Elementare Zahlentheorie

Wintersemester 2017/18

Dr. Hendrik Kasten (Skript von Dr. Denis Vogel)

7. Februar 2018

Inhaltsverzeichnis

KAPITEL I

Rechnen mit Restklassen

§1 Teilbarkeit

In diesem Skript werden wir die folgenden Notationen verwenden:

- $\mathbb{N} := \{1, 2, 3, \dots\}$ bezeichne die Menge der natürlichen Zahlen,
- $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ bezeichne die Menge der nichtnegativen ganzen Zahlen.

Definition 1.1. *Es seien $a, b \in \mathbb{Z}$. Die Zahl a heißt ein **Teiler** von b (Notation: $a|b$), wenn ein $q \in \mathbb{Z}$ mit $b = qa$ existiert. In diesem Fall nennt man die Zahl b auch ein **Vielfaches** von a.*

Die folgende Bemerkung beinhaltet einige sehr einfache Eigenschaften der Teilbarkeit, die sich unmittelbar aus der vorangegangenen Definition ergeben.

Proposition 1.2. *Es seien $a, b, c, d \in \mathbb{Z}$. Dann gilt:*

(a) *Aus $a \mid b$ und $a \mid c$ folgt $a \mid (b + c)$.*
(b) *Aus $a \mid b$ folgt $a \mid bc$.*
(c) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$*
(d) *Aus $a \mid c$ und $b \mid d$ folgt $ab \mid cd$.*

Beweis. Zum Nachweis von (a) gelte $a \mid b$ und $a \mid c$. Dann existieren $q_1, q_2 \in \mathbb{Z}$ mit $b = q_1 a$, $c = q_2 a$, somit ist $b + c = (q_1 + q_2)a$, d.h. $a \mid (b + c)$. Für den Beweis von (b) setzen wir $a \mid b$ voraus, d.h. es existiert ein $q \in \mathbb{Z}$ mit $b = qa$. Dann ist $bc = qca$, und somit gilt $a \mid bc$. Zu (c) bemerken wir, dass aus $a \mid b$ und $b \mid c$ die Existenz von $q_1, q_2 \in \mathbb{Z}$ mit $b = q_1 a$, $c = q_2 b$ folgt, und damit $c = q_2 q_1 a$, was $a \mid c$ impliziert. Es verbleibt der Beweis von (d). Dazu gelte $a \mid c$ und $b \mid d$. Dann existieren $q_1, q_2 \in \mathbb{Z}$ mit $c = q_1 a$, $d = q_2 b$, weswegen $cd = q_1 q_2 ab$ und daraufhin $ab \mid cd$ folgt. □

Der nächste Satz beschreibt ein Verfahren, das letztlich schon aus aus der Grundschule bekannt sein dürfte - die Division mit Rest auf den ganzen Zahlen. Nichtsdestotrotz ist das Verfahren unglaublich nützlich, wir werden den Satz später in sehr vielen Beweisen anwenden.

Satz 1.3 (Division mit Rest)**.** *Es seien $a, b \in \mathbb{Z},\ b \neq 0$. Dann gilt:*
Es gibt eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = qb + r \ \text{ und } \ 0 \leq r < |b\,| \,.$$

*Die Zahl r heißt der **Rest**, die Zahl q heißt der **ganzzahlige Quotient** bei Division von a durch b.*

Beweis. Wir zeigen zunächst die Existenz von $q, r \in \mathbb{Z}$ mit obigen Eigenschaften. Dazu setzen wir

$$R := \{a - \tilde{q}b \mid \tilde{q} \in \mathbb{Z}\} \cap \mathbb{N}_0 \subseteq \mathbb{N}_0.$$

Offenbar ist R eine nichtleere Teilmenge von $\mathbb{N}_0$, insbesondere besitzt R ein eindeutig bestimmtes kleinstes Element, welches wir im Folgenden mit r bezeichnen wollen. Es sei q diejenige ganze Zahl mit $a - qb = r$, also mit $a = qb + r$. Wir behaupten, dass $0 \leq r < |b|$ ist. Angenommen, es gilt $r \geq |b|$. Es ergibt sich

$$0 \leq r - |b| = a - qb - \operatorname{sgn}(b)b = \underbrace{a - (q + \operatorname{sgn}(b))b}_{\in R} < r,$$

im Widerspruch zur Minimalität von r.

