- $(n + 1)a = a + na$ für alle $n \in \mathbb{N}_0$.

Die *negativen Vielfachen* von $a \in R$ werden mithilfe des additiven Inversen von a festgelegt

$$(-n)a = n(-a) \quad \text{für alle } n \in \mathbb{N}_0. \tag{12.19}$$

Die *nichtnegativen Potenzen* von $a \in R$ werden induktiv definiert:

- $a^0 = 1$,
- $a^{n+1} = a \cdot a^n$ für alle $n \in \mathbb{N}_0$.

Lemma 12.6. *Sei R ein Ring und seien $a, b \in R$.*

- *Für alle ganzen Zahlen m und n gilt*

$$ma + na = (m+n)a,\ m(na) = (mn)a,\ n(a+b) = na + nb. \tag{12.20}$$

- *Für alle natürlichen Zahlen m und n gilt*

$$a^m \cdot a^n = a^{m+n} \text{ und } (a^m)^n = a^{mn}. \tag{12.21}$$

- *Ist R kommutativ, dann gilt für alle natürlichen Zahlen n*

$$(a \cdot b)^n = a^n \cdot b^n. \tag{12.22}$$

12.3 Beispiele für Ringe

Funktionenringe

Sei X eine nichtleere Menge und R ein Ring. Die Menge R^X aller Abbildungen von X nach R bildet einen Ring mit der Addition

$$(f+g)(x) = f(x) + g(x) \quad \text{für alle } x \in X \tag{12.23}$$

und der Multiplikation

$$(fg)(x) = f(x)g(x) \quad \text{für alle } x \in X. \tag{12.24}$$

Die Null ist die Nullabbildung $X \to R : x \mapsto 0$ und die Eins die Einsabbildung $X \to R : x \mapsto 1$. Das additive Inverse von $f \in R^X$ ist $-f$ mit

$$(-f)(x) = -f(x) \quad \text{für alle } x \in X. \tag{12.25}$$

Der Ring R^X heißt *Funktionenring* von X nach R. Er ist kommutativ, sofern R kommutativ ist.

Beispiel 12.7. Wir betrachten den Ring $R = \{0, 1\}$ mit den Verknüpfungen

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Der Funktionenring $R^{\{0,1\}}$ besteht aus den Elementen

a	$f_1(a)$	$f_2(a)$	$f_3(a)$	$f_4(a)$
0	0	0	1	1
1	0	1	0	1

Die Verknüpfungstafeln von $R^{\{0,1\}}$ sind

$+$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

$\cdot$	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_1	f_1
f_2	f_1	f_2	f_1	f_2
f_3	f_1	f_1	f_3	f_3
f_4	f_1	f_2	f_3	f_4

Direkte Produkte

Seien $(R, +, \cdot, 0, 1)$ und $(R', \oplus, \odot, 0', 1')$ Ringe. Das direkte Produkt $R \times R'$ bildet einen Ring mit komponentenweiser Addition

$$((a, a'), (b, b')) \mapsto (a + b, a' \oplus b') \tag{12.26}$$

und komponentenweiser Multiplikation (Hadamard-Produkt)

$$((a, a'), (b, b')) \mapsto (a \cdot b, a' \odot b'). \tag{12.27}$$

Die Null ist $(0, 0')$ und die Eins ist $(1, 1')$. Der Ring $R \times R'$ ist kommutativ, wenn R und R' kommutativ sind.

Matrizenringe

Sei R ein Ring und $n \in \mathbb{N}$. Die Menge aller $n \times n$-Matrizen mit Koeffizienten aus R bildet einen Ring mit der Addition

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \tag{12.28}$$

und der Multiplikation

$$(a_{ij})(b_{ij}) = (\sum_{k=1}^{n} a_{ik} b_{kj}). \tag{12.29}$$

Die Null ist die Nullmatrix und die Eins die Einheitsmatrix. Dieser Ring wird mit $R^{n \times n}$ bezeichnet und heißt *Matrizenring* der $n \times n$-Matrizen über R. Der Ring $R^{n \times n}$ ist im Falle $n = 1$ kommutativ.

12.4 Homomorphismen

Homomorphismen sind Struktur erhaltende Abbildungen zwischen algebraischen Strukturen desselben Typs. Seien $(R, +, \cdot, 0, 1)$ und $(R', \oplus, \odot, 0', 1')$ Ringe. Eine Abbildung $\varphi : R \to R'$ heißt ein *(unitärer) Homomorphismus*, wenn für alle $a, b \in R$ gilt $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$ und $\varphi(1) = 1'$.

Lemma 12.8. *Seien R und R' Ringe. Für jeden Homomorphismus $\varphi : R \to R'$ gilt $\varphi(0) = 0'$ und $\varphi(-a) = -\varphi(a)$ für alle $a \in R$.*

Beweis. Per definitionem gilt $\varphi(0) = \varphi(0+0) = \varphi(0) \oplus \varphi(0)$. Wird auf beiden Seiten $-\varphi(0)$ addiert, so folgt $0' = \varphi(0)$.

Sei $a \in R$. Mit der ersten Aussage ergibt sich $0' = \varphi(0) = \varphi(a + (-a)) = \varphi(a) \oplus \varphi(-a)$. Wegen Lemma 12.5 ist das additive Inverse von $\varphi(a)$ eindeutig bestimmt, woraus $-\varphi(a) = \varphi(-a)$ folgt. □

Ein injektiver Homomorphismus heißt *Monomorphismus*, ein surjektiver Homomorphismus *Epimorphismus* und ein bijektiver Homomorphismus *Isomorphismus*. Ein Homomorphismus $\varphi : R \to R$ mit gleicher Quell- und Zielmenge wird *Endomorphismus* genannt. Ein bijektiver Endomorphismus heißt *Automorphismus*. Zwei Ringe R und R' heißen *isomorph*, wenn es einen Isomorphismus $\varphi : R \to R'$ gibt.

Satz 12.9. *Der einzige Endomorphismen $\phi : \mathbb{Z} \to \mathbb{Z}$ ist die identische Abbildung.*

Beweis. Sei $\varphi : \mathbb{Z} \to \mathbb{Z}$ ein Endomorphismus. Wegen $\varphi(1) = 1$ muss für jede natürliche Zahl n gelten $\varphi(n) = \varphi(n1) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = n\varphi(1) = n1 = n$. Mit Lemma 12.8 folgt $\varphi(-n) = -\varphi(n) = -n$. Also ist φ die identische Abbildung. □

Der *Kern* eines Homomorphismus $\varphi : R \to R'$ ist die Menge aller Elemente in R, die auf die Null abgebildet werden

$$\ker \varphi = \{a \mid a \in R \wedge \varphi(a) = 0'\}. \tag{12.30}$$

Ein *Unterring* eines Rings R ist eine nichtleere Teilmenge U von R, die zusammen mit den Operationen von R einen Ring bildet und dabei die Null und Eins von R enthält.

Lemma 12.10. *Ist $\varphi : R \to R'$ ein Homomorphismus, dann ist das Bild $\varphi(R)$ ist ein Unterring von R'.*

Beweis. Sei $U = \varphi(R)$. Wegen $\varphi(0) = 0'$ und $\varphi(1) = 1'$ liegen die Null und Eins von R' in U. Seien $a', b' \in U$. Dann gibt es $a, b \in R$ mit $\varphi(a) = a'$ und $\varphi(b) = b'$. Definitionsgemäß folgt $a' \oplus b' = \varphi(a) \oplus \varphi(b) = \varphi(a + b) \in U$ und $a' \odot b' = \varphi(a) \odot \varphi(b) = \varphi(a \cdot b) \in U$. Nach Lemma 12.8 gilt $-a' = -\varphi(a) = \varphi(-a) \in U$. Die für R' geltenden Rechenregeln gelten auch für U. Also ist U ein Unterring von R'. □

12.5 Schleifenparallelisierung

Wir betrachten die zweifach geschachtelte Laufschleife

L_1: **for** $I_1 = 1$ to 4 **do**
L_2: **for** $I_2 = 1$ to 4 **do**
$H(I)$: $A(I_1, I_2) := A(I_1, I_2 - 1) + A(I_1 - 1, I_2)$
end for
end for

Diese Laufschleife wird in Form von Iterationen ausgeführt. In jeder Iteration $H(i)$ wird der Indexvektor I mit Werten $I_1 = i_1$ und $I_2 = i_2$ belegt und der zugehörige Rumpf $A(i_1, i_2) = A(i_1, i_2 - 1) + A(i_1 - 1, i_2)$ ausgeführt. Die Iterationen werden gemäß der Belegungen des Indexvektors in aufsteigender lexikographischer Reihenfolge ausgewertet: $(1,1)^T, (1,2)^T, \ldots, (2,1)^T, \ldots, (4,4)^T$.

Um die Zuweisung $A(i_1, i_2) = A(i_1, i_2 - 1) + A(i_1 - 1, i_2)$ auszuführen, müssen den Variablen $A(i_1, i_2 - 1)$ und $A(i_1 - 1, i_2)$ bereits Werte zugewiesen worden sein. Diese Abhängigkeiten zwischen den Iterationen zeigt Abb. 12.1.

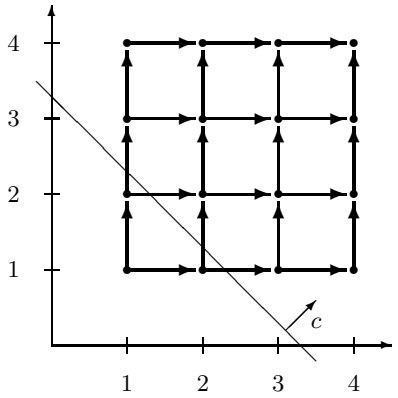

Abb. 12.1. Die Abhängigkeiten zwischen den Iterationen der Laufschleife und ein durch den Vektor $c = (1,1)^T$ definierter linearer Schedule.

Laufschleifen werden anhand von Schedules parallelisiert. Ein *Schedule* für eine n-fach geschachtelte Laufschleife ist eine Abbildung $\sigma : \mathbb{Z}^n \to \mathbb{Z}$, die jeder Iteration $H(i)$ einen Ausführungszeitpunkt $\sigma(i)$ zuordnet. Ein Schedule heißt *kausal*, wenn $\sigma(i) < \sigma(j)$ gilt, falls $H(j)$ von $H(i)$ abhängt.

Beispielsweise definiert die Abbildung $\sigma : \mathbb{Z}^2 \to \mathbb{Z} : i \to i_1 + i_2$ einen Schedule für obige Laufschleife. Diese Abbildung ist linear und wird anhand der Zuordnung $\sigma(i) = c^T i$, $c = (1,1)^T$, definiert. Der lineare Schedule σ definiert eine Hyperebene $\{x \in \mathbb{R}^2 \mid c^T x = \text{const.}\}$, auf der der Vektor c senkrecht steht

(Abb. 12.1). Alle auf einer Hyperebene liegenden Iterationen werden zum selben Zeitpunkt ausgeführt. Der Schedule ist kausal, denn $\sigma(i_1, i_2) > \sigma(i_1 - 1, i_2)$ und $\sigma(i_1, i_2) > \sigma(i_1, i_2 - 1)$.

Selbsttestaufgaben

12.1. (Monotonie von Addition und Multiplikation) Zeige, dass für beliebige ganze Zahlen a und b aus $a \leq b$ stets $a + c \leq b + c$ für alle $c \in \mathbb{Z}$ und $ac \leq bc$ für alle $c \in \mathbb{N}_0$ folgt.

12.2. (Kürzungsregel) Zeige, dass für beliebige ganze Zahlen a, b und c aus $a \neq 0$ und $ab = ac$ stets $b = c$ folgt.

12.3. Beweise die Potenzgesetze 12.6.

12.4. (Binomialsatz) Zeige, dass in einem kommutativen Ring r für alle Elemente $a, b \in R$ und alle natürlichen Zahlen n gilt

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

12.5. (Multinomialsatz) Sei R ein kommutativer Ring. Zeige, dass für alle Elemente $a_1, \ldots, a_n \in R$ und alle natürlichen Zahlen k gilt

$$(a_1 + \ldots + a_n)^k = \sum \binom{k}{k_1, \ldots, k_n} a_1^{k_1} \cdots a_n^{k_n},$$

wobei über alle nichtnegativen ganzen Zahlen $k_1, \ldots, k_n$ mit $k_1 + \ldots + k_n = k$ summiert wird.

12.6. Sei R ein Ring. Eine Teilmenge I von R heißt ein *Ideal* von R, wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und für alle $i \in I$ und $r \in R$ gilt $ir \in I$ und $ri \in I$. Zeige, dass der Kern eines Ringhomomorphismus' $\phi : R \to S$ ein Ideal von R ist.

12.7. Sei R ein Ring und I ein Ideal von R. Zeige, dass die Menge $R/I = \{r + I \mid r \in R\}$, mit $r + I = \{r + i \mid i \in I\}$, zusammen mit der Addition

$$(r + I) + (s + I) = (r + s) + I, \quad r, s \in R,$$

und der Multiplikation

$$(r + I) \cdot (s + I) = (rs) + I, \quad r, s \in R,$$

einen Ring mit dem Einselement $1 + I$ definiert. Der Ring R/I wird *Restklassenring von R nach I* genannt.

12.8. Sei R ein Ring. Wir definieren eine neue Multiplikation $\circ : R \times R \to R$ durch $r \circ s = sr$, wobei sr das Produkt aus $(R, +, \cdot)$ bedeutet. Zeige, dass $(R, +, \circ)$ ein Ring ist. Dieser Ring heißt der zu R entgegengesetzte Ring und wird mit R^{opp} (R-opposite) bezeichnet. Wann ist $R = R^{\text{opp}}$?

12.9. Zeige, dass folgende Aussagen gelten: $\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{C}$. $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ ist ein Unterring von $\mathbb{R}$. Für $n \in \mathbb{Z}$, $n \neq 0$, ist $R_n = \{\frac{m}{n^k} \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$ ein Unterring von $\mathbb{Q}$.

12.10. Sei R ein kommutativer Ring und A^T die zu $A \in R^{n\times n}$ transponierte Matrix. Zeige, dass $A \mapsto A^T$ einen Isomorphismus von $R^{n\times n}$ nach $[R^{n\times n}]^{\mathrm{opp}}$ definiert.

13

Teilbarkeitslehre

In diesem Kapitel wird die Teilbarkeitslehre im Ring der ganzen Zahlen entwickelt. Sie gründet sich auf der Operation der Division mit Rest, mit deren Hilfe größte gemeinsame Teiler und kleinste gemeinsame Vielfache von ganzen Zahlen berechnet werden können. Zudem wird die Zerlegung von ganzen Zahlen in Primfaktoren behandelt. Diese Zerlegung wird dazu benutzt, um Wörter über einem endlichen Alphabet durch natürliche Zahlen zu kodieren.

13.1 Division mit Rest

Satz 13.1. (Divisionssatz) *Zu jedem Paar ganzer Zahlen a und $b \neq 0$ gibt es eindeutig bestimmte, ganze Zahlen q und r mit der Eigenschaft*

$$a = qb + r \quad \textit{und} \quad 0 \leq r \leq |b| - 1. \tag{13.1}$$

Beweis. Wir zeigen die Existenz zunächt für den Fall, dass a und b nichtnegativ sind. Im Falle $a < b$ erhalten wir die Darstellung für $q = 0$ und $r = a$ und im Falle $a = b$ ergibt sich die Darstellung für $q = 1$ und $r = 0$. Sei die Existenz der Darstellung für alle nichtnegativen ganzen Zahlen $< a$ bewiesen. O.B.d.A. können wir $a > b$ annehmen. Wir betrachten die Zahl $a - b > 0$. Nach Induktionsannahme gibt es ganze Zahlen q_1 und r mit $a - b = q_1 b + r$ und $0 \leq r < b$. Folglich ist $a = (q_1 + 1)b + r$ und somit die Existenz der Darstellung für nichtnegative a und b gezeigt. Aus der Darstellung für nichtnegative ganze Zahlen a und b folgt $a = (-q)(-b)+r$, $-a = (-q-1)b+(b-r)$ und $-a = (q+1)(-b) + (b-r)$. Damit ist die Existenz bewiesen.

Wir zeigen die Eindeutigkeit. Angenommen, es gäbe zwei Darstellungen $a = qb + r$ und $a = q'b + r'$ mit ganzen Zahlen q, q', r, r', $0 \leq r, r' \leq |b| - 1$. Dies bedeutet $(q - q')b = r' - r$. Wegen $-(|b| - 1) \leq r' - r \leq |b| - 1$ folgt $r' - r = 0$, also $(q - q')b = 0$. Mit der Kürzungsregel ergibt sich $q = q'$. □

Beispiel 13.2. Für $a = 9$ und $b = 4$ gilt $9 = 2 \cdot 4 + 1$, $9 = (-2) \cdot (-4) + 1$, $-9 = (-3) \cdot 4 + 3$ und $-9 = 3 \cdot (-4) + 3$.

In der Darstellung (13.1) wird die Zahl q *Quotient von a modulo n* und die Zahl r *Rest von a modulo b* genannt. Für die Infixoperatoren

$$a \texttt{ div } b := q \quad \text{und} \quad a \texttt{ mod } b := r, \quad b \neq 0, \tag{13.2}$$

gilt

$$a = (a \texttt{ div } b) \cdot b + (a \texttt{ mod } b), \quad b \neq 0. \tag{13.3}$$

Der größte gemeinsame Teiler

Seien $a, b \in \mathbb{Z}$. Wir sagen, *a teilt b*, kurz $a \mid b$, wenn es eine ganze Zahl c gibt mit $ac = b$. Diese Relation ist reflexiv und transitiv, aber nicht antisymmetrisch, denn es gilt $a \mid (-a)$ und $(-a) \mid a$. Diese Relation hat 0 als größtes und ± 1 als minimale Elemente.

Seien $a_1, \ldots, a_n$ ganze Zahlen. Eine ganze Zahl d heißt *größter gemeinsamer Teiler* (ggT) von $a_1, \ldots, a_n$, wenn

- d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist und
- jeder ganzzahlige Teiler von $a_1, \ldots, a_n$ auch d teilt.

Lemma 13.3. *Der ggT von ganzen Zahlen $a_1, \ldots, a_n$ ist eindeutig bestimmt bis auf das Vorzeichen.*

Zu ganzen Zahlen $a_1, \ldots, a_n$ gibt es also einen eindeutig bestimmten, nichtnegativen ggT, der mit $(a_1, \ldots, a_n)$ bezeichnet wird.

Satz 13.4. *Für alle ganzen Zahlen a, b und c gelten folgende Rechenregeln:*

- *Kommutativgesetz:*

$$(a, b) = (b, a). \tag{13.4}$$

- *Assoziativgesetz:*

$$(a, (b, c)) = ((a, b), c). \tag{13.5}$$

- *Idempotenzgesetz:*

$$(a, a) = |a|. \tag{13.6}$$

- *Gesetze für 0 und 1:*

$$(0, a) = |a| \quad \textit{und} \quad (1, a) = 1. \tag{13.7}$$

- *Distributivgesetz:*

$$a \cdot (b, c) = (ab, ac). \tag{13.8}$$

- *Absolutgesetz:*

$$(a, b) = (|a|, |b|). \tag{13.9}$$

- *Restegesetz:*

$$(a, b) = (b, a \texttt{ mod } b), \quad b \neq 0. \tag{13.10}$$

13.2 Der euklidische Algorithmus

Der ggT ganzer Zahlen wird mithilfe des *euklidischen Algorithmus* (Euklid, ca. 365-300 v.Chr.) berechnet. Seien a und $b \neq 0$ ganze Zahlen. Wir setzen $x_0 = a$ und $x_1 = b$ und erhalten eine Folge ganzen Zahlen x_i durch sukzessive Division mit Rest

$$\begin{aligned} x_0 &= q_1 x_1 + x_2 \\ x_1 &= q_2 x_2 + x_3 \\ x_2 &= q_3 x_3 + x_4 \\ &\dots \end{aligned} \tag{13.11}$$

Satz 13.5. *Seien a und $b \neq 0$ ganze Zahlen. In (13.11) gibt es eine Gleichung $x_n = q_{n+1}x_{n+1} + x_{n+2}$ mit $x_{n+1} \neq 0$ und $x_{n+2} = 0$. Die Zahl x_{n+1} ist der ggT von a und b.*

Beweis. Die Folge der Reste fällt streng monoton $|x_1| > x_2 > \ldots \geq 0$. Also existiert in der Folge eine Gleichung $x_n = q_{n+1}x_{n+1} + x_{n+2}$ mit $x_{n+1} \neq 0$ und $x_{n+2} = 0$.

