1 Der Ring der ganzen Zahlen

Letztendlich wird die Addition und Multiplikation in endlichen Körpern auf die Addition und Multiplikation von ganzen Zahlen zurückgeführt. Deswegen müssen wir die an sich selbstverständlichen Rechenoperationen in $\mathbb{Z}$ genauer analysieren.

In der Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ der natürlichen Zahlen ist eine Gleichung

$$a + x = b$$

nur dann lösbar, wenn $a < b$. In der Menge

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$$

der ganzen Zahlen ist sie jedoch immer lösbar, $x = b - a$. Dies ist eine der grundlegenden Eigenschaften der Addition in $\mathbb{Z}$; ingesamt wird die Addition und Multiplikation in $\mathbb{Z}$ durch fünf Gesetze geregelt:

R1 Addition und Multiplikation sind *assoziativ:*

$$(a + b) + c = a + (b + c) \quad \text{und} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

R2 Addition und Multiplikation sind *kommutativ:*

$$a + b = b + a \quad \text{und} \quad a \cdot b = b \cdot a$$

R3 Es existiert ein neutrales *Element* bez. der Addition ($= 0$, *Nullelement*) und ein neutrales Element bez. der Multiplikation ($= 1$, *Einselement*):

$$0 + a = a \quad \text{und} \quad 1 \cdot a = a$$

Es ist $0 \neq 1$.

R4 Die Gleichung $a + x = b$ besitzt eine eindeutige Lösung x in $\mathbb{Z}$.

R5 Es gilt das *Distributivgesetz*:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Wir definieren: Eine Menge $R = \{a, b, c, \ldots\}$ heißt **Ring**, wenn je zwei Elementen $a, b \in R$ eine *Summe* $a + b \in R$ und ein *Produkt* $a \cdot b \in R$ zugeordnet ist, so dass die Gesetze R1 bis R5 gelten; in R4 ist $\mathbb{Z}$ durch R zu ersetzen. Eigentlich spricht man von einem *kommutativen Ring*, denn in R2 fordern wir, dass die Multiplikation kommutativ ist, wir betrachten hier nur solche Ringe.

Aus R1 bis R5 ergeben sich weitere Regeln, die im Ring $\mathbb{Z}$ an sich selbstverständlich sind. Da wir gleich noch andere Ringe betrachten, formulieren wir allgemein.

Sei R Ring. Bezüglich der Addition ist R eine *abelsche Gruppe*, man nennt sie die *additive Gruppe* $= R(+)$ von R. Dies bedeutet, dass die Addition assoziativ und kommutativ ist (R1 und R2), ein neutrales Element $0 \in R$ existiert (R3) und die Gleichung $a + x = b$ in R eindeutig lösbar ist (R4). In Kapitel 6 behandeln wir Gruppen in einem allgemeineren Rahmen.

Insbesondere besitzt die Gleichung $a + x = 0$ genau eine Lösung, sie wird mit $-a$ bezeichnet. Also ist

$$a + (-a) = 0 \quad \text{und} \quad -(-a) = a \ .$$

Zur Abkürzung setzt man

$$a - b := a + (-b) \ .$$

Es ist

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

also ist $x = b - a$ die Lösung von $a + x = b$.

Anders verhält sich die Multiplikation. Eine Gleichung $a \cdot x = b$ muss in R nicht lösbar sein, auch wenn $a \neq 0$.

Existiert zu $a \neq 0$ ein $b \neq 0$ mit $a \cdot b = 0$, so heißt a *Nullteiler* von R.

Mit R^* bezeichnen wir die Menge aller von 0 verschiedenen Elemente von R. Besitzt R keinen Nullteiler, gilt also

$$a, b \in R^* \ \Rightarrow \ a \cdot b \in R^* \ ,$$

so heißt R *nullteilerfrei*; offensichtlich ist der Ring $\mathbb{Z}$ nullteilerfrei.