Es verbleibt der Beweis der Eindeutigkeit. Seien dazu $r, \tilde{r}, q, \tilde{q} \in \mathbb{Z}$ mit

$$a = qb + r = \tilde{q}b + \tilde{r}, \quad 0 \leq r, \tilde{r} < |b|.$$

Wir erhalten $(q - \tilde{q})b = \tilde{r} - r$, also $b \mid (\tilde{r} - r)$. Nach Voraussetzung ist $|\tilde{r} - r| < |b|$, weswegen sich $\tilde{r} - r = 0$, d.h. $r = \tilde{r}$, und $q = \tilde{q}$ ergibt. □

Definition 1.4. *Es seien $a_1, \ldots, a_n \in \mathbb{Z}$. Wir setzen*

$$\begin{aligned} T(a_1, \ldots, a_n) &:= \{t \in \mathbb{Z} \ \mid t \mid a_1, \ldots, t \mid a_n\} \\ &= T(a_1) \cap \ \ldots \ \cap T(a_n). \end{aligned}$$

*$T(a_1, \ldots, a_n)$ bezeichnet also die Menge der **gemeinsamen Teiler** von $a_1, \ldots, a_n$.*
*Eine Zahl $d \in \mathbb{Z}$ heißt ein **größter gemeinsamer Teiler** von $a_1, \ldots, a_n$, wenn folgendes gilt:*

(a) $d \geq 0$,

(b) $d \in T(a_1, \ldots, a_n)$,

(c) *Ist $t \in T(a_1, \ldots, a_n)$, dann gilt $t \mid d$.*

Aus dieser Definition geht nicht direkt hervor, ob ein größter gemeinsamer Teiler überhaupt existiert und inwieweit er eindeutig bestimmt ist. Natürlich könnten wir für $a_1, \ldots, a_n \in \mathbb{Z}$, $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ den größten gemeinsamer Teiler auch als das bzgl. „$\leq$" größte Element von $T(a_1, \ldots, a_n)$ festsetzen. Unsere Definition ist jedoch für die meisten Verwendungszwecke tauglicher. Dafür müssen wir für Existenz und Eindeutigkeit allerdings etwas Arbeit investieren.

Proposition 1.5. *Es seien $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt: $a_1, \ldots, a_n$ besitzen höchstens einen größten gemeinsamen Teiler.*

Beweis. Seien d_1, d_2 größte gemeinsame Teiler von $a_1, \ldots, a_n$. Da d_1 ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist, und d_2 ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist, folgt nach 1.4(c): $d_1 \mid d_2$. Analog erhalten wir $d_2 \mid d_1$. Somit existieren $q_1, q_2 \in \mathbb{Z}$ mit $d_2 = q_1 d_1, d_1 = q_2 d_2$. Es ergibt sich $d_1 = q_2 q_1 d_1$. Wir machen nun eine Fallunterscheidung. Ist $d_1 \neq 0$, so ist $q_2 q_1 = 1$, also $q_1 \in \{\pm 1\}$ und deshalb $d_2 = \pm d_1$. Aufgrund von $d_1, d_2 \geq 0$ (vgl. 1.4(a)) folgt $d_2 = d_1$. Ist $d_1 = 0$, folgt $d_2 = q_1 \cdot 0 = 0$. □

Der Beweis zeigt insbesondere: Lässt man in Definition 1.4 die Bedingung (a) weg, so gibt es höchstens zwei größte gemeinsame Teiler von $a_1, \ldots, a_n$; mit d wäre dann stets auch $-d$ ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.

Die folgende einfache Bemerkung spielt eine Schlüsselrolle in der Konstruktion eines größten gemeinsamen Teilers zweier ganzer Zahlen.