Sei $d = x_{n+1}$. Wir zeigen, dass d jede Zahl x_i, $0 \leq i \leq n+1$, teilt. Der Induktionsanfang ist klar. Sei die Aussage für alle Zahlen x_j mit $j \geq i$ schon gezeigt. Wegen $x_{i-1} = q_i x_i + x_{i+1}$ ist d nach Induktionsannahme auch ein Teiler von x_{i-1}. Somit teilt d auch $x_0 = a$ und $x_1 = b$.

Sei c ein Teiler von a und b. Wir zeigen, dass c jede Zahl x_i, $0 \leq i \leq n+1$, teilt. Der Induktionsanfang ist klar. Sei die Aussage für alle Zahlen x_j mit $j \leq i$ schon bewiesen. Wegen $x_{i-1} = q_i x_i + x_{i+1}$ ist c nach Induktionsannahme auch ein Teiler von x_{i+1}. Folglich teilt c auch $x_{n+1} = d$. □

Das obige Verfahren führt auf den euklidischen Algorithmus (13.1).

Algorithmus 13.1 Euklidischer Algorithmus

Eingabe: ganze Zahlen a und $b > 0$
Ausgabe: ggT von a und b

```
1: x := a
2: y := b
3: while y ≠ 0 do
4:     x := y {Schleifeninvariante {(x, y) = (a, b)}}
5:     y := x mod y
6: end while
7: return x
```

Beispiel 13.6. Für $a = 385$ und $b = 252$ liefert der euklidische Algorithmus

$$\begin{aligned} 386 &= 1 \cdot 252 + 133 \\ 252 &= 1 \cdot 133 + 119 \\ 133 &= 1 \cdot 119 + 14 \\ 119 &= 8 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0. \end{aligned}$$

Also ist $(385, 252) = 7$.

Satz 13.7. *Für alle ganzen Zahlen $a_1, \ldots, a_n$ gilt*

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n). \tag{13.12}$$

Beweis. Seien $d_{n-1} = (a_1, \ldots, a_{n-1})$ und $d_n = (d_{n-1}, a_n)$. Es wird gezeigt, dass d_n der ggT von $a_1, \ldots, a_n$ ist. Erstens ist d_n ein Teiler von $a_1, \ldots, a_n$, denn d_n teilt a_n und d_{n-1} und deshalb auch $a_1, \ldots, a_{n-1}$. Zweitens sei c ein Teiler von $a_1, \ldots, a_n$. Dann ist c ein Teiler von a_n und des ggT d_{n-1} von $a_1, \ldots, a_{n-1}$. Also ist c auch ein Teiler des ggT d_n von a_n und d_{n-1}. □

Beispiel 13.8. Mit 13.6 folgt $(385, 252, 707) = ((385, 252), 707) = (7, 707) = 7$.

Satz 13.9. (Bezout) *Der ggT ganzer Zahlen $a_1, \ldots, a_n$ ist als ganzzahlige Linearkombination dieser Zahlen darstellbar, d. h. es gibt ganze Zahlen $s_1, \ldots, s_n$ mit*

$$(a_1, \ldots, a_n) = s_1 a_1 + \ldots + s_n a_n. \tag{13.13}$$

Beweis. Wir benutzen vollständige Induktion nach n. Sei $n = 2$. Wir zeigen mit dem euklidischen Algorithmus (13.11), dass d als ganzzahlige Linearkombination von konsekutiven Zahlen x_i und x_{i+1}, $0 \leq i \leq n-1$, darstellbar ist. Es gilt $d = x_{n-1} - q_n x_n$. Sei $d = sx_i + tx_{i+1}$ mit $s, t \in \mathbb{Z}$. Wegen $x_{i-1} = q_i x_i + x_{i+1}$ folgt $d = tx_{i-1} + (s - q_i)x_i$. Daraus folgt, dass d als ganzzahlige Linearkombination von $x_0 = a$ und $x_1 = b$ darstellbar ist.

Sei $n \geq 2$ und seien $a_1, \ldots, a_{n+1}$ ganze Zahlen. Dann gilt

$$\begin{aligned} (a_1, \ldots, a_n, a_{n+1}) &= ((a_1, \ldots, a_n), a_{n+1}), \quad \text{nach (13.12)} \\ &= s(a_1, \ldots, a_n) + s_{n+1} a_{n+1}, \quad \text{nach Ind.anfang} \\ &= (ss_1)a_1 + \ldots + (ss_n)a_n + s_{n+1} a_{n+1}, \quad \text{nach Ind.ann.} \end{aligned}$$

Damit ist die Aussage bewiesen. □

Der ggT von a und b wird als Linearkombination von a und b durch sukzessives rückwärtiges Einsetzen in den euklidischen Algorithmus erhalten. Dieser so ergänzte Algorithmus wird *erweiterter euklidischen Algorithmus* genannt.

Beispiel 13.10. Aus der Berechnung des ggT von 385 und 252 in 13.6 ergibt sich durch rückwärtiges Einsetzen

$$\begin{aligned} 7 &= 119 - 8 \cdot 14 \\ &= 119 - 8 \cdot (133 - 1 \cdot 119) = (-8) \cdot 133 + 9 \cdot 119 \\ &= (-8) \cdot 133 + 9 \cdot (252 - 1 \cdot 133) = 9 \cdot 252 + (-17) \cdot 133 \\ &= 9 \cdot 252 + (-17) \cdot (385 - 1 \cdot 252) \\ &= (-17) \cdot 385 + 26 \cdot 252. \end{aligned}$$

Das kleinste gemeinsame Vielfache

Seien $a_1, \ldots, a_n$ ganze Zahlen. Eine ganze Zahl k heißt *kleinstes gemeinsames Vielfaches* (kgV) von $a_1, \ldots, a_n$, wenn

- k ein gemeinsames Vielfaches von $a_1, \ldots, a_n$ ist und
- jedes ganzzahlige Vielfache von $a_1, \ldots, a_n$ ein Vielfaches von k ist.

Lemma 13.11. *Das kgV von ganzen Zahlen $a_1, \ldots, a_n$ ist eindeutig bestimmt bis auf das Vorzeichen.*

Zu ganzen Zahlen $a_1, \ldots, a_n$ gibt es also ein eindeutig bestimmtes, nichtnegatives kgV, das mit $[a_1, \ldots, a_n]$ bezeichnet wird.

Satz 13.12. *Für alle ganzen Zahlen $a_1, \ldots, a_n$ gilt*

$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n]. \tag{13.14}$$

13.3 Primfaktorisierung

Eine ganze Zahl $p > 1$ heißt *prim* oder eine *Primzahl*, wenn p nur die *trivialen Teiler* ± 1 und $\pm p$ besitzt. Andernfalls heißt p *zusammengesetzt*. Die ersten zehn Primzahlen lauten 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Beispiele 13.13. Es gibt zwei berühmte Zahlenfolgen, die Primzahlen enthalten:

- Die *Fermat-Zahlen* (Pierre de Fermat, 1601-1665) sind

$$f_n = 2^{2^n} + 1, \quad n \geq 0. \tag{13.15}$$

  Die ersten fünf Fermat-Zahlen sind prim: $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$ und $f_4 = 65537$. Die nächste Fermat-Zahl hat den Teiler 641. Bis heute sind keine weiteren Fermat-Primzahlen bekannt. Die Zahl f_{31} ist die kleinste Fermat-Zahl, für die unbekannt ist, ob sie prim ist.

- Die *Mersenne-Zahlen* (Marin Mersenne, 1588-1648) sind

$$m_n = 2^n - 1, \quad n \geq 1. \tag{13.16}$$

  Eine Mersenne-Zahl m_n kann nur dann prim sein, wenn n prim ist, denn aus $d \mid n$ folgt stets $(2^d - 1) \mid (2^n - 1)$. Für die ersten 37 Primzahlen p ist bekannt, ob m_p prim sind. Erst kürzlich wurde eine noch größere Mersenne-Primzahl, $m_{6972593}$, mit mehr als zwei Millionen Dezimalstellen entdeckt.

Ganze Zahlen $a_1, \ldots, a_n$ heißen *teilerfremd* oder *relativ prim*, wenn sie ggT 1 haben.

Lemma 13.14. *Sei p eine Primzahl und seien $a_1, \ldots, a_n$ ganze Zahlen. Teilt p das Produkt $a_1 \cdot \ldots \cdot a_n$, dann teilt p einen der Faktoren a_i.*

Beweis. Wir verwenden vollständige Induktion nach n. Sei $n = 2$. Angenommen, p teile das Produkt $a_1 a_2$, aber nicht a_1. Da p prim ist, sind p und a_1 teilerfremd. Also gibt es nach dem Satz von Bezout ganze Zahlen s und t mit $1 = sp + ta_1$. Durch Multiplizieren mit a_2 ergibt sich $a_2 = sa_2p + ta_1a_2$. Da p die Produkte a_1a_2 und sa_2p teilt, teilt p auch a_2.

Sei $n \geq 2$. Angenommen, p teile das Produkt $a_1 \cdot \ldots \cdot a_{n+1}$. Wenn p das Teilprodukt $a_1 \cdot \ldots \cdot a_n$ teilt, dann folgt mit der Induktionsannahme, dass p einen der Faktoren a_i, $1 \leq i \leq n$, teilt. Andernfalls sind p und $a_1 \cdot \ldots \cdot a_n$ teilerfremd und wie im Induktionsanfang wird gezeigt, dass p die Zahl a_{n+1} teilt. □

Fundamentalsatz der Arithmetik

Satz 13.15. *Jede natürliche Zahl $n \geq 2$ ist darstellbar als ein Produkt von Primzahlen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.*

Beweis. Die Existenz der Darstellung wird durch vollständige Induktion bewiesen. Im Falle $n = 2$ ist die Aussage klar. Sei $n > 2$. Ist n prim, dann ist nichts zu beweisen. Andernfalls lässt sich n darstellen als Produkt $n = l \cdot m$ natürlicher Zahlen l und m mit $2 \leq l, m < n$. Nach Induktionsannahme gibt es Darstellungen für l und m, weshalb es auch eine Darstellung für n gibt.

Die Eindeutigkeit der Darstellung wird ebenfalls per vollständiger Induktion gezeigt. Im Falle $n = 2$ ist die Aussage klar. Sei $n > 2$. Es werden zwei Darstellungen von n durch Primfaktoren p_i, q_j betrachtet

$$p_1 \cdot \ldots \cdot p_r = n = q_1 \cdot \ldots \cdot q_s.$$

Nach Lemma 13.15 teilt p_1 eine der Primzahlen q_j, nach Umnummerierung etwa q_1. Es folgt $p_1 = q_1$ und mit der Kürzungsregel ergibt sich

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s.$$

Nach Induktionsannahme hat diese Zahl eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung durch Primfaktoren, weshalb auch n eine solche Darstellung besitzt. □

In der Primfaktorzerlegung einer natürlichen Zahl n werden gleiche Primzahlen zu Primzahlpotenzen zusammengefasst. Dies ergibt die *kanonische Primfaktordarstellung* von n:

$$n = p_1^{v_1} \cdot \ldots \cdot p_s^{v_s}, \quad p_1 < p_2 < \ldots < p_k. \tag{13.17}$$

Satz 13.16. *Es gibt unendlich viele Primzahlen.*

Beweis. Es wird induktiv eine Folge $F = (p_n)$ von Primzahlen konstruiert:

- Setze $p_1 = 2$.
- Sei $P = (p_1, \ldots, p_k)$. Die Zahl $q = p_1 \cdot \ldots \cdot p_k + 1$ wird von keiner der Primzahlen in der Liste P geteilt. Also ist q nach dem Fundamentalsatz der Arithmetik als Produkt anderer Primfaktoren darstellbar. Die kleinste Primzahl in der Primfaktorisierung von q wird als Glied p_{k+1} in die Liste P aufgenommen. □

13.4 Gödelisierung

Die Menge aller Wörter über einem endlichen Alphabet A lassen sich durch Ausnutzen der Primfaktorzerlegung durch natürliche Zahlen codieren. Sei A^* die Menge aller Wörter über dem Alphabet A. Eine *Codierung* von A^* ist eine injektive Abbildung $g : A^* \to \mathbb{N}_0$, die nach Kurt Gödel (1906-1978) auch *Gödelisierung* genannt wird.

In der so genannten *Standard-Gödelisierung* wird A mithilfe einer injektiven Abbildung $f : A \to \{1, \ldots, |A|\}$ codiert. Sei (p_n) die aufsteigende Folge der Primzahlen, also $p_1 = 2$, $p_2 = 3$, usw. Die Standard-Gödelisierung $g : A^* \to \mathbb{N}_0$ von A^* ist definiert durch

- $g(\epsilon) = 1$,
- $g(x_1 \ldots x_n) = p_1^{f(x_1)} \cdot \ldots \cdot p_n^{f(x_n)}$ für jedes Wort $x_1 \ldots x_n$.

Wird das lateinische Alphabet gemäß der lexikographischen Ordnung codiert, also $f(a) = 1$, $f(b) = 2$, usw., so erhalten wir beispielsweise $g(\text{claire}) = 2^3 3^{11} 5^1 7^9 11^5$. Durch Gödelisierung lassen sich ganze Texte oder Programme anhand natürlicher Zahlen codieren.

Selbsttestaufgaben

13.1. Bestimme den ggT der Zahlen 315 und 308 und drücke ihn als Linearkombination der beiden Zahlen aus.

13.2. Beweise das Lemma 13.3.

13.3. Beweise das Lemma 13.11.

13.4. Beweise den Satz 13.12.

13.5. Restegesetz: Beweise, dass für alle ganzen Zahlen a und $b \neq 0$ gilt $(a, b) = (b, a \texttt{ mod } b)$.

13.6. Distributivgesetz: Zeige, dass für alle ganzen Zahlen a, b, c gilt $(a, [b, c]) = [(a, b), (a, c)]$ und $[a, (b, c)] = ([a, b], [a, c])$.

13.7. Verschmelzungsgesetz: Beweise, dass für alle ganzen Zahlen a und b gilt $(a, [a, b]) = a$ und $[a, (a, b)] = a$.

13.8. Seien a und b natürliche Zahlen mit der kanonischen Primfaktorisierung

$$a = p_1^{m_1} \cdot \ldots \cdot p_l^{m_l} \quad \text{und} \quad b = p_1^{n_1} \cdot \ldots \cdot p_l^{n_l}, \quad m_i, n_i \in \mathbb{N}_0.$$

Zeige

$$(a, b) = p_1^{\min\{m_1, n_1\}} \cdot \ldots \cdot p_l^{\min\{m_l, n_l\}}$$

und

$$[a, b] = p_1^{\max\{m_1, n_1\}} \cdot \ldots \cdot p_l^{\max\{m_l, n_l\}}.$$

13.9. Zeige, dass jedes Ideal in $\mathbb{Z}$ die Gestalt $a\mathbb{Z} = \{ab \mid b \in \mathbb{Z}\}$, $a \in \mathbb{Z}$, besitzt.

14

Restklassenringe

In diesem Kapitel wird der Restklassenring modulo n eingeführt. Restklassenringe sind grundlegend für viele Anwendungen wie etwa in der modernen Kryptographie und der Codierungstheorie. Wir behandeln die Zerlegung von Restklassenringen mithilfe linearer Kongruenzensysteme und zeigen, dass anhand solcher Zerlegungen arithmetische Operationen im Ring der ganzen Zahlen durchgeführt werden können.

14.1 Restklassenringe

Kongruenz modulo n

Wir stellen uns die ganzen Zahlen auf einer Zahlengeraden vor. In der *4er-Uhr-Arithmetik* ist diese Zahlengerade bei 4 abgeschnitten und auf die 0 zurückgebogen. Die einzigen ganzen Zahlen in der 4er-Uhr-Arithmetik sind also 0, 1, 2 und 3 (Abb. 14.1). Um etwa die Zahlen 2 und 3 in der 4er-Uhr-Arithmetik zu addieren, wird von der 2 aus drei Schritte im Uhrzeigersinn weitergezählt. Die erreichte Zahl ist 1, also ist $2 + 3 = 1$. Das Multiplizieren in der 4-er-Uhr-Arithmetik ist analog definiert. Die n-Uhr-Arithmetik wird anhand einer Äquivalenz auf der Menge der ganzen Zahlen eingeführt.

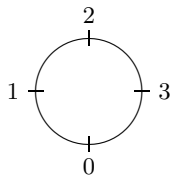

Abb. 14.1. 4er-Uhr-Arithmetik.

Sei n eine natürliche Zahl. Zwei ganze Zahlen a und b heißen *kongruent modulo* n, geschrieben $a \equiv b \bmod n$, wenn n ein Teiler von $a - b$ ist. Die Zahl n wird *Modulus* der Relation genannt.

Beispiel 14.1. Es gilt $-1 \equiv 3 \bmod 2$, $5 \equiv -4 \bmod 3$ und $10 \equiv 2 \bmod 4$.

Satz 14.2. *Die Kongruenz modulo n ist eine Äquivalenz auf der Menge der ganzen Zahlen.*

Beweis. Seien a, b und c ganze Zahlen. Die Relation ist reflexiv, denn $a - a = 0 = 0n$, d. h. $a \equiv a \bmod n$. Die Relation ist transitiv, denn aus $a \equiv b \bmod n$ und $b \equiv c \bmod n$, d. h. $a = b + kn$ und $b = c + ln$ für gewisse $k, l \in \mathbb{Z}$, folgt $a = c + (k + l)n$, d. h. $a \equiv c \bmod n$. Die Relation ist symmetrisch, denn aus $a \equiv b \bmod n$, d. h. $a = b + kn$ für ein $k \in \mathbb{Z}$, ergibt sich $b = a + (-k)n$, d. h. $b \equiv a \bmod n$. □

Satz 14.3. *Für alle ganzen Zahlen a, b und c gelten folgende Rechenregeln:*

- *Restegesetz:*

$$a \equiv b \bmod n \quad \Longleftrightarrow \quad a \texttt{ mod } n = b \texttt{ mod } b. \tag{14.1}$$

- *Additionsgesetz:*

$$a \equiv b \bmod n \Rightarrow a + c \equiv b + c \bmod n. \tag{14.2}$$

- *Multiplikationsgesetz:*

$$a \equiv b \bmod n \Rightarrow ac \equiv bc \bmod n. \tag{14.3}$$

- *Potenzgesetz:*

$$a \equiv b \bmod n \Rightarrow a^m \equiv b^m \bmod n, \quad m \geq 1. \tag{14.4}$$

Beweis. Sei $a \equiv b \bmod n$. Nach dem Divisionssatz gibt es ganze Zahlen q, q', r, r' mit $a = qn + r$, $b = q'n + r'$ und $0 \leq r, r' < n$. Es folgt $a - b = (q - q')n + (r - r')$. Nach Voraussetzung ist $a - b$ durch n teilbar. Also ist $r - r'$ durch n teilbar, was wegen $-n < r - r' < n$ nur $r = r'$ bedeuten kann. Umgekehrt sei $a \texttt{ mod } n = b \texttt{ mod } b \bmod n$. Nach dem Divisionssatz gibt es ganze Zahlen q, q', r mit $a = qn + r$, $b = q'n + r'$ und $0 \leq r, r' < n$. Nach Voraussetzung ist $r = r'$, also $a - b = (q - q')n$ durch n teilbar.