Multipliziert man $a \in R$ mit sich selber, so erhält man die *Potenzen* a^i, $i \in \mathbb{N}_0$. Man setzt $a^0 := 1$, $a^1 := a$, $a^2 := a \cdot a$ und

$$a^3 := a \cdot a^2 = a \cdot (a \cdot a) \stackrel{!}{=} (a \cdot a) \cdot a = a^2 \cdot a \ ,$$

man beachte das Assoziativgesetz! Deshalb lässt man die Klammern weg und schreibt $a^3 = a \cdot a \cdot a$. Genauso behandelt man die höheren Potenzen:

$$a^i := a \cdot a^{i-1} = \underbrace{a \cdot a \cdot \cdots \cdot a}_{i} \ .$$

Daraus ergeben sich die *Potenzgesetze* :

$$a^{i+j} = a^i \cdot a^j \quad \text{und} \quad (a^i)^j = a^{i \cdot j} \ , \quad i, j \geq 0 \ .$$

Eine Diskussion der Potenzgesetze, insbesondere deren additive Variante findet sich in Kap. 6.

Das Distributivgesetz R5 verklammert die Addition und Multiplikation. Aus ihm folgen die zwei Regeln

$$0 \cdot a = 0 \quad \text{und} \quad (-a) \cdot b = -(a \cdot b) \ .$$

Zum Beweis von $0 \cdot a = 0$ lösen wir die Geichung $0 \cdot a + x = 0 \cdot a$. Nach R3 hat sie die Lösung $x = 0$; andererseits ist auch $0 \cdot a$ Lösung, denn

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

mit R4 folgt $0 = 0 \cdot a$. Zum Beweis der zweiten Regel schreiben wir

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

wegen $0 = a \cdot b - (a \cdot b)$ folgt die Behauptung wieder mit R4.

Zum Beispiel ergibt sich nun

$$(-a)(-b) = -(a(-b)) = -(-ab) = ab \ .$$

Aus dem Distributivgesetz folgt die *Kürzregel* , die wir gesondert formulieren:

1.1 In einem nullteilerfreien Ring kann gekürzt werden, d. h. es gilt:

$$a \cdot b = a \cdot c \ , \quad a \neq 0 \quad \Rightarrow \quad b = c \ .$$

Beweis $a \cdot b = a \cdot c$ impliziert

$$0 = a \cdot b - a \cdot c = a \cdot (b - c) \ .$$

Wegen $a \neq 0$ folgt $b - c = 0$, d. h. $b = c$. □

Wir fassen zusammen:

1.2 Die Menge $\mathbb{Z}$ der ganzen Zahlen bildet bezüglich der Addition und Multiplikation einen nullteilerfreien Ring. □

Sei $n \in \mathbb{N}$. Die Menge aller Vielfachen von n in $\mathbb{Z}$ bezeichnen wir mit $n\mathbb{Z}$, also ist

$$n\,\mathbb{Z} = \{n \cdot i \mid i \in \mathbb{Z}\} \ .$$

Es ist $n\mathbb{Z} = \{0\}$, wenn $n = 0$, und $n\mathbb{Z} = \mathbb{Z}$, wenn $n = 1$. Zum Beispiel ist $2\mathbb{Z}$ die Menge aller geraden Zahlen.

Die Teilmenge

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$

von $\mathbb{Z}$ spielt im Folgenden eine wichtige Rolle; es ist $|\mathbb{Z}_n| = n$.

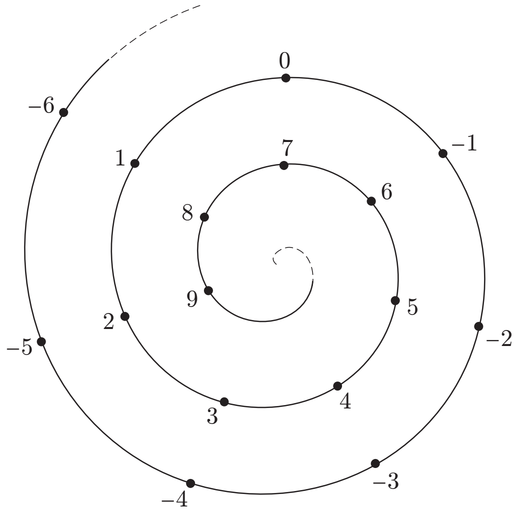
Eine Teilmenge von $\mathbb{Z}$ der Form

$$r + n\mathbb{Z} := \{r + n \cdot f \mid f \in \mathbb{Z}\} \ , \quad r \in \mathbb{Z}_n \ ,$$

heißt *Restklasse modulo* n, sie besteht aus den Zahlen in $\mathbb{Z}$, die geteilt durch n den Rest r haben. Ein fundamentales Gesetz in $\mathbb{Z}$ besagt, dass jede Zahl $a \in \mathbb{Z}$ in genau einer dieser n Restklasse modulo n liegt.[1] Dies bedeutet:

1.3 **Division mit Rest:** Zu $a \in \mathbb{Z}$ existieren eindeutig bestimmte Zahlen $f \in \mathbb{Z}$ und $r \in \mathbb{Z}_n$, so dass $a = n \cdot f + r$. □

Wir „malen“ die Restklassen modulo 7:



[1] Dies problematisieren wir hier nicht.