Proposition 1.6. *Es seien $a, b \in \mathbb{Z}$. Dann gilt: Sind $q, r \in \mathbb{Z}$ mit $a = qb + r$, dann ist*

$$T(a, b) = T(b, r).$$

Beweis. Ist $t \in T(a, b)$, dann folgt $t \mid (a - qb) = r$, also $t \in T(b, r)$. Umgekehrt ergibt sich aus $t \in T(b, r)$, dass $t \mid (qb + r) = a$ gilt und somit $t \in T(a, b)$. □

Sind $a, b \in \mathbb{N}$, o.E. $a \geq b$, so folgt aus der obigen Bemerkung, dass man durch Division mit Rest, etwa in der Form $a = qb + r$ mit $0 \leq r < |b|$, die Berechnung der Menge der gemeinsamen Teiler $T(a, b)$ auf die Berechnung der Menge der gemeinsamen Teiler $T(b, r)$ zurückführen kann - hierbei ist jetzt r kleiner als b und damit auch kleiner als a. Durch Iteration dieses Verfahrens kann man die Berechnung von $T(a, b)$ auf die Berechnung gemeinsamer Teilermengen immer kleiner werdender Zahlen zurückführen. Das ist die Grundidee des Euklidischen Algorithmus.

Satz 1.7 (Euklidischer Algorithmus)**.** *Es seien $a \geq b \in \mathbb{Z}$. Dann gilt:*

(a) *a, b besitzen einen eindeutig bestimmten größten gemeinsamen Teiler. Dieser wird mit $\mathrm{ggT}(a, b)$ bezeichnet und **der größte gemeinsame Teiler** von a und b genannt.*

(b) *$\mathrm{ggT}(a, b)$ kann mit dem Euklidischen Algorithmus bestimmt werden:*
Ist $b \neq 0$, setze $z_1 := a$, $z_2 := |b|$ und erhalte $z_3, z_4, \ldots \in \mathbb{N}_0$ durch die Gleichungen

$$\begin{aligned} (G_1) \quad & z_1 = q_1 z_2 + z_3 \quad \textit{mit} \quad 0 \leq z_3 < z_2\,, \\ (G_2) \quad & z_2 = q_2 z_3 + z_4 \quad \textit{mit} \quad 0 \leq z_4 < z_3\,, \end{aligned}$$

usw. Dieser Prozess bricht nach endlich vielen Schritten (etwa nach r Schritten) ab:

$$\begin{aligned} (G_{r-1}) \quad & z_{r-1} = q_{r-1} z_r + z_{r+1} \quad \textit{mit} \quad 0 \leq z_{r+1} < z_r \\ (G_r) \quad & z_r = q_r z_{r+1} + 0 \end{aligned}$$

und es gilt: $\mathrm{ggT}(a, b) = z_{r+1}$.
Im Fall $b = 0$ ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, 0) = |a|$.

(c) *Es gibt $u, v \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(a,b) = ua + vb.$$

(„erweiterter Euklidischer Algorithmus“)

Beweis. Wir betrachten zunächst den Fall $b = 0$: Offenbar gilt $|a| \mid a$ sowie $|a| \mid 0$. Ist $t \in T(a,0) = T(a)$, so folgt $t \mid |a|$. Demnach ist $|a|$ ist ein größter gemeinsamer Teiler von a und 0, die Eindeutigkeit folgt aus 1.5. Außerdem ist $|a| = \mathrm{ggT}(a,0) = \mathrm{sgn}(a) \cdot a + 0 \cdot 0$, was in diesem Spezialfall die Gültigkeit der Aussage (c) impliziert.
Im Folgenden sei $b \neq 0$. Für die Folge der Reste gilt $z_2 > z_3 > z_4 > \ldots$, d.h. nach endlich vielen Schritten, etwa nach r Schritten, stoppt das Verfahren. Die letzten beiden Gleichungen sind dann von der Form

$$\begin{array}{lll} (G_{r-1}) & z_{r-1} = q_{r-1}z_r + z_{r+1} \text{ mit } 0 \leq z_{r+1} < z_r \\ (G_r) & z_r = q_r z_{r+1} + 0 \end{array}$$

Wegen 1.6 ist

$$\begin{aligned} T(a,b) &= T(a,|b|) = T(z_1,z_2) \overset{1.6}{=} T(z_2,z_3) \\ &\overset{1.6}{=} \ldots \overset{1.6}{=} T(z_r,z_{r+1}) \overset{1.6}{=} T(z_{r+1},0) \\ &= T(z_{r+1})\,. \end{aligned}$$