Sei $a \equiv b \bmod n$, also n ein Teiler von $a - b$. Für jede ganze Zahl c ist $(a + c) - (b + c) = a - b$ und somit n ein Teiler von $(a + c) - (b + c)$, also $a + c \equiv b + c \bmod n$.

Sei $a \equiv b \bmod n$, d. h., n ein Teiler von $a - b$. Für jede ganze Zahl c gilt $ac - bc = (a - b)c$, weshalb n auch ein Teiler von $ac - bc$ ist, also $ac \equiv bc \bmod n$.

Sei $a \equiv b \bmod n$. Die Aussage wird durch vollständige Induktion gezeigt. Für $m = 1$ ist die Aussage ist klar. Sei $m \leq 1$. Nach Induktionsannahme gilt $a^m \equiv b^m \bmod n$. Mit dem Multiplikationsgesetz folgt $a^{m+1} \equiv ab^m \bmod n$ und $ab^m \equiv b^{m+1} \bmod n$, woraus sich mittels Transitivität $a^{m+1} \equiv b^{m+1} \bmod n$ ergibt. □

Der Restklassenring modulo n

Die Kongruenz modulo n ist eine Äquivalenz auf der Menge der ganzen Zahlen und bewirkt somit eine Einteilung in Äquivalenzklassen, die in diesem Zusammenhang auch *Restklassen modulo n* genannt werden

$$\overline{a} = \{b \mid b \in \mathbb{Z} \wedge a \equiv b \bmod n\}, \quad a \in \mathbb{Z}. \tag{14.5}$$

Mit dem Restegesetz folgt, dass für die Menge aller Restklassen modulo n gilt

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}. \tag{14.6}$$

Beispiel 14.4. Die Restklassen modulo 4 sind $\overline{0} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$, $\overline{1} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$, $\overline{2} = \{\pm 2, \pm 6, \pm 10, \ldots\}$, $\overline{3} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

Auf der Menge der Restklassen modulo n werden Addition und Multiplikation definiert durch

$$\overline{a} + \overline{b} := \overline{a+b} \quad \text{und} \quad \overline{a} \cdot \overline{b} := \overline{a \cdot b}. \tag{14.7}$$

Beide Operationen sind anhand von Repräsentanten der Äquivalenzklassen festgelegt. Deshalb ist zu zeigen, dass die Operationen wohldefiniert (d. h., unabhängig von der Wahl der Repräsentanten) sind. Beispielsweise soll für Restklassen modulo 4 wegen $\overline{2} = \overline{-6}$ und $\overline{3} = \overline{11}$ gelten $\overline{2} + \overline{3} = \overline{-6} + \overline{11}$ und $\overline{2} \cdot \overline{3} = \overline{-6} \cdot \overline{11}$.

Satz 14.5. *Die Addition und Multiplikation in $\mathbb{Z}_n$ sind wohldefiniert.*

Beweis. Seien $\overline{a} = \overline{b}$ und $\overline{c} = \overline{d}$, d. h., $a - b = kn$ und $c - d = ln$ für gewisse $k, l \in \mathbb{Z}$. Dann ist $(a + c) - (b + d) = (a - b) + (c - d) = (k + l)n$ und somit $\overline{a+c} = \overline{b+d}$. Ferner ist $ac - bd = (b + kn)(d + ln) - bd = (bl + dk + kln)n$ und folglich $\overline{ac} = \overline{bd}$. □

Satz 14.6. *Sei $n \geq 2$ eine natürliche Zahl. Die Menge $\mathbb{Z}_n$ bildet einen kommutativen Ring.*

Beweis. Die Ringeigenschaften werden auf die entsprechenden Eigenschaften des Rings der ganzen Zahlen zurückgeführt. Beispielsweise wird die Kommutativität der Addition in $\mathbb{Z}_n$ mithilfe der Kommutativität der Addition in $\mathbb{Z}$ bewiesen: $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$. Die Null ist $\overline{0}$ und die Eins ist $\overline{1}$. □

Der Ring $\mathbb{Z}_n$ heißt *Restklassenring modulo n*. Im Folgenden wird jede Restklasse $\overline{a}$ modulo n durch den kleinsten, nichtnegativen Rest modulo n repräsentiert, also durch die Zahl a `mod` n.

Beispiel 14.7. Die Verknüpfungstafeln von $\mathbb{Z}_6$ lauten

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Satz 14.8. *Die Abbildung $\pi_n : \mathbb{Z} \to \mathbb{Z}_n : a \mapsto \overline{a}$ ist ein Epimorphismus.*

Beweis. Die Abbildung π_n ist surjektiv, die Einsen werden aufeinander abgebildet, $\pi_n(1) = \overline{1}$, und für beliebige ganze Zahlen a und b gilt $\pi_n(a) + \pi_n(b) = \overline{a} + \overline{b} = \overline{a + b} = \pi_n(a + b)$ und $\pi_n(a) \cdot \pi(b) = \overline{a} \cdot \overline{b} = \overline{a \cdot b} = \pi_n(a \cdot b)$. □

14.2 Rechnen in Restklassenringen

Potenzieren in Restklassenringen

Sei a eine ganze Zahl und m eine natürliche Zahl. In $\mathbb{Z}_n$ wird die Potenz a^m in zwei Schritten berechnet. Erstens wird der Exponent m binär dargestellt

$$m = m_k 2^k + \ldots + m_1 2 + m_0, \quad m_i \in \{0, 1\}, \tag{14.8}$$

und im *Horner-Schema* entwickelt

$$m = (\ldots (m_k 2 + m_{k-1})2 + \ldots + m_1)2 + m_0. \tag{14.9}$$

Mit den Potenzgesetzen folgt

$$a^m = (\ldots ((a^{m_k})^2 a^{m_{k-1}})^2 a^{m_{k-2}})^2 \cdots a^{m_1})^2 a^{m_0}. \tag{14.10}$$

Dadurch wird Potenzieren auf fortgesetztes Quadrieren und Multiplizieren zurückgeführt. Beispielsweise hat die Zahl $m = 25$ die Horner-Darstellung

$$25 = (((1 \cdot 2 + 1) \cdot 2 + 0) \cdot 2 + 0) \cdot 2 + 1.$$

Daraus folgt

$$a^{25} = (((a^2 a)^2)^2)^2 a.$$

Zweitens wird das Ergebnis beim Quadrieren oder Multiplizieren in $\mathbb{Z}_n$ jeweils durch den Rest modulo n dargestellt und mit den Resten weitergerechnet. Beispielsweise wird 99^{25} in $\mathbb{Z}_{13}$ wegen $99 \equiv 8 \bmod 13$ wie folgt berechnet

$$\begin{aligned}
8^{25} &= (((8^2 \cdot 8)^2)^2)^2 \cdot 8, \quad 8^2 \equiv 12 \bmod 13 \\
&= (((12 \cdot 8)^2)^2)^2 \cdot 8, \quad 12 \cdot 8 \equiv 5 \bmod 13 \\
&= ((5^2)^2)^2 \cdot 8, \quad 5^2 \equiv 12 \bmod 13 \\
&= (12^2)^2 \cdot 8, \quad 12^2 \equiv 1 \bmod 13 \\
&= 1^2 \cdot 8, \quad 1^2 \equiv 1 \bmod 13 \\
&= 8.
\end{aligned}$$

Neunerprobe

Satz 14.9. *Jede natürliche Zahl lässt bei Division durch 9 denselben Rest wie ihre Quersumme.*

Beweis. Sei a eine natürliche Zahl mit der Dezimaldarstellung $a = a_m 10^m + \ldots + a_1 10 + a_0$, wobei $a_i \in \{0, 1, \ldots, 9\}$. Wegen $10 \equiv 1 \bmod 9$ folgt $\overline{a} = \overline{a_m 10^m + \ldots + a_1 10 + a_0} = \overline{a_m}\,\overline{10}^m + \ldots + \overline{a_1}\,\overline{10} + \overline{a_0} = \overline{a_m} + \ldots + \overline{a_1} + \overline{a_0} = \overline{a_m + \ldots + a_1 + a_0}$. Dies ist definitionsgemäß gleichbedeutend mit $a \equiv (a_m + \ldots + a_1 + a_0) \bmod 9$. □

14.3 Lineare Kongruenzensysteme

Drei chinesische Bauern bauen Reis gemeinsam an und teilen den Ertrag gleichmäßig nach der Ernte. In einem Jahr ging jeder Bauer auf einen anderen Markt, um sein Drittel zu verkaufen. Die Märkte kaufen Reis nur im Vielfachen eines Grundgewichts. Der erste Bauer verkaufte auf einem Markt, auf dem das Grundgewicht 11 Pfund betrug. Er verkaufte so viel wie möglich und behielt 3 Pfund übrig. Entsprechend verkaufte der zweite und dritte Bauer auf einem Markt, auf dem das Grundgewicht 8 bzw. 15 Pfund betrug, und behielt 6 bzw. 13 Pfund übrig. Wie viel Reis haben die Bauern insgesamt zu Markte getragen? Dieses Problem lässt sich durch ein lineares Kongruenzensystem beschreiben.

Seien $n_1, n_2, \ldots, n_r$ natürliche Zahlen und $b_1, b_2, \ldots, b_r$ ganze Zahlen. Gesucht ist die Menge aller ganzzahligen Lösungen des Kongruenzensystems

$$x \equiv b_i \bmod n_i, \quad 1 \le i \le r. \tag{14.11}$$

Satz 14.10. (Chinesischer Restesatz) *Seien $n_1, n_2, \ldots, n_r$ paarweise teilerfremde Moduli und sei $n = \prod_i n_i$. Das Kongruenzensystem (14.11) hat eine eindeutig bestimmte Lösung x_0 mit $0 \le x_0 < n$. Die Menge aller Lösungen dieses Kongruenzensystems ist $\{x_0 + kn \mid k \in \mathbb{Z}\}$.*

Beweis. Zuerst wird für jedes i, $1 \le i \le r$, ein spezielles Kongruenzensystem gelöst

$$\begin{aligned} x &\equiv 1 \bmod n_i \\ x &\equiv 0 \bmod n_j, \quad j \ne i. \end{aligned} \tag{14.12}$$

Die Zahlen $\frac{n}{n_i}$ und n_i sind teilerfremd. Also gibt es nach dem Satz von Bezout ganze Zahlen s_i und t_i mit

$$s_i \frac{n}{n_i} + t_i n_i = 1.$$

Daraus folgt

$$s_i \frac{n}{n_i} \equiv 1 \bmod n_i.$$

Für jedes j mit $j \neq i$ ist n_j ein Teiler von $\frac{n}{n_i}$ und somit

$$s_i \frac{n}{n_i} \equiv 0 \bmod n_j.$$

Also ist $x_i = s_i \frac{n}{n_i}$ eine Lösung des Kongruenzensystems (14.12). Folglich ist $x = b_1 x_1 + \ldots + b_r x_r$ eine Lösung des Kongruenzensystems (14.11).

Für jede ganze Zahl k ist $x + kn$ eine weitere Lösung von (14.11), weil jedes n_i ein Teiler von n ist.

Seien x und x' Lösungen von (14.11). Dann ist $x - x' \equiv 0 \bmod n_i$ für alle $1 \leq i \leq r$. Also ist jedes n_i ist ein Teiler von $x - x'$ und somit das kgV der Moduli $n_1, \ldots, n_r$ ein Teiler von $x - x'$. Weil aber die Moduli paarweise teilerfremd sind, ist ihr kgV gleich n. Also ist n ein Teiler von $x - x'$ und somit $x' = x + kn$ für ein $k \in \mathbb{Z}$. □

Beispiel 14.11. Das Problem der Reisbauern führt auf das Kongruenzensystem

$$\begin{aligned} x &\equiv 3 \bmod 11 \\ x &\equiv 6 \bmod 8 \\ x &\equiv -2 \bmod 15. \end{aligned} \tag{14.13}$$

Zuerst werden drei spezielle Kongruenzensysteme gelöst, das erste davon lautet

$$\begin{aligned} x_1 &\equiv 1 \bmod 11 \\ x_1 &\equiv 0 \bmod 8 \\ x_1 &\equiv 0 \bmod 15. \end{aligned}$$

Der ggT von $n_1 = 11$ und $\frac{n}{n_1} = 8 \cdot 15 = 120$ wird als Linearkombination beider Zahlen entwickelt: $1 = 11 \cdot 11 + (-1) \cdot 120$. Also ist $x_1 = -120$ eine Lösung des ersten Kongruenzensystems. Auf analoge Weise ergeben sich Lösungen des zweiten und dritten Kongruenzensystems $x_2 = -495$ und $x_3 = 616$. Daraus erhalten wir eine spezielle Lösung des Kongruenzensystems (14.13)

$$x = 3 \cdot (-120) + 6 \cdot (-495) + (-2) \cdot 616 = -4562.$$

Mithin haben alle Lösungen des Kongruenzensystems (14.13) die Form $4562 + k \cdot 1320$ für $k \in \mathbb{Z}$. Die kleinste, nichtnegative Lösung lautet $x = 718$.

14.4 Kanonische Zerlegung von Restklassenringen

Der Restklassenring $\mathbb{Z}_n$ mit zusammengesetztem Modulus n ist in ein direktes Produkt von Restklassenringen anhand der kanonischen Primfaktorzerlegung von n zerlegbar.

Satz 14.12. *Seien $n_1, \ldots, n_r$ paarweise teilerfremde, natürliche Zahlen und sei $n = \prod_i n_i$. Der Restklassenring $\mathbb{Z}_n$ ist isomorph zum direkten Produkt der Restklassenringe $\mathbb{Z}_{n_i}$.*

Beweis. Sei $\phi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r} : a \mapsto (\pi_{n_1}(a), \ldots, \pi_{n_r}(a))$. Sei $(b_1, \ldots, b_r)$ ein Element von $\prod_i \mathbb{Z}_{n_i}$. Nach Satz 14.10 gibt es eine ganze Zahl a mit $0 \leq a \leq n$, die das Kongruenzensystem (14.11) löst. Also ist $\phi(a) = (b_1, \ldots, b_r)$ und somit ϕ surjektiv. Die Ringe $\mathbb{Z}_n$ und $\prod_i \mathbb{Z}_{n_i}$ haben dieselbe Mächtigkeit. Also ist ϕ nach Satz 6.8 bijektiv. Für beliebige Elemente $a, b \in \mathbb{Z}_n$ gilt

$$\begin{aligned}
\phi(a+b) &= (\pi_{n_1}(a+b), \ldots, \pi_{n_r}(a+b)), \quad \text{Definition von } \phi \\
&= (\pi_{n_1}(a) + \pi_{n_1}(b), \ldots, \pi_{n_r}(a) + \pi_{n_r}(b)), \quad \text{Homomorphismen } \pi_{n_i} \\
&= (\pi_{n_1}(a), \ldots, \pi_{n_r}(a)) + (\pi_{n_r}(b), \ldots, \pi_{n_r}(b)), \quad \text{Definition Addition} \\
&= \phi(a) + \phi(b).
\end{aligned}$$

Ähnliches gilt für die Multiplikation. Die Eins von $\mathbb{Z}_n$ wird auf die Eins $\phi(1) = (1, \ldots, 1)$ von $\prod_i \mathbb{Z}_{n_i}$ abgebildet. Damit ist alles bewiesen. □

Korollar 14.13. *Ist n eine natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{e_1} \ldots p_r^{e_r}$, dann ist der Restklassenring $\mathbb{Z}_n$ isomorph zum direkten Produkt der Restklassenringe $\mathbb{Z}_{p_i{}^{e_i}}$.*

Beispiel 14.14. Der Restklassenring $\mathbb{Z}_6$ ist isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_3$. Der Isomorphismus ϕ ist definiert durch die Zuordnung

a	0	1	2	3	4	5
$\phi(a)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$

14.5 Modulares Rechnen

Wir verwenden die Zerlegung von Restklassenringen dazu, um den Aufwand für arithmetische Operationen zu reduzieren. Hierbei werden arithmetische Berechnungen modulo paarweise teilerfremder Moduli n_i, $1 \leq i \leq r$, genommen, die Rechnungen in Restklassenringen $\mathbb{Z}_{n_i}$ durchgeführt und am Ende die Ergebnisse mit Hilfe des Chinesischen Restesatzes wieder zusammengefügt. Die Moduli sollten so gewählt sein, dass das Ergebnis der arithmetischen Rechnung mit der kleinsten, nichtnegativen Lösung des durch den Chinesischen Restesatz gegebenen Kongruenzensystems übereinstimmt.

Ein typisches Beispiel ist die Berechnung der Determinante einer ganzzahligen $n \times n$-Matrix $A = (a_{ij})$. Auch bei kleiner Determinante können große Zwischenergebnisse auftreten. Eine obere Schranke für die zu erwartende Größe der Determinante von A liefert die *Hadamard-Schranke*

$$|\det(A)| \leq \sqrt{\prod_{i=1}^{n} \sum_{j=1}^{n} a_{ij}^2}. \tag{14.14}$$

Wir schildern die Vorgehensweise beim modularen Rechnen der Einfachheit halber an der Multiplikation ganzer Zahlen.

Beispiel 14.15. Um ganze Zahlen $a = 13$ und $b = 17$ zu multiplizieren, wird das Produkt nach oben abgeschätzt, etwa durch $ab \leq 20 \cdot 20 = 400$. Die Moduli n_i werden so gewählt, dass deren Produkt oberhalb der Schranke liegt. Für die Moduli $n_1 = 4$, $n_2 = 3$, $n_3 = 5$ und $n_4 = 7$ gilt $n = \prod_i n_i = 420$. Das Produkt ab wird in drei Schritten berechnet:

1. Der Isomorphismus $\phi : \mathbb{Z}_{420} \to \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ liefert
$$\phi(a) = (1, 1, 3, 6) \quad \text{und} \quad \phi(b) = (1, 2, 2, 3).$$
2. Die Bilder $\phi(a)$ und $\phi(b)$ werden im Produktring $\prod_i \mathbb{Z}_{n_i}$ multipliziert
$$\phi(a)\phi(b) = (1 \cdot 1, 1 \cdot 2, 3 \cdot 2, 6 \cdot 3) = (1, 2, 1, 4).$$
3. Das lineare Kongruenzensystem
$$\begin{aligned} x &\equiv 1 \bmod 4 \\ x &\equiv 2 \bmod 3 \\ x &\equiv 1 \bmod 5 \\ x &\equiv 4 \bmod 7 \end{aligned}$$
hat die kleinste, nichtnegative Lösung $ab = 221$.

Ein nach dem Prinzip des modularen Rechnens arbeitendes Rechenwerk zeigt Abb. 14.2.

Selbsttestaufgaben

14.1. Bestätige $(1\,323\,744 \cdot 101\,657) \equiv 8 \bmod 10$.

14.2. Elferprobe: Sei a eine natürliche Zahl mit der Dezimaldarstellung $a = a_m 10^m + \ldots + a_1 10 + a_0$, wobei $a_i \in \{0, 1, \ldots, 9\}$. Zeige, dass gilt

$$a \equiv \sum_{i=0}^{m} (-1)^i a_i \bmod 11.$$

Ist 1 014 598 740 133 durch 11 teilbar?