Seien a, n, r wie in 1.3. Wir nennen r den *Rest modulo* n und schreiben

$$r = \varrho_n(a) \;.$$

Zum Beispiel ist $\varrho_5(12) = 2$ und $\varrho_5(-12) = 3$, denn $12 = 2 \cdot 5 + 2$ und $-12 = (-3) \cdot 5 + 3$. Es ist $\varrho_5(4) = 4$, denn $4 = 0 \cdot 5 + 4$.

Wir fassen ϱ_n als (Rest-)Abbildung auf, ordnen also jedem $a \in \mathbb{Z}$ den Rest $r = \varrho_n(a) \in \mathbb{Z}_n$ zu. Man schreibt

$$\varrho_n : \mathbb{Z} \to \mathbb{Z}_n \quad \text{mit} \quad a \mapsto \varrho_n(a) \;.$$

1.4

a) $\varrho_n(a) = a \;\Leftrightarrow\; a \in \mathbb{Z}_n$

b) $\varrho_n(a) = 0 \;\Leftrightarrow\; a \in n\mathbb{Z}$

c) $\varrho_n(a) = \varrho_n(b) \;\Leftrightarrow\; a - b \in n\mathbb{Z}$

d) $\varrho_n(a + b) = \varrho_n\left(\varrho_n(a) + \varrho_n(b)\right)$

e) $\varrho_n(a \cdot b) = \varrho_n\left(\varrho_n(a) \cdot \varrho_n(b)\right)$

Beweis Die ersten drei Aussagen ergeben sich unmittelbar aus der Definition von ϱ_n. Für den Beweis von d), e) sei

$$\begin{aligned} a &= f \cdot n + r \;, \quad & r &= \varrho_n(a) \;, \\ b &= g \cdot n + s \;, \quad & s &= \varrho_n(b) \,. \end{aligned}$$

Dann ist

$$\begin{aligned} a + b &= (f + g) \cdot n + (r + s) \;, \\ a \cdot b &= (f \cdot g \cdot n + f \cdot s + g \cdot r) \cdot n + r \cdot s \;, \end{aligned}$$

also $(a + b) - (r + s) \in n\mathbb{Z}$ und $a \cdot b - r \cdot s \in n\mathbb{Z}$. Mit c) folgt die Behauptung. □

Wir machen ein Beispiel zu d) und e), sei $n = 7$. Es ist

$$\begin{aligned} \varrho_7(11 + 13) &= \varrho_7(24) = 3 \\ \varrho_7(11 \cdot 13) &= \varrho_7(143) = 3 \end{aligned}$$

und nach d), e)

$$\begin{aligned} \varrho_7(11 + 13) &= \varrho_7(\varrho_7(11) + \varrho_7(13)) = \varrho_7(4 + 6) = \varrho_7(10) = 3 \\ \varrho_7(11 \cdot 13) &= \varrho_7(\varrho_7(11) \cdot \varrho_7(13)) = \varrho_7(4 \cdot 6) = \varrho_7(24) = 3 \;. \end{aligned}$$

Gilt $\varrho_n(a) = \varrho_n(b)$ für zwei Zahlen $a, b \in \mathbb{Z}$, so heißt a *kongruent* b *modulo* n, man schreibt gerne $a \equiv b \pmod{n}$.

Sei $n \geq 2$. Die Menge $\mathbb{Z}_n$ machen wir zu einem Ring, indem wir auf ihr eine Addition $+_n$ und Multiplikation $\cdot_n$ *modulo* n erklären. Für $a, b \in \mathbb{Z}_n$ sei

$$\begin{aligned} a +_n b &:= \varrho_n(a + b) \\ a \cdot_n b &:= \varrho_n(a \cdot b) \ . \end{aligned}$$

Wir zeigen, dass die Abbildung $\varrho_n : \mathbb{Z} \to \mathbb{Z}_n$ die Ringstruktur von $\mathbb{Z}$ auf $\mathbb{Z}_n$ überträgt, so dass $\mathbb{Z}_n$ bezüglich der Addition $+_n$ und der Multiplikation $\cdot_n$ ein Ring wird.