Es ist $z_{r+1} \in T(z_{r+1}) = T(a,b)$. Ist $t \in T(a,b) = T(z_{r+1})$, so folgt $t \mid z_{r+1}$. Nach Konstruktion ist $z_{r+1} > 0$. Wir haben damit nachgewiesen, dass z_{r+1} ist ein größter gemeinsamer Teiler von a, b ist, die Eindeutigkeitsaussage ergibt sich aus 1.5. Hiermit sind die Aussagen (a) und (b) gezeigt, es verbleibt uns, Aussage (c) zu zeigen. Wegen

$$\begin{array}{lll} (G_{r-2}) & z_{r-2} = q_{r-2}\, z_{r-1} + z_r \\ (G_{r-1}) & z_{r-1} = q_{r-1}\, z_r + \mathrm{ggT}(a,b) \end{array}$$

ergibt sich

$$\begin{aligned} \mathrm{ggT}(a,b) &= z_{r-1} - q_{r-1}\, z_r = z_{r-1} - q_{r-1}(z_{r-2} - q_{r-2}\, z_{r-1}) \\ &= v_{r-1}z_{r-1} + u_{r-1}\, z_{r-2} \quad \text{mit geeigneten} \quad u_{r-1}, v_{r-1} \in \mathbb{Z}\,. \end{aligned}$$

Wir benutzen nun (G_{r-3}), um z_{r-1} über z_{r-3}, z_{r-2} auszudrücken usw. Aus (G_1) erhalten wir schließlich $u_2, v_2 \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a,b) = v_2 z_2 + u_2 z_1 = v_2|b| + u_2 a\,.$$

Wir setzen $u := u_2$, $v := v_2\,\mathrm{sgn}(b)$, dann ist $\mathrm{ggT}(a,b) = ua + vb$. □

Beispiel 1.8. *Wir bestimmen mit Hilfe des Euklidischen Algorithmus den* ggT *von* 6930 *und* 1098*:*

$$\begin{aligned} 6930 &= 6 \cdot 1098 + 342 \\ 1098 &= 3 \cdot 342 + 72 \\ 342 &= 4 \cdot 72 + 54 \\ 72 &= 1 \cdot 54 + 18 \\ 54 &= 3 \cdot 18 + 0 \end{aligned}$$

Wir erhalten $\mathrm{ggT}(6930, 1098) = 18$. *Das im obigen Beweis dafür gegebene Argument lautet hier konkret (unter Verwendung von 1.6):*

$$\begin{aligned} T(6930,1098) &= T(1098,342) = T(342,72) = T(72,54) = T(54,18) = T(18,0) \\ &= T(18). \end{aligned}$$

Darüber hinaus ergibt sich

$$\begin{aligned} \mathrm{ggT}(6930,\, 1098) &= 18 = 72 - 1 \cdot 54 = 72 - (342 - 4 \cdot 72) = 5 \cdot 72 - 342 \\ &= 5 \cdot (1098 - 3 \cdot 342) - 342 = 5 \cdot 1098 - 16 \cdot 342 \\ &= 5 \cdot 1098 - 16 \cdot (6930 - 6 \cdot 1098) \\ &= (-16) \cdot 6930 + 101 \cdot 1098. \end{aligned}$$

Die lineare Kombinierbarkeit von $\mathrm{ggT}(a, b)$ aus a, b durch den erweiterten Euklidischen Algorithmus ist eine sehr wichtige Eigenschaft des größten gemeinsamen Teilers, die man sehr häufig in Beweisen benötigt. Als Beispiel dafür dient der Beweis der folgenden Proposition.

Proposition 1.9. *Es seien* $a, b, c, d \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, b) = 1$. *Dann gilt:*

(a) *Aus* $a \mid bc$ *folgt* $a \mid c$

(b) *Aus* $a \mid d$ *und* $b \mid d$ *folgt* $ab \mid d$.