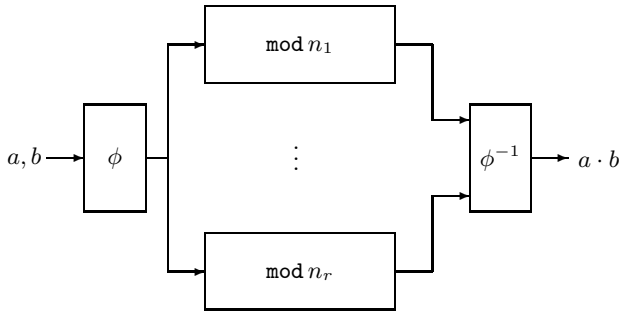

Abb. 14.2. Modulares Rechenwerk.

14.3. Löse im Restklassenring $\mathbb{Z}_7$ das Gleichungssystem $x + 3y = 4$, $2x + y = 0$.

14.4. Ermittle 33^{57} in $\mathbb{Z}_{17}$.

14.5. Berechne alle Lösungen des Kongruenzensystems

$$x \equiv -3 \bmod 31$$
$$x \equiv 2 \bmod 17$$
$$x \equiv 9 \bmod 16.$$

14.6. Zerlege $\mathbb{Z}_{180}$ in ein Produkt von Restklassenringen.

14.7. Betrachte in $\mathbb{Z}_{21} = \mathbb{Z}_3 \times \mathbb{Z}_7$ das Gleichungssystem $13x+11y = 14$ und $5x+6y = 5$. Löse dieses System durch modulares Rechnen in $\mathbb{Z}_3$ und $\mathbb{Z}_7$.

15

Einheiten in Restklassenringen

In diesem Kapitel wird die multiplikative Struktur von Restklassenringen untersucht. Diese Untersuchungen führen auf wichtige algebraische Grundstrukturen, Gruppen Integritätsringe und Körper. Abschließend wird das für die Datensicherheit wichtige RSA-Verfahren vorgestellt.

15.1 Einheiten und Nullteiler

Lineare Kongruenzen

Die lineare Gleichung im Restklassenring $\mathbb{Z}_n$

$$ax = b, \quad a, b \in \mathbb{Z}_n, \tag{15.1}$$

ist äquivalent zur linearen Kongruenz

$$ax \equiv b \bmod n, \quad a, b \in \mathbb{Z}. \tag{15.2}$$

Satz 15.1. *Seien a und b ganze Zahlen. Die lineare Kongruenz $ax \equiv b \bmod n$ ist lösbar genau dann, wenn $(a, n) \mid b$.*

Beweis. Sei $x = c$ eine Lösung von $ax \equiv b \bmod n$. Dann gibt es ein $k \in \mathbb{Z}$ mit $ac = b + kn$. Also ist jeder gemeinsame Teiler von a und n auch ein Teiler von b.

Sei $d = (a, n)$ ein Teiler von b, also $b = cd$ für ein $c \in \mathbb{Z}$. Nach dem Satz von Bezout gibt es ganze Zahlen s und t mit $d = sa + tn$, also $b = (cs)a + (ct)n$. Somit löst $x = cs$ die lineare Kongruenz. □

Einheiten

Ein Element $a \in \mathbb{Z}_n$ heißt eine *Einheit* oder *invertierbar* in $\mathbb{Z}_n$, wenn es ein $b \in \mathbb{Z}_n$ gibt mit $ab = 1$. Eine solches Element b wird *Inverses* von a genannt.

Lemma 15.2. *Jede Einheit in $\mathbb{Z}_n$ hat ein eindeutig bestimmtes Inverses.*

Beweis. Sind b und c Inverse von a, dann gilt definitionsgemäß $b = 1b = (ac)b = (ca)b = c(ab) = c1 = c$. □

Das Inverse einer Einheit $a \in \mathbb{Z}_n$ wird im Folgenden mit a^{-1} bezeichnet.

Satz 15.3. *Ein Element $a \in \mathbb{Z}_n$ ist eine Einheit genau dann, wenn a und n teilerfremd sind.*

Beweis. Definitionsgemäß ist a eine Einheit in $\mathbb{Z}_n$ genau dann, wenn $ax = 1$ in $\mathbb{Z}_n$ lösbar ist. Dies ist nach Satz 15.1 genau dann der Fall, wenn a und n teilerfremd sind. □

Inversenberechnung

Sei a eine Einheit in $\mathbb{Z}_n$. Nach Satz 15.3 müssen a und n teilerfremd sein. Nach dem Satz von Bezout gibt es ganze Zahlen s und t mit $sa + tn = 1$. Das Inverse von a ist dann

$$a^{-1} = s \bmod n. \tag{15.3}$$

Beispiel 15.4. Das Inverse von $a = 36$ in $\mathbb{Z}_{55}$ wird mit dem erweiterten euklidischen Algorithmus bestimmt: $26 \cdot 36 + (-17) \cdot 55 = 1$. Folglich ist $36^{-1} = 26$.

Nullteiler

Ein von Null verschiedenes Element $a \in \mathbb{Z}_n$ heißt ein *Nullteiler* in $\mathbb{Z}_n$, wenn es ein $b \neq 0$ in $\mathbb{Z}_n$ gibt mit $ab = 0$. Die Null wird nicht als Nullteiler angesehen.

Lemma 15.5. *Eine Einheit in $\mathbb{Z}_n$ ist kein Nullteiler.*

Beweis. Sei $a \in \mathbb{Z}_n$ eine Einheit. Angenommen, a wäre ein Nullteiler. Dann gibt es ein $b \neq 0$ in $\mathbb{Z}_n$ mit $ab = 0$. Es folgt $0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$, was der Annahme $b \neq 0$ widerspricht. □

Satz 15.6. *Jedes von Null verschiedene Element in $\mathbb{Z}_n$ ist entweder eine Einheit oder ein Nullteiler.*

Beweis. Sei $a \neq 0$ ein Element von $\mathbb{Z}_n$ Seien a und n teilerfremd. Nach Satz 15.3 ist dann a eine Einheit in $\mathbb{Z}_n$.

Sei $d = (a, n) > 1$, also $n = cd$ für ein $c \in \mathbb{Z}$. Nach dem Satz von Bezout existieren ganze Zahlen s und t mit $d = sa+tn$. Es folgt $n = cd = (cs)a+(ct)n$. Somit ist $(cs)a = 0$ in $\mathbb{Z}_n$. Angenommen, es wäre $cs = 0$ in $\mathbb{Z}_n$, also $n = (ct)n$. Mit der Kürzungsregel in $\mathbb{Z}$ folgt $ct = 1$, so dass c nach Lemma 15.5 widersprüchlicherweise eine Einheit in $\mathbb{Z}_n$ ist. Also ist $cs \neq 0$ und somit a ein Nullteiler in $\mathbb{Z}_n$. □

Beispiel 15.7. Der Restklassenring $\mathbb{Z}_8$ besitzt die Einheiten 1, 3 ($3^{-1} = 3$), 5 ($5^{-1} = 5$) und 7 ($7^{-1} = 7$) sowie die Nullteiler 2, $4(2 \cdot 4 = 0)$ und 6 ($6 \cdot 4 = 0$).

15.2 Die Anzahl der Einheiten

Die eulersche Φ-Funktion

Die Menge aller Einheiten in $\mathbb{Z}_n$ ist nach Satz 15.3 gegeben durch

$$\mathbb{Z}_n^* = \{a \mid a \in \mathbb{Z}_n, (a,n) = 1\}. \tag{15.4}$$

Die Abbildung $\Phi : n \to |\mathbb{Z}_n^*|$ wird *eulersche Φ-Funktion* genannt (Leonhard Euler, 1707-1783). Den anfänglichen Verlauf der eulerschen Φ-Funktion zeigt folgende Tabelle

n	$\Phi(n)$	$\mathbb{Z}_n^*$
2	1	1
3	2	1, 2
4	2	1, 3
5	4	1, 2, 3, 4
6	2	1, 5
7	6	1, 2, 3, 4, 5, 6
8	4	1, 3, 5, 7
9	6	1, 2, 4, 6, 7, 8
10	4	1, 3, 7, 9
11	10	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
12	4	1, 5, 7, 11

Satz 15.8. *Ist $n \geq 2$ eine natürliche Zahl mit kanonischen Primfaktorzerlegung $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, dann gilt*

$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right). \tag{15.5}$$

Beweis. Sei $A = \underline{n}$. Sei A_i die Menge aller Vielfachen von p_i in A für $1 \leq i \leq r$. Die Menge der zu n teilerfremden Zahlen $a \in A$ ist dann

$$A \setminus (\bigcup_{i=1}^{r} A_i).$$

Der Durchschnitt $A_{i_1} \cap \ldots \cap A_{i_s}$, $1 \leq i_1 < \ldots < i_s \leq r$, besteht aus allen ganzzahligen Vielfachen von $P = p_{i_1} \cdot \ldots \cdot p_{i_s}$, also $P, 2P, \ldots, \frac{n}{P}P$, und hat somit die Mächtigkeit $\frac{n}{P}$. Mit der Siebformel folgt

$$\begin{aligned}\Phi(n) = |A \setminus (\bigcup_{i=1}^{r} A_i)| &= |A| - \sum_{\substack{I \subseteq \underline{r} \\ I \neq \emptyset}} (-1)^{|I|-1} |\bigcap_{j \in I} A_j| \\ &= n - n\sum_{i=1}^{r} \frac{1}{p_i} + n \sum_{1 \leq i < j \leq r} \frac{1}{p_i p_j} - n \sum_{1 \leq i < j < k \leq r} \frac{1}{p_i p_j p_k} + \ldots\end{aligned}$$

$$\ldots + (-1)^{r-1} n \frac{1}{p_1 p_2 \cdots p_r}$$
$$= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

□

Beispiel 15.9. Wegen $1540 = 2^2 \cdot 5 \cdot 7 \cdot 11$ gilt

$$\Phi(1540) = 1540(1 - \frac{1}{2})(1 - \frac{1}{5})(1 - \frac{1}{7})(1 - \frac{1}{11}) = 480.$$

Die Sätze von Euler und Fermat

Satz 15.10. (Euler) *Für jede Einheit $a \in \mathbb{Z}_n$ gilt*

$$a^{\Phi(n)} = 1 \tag{15.6}$$

Beweis. Sei $\mathbb{Z}_n^* = \{a_1, \ldots, a_k\}$ die Menge aller Einheiten in $\mathbb{Z}_n$ und $P = \prod_i a_i$. Sei $a \in \mathbb{Z}_n^*$ und $a\mathbb{Z}_n^* = \{ab \mid b \in \mathbb{Z}_n^*\}$. Wir zeigen, dass $a\mathbb{Z}_n^* = \mathbb{Z}_n^*$. Einerseits ist $a\mathbb{Z}_n^* \subseteq \mathbb{Z}_n^*$, weil mit jeder Einheit b auch das Produkt ab nach Lemma 15.14 ein Einheit ist. Andererseits ist $\mathbb{Z}_n^* \subseteq a\mathbb{Z}_n^*$, weil jedes $b \in \mathbb{Z}_n^*$ in der Form $b = a(a^{-1}b)$ geschrieben werden kann und mit a und b wegen Lemma 15.14 auch $a^{-1}b$ ein Einheit ist. Daraus folgt $P = \prod_i (aa_i) = a^k P$. Nach Lemma 15.14 ist P als Produkt von Einheiten wiederum eine Einheit. Durch Multiplizieren von $P = a^k P$ mit P^{-1} ergibt sich $a^k = 1$. Wegen $\Phi(n) = k$ ergibt sich die Behauptung. □

Aus dem Satz von Euler und Satz 15.3 ergibt sich als Spezialfall der folgende

Satz 15.11. (Fermat) *Sei p eine Primzahl. Für jedes Element $a \neq 0$ von $\mathbb{Z}_p$ gilt*

$$a^{p-1} = 1. \tag{15.7}$$

Korollar 15.12. *Sei p eine Primzahl. Für jedes Element $a \in \mathbb{Z}_p$ gilt*

$$a^p = a. \tag{15.8}$$

Beweis. Die Gleichung (15.8) gilt nach dem Satz von Fermat für jedes $a \neq 0$ und sie gilt offenbar auch für $a = 0$. □

Potenzieren in Restklassenringen

Sei p prim. Der Aufwand für das Potenzieren in $\mathbb{Z}_p$ kann mithilfe des Satzes von Fermat verringert werden. Sei a eine ganze Zahl und m eine natürliche Zahl. Um die Potenz a^m in $\mathbb{Z}_p$ zu berechnen, wird der Exponent im p-adische Zahlensystem dargestellt

$$m = m_k p^k + \ldots + m_1 p + m_0, \quad m_i \in \{0, \ldots, p-1\}, \tag{15.9}$$

und im Horner-Schema entwickelt

$$m = (\ldots (m_k p + m_{k-1})p + \ldots + m_1 p) + m_0. \tag{15.10}$$

Mit den Potenzgesetzen und dem Satz von Fermat folgt

$$\begin{aligned} a^m &= (\ldots ((a^{m_k})^p a^{m_{k-1}})^p a^{m_{k-2}})^p \cdots a^{m_1})^p a^{m_0} \\ &= a^{m_k + m_{k-1} + \ldots + m_0}. \end{aligned} \tag{15.11}$$

Beispiel 15.13. Die Potenz 99^{25} wird in $\mathbb{Z}_{13}$ wegen $99 \equiv 8 \bmod 13$ wie folgt berechnet

$$\begin{aligned} \overline{8^{25}} = \overline{8}^{25} &= \overline{8}^{1 \cdot 13 + 12} \\ &= \overline{8}^{1+12}, \quad \text{nach (15.11)} \\ &= \overline{8}, \quad \text{nach (15.8)}. \end{aligned}$$

15.3 Integritätsringe und Körper

Einheiten in Ringen

Sei R ein Ring. Ein Element $a \in R$ heißt eine *Einheit* oder *invertierbar* in R, wenn es ein $b \in R$ gibt mit $a \cdot b = 1 = b \cdot a$. Das Element b wird dann *Inverses* von a genannt. Das Inverse von a ist nach dem Beweis von Lemma 15.2 eindeutig bestimmt und wird im Folgenden mit a^{-1} bezeichnet.

Lemma 15.14. *Sei R ein Ring und seien a, $b \in R$.*

- *Ist a eine Einheit, dann ist auch a^{-1} eine Einheit und es gilt*

$$(a^{-1})^{-1} = a. \tag{15.12}$$

- *Sind a und b Einheiten, so ist auch $a \cdot b$ eine Einheit und es gilt*

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}. \tag{15.13}$$

- *Ist a eine Einheit, dann ist a^m für jede natürliche Zahl m eine Einheit und es gilt*

$$(a^{-1})^m = (a^m)^{-1}. \tag{15.14}$$

Die negativen Potenzen einer Einheit $a \in R$ werden anhand der Inversen von a definiert

$$a^{-n} = (a^{-1})^n \quad \text{für alle } n \in \mathbb{N}. \tag{15.15}$$

Lemma 15.15. *Sei R ein Ring. Für jede Einheit $a \in R$ und alle ganzen Zahlen l und m gilt*

$$a^l \cdot a^m = a^{l+m} \quad \textit{und} \quad (a^l)^m = a^{lm}. \tag{15.16}$$

Ein kommutativer Ring heißt ein *Integritätsring*, wenn er keine Nullteiler enthält.

Satz 15.16. (Kürzungsregel) *Sei R ein Integritätsring und seien $a, b, c \in R$. Aus $ab = ac$ und $a \neq 0$ folgt $b = c$.*

Beweis. Sei $a \neq 0$ mit $ab = ac$, d. h., $a(b - c) = 0$. Da a kein Nullteiler ist, folgt $b - c = 0$. □

Satz 15.17. *Der Ring der ganzen Zahlen ist ein Integritätsring.*

Beweis. Angenommen, $a \in \mathbb{Z}$, $a \neq 0$, wäre ein Nullteiler. Dann gibt es ein von 0 verschiedenes Element $b \in \mathbb{Z}$ mit $ab = 0$. Es folgt $ab = 0 = a0$, woraus aufgrund der Kürzungsregel widersprüchlicherweise $b = 0$ folgt. □

Ein kommutativer Ring R heißt ein *Körper*, wenn jedes von Null verschiedene Element in R eine Einheit ist.

Satz 15.18. *Sei $n \geq 2$ eine natürliche Zahl. Der Restklassenring $\mathbb{Z}_n$ ist ein Körper genau dann, wenn n prim ist.*

Beweis. Nach Satz 15.3 sind alle von Null verschiedenen Elemente in $\mathbb{Z}_n$ Einheiten genau dann, wenn für alle ganzen Zahlen $a = 1, \ldots, n-1$ gilt $(a, n) = 1$. Dies ist genau dann der Fall, wenn n prim ist. □

15.4 Gruppen

Eine *Gruppe* ist ein Tripel $(G, \circ, e)$, bestehend aus einer nichtleeren Menge G, einer Operation $\circ : G \times G \to G : (a, b) \mapsto a \circ b$ und einem Element $e \in G$, wobei folgende Rechenregeln gelten:

- Die Operation $\circ$ is assoziativ, d. h., $(f \circ g) \circ h = f \circ (g \circ h)$ für alle $f, g, h \in G$.
- Das Element e ist *neutral*, d. h., $g \circ e = g = e \circ g$ für alle $g \in G$.
- Zu jedem Element $g \in G$ gibt es ein $h \in G$ mit $g \circ h = e = h \circ g$, ein solches Element h wird *Inverses* von g genannt.

Wenn keine Verwechslungen zu befürchten sind, wird eine Gruppe $(G, \circ, e)$ mit $(G, \circ)$ oder noch kürzer mit G bezeichnet. Das Produkt $g \circ h$ wird auch gh geschrieben. Eine Gruppe G heißt *abelsch*, wenn die Operation kommutativ ist. Eine Gruppe G heißt *endlich*, wenn die Menge G endlich ist. Als *Ordnung* einer Gruppe G wird die Anzahl der Elemente von G bezeichnet.

Lemma 15.19. *In einer Gruppe G ist das neutrale Element eindeutig bestimmt und jedes Element in G hat ein eindeutig bestimmtes Inverses.*

Das Inverse eines Gruppenelements $g \in G$ wird im Folgenden mit g^{-1} bezeichnet.

Beispiele 15.20.
- In einem Ring R ist die additive Teilstruktur $(R, +, 0)$ eine abelsche Gruppe, wie etwa $(\mathbb{Z}, +, 0)$ und $(\mathbb{Z}_n, +, 0)$.
- Multiplikative abelsche Gruppen sind $(\{\pm 1\}, \cdot)$, $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$ und $(\mathbb{C}\setminus\{0\}, \cdot)$.

Verknüpfungstafel

Satz 15.21. *Die Verknüpfungstafel einer endlichen Gruppe G bildet ein lateinisches Quadrat, d. h., in jeder Zeile und Spalte der Tafel tritt jedes Element aus G genau einmal auf.*

Beweis. Sei $G = \{g_1, \ldots, g_n\}$. Die Einträge in der i-ten Zeile der Verknüpfungstafel von G sind $g_i g_1, \ldots, g_i g_n$. Diese Einträge sind genau die Bilder der Linksmultiplikation $G \to G : g \mapsto g_i g$. Diese Abbildung ist injektiv, denn aus $g_i g = g_i h$ folgt durch Multiplikation beider Seiten mit dem Inversen von g_i sofort $g = h$. Nach Satz 6.8 ist diese Abbildung sogar bijektiv. Für die Spalten wird die Rechtsmultiplikation $G \to G : g \mapsto g g_i$ benutzt. □

Beispiel 15.22. Die kleinsche Vierergruppe (Felix Klein, 1849-1925) $V_4 = \{e, a, b, c\}$ ist durch folgende Verknüpfungstafel gegeben

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Diese Gruppe ist die kleinste nichtzyklische Gruppe. Jedes Gruppenelement ist selbstinvers.