Dazu schreiben wir kürzer ϱ anstatt ϱ_n. Für $a, b \in \mathbb{Z}_n$ ist

$$\begin{aligned} a +_n b &= \varrho(a + b) = \varrho(b + a) = b +_n a \\ a +_n 0 &= \varrho(a + 0) = \varrho(a) = a \\ a \cdot_n b &= \varrho(a \cdot b) = \varrho(b \cdot a) = b \cdot_n a \\ a \cdot_n 1 &= \varrho(a \cdot 1) = \varrho(a) = a \ . \end{aligned}$$

Also gelten R2 und R3. Um R4 nachzuweisen, lösen wir die Gleichung $a +_n x = b$ in $\mathbb{Z}_n$. Im Fall $a \leq b$ ist $x = b - a \in \mathbb{Z}_n$ Lösung, denn

$$a +_n (b - a) = \varrho(a + b - a) = \varrho(b) = b \ ,$$

und im Fall $a > b$ ist $x = n + b - a \in \mathbb{Z}_n$ eine Lösung, denn

$$a +_n (n + b - a) = \varrho(a + n + b - a) = \varrho(b + n) = \varrho(b) = b \ .$$

Man überzeuge sich, dass in beiden Fällen x die einzige Lösung ist.

Es bleibt noch das Assoziativ- und Distributivgesetz nachzuweisen. Seien $a, b, c \in \mathbb{Z}_n$, nach 1.4.a ist

$$a = \varrho(a) \ , \quad b = \varrho(b) \ , \quad c = \varrho(c) \ .$$

Mit 1.4.d folgt

$$a +_n (b +_n c) = \varrho(a) +_n \varrho(b + c) = \varrho(\varrho(a) + \varrho(b + c)) = \varrho(a + (b + c))$$

und genauso $(a +_n b) +_n c = \varrho((a + b) + c)$. Die Addition in $\mathbb{Z}_n$ ist also assoziativ, weil sie in $\mathbb{Z}$ assoziativ ist. Analog ergibt sich mit 1.4.e

$$a \cdot_n (b \cdot_n c) = \varrho(a) \cdot_n \varrho(b \cdot c) = \varrho(\varrho(a) \cdot \varrho(b \cdot c)) = \varrho(a \cdot (b \cdot c))$$

und genauso $(a \cdot_n b) \cdot_n c = \varrho((a \cdot b) \cdot c)$. Also ist auch die Multiplikation assoziativ, denn sie ist es in $\mathbb{Z}$. Ähnlich folgt das Distributivgesetz:

$$\begin{aligned} a \cdot_n (b +_n c) &= \varrho(a) \cdot_n \varrho(b + c) = \varrho(\varrho(a) \cdot \varrho(b + c)) = \varrho(a \cdot (b + c)) \\ &= \varrho(a \cdot b + a \cdot c) = \varrho(\varrho(a \cdot b) + \varrho(a \cdot c)) = \varrho(a \cdot_n b + a \cdot_n c) \\ &= (a \cdot_n b) +_n (a \cdot_n c) . \end{aligned}$$

Wir fassen zusammen:

Satz Sei $n > 1$. Bezüglich der Addition und Multiplikation modulo n ist $\mathbb{Z}_n$ ein Ring mit Nullelement $0 \in \mathbb{Z}_n$ und Einselement $1 \in \mathbb{Z}_n$. □ **1.5**

Nachdem $\mathbb{Z}_n$ Ring ist, können wir formulieren:

Die Restabbildung ϱ_n ist verträglich mit der Addition und Multiplikation in den Ringen $\mathbb{Z}$ und $\mathbb{Z}_n$, d. h. es gilt[2] **1.6**

$$\begin{aligned} \varrho_n(a + b) &= \varrho_n(a) +_n \varrho_n(b) \\ \varrho_n(a \cdot b) &= \varrho_n(a) \cdot_n \varrho_n(b) . \end{aligned}$$

Insbesondere ist

$$\varrho_n(-a) = -\varrho_n(a) \quad \text{und} \quad \varrho_n(a - b) = \varrho_n(a) -_n \varrho_n(b) .$$