Beweis. Wir bemerken zunächst, dass es wegen $\mathrm{ggT}(a, b) = 1$ nach dem erweiterten Euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit $ua + vb = 1$ gibt. Setzen wir $a \mid bc$ voraus, so existiert ein $q \in \mathbb{Z}$ mit $bc = qa$. Es ist dann

$$c = c \cdot 1 = c(ua + vb) = cua + vbc = cua + vqa = a(cu + vq),$$

was $a \mid c$ und somit Aussage (a) impliziert. Gilt $a \mid d$ und $b \mid d$, dann gibt es $q_1, q_2 \in \mathbb{Z}$ mit $d = q_1 a, d = q_2 b$. Wir erhalten

$$d = d \cdot 1 = d(ua + vb) = dua + dvb = q_2 bua + q_1 avb = ab(q_2 u + q_1 v)$$

und deshalb $ab \mid d$, was den Beweis von Aussage (b) beendet. □

Nachdem wir den Spezialfall des größten gemeinsamen Teilers zweier Zahlen abgehandelt haben, wenden wir uns nun dem allgemeinen Fall zu. Dafür ist es sehr nützlich, sich mit Idealen in $\mathbb{Z}$ zu beschäftigen.

Definition 1.10. *Es sei* $\mathfrak{a} \subseteq \mathbb{Z}$. *Dann heißt* $\mathfrak{a}$ *ein* ***Ideal*** *in* $\mathbb{Z}$, *wenn die folgenden Bedingungen erfüllt sind:*

(a) $0 \in \mathfrak{a}$

(b) *Sind* $a_1, a_2 \in \mathfrak{a}$, *dann ist* $a_1 + a_2 \in \mathfrak{a}$

(c) *Sind* $a \in \mathfrak{a}$, $r \in \mathbb{Z}$, *dann ist* $ra \in \mathfrak{a}$.

Die nächste Proposition zeigt, dass Ideale in $\mathbb{Z}$ von einer einfachen Form sind.

Proposition 1.11. *Es sei $\mathfrak{a}$ ein Ideal in $\mathbb{Z}$. Dann gibt es ein eindeutig bestimmtes $m \in \mathbb{N}_0$, so dass*

$$\mathfrak{a} = m\mathbb{Z} := \{mr \mid r \in \mathbb{Z}\}$$

ist.

Beweis. Wir zeigen zunächst die Existenz eines $m \in \mathbb{N}_0$ mit $\mathfrak{a} = m\mathbb{Z}$. Falls $\mathfrak{a} = \{0\}$ ist, so ist $\mathfrak{a} = 0 \cdot \mathbb{Z}$, und wir sind fertig. Im folgenden sei $\mathfrak{a} \neq \{0\}$. Aufgrund von 1.10(c) folgt aus $n \in \mathfrak{a}$ stets $-n \in \mathfrak{a}$, insbesondere ist $\mathfrak{a} \cap \mathbb{N}$ nichtleer und besitzt deshalb ein eindeutig bestimmtes kleinstes Element m. Wir behaupten, dass $\mathfrak{a} = m\mathbb{Z}$ ist. Jedes Element aus $m\mathbb{Z}$ ist von der Form rm mit $r \in \mathbb{Z}$. Wegen $m \in \mathfrak{a}$ folgt mit 1.10(c), dass $rm \in \mathfrak{a}$ ist, es gilt also $m\mathbb{Z} \subseteq \mathfrak{a}$. Sei nun $a \in \mathfrak{a}$. Durch Division mit Rest erhalten wir $q, r \in \mathbb{Z}$ mit $a = qm + r$, $0 \leq r < m$. Wegen

$$r = a - qm = \underset{\in\mathfrak{a}}{a} + \underbrace{(-q)m}_{\in\mathfrak{a}} \in \mathfrak{a}$$

ergibt sich aus der Minimalität von m in $\mathfrak{a} \cap \mathbb{N}$, dass $r = 0$ ist. Deswegen ist $a = qm \in m\mathbb{Z}$, wir haben damit die Inklusion $\mathfrak{a} \subseteq m\mathbb{Z}$ gezeigt.