Beispiele für Gruppen

Satz 15.23. *Sei R ein Ring. Die Menge aller Einheiten in R bildet zusammen mit der Multiplikation in R eine Gruppe.*

Beweis. Nach Lemma 15.14 ist das Produkt von Einheiten in R wiederum eine Einheit. Die Multiplikation in R ist assoziativ und das Einselement in R ist das neutrale Element. Nach Lemma 15.14 hat jede Einheit in R ein Inverses, das ebenfalls eine Einheit ist. □

Beispiele 15.24.
- Die Menge aller Einheiten eines Restklassenrings $\mathbb{Z}_n$ bildet eine Gruppe.
- Die Menge aller invertierbaren Matrizen $\mathrm{Gl}(n, \mathbb{K})$ in der Menge aller $n \times n$-Matrizen über einem Körper $\mathbb{K}$ bildet eine Gruppe. Die invertierbaren Matrizen sind genau die Matrizen mit von Null verschiedener Determinante.

Satz 15.25. *Sei A eine Menge. Die Menge aller bijektiven Abbildungen $f : A \to A$ bildet zusammen mit der Komposition eine Gruppe.*

Beweis. Nach Satz 6.6 ist die Komposition von bijektiven Abbildungen wiederum eine bijektive Abbildung. Gemäß Satz 6.4 ist die Komposition assoziativ und die identische Abbildung ist das neurale Element. Wegen Satz 6.7 hat jede bijektive Abbildung ein Inverses, das wiederum bijektiv ist. □

Die Gruppe $S_A = \{f \mid f : A \to A \text{ bijektiv}\}$ wird *symmetrische Gruppe* von A genannt. Für $A = \underline{n}$ heißt $S_{\underline{n}}$ auch *symmetrische Gruppe vom Grad n*, sie wird auch mit S_n bezeichnet. Die Gruppe S_n besteht aus allen Permutationen vom Grad n und hat nach Korollar 10.14 die Ordnung $n!$.

Beispiel 15.26. Die symmetrische Gruppe S_3 hat nach 6.14 die Verknüpfungstafel

	id	δ_1	δ_2	σ_1	σ_2	σ_3
id	id	δ_1	δ_2	σ_1	σ_2	σ_3
δ_1	δ_1	δ_2	id	σ_2	σ_3	σ_1
δ_2	δ_2	id	δ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	id	δ_2	δ_1
σ_2	σ_2	σ_1	σ_3	δ_1	id	δ_2
σ_3	σ_3	σ_2	σ_1	δ_2	δ_1	id

Untergruppen

Sei G eine Gruppe. Eine nichtleere Teilmenge U von G heißt eine *Untergruppe* von G, wenn U mit der Operation von G selbst eine Gruppe ist.

Lemma 15.27. (Untergruppenkriterium) *Sei G eine Gruppe. Eine nichtleere Teilmenge U von G ist eine Untergruppe von G genau dann, wenn für alle $u, v \in U$ gilt $uv^{-1} \in U$.*

Beweis. Sei U eine Untergruppe von G. Sei u_0 das neutrale Element in U. Dann folgt $u_0 = eu_0 = (u_0^{-1}u_0)u_0 = u_0^{-1}(u_0u_0) = u_0^{-1}u_0 = e$. Also ist das Inverse von $u \in U$ in beiden Gruppen dasselbe. Mit $v \in U$ liegt nach Voraussetzung auch v^{-1} in U und mit einem weiteren Element $u \in U$ auch das Produkt uv^{-1}.

Umgekehrt sei U eine nichtleere Teilmenge von G, für die die angegebene Bedingung gelte. Aus $v \in U$ folgt $e = vv^{-1} \in U$ und somit $v^{-1} = ev^{-1} \in U$. Mit einem weiteren Element $u \in U$ gilt also $uv = u(v^{-1})^{-1} \in U$. Also ist durch $U \times U \to U : (u, v) \mapsto uv$ eine Operation auf U gegeben, die als Einschränkung der Operation auf G ebenfalls assoziativ ist. Somit ist U eine Untergruppe von G. □

Beispiele 15.28.
- In jeder Gruppe G sind G und $\{e\}$ Untergruppen, die so genannten *trivialen Untergruppen* von G.
- Die nichttrivialen Untergruppen der kleinschen Vierergruppe sind $\{e, a\}$, $\{e, b\}$ und $\{e, c\}$.
- Jede Untergruppe der symmetrischen Gruppe S_n heißt eine *Permutationsgruppe vom Grad n*. Etwa bildet die Menge aller Drehungen $id = (1)(2)(3)$, $\delta_1 = (123)$ und $\delta_2 = (132)$ eines gleichseitigen Dreiecks nach 15.26 eine Permutationsgruppe vom Grad 3.
- Sei n eine ganze Zahl. Die Menge aller ganzzahligen Vielfachen $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ von n bildet eine Untergruppe von $(\mathbb{Z}, +)$.
- Sei n eine natürliche Zahl. Die Menge aller geraden Permutationen vom Grad n bildet nach Abs. 6.4 eine Untergruppe von S_n, die *alternierende Gruppe* $A_n = \{\pi \mid \pi \in S_n, \operatorname{sgn}(\pi) = 1\}$. Die alternierende Gruppe A_n ist nichtabelsch, falls $n \geq 5$.

Sei G eine Gruppe und $S \subseteq G$. Jede Untergruppe, die S enthält, muss auch $SS = \{ss' \mid s, s' \in S\}$ und $S^{-1} = \{s^{-1} \mid s \in S\}$ und damit alle endlichen Produkte enthalten, die aus den Elementen von $S \cup S^{-1}$ gebildet werden können.

Lemma 15.29. *Sei G eine Gruppe und $S \subseteq G$. Die kleinste Untergruppe von G, die S enthält, lautet*

$$\langle S \rangle = \{s_1 \cdots s_n \mid s_i \in S \cup S^{-1}, n \geq 0\}. \tag{15.17}$$

Beweis. Seien $s = s_1 \cdots s_m$ und $t = t_1 \ldots t_n$ Elemente von $\langle S \rangle$. Dann ist auch $st^{-1} = s_1 \cdots s_m t_n^{-1} \ldots t_1^{-1}$ ein endliches Produkt von Elementen aus $S \cup S^{-1}$, also $st^{-1} \in \langle S \rangle$. Nach dem Untergruppenkriterium ist $\langle S \rangle$ eine Untergruppe von G.

Sei U eine Untergruppe von G, die S enthält. Nach dem oben Gesagten muss U alle endlichen Produkte von Elementen aus $S \cup S^{-1}$ enthalten. Daraus folgt $\langle S \rangle \subseteq U$. □

Beispiel 15.30. Sei n eine natürliche Zahl. In der reellen euklidischen Ebene betrachten wir die Drehung d im Nullpunkt um den Winkel $2\pi/n$ und die

Spiegelung s an der y-Achse. Die von d und s erzeugte Gruppe heißt *Diedergruppe* D_n. Es gilt $d^n = id$, $s^2 = id$ und $dsd = s$. Mit Lemma 15.29 folgt, dass jedes Element in D_n von der Form $s^i d^j$ ist. Es ergibt sich

$$D_n = \langle\{s, d\}\rangle = \{id, d, \ldots, d^{n-1}, s, sd, \ldots, sd^{n-1}\}. \tag{15.18}$$

Also hat D_n die Ordnung $2n$.

Eine Gruppe G heißt *zyklisch*, wenn G von einem ihrer Elemente erzeugt wird, d. h., wenn es ein $g \in G$ gibt mit $G = \langle\{g\}\rangle$. Aus Lemma 15.29 folgt

$$G = \langle\{g\}\rangle = \{g^n \mid n \in \mathbb{Z}\}. \tag{15.19}$$

Wegen $g^m g^n = g^n g^m$ ist jede zyklische Gruppe abelsch.

Beispiele 15.31.
- Die additive Gruppe der ganzen Zahlen $\mathbb{Z}$ ist wegen $m = m1$ zyklisch und wird von 1 erzeugt. Ebenso ist die Gruppe der ganzzahligen Vielfachen $n\mathbb{Z}$ von n zyklisch und wird von n generiert.
- Die additive Gruppe $\mathbb{Z}_n$ ist wegen $m = m1$ zyklisch und wird von 1 erzeugt.
- Sei n eine natürliche Zahl. In der reellen euklidischen Ebene betrachten wir die Drehung d im Nullpunkt um den Winkel $2\pi/n$. Für die von d erzeugte zyklische Gruppe gilt

$$C_n = \langle\{d\}\rangle = \{id, d, \ldots, d^{n-1}\}. \tag{15.20}$$

  Also ist C_n eine Untergruppe von D_n.

Die Ordnung der von $g \in G$ erzeugten zyklischen Untergruppe von G heißt die *Ordnung* von g, sie wird mit $\mathrm{ord}(g)$ bezeichnet.

Satz 15.32. *Sei G eine Gruppe und $g \in G$. Die Ordnung von g ist unendlich oder gleich der kleinsten positiven Zahl n mit $g^n = e$. Hat g endliche Ordnung n, dann gilt*

$$\langle\{g\}\rangle = \{e, g, \ldots, g^{n-1}\}. \tag{15.21}$$

Beweis. Wir betrachten eine zyklische Untergruppe $\langle\{g\}\rangle = \{g^n \mid n \in \mathbb{Z}\}$. Entweder sind sämtliche Potenzen von g verschieden und g hat unendliche Ordnung, oder es gibt zwei ganze Zahlen i und j mit $g^i = g^j$. Hieraus folgt $g^k = e$ für $k = i - j > 0$. Sei m die kleinste natürliche Zahl mit $g^m = e$. Dann sind in $U = \{e, g, \ldots, g^{m-1}\}$ alle Elemente voneinander verschieden Wegen $g^m = e$ bildet U eine Untergruppe von G und wir haben $U = \langle\{g\}\rangle$. □

Nebenklassenzerlegung

Sei U eine Untergruppe von G. Zwei Elemente $g, h \in G$ heißen *U-äquivalent*, kurz $g \equiv_U h$, wenn es ein $u \in U$ gibt mit $gu = h$.

Lemma 15.33. *Die Relation $\equiv_U$ ist eine Äquivalenz auf G.*

Beweis. Für jedes $g \in G$ gilt $ge = g$ und somit $g \equiv_U g$. Also ist $\equiv_U$ reflexiv. Seien $g, h \in G$ mit $g \equiv_U h$, also $gu = h$ für ein $u \in U$. Dann ist $hu^{-1} = g$ und deshalb $h \equiv g$. Somit ist $\equiv_U$ symmetrisch. Seien $g, h, k \in G$ mit $g \equiv_U h$ und $h \equiv_U k$, also $gu = h$ und $hv = k$ für gewisse $u, v \in U$. Dann ist $g(uv) = k$ und folglich $g \equiv_U k$. Mithin ist $\equiv_U$ transitiv. □

Die Äquivalenzklasse von $g \in G$ hat die Gestalt $gU = \{gu \mid u \in U\}$, denn es gilt

$$h \in \overline{g} \Longleftrightarrow g \equiv_U h \Longleftrightarrow g^{-1}h \in U \Longleftrightarrow h \in gU. \tag{15.22}$$

Die Mengen gU, $g \in G$, werden *Linksnebenklassen* von U in G genannt. Mit G/U wird die Menge aller Linksnebenklassen von U in G bezeichnet, also die Quotientenmenge der U-Äquivalenz auf G. Die Anzahl der Linksnebenklassen von U in G heißt *Index* von U in G und wird mit $|G : U|$ bezeichnet.

Satz 15.34. (Lagrange, 1736-1813) *Ist U eine Untergruppe von G, dann gilt*

$$|G| = |U| \cdot |G : U|. \tag{15.23}$$

Beweis. Nach Satz 5.5 und Lemma 15.33 ist klar, dass G die disjunkte Vereinigung der Linksnebenklassen von U in G ist. Wir zeigen, dass die Abbildung $u \mapsto gu$ von U nach gU bijektiv ist. Offenbar ist diese Abbildung surjektiv. Sie ist injektiv, denn aus $gu = gv$ für $u, v \in U$ folgt durch Linksmultiplikation mit g^{-1} sofort $u = v$. Mithin erhellt sich $|U| = |gU|$ für alle $g \in G$. Daraus folgt die Behauptung. □

Für zyklische Untergruppen erhalten wir hieraus das folgende

Korollar 15.35. *In einer endlichen Gruppe ist die Ordnung jedes Gruppenelements ein Teiler der Gruppenordnung.*

Daraus erhellt sich sofort das nächste

Korollar 15.36. (Fermat) *In einer endlichen Gruppe G gilt $g^{|G|} = e$ für jedes Element $g \in G$.*

Normalteiler

Ist U eine Untergruppe von G und $g \in G$, dann setzen wir

$$gUg^{-1} = \{gug^{-1} \mid u \in U\}. \tag{15.24}$$

Ein *Normalteiler* ist eine Untergruppe U von G, in der für alle $g \in G$ gilt $gUg^{-1} = U$. Diese Bedingung ist äquivalent zu $gU = Ug$ für alle $g \in G$.

Satz 15.37. *Ist U ein Normalteiler von G, dann bildet G/U eine Gruppe mit der Operation*

$$G/U \times G/U \to G/U : (gU, hU) \mapsto ghU. \tag{15.25}$$

Beweis. Wir zeigen zuerst, dass die Operation wohldefiniert ist, da sie anhand von Repräsentanten festgelegt ist. Seien $g, g', h, h' \in G$ mit $gU = g'U$ und $hU = h'U$. Dann gibt es $u, v \in U$ mit $g' = gu$ und $h' = hv$. Also folgt $g'h'U = guhvU$. Wegen $hU = Uh$ gibt es ein $u' \in U$ mit $uh = hu'$. Damit erhellt sich $guhvU = ghu'vU = ghU$, was zu prüfen war. Weiter ist obige Operation assoziativ, da $(gU\,hU)g'U = ghUg'U = (gh)g'U = g(hg')U = gUhg'U = gU(hU\,g'U)$. Das neutrale Element ist $eU = U$, weil $eUgU = egU = gU = geU = gUeU$. Das Inverse von gU ist $g^{-1}U$, denn $gUg^{-1}U = gg^{-1}U = eU = g^{-1}gU = g^{-1}UgU$. □

Die Gruppe G/U heißt *Faktorgruppe* von G nach U.

Beispiele 15.38.
- Die trivialen Untergruppen einer Gruppe G sind stets Normalteiler von G.
- In jeder abelschen Gruppe ist jede Untergruppe ein Normalteiler.
- Die zyklische Gruppe C_n ist ein Normalteiler der Diedergruppe D_n, denn nach 15.30 gilt $dsd = s$ und somit $sC_ns = C_n$.
- Die Permutationsgruppe $U = \{id, \sigma_1\}$ ist kein Normalteiler der symmetrischen Gruppe S_3 in 15.26, denn es gilt $\delta_1 U = \{\delta_1, \sigma_3\}$ und $U\delta_1 = \{\delta_1, \sigma_2\}$.

Homomorphismen

Seien G und H Gruppen. Eine Abbildung $\nu : G \to H$ heißt ein *Homomorphismus*, wenn $\nu(gg') = \nu(g)\nu(g')$ für alle $g, g' \in G$. Für spezielle Homomorphismen werden die in Abs. 12.4 eingeführten Begriffe verwendet.

Lemma 15.39. *Sei $\nu : G \to H$ ein Homomorphismus. Der Kern von ν ist ein Normalteiler von G. Das Bild von G unter ν ist eine Untergruppe von H.*

Satz 15.40. (Homomorphiesatz) *Ist $\nu : G \to H$ ein Homomorphismus, dann ist die Abbildung $\psi : G/\ker(\nu) \to \nu(G) : g\ker(\nu) \mapsto \nu(g)$ ein Isomorphismus.*

Beweis. Sei $U = \ker(\nu)$. Seien $g, h \in G$ und $u, v \in U$. Es gilt $\psi(guU) = \nu(gu) = \nu(g)\nu(u) = \nu(g) = \nu(g)\nu(v) = \nu(gv) = \psi(gvU)$. Also ist ψ wohldefiniert. Ferner gilt definitionsgemäß $\psi(gU)\psi(hU) = \nu(g)\nu(h) = \nu(gh) = \psi(ghU) = \psi(gU\,hU)$. Die Abbildung ψ ist per definitionem surjektiv. Sie ist auch injektiv, denn aus $\nu(g) = \nu(h)$ folgt $\nu(h^{-1}g) = \nu(h)^{-1}\nu(g) = e$ in H, also $h^{-1}g \in U$, was $gU = hU$ zur Folge hat. □

Beispiele 15.41.
- Die Exponentialfunktion $x \mapsto e^x$ auf $\mathbb{R}$ ist ein Homomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R} \setminus \{0\}, \cdot)$.
- Die Abbildung $S_n \to (\{\pm 1\}, \cdot) : \pi \mapsto \operatorname{sgn}(\pi)$ ist nach Abs. 6.4 ein Homomorphismus. Der Kern dieses Homomorphismus ist die alternierende Gruppe A_n. Also ist die Abbildung $S_n/A_n \to (\{\pm 1\}, \cdot) : \pi A_n \mapsto \operatorname{sgn}(\pi)$ ein Isomorphismus.
- Die Abbildung $\mathbb{Z} \mapsto \mathbb{Z}_n : a \mapsto \overline{a}$ ist ein Epimorphismus mit dem Kern $n\mathbb{Z}$. Also ist $\mathbb{Z}/n\mathbb{Z}$ isomorph zu $\mathbb{Z}_n$.
- Der Multiplikationssatz für Determinanten, $\det(AB) = \det(A)\det(B)$, zeigt, dass $A \mapsto \det(A)$ einen Homomorphismus von $\mathrm{Gl}(n, \mathbb{K})$ auf $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ liefert. Der Kern hiervon ist $\mathrm{Sl}(n, \mathbb{K}) = \{A \in \mathrm{Gl}(n, \mathbb{K}) \mid \det(A) = 1\}$. Also ist $\mathrm{Gl}(n, \mathbb{K})/\mathrm{Sl}(n, \mathbb{K})$ isomorph zu $\mathbb{K}^*$.

Satz 15.42. *Jede Gruppe G ist isomorph zu einer Gruppe von Permutationen von G.*

Beweis. Für jedes $g \in G$ definiere die Linksmultiplikation $L(g) : G \to G : h \mapsto gh$. Diese Abbildung ist bijektiv, also $L(g) \in S_G$. Die Menge aller Linksmultiplikation $L(G) = \{L(g) \mid g \in G\}$ bildet eine Gruppe mit der Komposition von Abbildungen. Mithin ist $L(G)$ eine Untergruppe von S_G. Schließlich ist die Abbildung $\phi : G \to L(G) : g \mapsto L(g)$ ein Isomorphismus. □

Korollar 15.43. *Jede Gruppe der Ordnung n ist isomorph zu einer Permutationsgruppe vom Grad n.*

Beispiel 15.44. Die kleinsche Vierergruppe $V_4 = \{e, a, b, c\}$ ist isomorph zur Permutationsgruppe $G = \{id, (12)(34), (13)(24), (14)(23)\}$ vom Grad vier.