Beweis Infolge der Definition der Addition und Multiplikation in $\mathbb{Z}_n$ sind die ersten Behauptungen klar. Wir begründen nur die zwei letzten. Es ist

$$0 = \varrho_n(0) = \varrho_n(a - a) = \varrho_n(a + (-a)) = \varrho_n(a) +_n \varrho_n(-a) ,$$

d. h. im Ring $\mathbb{Z}_n$ gilt $\varrho_n(-a) = -\varrho_n(a)$. Es folgt

$$\begin{aligned} \varrho_n(a - b) &= \varrho_n(a + (-b)) = \varrho_n(a) +_n (-\varrho_n(b)) \\ &= \varrho_n(a) -_n \varrho_n(b) . \end{aligned}$$

□

[2] Man spricht von einem *Ring-Homomorphismus.*

Als Beispiele notieren wir die Additions- und Multiplikationstafeln der Ringe $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ und $\mathbb{Z}_5$

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	1	2
1	1	2
2	2	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Wir definieren: Sei $\mathbb{F}$ ein Ring. Dann heißt $\mathbb{F}$ **Körper**, wenn im Ring $\mathbb{F}$ neben R1 bis R5 noch folgende zwei Gesetze gelten:

K1 $a, b \in \mathbb{F}^* \;\Rightarrow\; a \cdot b \in \mathbb{F}^*$ (d. h. $\mathbb{F}$ ist nullteilerfrei)
K2 Die Gleichung $a \cdot x = b$ $(a, b \in \mathbb{F}^*)$ besitzt genau eine Lösung x in $\mathbb{F}^*$.

Insbesondere ist dann die Gleichung $a \cdot x = 1$ eindeutig lösbar, man schreibt

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

Daraus ergibt sich auch die Lösung von $a \cdot x = b$ zu $x = a^{-1} \cdot b$, denn

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

Man schreibt

$$a \cdot b^{-1} = \frac{a}{b} \ .$$

Da die Multiplikation im Ring $\mathbb{F}$ assoziativ ist und $\mathbb{F}$ ein Einselement besitzt, besagen die zwei Gesetze K1, K2, dass $\mathbb{F}^*$ bezüglich der Multiplikation eine abelsche Gruppe ist (siehe Kap. 6, Seite 79). Diese Gruppe heißt die **multiplikative Gruppe des Körpers** $\mathbb{F}$, sie wird mit $\mathbb{F}^*$ notiert.

Wir zeigen nun, dass der Ring $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n eine Primzahl ist. Dabei nennt man eine Zahl $p \in \mathbb{N}$, $p > 1$, **Primzahl**, wenn sie *unzerlegbar* ist, also 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind (in $\mathbb{Z}$ kommen die Teiler -1 und $-p$ hinzu).

Für $a \in \mathbb{Z},\ a \neq 0$, sei $\mathcal{P}(a)$ die Menge der Primzahlen, die a teilen; z. B. ist $\mathcal{P}(12) = \mathcal{P}(-12) = \{2, 3\}$. Die für uns wichtigste Eigenschaft von Primzahlen ist:

PRIM $\quad \mathcal{P}(a \cdot b) = \mathcal{P}(a) \cup \mathcal{P}(b) \qquad$ (Vereinigungsmenge)

Diese an sich selbstverständliche Beziehung bedeutet, dass eine Primzahl, die $a \cdot b$ teilt, schon a oder b teilt. Dies ergibt sich aus der eindeutigen Primfaktorzerlegung der Zahlen a, b und $a \cdot b$. Wir erklären dies genauer in Kap. 3.

Sei $n \in \mathbb{N},\ n \geq 2$. Ist n keine Primzahl, so existieren a, b in $\mathbb{Z}_n$, $a \neq 0 \neq b$, mit $n = a \cdot b$, d. h.

$$a \cdot_n b = \varrho_n(n) = 0 \ ,$$

der Ring $\mathbb{Z}_n$ ist also nicht nullteilerfrei. Genauer gilt:

Der Ring $\mathbb{Z}_n$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist. **1.7**

Beweis Sei n Primzahl. Wir nehmen an, dass $\mathbb{Z}_n$ nicht nullteilerfrei ist, dann existieren $a, b \neq 0$ in $\mathbb{Z}_n$ mit

$$a \cdot_n b = 0 \, , \quad \text{d. h.} \quad \varrho_n(a \cdot b) = 0 \ .$$

Also ist n Teiler von $a \cdot b$ und wegen PRIM auch Teiler von a oder b im Widerspruch zu $a, b < n$. Dies beweist 1.7. $\square$

1.8 **Satz** Genau dann ist der Ring $\mathbb{Z}_n$ ein Körper, wenn n eine Primzahl ist.