Zum Nachweis der Eindeutigkeit seien $m, n \in \mathbb{N}_0$ mit $m\mathbb{Z} = n\mathbb{Z}$. Dann gilt $n \in m\mathbb{Z}$ und $m \in n\mathbb{Z}$, d.h. es existieren $r, \tilde{r} \in \mathbb{Z}$ mit $n = mr$, $m = n\tilde{r}$. Dies liefert $n = mr = n\tilde{r}r$. Falls $n = 0$ ist, folgt $m = 0 \cdot \tilde{r} = 0$. Falls $n \neq 0$ ist, so folgt $r = \tilde{r} = 1$ oder $r = \tilde{r} = -1$. Wegen $m, n \in \mathbb{N}_0$ ergibt sich $r = 1$, denn andernfalls wäre $m = -n < 0$. Wir erhalten $m = n$. □

Aus zwei Idealen in $\mathbb{Z}$ lässt sich auf einfache Weise ein weiteres Ideal erzeugen:

Definition 1.12. *Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathbb{Z}$. Wir setzen*

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a},\ b \in b\}.$$

*und nennen $\mathfrak{a} + \mathfrak{b}$ die **Summe** der Ideale $\mathfrak{a}$ und $\mathfrak{b}$.*

Proposition 1.13. *Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathbb{Z}$. Dann gilt: $\mathfrak{a} + \mathfrak{b}$ ist ein Ideal in $\mathbb{Z}$.*

Beweis. Aufgrund von $0 = 0 + 0$, $0 \in \mathfrak{a}$, $0 \in \mathfrak{b}$ ist 0 in $\mathfrak{a} + \mathfrak{b}$ enthalten.
Sind $c_1, c_2 \in \mathfrak{a} + \mathfrak{b}$, dann existieren $a_1, a_2 \in \mathfrak{a}, b_1, b_2 \in \mathfrak{b}$, mit $c_1 = a_1 + b_1, c_2 = a_2 + b_2$, also ist

$$c_1 + c_2 = (a_1 + b_1) + (a_2 + b_2) = (\underbrace{a_1 + a_2}_{\in\mathfrak{a}}) + (\underbrace{b_1 + b_2}_{\in\mathfrak{b}}) \in \mathfrak{a} + \mathfrak{b}.$$

Ist $c \in \mathfrak{a} + \mathfrak{b}$ und $r \in \mathbb{Z}$, dann gibt es Elemente $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, sodass $c = a + b$ ist. Das liefert

$$rc = r(a + b) = \underset{\in\mathfrak{a}}{ra} + \underset{\in\mathfrak{b}}{rb} \in \mathfrak{a} + \mathfrak{b}.$$

□

Das folgende Beispiel legt nahe, dass ein sehr enger Zusammenhang zwischen Summen von Idealen in $\mathbb{Z}$ und größten gemeinsamen Teilern besteht.

Beispiel 1.14. *Es ist* $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$*, denn:*

$$1 = \mathrm{ggT}(2,3) = (-1)\cdot 2 + 1 \cdot 3 \in 2\mathbb{Z} + 3\mathbb{Z},$$

und für alle $r \in \mathbb{Z}$ *ist* $r = r \cdot 1 \in 2\mathbb{Z} + 3\mathbb{Z}$.

Die obige Definition 1.12 und nachfolgende Bemerkung 1.13 verallgemeinern sich in naheliegender Weise auf Summen von Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ aus $\mathbb{Z}$. Offenbar ist Summenbildung von Idealen assoziativ. Wir erhalten mit dem folgenden Satz eine explizite Beschreibung von Summen von Idealen aus $\mathbb{Z}$ und damit gleichzeitig die Existenz des größten gemeinsamen Teilers ganzer Zahlen $a_1, \ldots, a_n$.

Satz 1.15. *Es seien* $a_1, \ldots, a_n \in \mathbb{Z}$*. Dann besitzen die Zahlen* $a_1, \ldots, a_n$ *einen eindeutig bestimmten größten gemeinsamen Teiler. Dieser wird mit* $\mathrm{ggT}(a_1, \ldots, a_n)$ *bezeichnet. Es ist*

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = \mathrm{ggT}(a_1, \ldots, a_n)\mathbb{Z}\,.$$

Insbesondere gibt es $u_1, \ldots, u_n \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a_1, \ldots, a_n) = u_1a_1 + \cdots + u_na_n$.