15.5 RSA-Verfahren

Das RSA-Verfahren wurde von Rivest, Shamir und Adleman (1978) zur Verschlüsselung von Nachrichten entwickelt. Es gilt als das prototypische Verfahren mit öffentlichen Schlüsseln (Public-Key-Verfahren).

Allgemeines Public-Key-Verfahren

Über ein Kommunikationsnetz sollen Teilnehmer geheime Nachrichten austauschen können. Das Konzept von Diffie und Hellman (1976) sah vor, jeden

Teilnehmer T mit einem *öffentlichen Schlüssel* und einem *privaten Schlüssel* auszustatten. Während der private Schlüssel geheim gehalten wird, wird der öffentliche Schlüssel in einem öffentlichen Verzeichnis abgelegt und so allen Teilnehmern zugänglich gemacht. Der öffentliche Schlüssel bestimmt die Chiffrierung und der private Schlüssel die Dechiffrierung einer Nachricht.

Ein Teilnehmer T, der eine Nachricht an einen Teilnehmer T' senden möchte, geht wie folgt vor:

- Der Teilnehmer T entnimmt den öffentlichen Schlüssel des Empfängers aus dem Verzeichnis, chiffriert die Nachricht mithilfe dieses Schlüssels und sendet die chiffrierte Nachricht an den Empfänger.
- Der Empfänger dechiffriert die erhaltene Nachricht mithilfe seines privaten Schlüssels.

Die Chiffrierung und Dechiffrierung müssen folgenden Anforderungen genügen:

- Das Chiffrieren wird durch Dechiffrieren rückgängig gemacht.
- Die Verfahren des Chiffierens und Dechiffrierens sind effizient realisierbar und beide Verfahren sind allen Teilnehmern bekannt.
- Der private Schlüssel eines Teilnehmers kann nicht aus seinem öffentlichen Schlüssel hergeleitet werden.

Öffentliche und private Schlüssel

Das RSA-Verfahren realisiert das Konzept von Diffie und Hellman. Dabei wählt jeder Teilnehmer zwei große Primzahlen p und q und berechnet das Produkt $N = pq$ sowie $\Phi(N) = (p-1)(q-1)$. Er wählt eine Einheit e modulo $\Phi(N)$, am besten eine Primzahl, und berechnet deren Inverses d modulo $\Phi(N)$ anhand des erweiterten euklidischen Algorithmus'

$$ed \equiv 1 \bmod \Phi(N). \tag{15.26}$$

Der öffentliche Schlüssel des Teilnehmers T ist durch das Paar (N, e) gegeben, während der private Schlüssel die Zahl d bildet.

Chiffrierung und Dechiffrierung

Eine zu chiffrierende Nachricht wird anhand einer Zahl aus der Menge $\{0, 1, \ldots, N-1\}$ codiert. Ist die Nachricht zu lang, dann wird sie in eine entsprechenden Zahlenfolge zerlegt und jedes Glied der Folge separat chiffriert. Eine Nachricht wird *chiffriert* anhand der Abbildung

$$\gamma : \mathbb{Z}_N \to \mathbb{Z}_N : a \mapsto a^e. \tag{15.27}$$

Eine empfangene Nachricht wird *dechiffriert* vermöge der Abbildung

$$\delta : \mathbb{Z}_N \to \mathbb{Z}_N : a \mapsto a^d. \tag{15.28}$$

Beide Abbildungen sind durch fortgesetztes Quadrieren und Multiplizieren effizient realisiert.

Satz 15.45. *Es gilt* $\delta\gamma = id_{\mathbb{Z}_N}$.

Beweis. Nach (15.26) gibt es eine ganze Zahl k mit $ed = 1 + k\Phi(N)$. Nach Satz 14.12 gibt es einen Isomorphismus $\pi : \mathbb{Z}_N \to \mathbb{Z}_p \times \mathbb{Z}_q : a \mapsto (\pi_p(a), \pi_q(a))$. Für jedes $a \in \mathbb{Z}_N$ gilt mit dem Satz von Fermat $\pi(a^{ed}) = \pi(a)^{ed} = (\pi_p(a), \pi_q(a))^{ed} = (\pi_p(a)^{ed}, \pi_q(a)^{ed}) = (\pi_p(a), \pi_q(a)) = \pi(a)$. Da π ein Isomorphismus ist, folgt $a^{ed} = a$. □

Die praktische Sicherheit des RSA-Verfahrens beruht darauf, dass es schwierig ist, den Modulus N in Primfaktoren zu zerlegen, wenn seine Faktoren p und q sehr groß sind (genauer, etwa gleich groß und mindestens 100-stellig). Große Primzahlen lassen sich schnell mithilfe eines probabilistischen Primzahltests erzeugen.

Selbsttestaufgaben

15.1. Beweise die Lemmata 15.14 und 15.15.

15.2. Zeige, dass für die eulersche Φ-Funktion gilt

- $\Phi(p) = p - 1$ für jede Primzahl p.
- $\Phi(p^n) = p^{n-1}(p-1)$ für Primzahlpotenz p^n.
- $\Phi(pq) = \Phi(p)\Phi(q)$, falls p und q verschiedene Primzahlen sind.

15.3. Berechne alle Einheiten und Nullteiler in $\mathbb{Z}_{20}$.

15.4. Zeige, dass die Menge aller Matrizen der Form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a, b \in \mathbb{R},$$

einen Körper mit den üblichen Matrizenoperationen bildet.

15.5. Sei p eine Primzahl. Zeige, dass ± 1 die einzigen Elemente in $\mathbb{Z}_p$ sind, die selbstinvers sind.

15.6. Ein Ring R heißt *einfach*, wenn R außer $\{0\}$ und R keine weiteren Ideale besitzt. Zeige, dass der Matrizenring $\mathbb{K}^{n\times n}$ über einem Körper $\mathbb{K}$ einfach ist.

15.7. Sei eine binäre Relation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definiert durch

$$(a, b) \simeq (c, d) \quad :\Longleftrightarrow \quad ad = bc.$$

Zeige, dass diese Relation eine Äquivalenz ist. Die Äquivalenzklasse von (a, b) sei mit $\frac{a}{b}$ bezeichnet. Zeige, dass die Menge aller Äquivalenzklassen zusammen mit der Addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und der Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

einen Körper bildet. Dies ist der *Körper der rationalen Zahlen* $\mathbb{Q}$.

15.8. Beweise das Lemma 15.19.

15.9. Zeige, dass jede Untergruppe einer zyklischen Gruppe zyklisch ist. Folgere daraus, dass jede Untergruppe von $\mathbb{Z}$ von der Form $n\mathbb{Z}$ ist, wobei $n = 0$ oder n die kleinste in der Untergruppe vorkommende natürliche Zahl ist.

15.10. Sei G eine abelsche Gruppe. Zeige, dass für alle Elemente g und h in G gilt $\mathrm{ord}(gh) = [\mathrm{ord}(g), \mathrm{ord}(h)]$.

15.11. Beweise das Lemma 15.39.

15.12. Vervollständige den Beweis von Satz 15.42.

15.13. Sei U eine Untergruppe und V ein Normalteiler einer Gruppe G. Zeige, dass UV eine Untergruppe von G, $U \cap V$ ein Normalteiler von U und UV/V isomorph zu $U/U \cap V$ ist. Folgere daraus, dass S_4/V_4 isomorph zu S_3 ist.

15.14. Seien U und V Normalteiler einer Gruppe G mit $U \subseteq V$. Zeige, dass V/U ein Normalteiler von G/U ist und $(G/U)/(V/U)$ isomorph zu G/V ist. Formuliere diese Aussagen für die Untergruppen von $\mathbb{Z}$.

16

Polynome

In diesem Kapitel wird die Teilbarkeitslehre in Polynomringen ganz analog zur Teilbarkeitslehre im Ring der ganzen Zahlen entwickelt. Zudem wird am Ende des Kapitels eine elektronisch realisierbare Schaltung für die Polynomdivision vorgestellt.

16.1 Polynomringe

Sei R ein kommutativer Ring. Ein *Polynom* über R ist eine unendliche Folge $f = (f_i)$ mit Koeffizienten in R, in der *fast alle* (d. h., alle bis auf endlich viele) Glieder 0 sind. Ein Polynom $f = (f_0, f_1, \ldots, f_n, 0, 0, \ldots)$ wird als formale Summe geschrieben

$$f = f_0 + f_1 x + \ldots + f_n x^n \tag{16.1}$$

und als Polynom in einer *Unbestimmten* x über R bezeichnet. Die Unbestimmte x ist also Teil der Notation. Das Glied f_i heißt *i-ter Koeffizient* von f. Der 0-te Koeffizient f_0 wird auch *konstantes Glied* genannt.

Der *Grad* eines Polynoms f ist der größte Index n mit $f_n \neq 0$, abgekürzt $\operatorname{grad}(f) = n$, das Glied f_n heißt auch *Leitkoeffizient* von f. Im Falle $f_n = 1$ heißt f *normiert*. Sind alle Koeffizienten von f gleich 0, dann ist f das *Nullpolynom*. Dem Nullpolynom wird kein Grad zugeordnet. Die Polynome vom Grad 0 heißen *konstante Polynome* und die Polynome vom Grad 1 *lineare Polynome*.

Polynomringe

Im Folgenden bezeichne $R[x]$ die Menge aller Polynome in der Unbestimmten x über R. Auf $R[x]$ werden *Addition* und *Multiplikation* definiert

$$f + g = \sum_{i=0}^{\max\{m,n\}} (f_i + g_i) x^i \tag{16.2}$$

und

$$fg = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} f_j g_{i-j} \right) x^i, \tag{16.3}$$

wobei $m = \text{grad}(f)$ und $n = \text{grad}(g)$.

Satz 16.1. *Sei R ein kommutativer Ring. Die Menge $R[x]$ aller Polynome in x über R bildet einen kommutativen Ring.*

Der Ring $R[x]$ wird *Polynomring* in x über R genannt.

Beispiel 16.2. Sind $f = 1 + 2x + 2x^2$ und $g = 3 + 2x$ Polynome in $\mathbb{Z}_4[x]$, dann gilt $f + g = (1 + 3) + (2 + 2)x + 2x^2 = 2x^2$ und $fg = (1 \cdot 3) + (1 \cdot 2 + 2 \cdot 3)x + (2 \cdot 2 + 2 \cdot 3)x^2 + (2 \cdot 2)x^3 = 3 + 2x^2$.

Eigenschaften von Polynomringen

Satz 16.3. *Der Polynomring $R[x]$ besitzt einen zum Koeffizientenring R isomorphen Unterring.*

Beweis. Für konstante Polynome in $R[x]$ gilt

$$(a_0, 0, \ldots) + (b_0, 0, \ldots) = (a_0 + b_0, 0, \ldots)$$

und

$$(a_0, 0, \ldots)(b_0, 0, \ldots) = (a_0 b_0, 0, \ldots).$$

Also sind Summe und Produkt von konstanten Polynomen wiederum konstante Polynome. Deshalb bildet die Menge aller konstanten Polynome in $R[x]$ einen Unterring R_0 von $R[x]$. Die Abbildung $R \to R_0 : a \mapsto (a, 0, \ldots)$ ist ein Isomorphismus. □

Lemma 16.4. *Für alle von Null verschiedenen Polynome $f, g \in R[x]$ gilt*

- $\text{grad}(f + g) \leq \max\{\text{grad}(f), \text{grad}(g)\}$, *falls* $f + g \neq 0$.
- $\text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g)$, *falls* $fg \neq 0$.
- $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$, *falls R ein Integritätsring ist.*

Beweis. Die Gradungleichungen folgen aus den Definitionen. Sei R ein Integritätsring und seien $f, g \in R[x]$ mit $fg \neq 0$. Ist f_n der Leitkoeffizient von f und g_m der Leitkoeffizient von g, dann ist $f_n g_m$ der Leitkoeffizient von fg, weil R nullteilerfrei ist. Also folgt $\text{grad}(fg) = n + m = \text{grad}(f) + \text{grad}(g)$. □

Aus dem letzten Teil des Beweises ergibt sich sofort der folgende

Satz 16.5. *Ist R ein Integritätsring, dann ist auch $R[x]$ ein Integritätsring.*

Satz 16.6. *Sei R ein Integritätsring. Die Einheiten in $R[x]$ sind genau die Einheiten in R.*

Beweis. Sei f eine Einheit in $R[x]$. Dann gibt es ein $g \in R[x]$ mit $fg = 1$. Für den Grad von fg gilt nach Lemma 16.4

$$0 = \text{grad}(1) = \text{grad}(fg) = \text{grad}(f) + \text{grad}(g).$$

Es folgt $\text{grad}(f) = \text{grad}(g) = 0$. Also ist f ein invertierbares konstantes Polynom, mithin nach Satz 16.3 eine Einheit in R. □

Zwei Polynome f und g in $R[x]$ heißen *assoziiert*, wenn es eine Einheit h in $R[x]$ gibt mit der Eigenschaft $f = hg$. Ist R ein Integritätsring, dann unterscheiden sich assozierte Polynome in $R[x]$ nach Satz 16.6 nur durch eine Einheit in R.

16.2 Teilbarkeitslehre

Die Teilbarkeitslehre in Polynomringen wird ganz analog zur Teilbarkeitslehre im Ring der ganzen Zahlen entwickelt. Im Folgenden sei $\mathbb{K}$ ein Körper und x eine Unbestimmte über $\mathbb{K}$.

Division mit Rest

Satz 16.7. (Divisionssatz) *Für jedes Paar von Polynomen f und $g \neq 0$ in $\mathbb{K}[x]$ gibt es eindeutig bestimmte Polynome q und r mit*

$$f = qg + r \quad \textit{und} \quad [r = 0 \quad \textit{oder} \quad \text{grad}(r) < \text{grad}(g)]. \tag{16.4}$$

Beweis. Ist f das Nullpolynom, dann liefert $q = r = 0$ die geforderte Darstellung. Gleiches gilt, wenn f einen kleineren Grad als g besitzt. In diesem Fall liefert $q = 0$ und $r = f$ die gewünschte Darstellung.

Sei die Aussage für alle Polynome f vom Grad $< m$ schon bewiesen. Seien $f = f_m x^m + \ldots + f_0 \in \mathbb{K}[x]$ vom Grad m und $g = g_n x^n + \ldots + g_0 \in \mathbb{K}[x]$ vom Grad n. O.B.d.A. können wir $m \geq n$ annehmen. Wir betrachten das Polynom

$$h = f - f_m g_n^{-1} x^{m-n} g.$$

In diesem Polynom ist der Koeffizient von x^m gleich 0, sodass sein Grad kleiner als m ist. Nach Induktionsannahme gibt es Polynome q_1 und r in $\mathbb{K}[x]$ mit $h = q_1 g + r$, wobei $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$. Dann folgt

$$f = f_m g_n^{-1} x^{m-n} g + h = (f_m g_n^{-1} x^{m-n} + q_1) g + r.$$

Damit ist die Existenz der Darstellung bewiesen.

Wir zeigen noch, dass q und r eindeutig bestimmt sind. Seien $f = qg + r$ und $f = q'g + r'$ zwei derartige Darstellungen. Dann folgt $(q - q')g = r' - r$. Angenommen, das Polynom $r' - r$ wäre von Null verschieden. Mit dem Lemma 16.4 folgt dann widersprüchlicherweise $\text{grad}(r - r') < \text{grad}(g) \leq \text{grad}((q - q')g)$. Also ist $r = r'$ und somit $(q - q')g = 0$. Da $\mathbb{K}[x]$ nach Satz 16.5 nullteilerfrei ist, impliziert $g \neq 0$ sofort $q = q'$. □

Dieser Beweis beschreibt das aus der Schulmathematik bekannte Divisionsverfahren für Polynome (Alg. 16.1).

Algorithmus 16.1 Polynomdivision

Eingabe: Polynome f und g, $\text{grad}(g) > 0$
Ausgabe: Polyome q und r mit $f = qg + r \wedge [r = 0 \vee \text{grad}(r) < \text{grad}(g)]$

```
 1: q := 0
 2: r := f
 3: while r ≠ 0 ∧ grad(r) ≥ grad(g) do
 4:    m := grad(r);
 5:    n := grad(g);
 6:    a := lk(r) {Leitkoeffizient}
 7:    b := lk(g)
 8:    q := q + (a/b) x^(m−n)
 9:    r := r − (a/b) x^(m−n) g
10: end while
11: return (q, r)
```

Beispiel 16.8. Seien $f = x^3 + 2x^2 + 3x + 1$ und $g = x^2 - x - 1$ Polynome mit reellwertigen Koeffizienten. Der Divisionsalgorithmus liefert $r_1 = f - xg = 3x^2 + 4x + 1$ und $r_2 = r_1 - 3g = 7x + 4$ sowie $q_1 = 0 + x = x$ und $q_2 = q_1 + 3 = x + 3$. Daraus folgt $f = (x + 3)g + (7x + 4)$.

In der Darstellung (16.4) wird q der *Quotient* und r der *Rest* von f *modulo* g genannt. Für die Infixoperatoren

$$f \,\texttt{div}\, g = q \quad \text{und} \quad f \,\texttt{mod}\, g = r \tag{16.5}$$

gilt

$$f = (f \,\texttt{div}\, g) \cdot g + (f \,\texttt{mod}\, g). \tag{16.6}$$

Teilbarkeitsrelation

Seien $f, g \in \mathbb{K}[x]$. Wir sagen, f *teilt* g, kurz $f \mid g$, wenn es ein Polynom $h \in \mathbb{K}[x]$ gibt mit $fh = g$.

Lemma 16.9. *Seien f und g von 0 verschiedene Polynome in $\mathbb{K}[x]$.*

- *Ist f ein Teiler von g, dann ist* $\text{grad}(f) \leq \text{grad}(g)$.
- *Sind f und g assoziiert, dann ist* $\text{grad}(f) = \text{grad}(g)$.
- *Es sind f und g assoziiert genau dann, wenn f ein Teiler von g und g ein Teiler von f.*
- *Sind f und g normiert, f ein Teiler von g und g ein Teiler von f, dann ist $f = g$.*

Beweis. Die erste Aussage folgt direkt aus Lemma 16.4. Die zweite Aussage ergibt sich mit Lemma 16.4 und Satz 16.6.

Seien f und g assoziiert, also $f = hg$ für eine Einheit $h \in \mathbb{K}[x]$. Dann folgt $g = h^{-1}f$ und somit die rechte Seite der Aussage. Umgekehrt sei f ein Teiler von g und g ein Teiler von f, also $f = hg$ und $g = h'f$ für gewisse $h, h' \in \mathbb{K}[x]$. Daraus ergibt sich $f = (hh')f$. Dann folgt mit Lemma 16.4 der Reihe nach $\operatorname{grad}(hh') = 0$ und $\operatorname{grad}(h) = \operatorname{grad}(h') = 0$.

Seien f und g normiert, f ein Teiler von g und g ein Teiler von f. Gemäß der letzten Aussage gibt es eine Einheit $h \in \mathbb{K}[x]$ mit $f = hg$. Wegen Satz 16.6 liegt h in $\mathbb{K}$. Da f und g normiert sind, folgt durch Vergleich der Leitkoeffizienten $h = 1$. □

Größte gemeinsame Teiler (ggT), *kleinste gemeinsame Vielfache* (kgV) und *Teilerfremdheit* von Polynomen werden wie im Ring der ganzen Zahlen definiert (Abs. 13.1).

Satz 16.10. *Der ggT von Polynomen $f_1, \ldots, f_n \in \mathbb{K}[x]$ ist eindeutig bestimmt bis auf assozierte Elemente.*

Für beliebige Polynome $f_1, \ldots, f_n$ in $\mathbb{K}[x]$ gibt es nach Satz 16.6 ein eindeutig bestimmtes, normiertes Polynom in $\mathbb{K}[x]$, das ggT von $f_1, \ldots, f_n$ ist. Dieses Polynom wird mit $(f_1, \ldots, f_n)$ bezeichnet.