Beweis Ist $\mathbb{F} := \mathbb{Z}_n$ Körper, gilt also K1, so ist n nach 1.7 eine Primzahl. Sei p Primzahl und

$$\mathbb{F} := \mathbb{Z}_p \ .$$

Wir behaupten, dass K1 und K2 in

$$\mathbb{F}^* = \{1, 2, \ldots, p-1\}$$

gelten. K1 ist 1.7. Für K2 ist zu zeigen, dass die Gleichung $a \cdot_p x = b$ für $a, b \in \mathbb{F}^*$ genau eine Lösung besitzt. Dazu bilden wir die Menge

$$M = \{a \cdot_p x \mid x \in \mathbb{F}^*\} \ .$$

Es ist $M \subseteq \mathbb{F}^*$. Seien $x, y \in \mathbb{F}^*$ mit $a \cdot_p x = a \cdot_p y$. Da $\mathbb{F}$ nullteilerfrei ist (1.7), können wir die Kürzregel 1.1 anwenden und erhalten $x = y$. Die Teilmenge M der endlichen Menge $\mathbb{F}^*$ enthält daher genau so viel Elemente wie $\mathbb{F}^*$; es folgt $M = \mathbb{F}^*$. Also existiert genau ein $x \in \mathbb{F}^*$ mit $a \cdot_p x = b$. □

Im Anschluss an diesen Beweis machen wir eine kleine Rechnung im Körper

$$\mathbb{F} :=\ \mathbb{Z}_p \ .$$

Sei $a \in \mathbb{F}^*$. Dann ist (s. o)

$$\mathbb{F}^* \ = \ \{a \cdot_n x \mid x \in \mathbb{F}^*\} \ .$$

Das Produkt aller $(p-1)$ Elemente $1, 2, \ldots, p-1$ von $\mathbb{F}^*$, welches wir mit b bezeichnen, ist also bis auf Reihenfolge gleich dem Produkt der $(p-1)$ Elemente $a \cdot_p x$, $x \in \mathbb{F}^*$, das wir mit c bezeichnen. Stellt man im Produkt c die Faktoren a an den Anfang, so folgt $c = a^{p-1} \cdot_p b$, und damit

$$a^{p-1} \cdot_p b \ = \ b \ .$$

Kürzt man durch b, so erhält man im Körper $\mathbb{F}$ die Relation

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

Wir schreiben diese etwas anders und erhalten den

Satz von Fermat Sei $a \neq 0$ eine Zahl in $\mathbb{Z}$, welche nicht durch die Primzahl p teilbar ist. Dann ist $\varrho_p\,(a^{p-1}) = 1$.[3] □ **1.9**

Ein Beispiel findet sich in einer Übungsaufgaben am Schluss des Kapitels.

Es sei bemerkt, dass dieser Satz die mathematische Grundlage für das RSA–Kryptographiesystem ist.

Ein endlicher Körper $\mathbb{F}$ heißt **Galoisfeld**, man schreibt $\mathbb{F} = \mathrm{GF}\,(q)$, wenn er q Elemente besitzt. Also ist $\mathbb{Z}_p = \mathrm{GF}\,(p)$. Wir werden in Kap. 10 sehen, dass q immer eine Primzahlpotenz p^n ist; bei fest gewähltem p ist also $\mathbb{Z}_p$ das kleinste Galoisfeld.