Beweis. Nach 1.13 und 1.11 existiert ein $d \in \mathbb{N}_0$ mit $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$. Wir behaupten, dass d ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist. Sei $i \in \{1, \ldots, n\}$. Aufgrund von

$$a_i = 0 \cdot a_1 + \cdots + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots + 0 \cdot a_n \in a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$$

folgt, dass es ein $r_i \in \mathbb{Z}$ mit $a_i = dr_i$ gibt, d.h. d ist ein Teiler von a_i. Das impliziert $d \in T(a_1, \ldots, a_n)$. Sei nun $t \in T(a_1, \ldots, a_n)$. Wegen $d \in d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ existieren $u_1, \ldots, u_n \in \mathbb{Z}$ mit $d = u_1a_1 + \cdots + u_na_n$. Aufgrund von $t \mid a_1, \ldots, t \mid a_n$ folgt dann $t \mid d$.
Die Eindeutigkeitsaussage ergibt sich aus 1.5. □

Der vorangegangene Beweis lässt sich für ein direktes Rechenverfahren zur Bestimmung von $\mathrm{ggT}(a_1, \ldots, a_n)$ nicht verwenden. Allerdings zeigt eine genauere Betrachtung, dass der Euklidische Algorithmus auch hier zum Ziel führt:

Korollar 1.16. *Es seien* $a_1, \ldots, a_n \in \mathbb{Z}$*. Dann gilt:*

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

Insbesondere kann $\mathrm{ggT}(a_1, \ldots, a_n)$ *durch sukzessives Anwenden des Euklidischen Algorithmus berechnet werden.*

Beweis. Anwendung von 1.15 liefert

$$\begin{aligned} \mathrm{ggT}(a_1, \ldots, a_n)\mathbb{Z} &= a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} \\ &= a_1\mathbb{Z} + \mathrm{ggT}(a_2, \ldots, a_n)\mathbb{Z} \\ &= \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))\mathbb{Z}. \end{aligned}$$

Die Behauptung ergibt sich aus der Eindeutigkeitsaussage in 1.11. □

§2 Primzahlen

Im folgenden Abschnitt werden uns mit einigen einfachen, aber für das Weitere sehr wichtigen Eigenschaften von Primzahlen beschäftigen.

Definition 2.1. *Ein natürliche Zahl $p > 1$ heißt **Primzahl**, wenn $T(p) = \{\pm 1, \pm p\}$, also $T(p) \cap \mathbb{N} = \{1, p\}$ ist. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$.*

Proposition 2.2. *Es sei $a \in \mathbb{N}$, $a > 1$. Dann ist der kleinste positive von 1 verschiedene Teiler von a eine Primzahl.*

Beweis. Wir setzen $T_+ := (T(a) \cap \mathbb{N})\backslash\{1\} = \{t \in \mathbb{N} \mid t \mid a,\ t \neq 1\}$. Wegen $a \in T_+$ ist $T_+ \neq \varnothing$, insbesondere hat T_+ ein kleinstes Element p. Wir behaupten, dass p eine Primzahl ist. Sei dazu $t \in \mathbb{N}$, $t \neq 1$ mit $t \mid p$. Aufgrund von $p \mid a$ ergibt sich mit 1.2(c), dass $t \mid a$ gilt, also $t \in T_+$. Da $t \mid p$ insbesondere $t \leq p$ nach sich zieht, folgt aus der Minimalität von p in T_+, dass $t = p$ ist und damit die Primalität von p. □

Die nächste Aussage war bereits in der Antike bekannt und findet sich etwa in Euklids „Elementen“.

Satz 2.3 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir nehmen an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_n$ gibt. Wir setzen $N := p_1 \cdot \ldots \cdot p_n + 1$. Insbesondere ist $N > 1$, nach 2.2 gibt es also eine Primzahl p mit $p \mid N$. Wegen $p \in \{p_1, \ldots, p_n\}$ folgt $p \mid p_1 \cdot \ldots \cdot p_n$. Somit erhalten wir $p \mid (N - p_1 \cdot \ldots \cdot p_n) = 1$, was ein Widerspruch ist. □

Die nachfolgende Charakterisierung von Primzahlen ist sehr wichtig und in vielen Beweisen tauglicher als die direkte Verwendung der Definition von Primzahlen.