Der euklidische Algorithmus

Der ggT von Polynomen wird mithilfe des *euklidischen Algorithmus* berechnet. Seien f und $g \neq 0$ Polynome in $\mathbb{K}[x]$. Wir setzen $f_0 = f$ und $f_1 = g$ und erhalten eine Folge von Polynomen f_i durch sukzessive Division mit Rest

$$\begin{aligned} f_0 &= q_1 f_1 + f_2 \\ f_1 &= q_2 f_2 + f_3 \\ f_2 &= q_3 f_3 + f_4 \\ &\ldots \end{aligned} \tag{16.7}$$

Satz 16.11. *Seien f und $g \neq 0$ Polynome in $\mathbb{K}[x]$. In (16.7) gibt es eine Gleichung $f_n = q_{n+1} f_{n+1} + f_{n+2}$ mit $f_{n+1} \neq 0$ und $f_{n+2} = 0$. Das Polynom f_{n+1} ist der ggT von f und g.*

Beweis. Die Folge der Grade der Polynome f_i in (16.7) fällt streng monoton: $\operatorname{grad}(f_1) > \operatorname{grad}(f_2) > \ldots$. Also existiert in der Folge eine Gleichung $f_n = q_{n+1} f_{n+1} + f_{n+2}$ mit $f_{n+1} \neq 0$ und $f_{n+2} = 0$.

Sei $d = f_{n+1}$. Wir zeigen, dass d jedes Polynom f_i, $0 \leq i \leq n+1$, teilt. Der Induktionsanfang ist klar. Sei die Aussage für alle Polynome f_j mit $j \geq i$ schon gezeigt. Wegen $f_{i-1} = q_i f_i + f_{i+1}$ ist d nach Induktionsannahme auch ein Teiler von f_{i-1}. Somit teilt d auch $f_0 = f$ und $f_1 = g$.

Sei c ein Teiler von f und g. Wir zeigen, dass c jedes Polynom f_i, $0 \leq i \leq n+1$, teilt. Der Induktionsanfang ist klar. Sei die Aussage für alle Polynome f_j mit $j \leq i$ schon bewiesen. Wegen $f_{i-1} = q_i f_i + f_{i+1}$ ist c nach Induktionsannahme auch ein Teiler von f_{i+1}. Folglich ist c auch ein Teiler von $f_{n+1} = d$. □

Das obige Verfahren führt auf den euklidischen Algorithmus (16.2).

Algorithmus 16.2 Euklidischer Algorithmus

Eingabe: Polynome f und $g \neq 0$
Ausgabe: ggT von f und g
1: $y := f$
2: $z := g$
3: **while** $z \neq 0$ **do**
4: $\quad y := z$
5: $\quad z := y \bmod z$
6: **end while**
7: **return** y

Beispiel 16.12. Für die reellwertigen Polynome $f = x^3 + 2x^2 + 3x + 1$ und $g = x^2 - x - 1$ liefert der euklidsche Algorithmus

$$\begin{aligned} x^3 + 2x^2 + 3x + 1 &= (x+3)(x^2 - x - 1) + (7x + 4) \\ x^2 - x - 1 &= (\frac{1}{7}x - \frac{11}{49})(7x + 4) - \frac{5}{49} \\ 7x + 4 &= (-\frac{343}{5}x - \frac{196}{5})(-\frac{5}{49}). \end{aligned}$$

Also ist $(f, g) = 1$.

Satz 16.13. (Bezout) *Seien $f_1, \ldots, f_n$ Polynome in $\mathbb{K}[x]$. Der ggT von $f_1, \ldots, f_n$ ist als Linearkombination dieser Polynome darstellbar, d. h., es gibt $s_1, \ldots, s_n \in \mathbb{K}[x]$ mit*

$$(f_1, \ldots, f_n) = s_1 f_1 + \ldots + s_n f_n. \tag{16.8}$$

Der Beweis verläuft ähnlich wie der der ganzzahligen Variante (Satz 13.9). Der ggT zweier Polynome f und g wird als Linearkombination von f und g durch sukzessives rückwärtiges Einsetzen in den euklidischen Algorithmus erhalten. Dieser so ergänzte Algorithmus heißt *erweiterter euklidischer Algorithmus*.

Beispiel 16.14. Aus der Berechnung des ggT der reellwertigen Polynome $f = x^3 + 2x^2 + 3x + 1$ und $g = x^2 - x - 1$ in 16.12 ergibt sich durch rückwärtiges Einsetzen

$$\begin{aligned}\frac{5}{49} &= x^2 - x - 1 - (\frac{1}{7}x - \frac{11}{49})(7x+4)\\ &= x^2 - x - 1 - (\frac{1}{7}x - \frac{11}{49})[x^3 + 2x^2 + 3x + 1 - (x+3)(x^2 - x - 1)]\\ &= -(\frac{1}{7}x - \frac{11}{49})f + (\frac{1}{7}x - \frac{11}{49})(x+4)g.\end{aligned}$$

16.3 Nullstellen

Im Folgenden sei $\mathbb{K}$ ein Körper und x eine Unbestimmte über $\mathbb{K}$.

Auswerten von Polynomen

Ein Polynom $f = f_n x^n + \ldots + f_1 x + f_0$ in $\mathbb{K}[x]$ wird an einer Stelle $\alpha \in \mathbb{K}$ *ausgewertet*, indem α in f eingesetzt wird

$$f(\alpha) = f_n \alpha^n + \ldots + f_1 \alpha + f_0 \in \mathbb{K}. \tag{16.9}$$

Die zugehörige Abbildung $F : \mathbb{K} \to \mathbb{K} : \alpha \mapsto f(\alpha)$ wird *Polynomabbildung* genannt.

Sei $P_{\mathbb{K}} = \{F \mid f \in \mathbb{K}[x]\}$ die Menge aller Polynomabbildungen, die zu den Polynomen in $\mathbb{K}[x]$ gehören. Auf $P_{\mathbb{K}}$ werden *Addition* und *Multiplikation* festgelegt durch

$$(F+G)(\alpha) = F(\alpha) + G(\alpha), \tag{16.10}$$

$$(FG)(\alpha) = F(\alpha)G(\alpha), \quad \alpha \in \mathbb{K}. \tag{16.11}$$

Satz 16.15. *Die Menge aller Polynomabbildungen $P_{\mathbb{K}}$ bildet zusammen mit obiger Addition und Multiplikation einen kommutativen Ring.*

Beispiel 16.16. Sei p prim. Für das Polynom $f = x^p - x \in \mathbb{Z}_p[x]$ ist die Polynomabbildung $F : \mathbb{Z}_p \to \mathbb{Z}_p : \alpha \mapsto f(\alpha)$ nach dem Satz von Fermat die Nullabbildung.

Ein Körper $\mathbb{L}$ heißt eine *Körpererweiterung* eines Körpers $\mathbb{K}$, wenn $\mathbb{K}$ ein Unterring von $\mathbb{L}$ ist.

Satz 16.17. *Sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ und sei $\alpha \in \mathbb{L}$. Die Abbildung $\eta_\alpha : \mathbb{K}[x] \to \mathbb{L} : f \mapsto f(\alpha)$ ist ein Homomorphismus.*

Beweis. Für beliebige Polynome $f, g \in \mathbb{K}[x]$ gilt

$$\eta_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \eta_\alpha(f) + \eta_\alpha(g)$$

und

$$\eta_\alpha(fg) = (fg)(\alpha) = f(\alpha) \cdot g(\alpha) = \eta_\alpha(f)\eta_\alpha(g).$$

Ferner ist $\eta_\alpha(1) = 1$. Mithin ist η_α ein Homomorphismus. □

Beispiel 16.18. Der Auswertungshomomorphismus $\eta_0 : \mathbb{K}[x] \to \mathbb{K} : f \to f(0)$ ordnet jedem Polynom f sein konstantes Glied $f(0) = f_0$ zu.

Nullstellen

Sei f ein Polynom in $\mathbb{K}[x]$ und sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Ein Element $\alpha \in \mathbb{L}$ mit $f(\alpha) = 0$ heißt eine *Nullstelle* oder *Wurzel* von f.

Beispiel 16.19. Das Polynom $x^2 - 2 \in \mathbb{Q}[x]$ besitzt die Nullstellen $\pm\sqrt{2}$.

Satz 16.20. (Wurzelsatz) *Sei $f \in \mathbb{K}[x]$ und sei $\alpha \in \mathbb{K}$. Das lineare Polynom $x - \alpha$ teilt f genau dann, wenn $f(\alpha) = 0$.*

Beweis. Sei $x - \alpha$ ein Teiler von f. Dann gibt es ein Polynom $g \in \mathbb{K}[x]$ mit $f = (x - \alpha)g$. Durch Auswerten an der Stelle α folgt $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0$. Umgekehrt sei $\alpha \in \mathbb{K}$ eine Wurzel von f. Nach dem Divisionssatz gibt es Polynome q und r mit $f = (x - \alpha)q + r$, wobei $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(x - \alpha) = 1$. Aus Gradgründen liegt also r in $\mathbb{K}$. Durch Auswerten an der Stelle α ergibt sich $0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r$. Somit ist $x - \alpha$ ein Teiler von f. □

Durch wiederholtes Anwenden des Wurzelsatzes ergibt sich der folgende

Satz 16.21. *Zu jedem Polynom $f \in \mathbb{K}[x]$ gibt es Elemente $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$, natürliche Zahlen $k_1, \ldots, k_m$ und ein Polynom $g \in \mathbb{K}[x]$, sodass*

$$f = (x - \alpha_1)^{k_1} \ldots (x - \alpha_m)^{k_m} g. \tag{16.12}$$

Das Polynom g kann so gewählt werden, dass es keine Nullstelle in $\mathbb{K}$ hat.

Beweis. Wir zeigen die Aussage durch vollständige Induktion nach m. Sei $\alpha_1 \in \mathbb{K}$ eine Nullstelle von f. Dann ist $x - \alpha_1$ nach dem Wurzelsatz ein Teiler von f, also $f = (x - \alpha_1)h_1$ für ein $h_1 \in \mathbb{K}[x]$. Hat h_1 ebenfalls α_1 als Nullstelle, dann folgt nach dem Wurzelsatz $h_1 = (x - \alpha_1)h_2$ für ein $h_2 \in \mathbb{K}[x]$, mithin $f = (x - \alpha_1)^2 h_2$. Diese Faktorisierung $h_i = (x - \alpha_1)h_{i+1}$, $i \in \mathbb{N}$, wird fortgesetzt. Sie muss wegen $\operatorname{grad}(h_i) = 1 + \operatorname{grad}(h_{i+1})$ abbrechen. Folglich gibt es einen Index k_1, so dass α_1 keine Nullstelle von $g = h_{k_1+1}$ ist. Damit ergibt sich $f = (x - \alpha_1)^{k_1} g$.

Sei die Aussage für alle Polynome $f \in \mathbb{K}[x]$ schon bewiesen, die wenigstens $m - 1$ paarweise verschiedene Nullstellen in $\mathbb{K}$ besitzen. Sei f ein Polynom in $\mathbb{K}[x]$, das Nullstellen $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ aufweist. Dann gibt es nach Induktionsannahme natürliche Zahlen $k_1, \ldots, k_{m-1}$ und ein Polynom $h \in \mathbb{K}[x]$ mit

$$f = (x - \alpha_1)^{k_1} \ldots (x - \alpha_{m-1})^{k_{m-1}} h.$$

Durch Auswerten beider Seiten an der Stelle α_m folgt

$$0 = f(\alpha_m) = (\alpha_m - \alpha_1) \ldots (\alpha_m - \alpha_{m-1}) h(\alpha_m).$$

Weil α_m von den übrigen $m - 1$ Nullstellen verschieden ist, muss $h(\alpha_m) = 0$ sein, weil ja $\mathbb{K}$ nullteilerfrei ist. Gemäß Induktionsanfang existiert eine natürliche Zahl k_m und ein Polynom $g \in \mathbb{K}[x]$ mit

$$h = (x - \alpha_m)^{k_m} g.$$

Daraus folgt die Behauptung. □

Satz 16.22. *Jedes Polynom in $\mathbb{K}[x]$ vom Grad n hat höchstens n Nullstellen in $\mathbb{K}$.*

Beweis. Sei $f \in \mathbb{K}[x]$ ein Polynom vom Grad n, das m Nullstellen in $\mathbb{K}$ hat. Wird das Polynom f in der Form (16.12) dargestellt, ergibt sich durch Gradvergleich $\text{grad}(f) = (k_1 + \ldots + k_m) + \text{grad}(g)$. Daraus folgt $m \leq k_1 + \ldots + k_m = \text{grad}(f) - \text{grad}(g) \leq \text{grad}(f) = n$. □

Satz 16.23. *Ist $\mathbb{K}$ ein unendlicher Körper, dann ist die Abbildung $\psi : \mathbb{K}[x] \to P_{\mathbb{K}} : f \mapsto F$ ein Isomorphismus.*

Beweis. Seien $f, g \in \mathbb{K}[x]$. Sei $F = G$, d. h., $F(\alpha) = G(\alpha)$ für alle $\alpha \in \mathbb{K}$. Wir betrachten das Polynom $h = f - g$. Für die zugehörige Polynomabbildung H gilt $H(\alpha) = F(\alpha) - G(\alpha) = 0$ für alle $\alpha \in \mathbb{K}$. Also hat h unendlich viele Wurzeln in $\mathbb{K}$. Nach Satz 16.22 muss h das Nullpolynom sein. Folglich ist $f = g$ und somit die Abbildung ψ injektiv. Die Abbildung ψ ist definitionsgemäß surjektiv. Die Homomorphieeigenschaft ist leicht nachzurechnen. □

Polynome und Polynomabbildungen über unendlichen Körpern sind also dasselbe. Dies gilt nicht für endliche Körper, denn etwa liefern die Polynome $x+1$ und $x^2 + 1$ über $\mathbb{Z}_2$ dieselbe Polynomabbildung $F : \mathbb{Z}_2 \to \mathbb{Z}_2$ mit $F(0) = 1$ und $F(1) = 0$.

Der Vollständigkeit halber wird der Fundamentalsatz der Algebra angegeben. Er wurde zuerst von Carl F. Gauss (1777-1855) bewiesen.

Satz 16.24. (Fundamentalsatz der Algebra) *Alle Nullstellen eines Polynoms in $\mathbb{C}[x]$ liegen in $\mathbb{C}$.*

Beispiel 16.25. Das Polynom $x^n - 1 \in \mathbb{Q}[x]$ hat als Nullstellen die *n-ten Einheitswurzeln*

$$x^n - 1 = \prod_{k=0}^{n-1} (x - e^{2\pi i k/n}). \tag{16.13}$$

Denn jede n-te Einheitswurzel $e^{2\pi i k/n}$, $0 \leq k \leq n-1$, ist eine Nullstelle von $x^n - 1$. Also ist die rechte Seite nach dem Wurzelsatz ein Teiler von $x^n - 1$. Beide Polynome haben denselben Grad, weshalb sie sich nach Satz 16.6 nur um eine Einheit in $\mathbb{K}$ unterscheiden. Weil beide Polynome normiert sind, ist diese Einheit gleich 1, d. h., beide Polynome sind identisch.

Satz 16.26. (Rationaler Nullstellentest) *Jede rationale Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[x]$ ist eine ganze Zahl, die das konstante Glied von f teilt.*

Beweis. O.B.d.A. sei $\alpha = \frac{r}{s}$ eine rationale Zahl mit teilerfremdem Zähler und Nenner. Durch Multiplizieren des Ausdrucks $f(\alpha)$ mit s^n ergibt sich

$$r^n + f_{n-1} r^{n-1} s + f_{n-2} r^{n-2} s^2 + \ldots + f_1 r s^{n-1} + f_0 s^n = 0, \tag{16.14}$$

also

$$r^n = (-f_{n-1}r^{n-1} - f_{n-2}r^{n-2}s - \ldots - f_1 r s^{n-2} - f_0 s^{n-1})s.$$

Somit ist s ein Teiler von r^n. Da aber r und s teilerfremd sind, erhellt sich $s = 1$. Folglich ist $\alpha = r$ ganzzahlig und (16.14) hat die Form

$$r(r^{n-1} + f_{n-1}r^{n-2} + \ldots + f_1) = -f_0.$$

Folglich ist $\alpha = r$ ein Teiler von f_0. □

Beispiele 16.27.

- Das Polynom $x^2 - 2 \in \mathbb{Z}[x]$ hat keine Nullstelle in $\mathbb{Q}$, denn nach Satz 16.26 kämen als Wurzeln nur ± 1 oder ± 2 in Frage.
- Das Polynom $x^2 + 1 \in \mathbb{Z}[x]$ hat ebenfalls keine Wurzel in $\mathbb{Q}$. denn nach Satz 16.26 kämen als Nullstellen nur ± 1 in Frage. Sei i eine Nullstelle von $x^2 + 1$, genannt *imaginäre Einheit*. Dann ist $i^2 = -1$ und somit $x^2 + 1 = (x - i)(x + i)$. Wegen $i^3 = -i$ und $i^4 = 1$ ist i eine vierte Einheitswurzel.
- Das Polynom $x^n - 1 \in \mathbb{Z}[x]$, $n \geq 1$, besitzt -1 als einzige rationale Nullstelle, wenn n gerade ist. Falls n ungerade ist, hat dieses Polynom nach Satz 16.26 keine rationalen Wurzeln.

16.4 Irreduzible Polynome

Die irreduziblen Polynome spielen in Polynomringen die gleiche Rolle wie die Primzahlen im Ring der ganzen Zahlen.

Sei R ein Integritätsbereich. Ein Polynom $f \in R[x]$ vom Grad ≥ 1 heißt *irreduzibel* über R, wenn in jeder Darstellung $f = gh$ mit Polynomen $g, h \in R[x]$ entweder g oder h eine Einheit in $R[x]$ ist. Ein irreduzibles Polynom kann also nur durch Ausklammern einer Einheit faktorisiert werden.

Beispiele 16.28.

- Jedes lineare Polynom $f = ax + b \in R[x]$, $a \neq 0$, ist irreduzibel über $\mathbb{K}$. Denn aus einer Darstellung $f = gh$ mit Polynomen $g, h \in \mathbb{K}[x]$ folgt mit Lemma 16.4 sofort $\operatorname{grad}(g) + \operatorname{grad}(h) = \operatorname{grad}(f) = 1$. Also ist $\operatorname{grad}(g) = 1$ und $\operatorname{grad}(h) = 0$, mithin h nach Satz 16.6 eine Einheit in $\mathbb{K}[x]$, oder umgekehrt.
- Das Polynom $f = x^2 - 2 \in \mathbb{Z}[x]$ ist irreduzibel über $\mathbb{Q}$. Denn aus $f = gh$ mit Polynomen $g, h \in \mathbb{Q}[x]$ folgt mit Lemma 16.4 sofort $\operatorname{grad}(g) + \operatorname{grad}(h) = \operatorname{grad}(f) = 2$. Angenommen, f wäre reduzibel. Dann besitzen beide Polynome g und h den Grad 1. O.B.d.A. sei $g = x - \alpha \in \mathbb{Q}[x]$ normiert. Nach dem Wurzelsatz hat f eine rationale Wurzel α, was nach 16.27 widersprüchlicherweise nicht sein kann.
- Das Polynom $x^2 + 1 \in \mathbb{Z}[x]$ ist irreduzibel über $\mathbb{Q}$. Der Nachweis kann wie im letzten Beispiel geführt werden.