Ausblick 1 Das abstrakte Argument im Beweis von 1.8 erklärt nicht, wie das inverse Element a^{-1} aus a konkret berechnet werden kann. Folgendes Beispiel zeigt, dass dies für kleines n nicht allzu schwierig ist; wir nehmen $\mathbb{Z}_{13}$ und setzen $\varrho = \varrho_{13}$.
$a = 2,\ 2 \cdot 7 = 14,\ \varrho(14) = 1 \Rightarrow a^{-1} = 7$
$a = 3,\ 3 \cdot 5 = 15,\ \varrho(15) = 2,\ 3 \cdot_{13} 5 \cdot_{13} 7 = 2 \cdot_{13} 7 = 1 \Rightarrow a^{-1} = 5 \cdot_{13} 7 = 9$
$a = 4,\ 4 \cdot 4 = 16,\ \varrho(16) = 3,\ 4 \cdot_{13} 4 \cdot_{13} 9 = 3 \cdot_{13} 9 = 1 \Rightarrow a^{-1} = 4 \cdot_{13} 9 = 10$
u. s. w.

Natürlich wird eine solche „Rekursion“ für größeres p immer länger. Schneller kommt der *erweiterte Euklidische Algorithmus* ans Ziel; diesen stellen wir in Kap. 4 vor.

Ausblick 2 In Kapitel 3 behandeln wir die Teilbarkeit im Ring $\mathbb{Z}$ genauer. Dies ermöglicht einen konstruktiven Beweis von 1.8, siehe Seite 50.

Ausblick 3 Sei p Primzahl. Durch Ausprobieren findet man im Körper $\mathbb{Z}_p$ ein Element z, so dass jedes $a \in \mathbb{Z}_p$, $a \neq 0$, eine Potenz von z ist. Ein solches Element z heißt *primitives Element* des Körpers $\mathbb{Z}_p$. In $\mathbb{Z}_5$ ist z. B. $z = 2$ primitiv, denn

$$z^1 = 2\,, \quad z^2 = 4\,, \quad z^3 = 3\,, \quad z^4 = 1\,,$$

aber 4 kein primitives Element, denn $4 \cdot_5 4 = 1$. In Kap. 6 werden wir zeigen, dass mit z auch jede Potenz z^i primitiv ist, sofern die Zahl i teilerfremd zu $p-1$ ist (6.11 auf Seite 88).

[3] Üblicherweise schreibt man $a^{p-1} \equiv 1 \pmod{p}$.

Mit Hilfe eines primitiven Elements z kann die Multiplikation in einem endlichen Körper sehr übersichtlich organisiert werden, siehe Kap. 8.

Ein relativ tiefliegender Satz besagt, dass in jedem endlichen Körper ein primitives Element existiert. Diesen Satz beweisen wir in Kap. 7, siehe 7.2 auf Seite 95.

Vorschlag Wir rechnen im letzten Kapitel 12 zwei Beispiele in einem Reed–Solomon Code, das erste im Körper $\mathrm{GF}(7) = \mathbb{Z}_7$ und das zweite im Körper $\mathrm{GF}(2^3)$. Wir empfehlen dem Leser, schon jetzt die ersten Seiten dieses Kapitels zu lesen, um sich von der Relevanz endlicher Körper in der Praxis der Nachrichtenübertragung zu überzeugen.

Übungen

1. Wieviele Nullteiler besitzt der Ring $\mathbb{Z}_8$ und wieviele der Ring $\mathbb{Z}_{13}$?
2. Berechne die Additions- und die Multiplikationstafel des Rings $\mathbb{Z}_7$.
3. Für welche Elemente a des Rings $\mathbb{Z}_6$ existiert ein $b \in \mathbb{Z}_6$ mit $a \cdot_6 b = 1$?
4. Gibt es einen Körper mit 31 Elementen?
5. Bestimme alle inversen Elemente $a^{-1}, a \neq 0$, im Körper $\mathbb{Z}_{13}$.
6. Bestimme ein primitives Element im Körper $\mathbb{Z}_7$ und im Körper $\mathbb{Z}_{11}$.
7. Löse über dem Körper $\mathbb{Z}_p$ folgende lineare Gleichungssysteme:
   $p = 2$ und
   $$\begin{aligned} x_1 +_2 x_2 +_2 x_3 &= 1 \\ x_1 +_2 x_2 &= 0 \\ x_2 +_2 x_3 &= 1\ , \end{aligned}$$
   $p = 3$ und
   $$\begin{aligned} 2 \cdot_3 x_1 +_3 x_2 +_3 2 \cdot_3 x_3 &= 2 \\ x_1 +_3 x_2 +_3 2 \cdot_3 x_3 &= 0 \\ x_1 +_3 2 \cdot_3 x_2 &= 0\ . \end{aligned}$$
8. Bestimme die Zahl $\varrho_{43}(20576^{42})$.