Lemma 16.29. *Sei $f \in \mathbb{K}[x]$ irreduzibel und seien $f_1, \ldots, f_n \in \mathbb{K}[x]$. Teilt f das Produkt $f_1 \cdot \ldots \cdot f_n$, dann teilt f einen der Faktoren f_i.*

Der Beweis ist dem ganzzahligen Analogon sehr ähnlich (Lemma 13.14).

Fundamentalsatz der Polynomfaktorisierung

Satz 16.30. *Jedes Polynom in $\mathbb{K}[x]$ vom Grad ≥ 1 ist darstellbar als Produkt von irreduziblen Polynomen über $\mathbb{K}$. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren und die Multiplikation mit Einheiten.*

Beweis. Zuerst wird die Existenz der Darstellung gezeigt. Jedes Polynom vom Grad 1 ist nach 16.28 irreduzibel über $\mathbb{K}$. Sei $f \in \mathbb{K}[x]$ mit $\text{grad}(f) = n \geq 2$. Ist f irreduzibel über $\mathbb{K}$, dann ist nichts zu beweisen. Andernfalls gibt es Polynome $g, h \in \mathbb{K}[x]$ vom Grad ≥ 1 mit $f = gh$. Nach Lemma 16.4 ist $\text{grad}(f) = \text{grad}(g) + \text{grad}(h)$. Somit haben g und h kleineren Grad als f. Nach Induktionsannahme sind g und h darstellbar als Produkte von irreduziblen Polynomen über $\mathbb{K}$. Damit hat auch f eine solche Darstellung.

Schließlich wird die Eindeutigkeit der Darstellung bewiesen. Für lineare Polynome $ax + b, cx + d \in \mathbb{K}[x]$, $a \neq 0 \neq c$, folgt aus $ax + b = cx + d$, also $(a - c)x + (b - d) = 0$, durch Koeffizientenvergleich $a = c$ und $b = d$. Sei $f \in \mathbb{K}[x]$ mit $\text{grad}(f) = n \geq 2$. Wir betrachten zwei Darstellungen von f durch irreduzible Faktoren

$$f_1 \cdot \ldots \cdot f_m = f = g_1 \cdot \ldots \cdot g_l.$$

Das Polynom f_1 teilt nach Lemma 16.29 eines der Faktoren g_j, nach Umnummerierung etwa g_1. Weil f_1 und g_1 irreduzibel über $\mathbb{K}$ sind, folgt $g_1 = \alpha_1 f_1$ für ein $0 \neq \alpha_1 \in \mathbb{K}$. Es ergibt sich

$$f_1 f_2 \cdot \ldots \cdot f_m = \alpha_1 f_1 g_2 \cdot \ldots \cdot g_l.$$

Da $\mathbb{K}[x]$ nach Satz 16.5 ein Integritätsring ist, kann wegen Satz 15.16 durch f_1 gekürzt werden

$$f_2 \ldots f_m = \alpha_1 g_2 \ldots g_l.$$

Dieses Polynom hat aus Gradgründen einen kleineren Grad als f und somit nach Induktionsannahme eine bis auf die Reihenfolge der Faktoren und die Multiplikation mit Einheiten eindeutige Darstellung. Somit hat auch f eine solche Darstellung. □

Modulares Irreduzibilitätskriterium

Sei p eine Primzahl. Der Epimorphismus $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$ in Satz 14.8 wird zu einem Epimorphismus $\pi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ fortgesetzt anhand der Zuordnung $f_n x^n + \ldots + f_1 x + f_0 \mapsto \pi_p(f_n)x^n + \ldots + \pi_p(f_1)x + \pi_p(f_0)$.

Satz 16.31. *Seien $f \in \mathbb{Z}[x]$ ein Polynom vom Grad ≥ 1 und p eine Primzahl, die den Leitkoeffizienten von f nicht teilt. Ist $\pi_p(f)$ irreduzibel über $\mathbb{Z}_p$, dann ist f auch irreduzibel über $\mathbb{Z}$.*

Beweis. Angenommen, f wäre reduzibel über $\mathbb{Z}$. Dann gibt es Polynome $g, h \in \mathbb{Z}[x]$ vom Grad ≥ 1 mit $f = gh$. Da π_p ein Epimorphismus ist, folgt $\pi_p(f) = \pi_p(g)\pi_p(h)$. Nach Voraussetzung ist $\pi_p(f) \neq 0$ und $\operatorname{grad}(f) = \operatorname{grad}(\pi_p(f))$. Mit Lemma 16.4 ergibt sich $\operatorname{grad}(g) + \operatorname{grad}(h) = \operatorname{grad}(f) = \operatorname{grad}(\pi_p(f)) = \operatorname{grad}(\pi_p(g)) + \operatorname{grad}(\pi_p(h))$. Diese Gleichung kann wegen $\operatorname{grad}(g) \geq \operatorname{grad}(\pi_p(g))$ und $\operatorname{grad}(h) \geq \operatorname{grad}(\pi_p(h))$ nur bestehen, wenn $\operatorname{grad}(g) = \operatorname{grad}(\pi_p(g))$ und $\operatorname{grad}(h) = \operatorname{grad}(\pi_p(h))$. Also ist das Polynom $\pi_p(f)$ widersprüchlicherweise reduzibel über $\mathbb{Z}_p$. □

Beispiel 16.32. Das Polynom $f = x^3 + 6x^2 + 8x + 4$ ist irreduzibel über $\mathbb{Z}$. Für den Beweis wird der Epimorphismus $\pi_3 : \mathbb{Z}[x] \to \mathbb{Z}_3[x]$ herangezogen. Angenommen, $\pi_3(f) = x^3 + 2x + 1$ wäre reduzibel über $\mathbb{Z}_3$. Dann wird $\pi_3(f)$ aus Gradgründen von einem linearen Faktor $x - \alpha \in \mathbb{Z}_3[x]$ geteilt. Nach dem Wurzelsatz ist $\alpha \in \mathbb{Z}_3$ sogar eine Nullstelle von $\pi_3(f)$. Allerdings hat $\pi_3(f)$ keine Wurzeln in $\mathbb{Z}_3$, denn $f_3(0) = f_3(1) = f_3(2) = 1$. Somit ist $\pi_3(f)$ irreduzibel über $\mathbb{Z}_3$ und folglich f nach Satz 16.31 irreduzibel über $\mathbb{Z}$.

16.5 Polynom-Interpolation

Wir untersuchen zuerst polynomiale Kongruenzensysteme. Sei $\mathbb{K}$ ein Körper. Seien $h_1, \ldots, h_n$ paarweise teilerfremde Polynome in $\mathbb{K}[x]$ und $g_1, \ldots, g_n$ Polynome in $\mathbb{K}[x]$. Gesucht sind alle Lösungen des Kongruenzensystems

$$f \equiv g_i \bmod h_i, \quad 1 \leq i \leq n. \tag{16.15}$$

Satz 16.33. (Chinesischer Restesatz) *Das Kongruenzensystem (16.15) hat eine eindeutig bestimmtes Lösung $f \in \mathbb{K}[x]$, so dass entweder $f = 0$ oder $\operatorname{grad}(f) < \operatorname{grad}(h)$, wobei $h = \prod_{i=1}^{n} h_i$. Die Menge aller Lösungen dieses Kongruenzensystems ist $\{f + gh \mid g \in \mathbb{K}[x]\}$.*

Der Beweis verläuft ähnlich wie die integrale Fassung.

Der Chinesische Restesatz erhält in Verbindung mit dem Auswertungshomomorphismus eine etwas andere Bedeutung.

Korollar 16.34. *Seien $\alpha_1, \ldots, \alpha_n$ paarweise verschiedene Elemente in $\mathbb{K}$ und $\beta_1, \ldots, \beta_n$ beliebige Elemente in $\mathbb{K}$. Es gibt ein eindeutig bestimmtes Polynom $f \in \mathbb{K}[x]$ vom Grad $< n$ mit der Eigenschaft*

$$f(\alpha_i) = \beta_i, \quad 1 \leq i \leq n. \tag{16.16}$$

Beweis. Das Kongruenzensystem

$$f \equiv \beta_i \bmod x - \alpha_i, \quad 1 \leq i \leq n,$$

hat nach Satz 16.33 eine eindeutig bestimmte Lösung $f \in \mathbb{K}[x]$. Nach Definition der Kongruenz gibt es zu jedem i, $1 \leq i \leq n$, ein $q_i \in \mathbb{K}[x]$ mit $f(x) = q_i(x)(x - \alpha_i) + \beta_i$. Durch Einsetzen von α_i erhellt sich $f(\alpha_i) = \beta_i$. □

Nach obigem Korollar gibt es zu n Punkten $(\alpha_i, \beta_i) \in \mathbb{K}^2$ mit lauter verschiedenen Abzissenwerten α_i genau ein Polynom $f \in \mathbb{K}(x]$ vom Grad $< n$, so dass $f(\alpha_i) = \beta_i$ für $1 \leq i \leq n$. Dieses Polynom f kann mithilfe der Interpolationsformel von Jean-Joseph Lagrange (1736-1813) berechnet werden.

Sei $h = (x - \alpha_1) \dots (x - \alpha_n)$ wie in Korollar 16.34. Für die Ableitung von h gilt

$$h' = \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j), \tag{16.17}$$

wobei der i-te Summand folgende Form besitzt

$$\frac{h}{x - \alpha_i} = \prod_{j \neq i} (x - \alpha_j). \tag{16.18}$$

Das Polynom

$$l_i = \frac{h}{h'(\alpha_i)(x - \alpha_i)} = \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)} \tag{16.19}$$

wird als *Lagrange-Interpolator* von h bezeichnet. Es gilt

$$l_i(\alpha_i) = 1 \quad \text{und} \quad l_i(\alpha_j) = 0 \quad \text{für alle } j \neq i. \tag{16.20}$$

Also erhebt sich

$$f = \beta_1 l_1 + \ldots + \beta_n l_n \tag{16.21}$$

als eine Lösung des Kongruenzensystems (16.16). Weil jeder Lagrange-Interpolator l_i den Grad $n - 1$ besitzt, ist f vom Grad $< n$ und somit die eindeutig bestimmte Lösung des Kongruenzensystems vom Grad $< n$. Die Gleichung (16.21) wird *Lagrange-Interpolationsformel* genannt.

Beispiel 16.35. Gesucht ist ein Polynom $f \in \mathbb{Q}[x]$ mit $f(-1) = 1$, $f(0) = 1$ und $f(1) = 3$. Die zugehörigen Lagrange-Interpolatoren sind

$$\begin{aligned} l_1 &= \frac{1}{2} x(x - 1), \\ l_2 &= -(x + 1)(x - 1), \\ l_3 &= \frac{1}{2}(x + 1)x. \end{aligned}$$

Also ergibt sich als Lösung kleinsten Grades das Polynom

$$f = l_1 + l_2 + 3l_3 = x^2 + x + 1.$$

Die Lagrange-Interpolation kann zum Beispiel dazu verwendet werden, das charakteristische Polynom

$$\det(A - x \cdot I_n) = (-1)^n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0 \qquad (16.22)$$

einer $n \times n$-Matrix A zu bestimmen, hier ist I_n die $n \times n$-Einheitsmatrix. Die Nullstellen des charakterischen Polynoms von A sind bekanntlich die Eigenwerte von A. Dabei wird das charakteristische Polynom von A an $n+1$ verschiedenen Stellen α_i ausgewertet, also

$$\beta_i = \det(A - \alpha_i \cdot I), \quad 1 \leq i \leq n+1. \qquad (16.23)$$

Die Lagrange-Interpolation liefert dann das charakteristische Polynom von A.

16.6 Divisionsschieberegister

Abschließend wird eine elektronisch realisierbare Schaltung für die Polynomdivision beschrieben. Hierzu werden drei Schaltelemente benutzt: *Addierer*, *Multiplizierer* und *Speicherzellen* (Abb. 16.1).

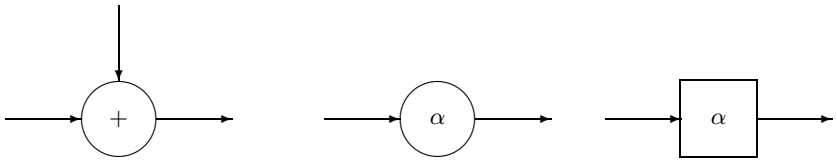

Abb. 16.1. Schaltsymbole für Addierer, Multiplizierer und Speicherzellen

Sei $g = x^m + g_{m-1}x^{m-1} + \ldots + g_1 x + g_0$ ein normiertes Polynom über einem Körper $\mathbb{K}$. Ein *m-stufiges Divisionsschieberegister* mit dem *Rückkopplungspolynom g* zeigt die Abb. 16.2. Diese Schaltung verfügt über zwei Eingänge A und B und soll getaktet arbeiten: Addierer und Multiplizierer verarbeiten Eingaben im selben Taktzyklus, während eine Speicherzelle eine Eingabe erst im nächsten Taktzyklus speichert. Das Einschrittverhalten des Divisionsschieberegisters beschreibt der folgende

Satz 16.36. *Das Divisionsschieberegister in Abb. 16.2 enthalte die Koeffizienten des Polynoms $f = \sum_{i=0}^{m-1} f_i x^i \in \mathbb{K}[x]$ und empfange im selben Taktzyklus $\alpha, \beta \in \mathbb{K}$ als Eingaben. Dann enthält das Divisionsschieberegister im nächsten Taktzyklus die Koeffizienten des Polynoms*

$$xf + \alpha + \beta x^m \bmod g. \qquad (16.24)$$

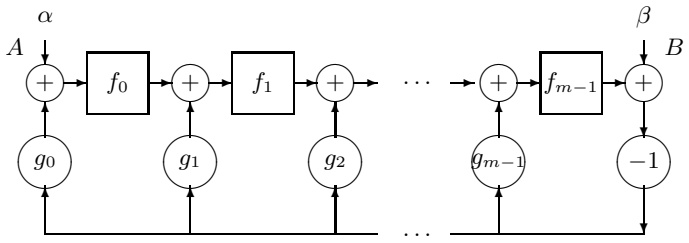

Abb. 16.2. Ein Divisionsschieberegister.

Beweis. Sei der Inhalt des Divisionschieberegisters nach besagtem Taktzyklus durch die Koeffizienten von $h = \sum_{i=0}^{m-1} h_i x^i$ gegeben. Dann gilt

$$h_0 = \alpha - (\beta + f_{m-1})g_0$$

und

$$h_i = f_{i-1} - (\beta + f_{m-1})g_i, \quad 1 \le i \le m-1.$$

Daraus folgt

$$\begin{aligned} h &= \alpha - (\beta + f_{m-1})g_0 + \sum_{i=1}^{m-1} (f_{i-1} - (\beta + f_{m-1})g_i)x^i \\ &= xf + \alpha + \beta x^m - (\beta + f_{m-1})g \\ &= xf + \alpha + \beta x^m \bmod g. \end{aligned}$$

□

Das Mehrschrittverhalten des Divisionsschieberegisters wird für den Fall skizziert, in dem alle Speicherzellen anfangs mit 0 vorbesetzt sind.

- Wenn am Eingang A die Koeffizienten von $f = \sum_{i=0}^{n} f_i x^i$ in der Reihenfolge $f_n, \ldots, f_0$ eingegeben werden und am Eingang B nichts eingegeben wird, dann ist der Inhalt des Divisionsschieberegisters nach $n+1$ Taktzyklen gleich $f \bmod g$.
- Wenn am Eingang B die Koeffizienten von $f = \sum_{i=0}^{n} f_i x^i$ in der Reihenfolge $f_n, \ldots, f_0$ eingelesen werden und am Eingang A nichts anliegt, dann ist der Inhalt des Divisionsschieberegisters nach $n+1$ Taktzyklen gleich $x^m f \bmod g$.

Selbsttestaufgaben

16.1. Berechne den ggT der Polynome $x^2 + x + 2$ und $x^3 + x^2 + 2$ von $\mathbb{Z}_3[x]$ und stelle ihn als Linearkombination der beiden Polynome dar.

16.2. Zeige an einem Beispiel, dass Satz 16.22 nicht für Koeffizientenringe mit Nullteilern gilt.

16.3. Beweise den Satz 16.15.

16.4. Die *Ableitung* eines Polynoms $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ ist das Polynom $f' = \sum_{i=1}^{n} i a_i x^{i-1}$. Beweise, dass die üblichen Ableitungsregeln gelten

$$(\alpha f + \beta g)' = \alpha f' + \beta g' \quad \text{und} \quad (fg)' = f'g + fg', \quad f, g \in \mathbb{K}[x],\ \alpha, \beta \in \mathbb{K}.$$

16.5. Beweise, dass ein Polynom $f \in \mathbb{K}[x]$ eine mehrfache Nullstelle genau dann besitzt, wenn f und f' einen gemeinsamen Teiler vom Grad ≥ 1 haben. Benutze diese Aussage, um zu zeigen, dass das Polynom $f = x^4 - 9x^2 + 4x + 12 \in \mathbb{Q}[x]$ eine mehrfache Nullstelle besitzt.

16.6. Zeige, dass für jede ungerade Primzahl p gilt $(p-1)! \equiv -1 \bmod p$.

16.7. Sei a eine natürliche Zahl. Zeige, dass das Polynom $x^n - a \in \mathbb{Q}[x]$ die Wurzeln $\sqrt[n]{a} \cdot e^{2\pi i k/n}$, $0 \leq k \leq n-1$, besitzt.

16.8. Ein Integritätsring R heißt *euklidisch*, wenn eine Abbildung $\nu : R \setminus \{0\} \to \mathbb{N}_0^+$ existiert, so dass es für beliebige Elemente $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ gibt, so dass $a = qb + r$, wobei entweder $r = 0$ oder $\nu(r) < \nu(b)$.

Zeige, dass folgende Ringe euklidisch sind: der Ring der ganzen Zahlen, jeder Körper und der Polynomring $R[x]$ über einem Integritätsring R.

16.9. Sei R ein kommutativer Ring. Ein Ideal I in R heißt ein *Hauptideal*, wenn es ein Element $r \in I$ gibt, so dass $I = \{ar \mid a \in R\}$. Zeige, dass jeder euklidische Ring ein Hauptidealring ist, d. h., jedes Ideal in R ein Hauptideal ist.

16.10. Zeige, dass das Polynom $f = 3x^4 + 3x^3 + 5x^2 + 5x + 3$ irreduzibel über $\mathbb{Z}$ ist.

16.11. Beweise, dass die Abbildung $\mathbb{C} \to \mathbb{C} : a + ib \mapsto a - ib$ ein Automorphismus ist. Die Zahl $\overline{z} = a - ib$ heißt *konjugiert-komplex* zu $z = a + ib \in \mathbb{C}$. Zeige ferner, dass jedes Polynom $f \in \mathbb{R}[x]$, welches $z \in \mathbb{C}$ als Nullstelle besitzt, auch $\overline{z}$ als Wurzel hat.

16.12. Zeige, dass jedes irreduzible Polynom in $\mathbb{R}[x]$ höchstens den Grad 2 besitzt.

16.13. Zeige, dass jedes Ideal in $\mathbb{K}[x]$ von der Form $f\mathbb{K}[x] = \{fg \mid g \in \mathbb{K}[x]\}$, $f \in \mathbb{K}[x]$, ist.

16.14. Zeichne das Schaltbild eines Divisionsschieberegisters mit dem Rückkopplungspolynom $g = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

16.15. Verifiziere das am Ende von Abschnitt 16.6 skizzierte Mehrschrittverhalten von Divisionsschieberegistern.