Proposition 2.4. *Es sei $p \in \mathbb{N}\backslash\{1\}$. Dann sind äquivalent:*

(i) *p ist eine Primzahl.*

(ii) *Aus $p \mid ab$ für $a, b \in \mathbb{Z}$ folgt stets $p \mid a$ oder $p \mid b$.*

Beweis. Wir zeigen zunächst die Implikation (i)$\Longrightarrow$(ii). Sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid ab$ und $p \nmid a$. Dann ist $\mathrm{ggT}(p, a) = 1$, und aus 1.9(a) erhalten wir $p \mid b$. Zum Nachweis der Implikation (ii)$\Longrightarrow$(i) sei $a \in \mathbb{N}$ mit $a \mid p$, d.h. es existiert ein $b \in \mathbb{Z}$ mit $p = ab$. Aufgrund von (ii) ergibt sich $p \mid a$ oder $p \mid b$. Außerdem gilt $a \mid p$ und $b \mid p$. Zusammengenommen erhalten wir, dass eine der beiden Aussagen $p \mid a$ und $a \mid p$ bzw. $p \mid b$ und $b \mid p$ zutrifft. Dies impliziert $a = p$ oder $b = p$, und demzufolge $a = 1$ oder $a = p$. Also ist p eine Primzahl. □

Als nächstes werden wir zeigen, dass die Primzahlen in gewissem Sinne die „Bausteine“ der natürlichen Zahlen darstellen. Wichtig für den Beweis ist die gerade eben gezeigte Charakterisierung von Primzahlen.

Satz 2.5 (Primfaktorzerlegung)**.** *Es sei $n \in \mathbb{N}$. Dann lässt sich die Zahl n bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen schreiben.*

Beweis. Wir zeigen die Aussage per Induktion nach n. Die Zahl $n = 1$ ist konventionsgemäß das leere Produkt, $n = 2$ ist selbst Primzahl. Sei $n > 2$. Ist n eine Primzahl, dann haben wir bereits eine Primfaktorzerlegung erreicht. Falls n keine Primzahl ist, so ist $n = ab$ für geeignete $a, b \in \mathbb{N}$ mit $1 < a, b < n$. Nach Induktionsvoraussetzung besitzen a, b eine Primfaktorzerlegung, das gilt dann aber auch für deren Produkt $n = ab$. Damit ist die Existenz einer Primfaktorzerlegung gezeigt. Zum Nachweis der Eindeutigkeit der Primfaktorzerlegung bis auf die Reihenfolge der Faktoren sei

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

mit Primzahlen $p_1, \ldots p_r, q_1, \ldots, q_s$. Insbesondere gilt dann $p_1 \mid q_1 \cdot \ldots \cdot q_s$. Weil p_1 eine Primzahl ist, erhalten wir aus 2.4, dass es ein $i \in \{1, \ldots, s\}$ mit $p_1 \mid q_i$ gibt. Nach Umnummerieren können wir o.E. annehmen, dass $p_1 \mid q_1$ gilt. Da q_1 und p_1 Primzahlen sind, folgt $p_1 = q_1$. Durch Kürzen von p_1 erhalten wir aus der Ausgangsgleichung

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s < n$$

Aus der Induktionsvoraussetzung können wir nun folgern, dass $r = s$ ist, und nach Vertauschen können wir $p_2 = q_2, \ldots, p_r = q_r$ erreichen. □

§3 Restklassenringe

Die nachfolgende Definition sollte aus der Vorlesung zur Linearen Algebra bekannt sein.

Definition 3.1. *Ein **Ring** ist eine Menge R zusammen mit zwei Verknüpfungen $+ : R \times R \to R, \cdot : R \times R \to R$, so dass gilt:*

(a) *$(R, +)$ ist eine abelsche Gruppe*

(b) *$(R, \cdot)$ ist eine Halbgruppe (d. h. es gilt das Assoziativgesetz) mit neutralem Element.*

(c) *Es gelten die Distributivgesetze*

$$(a + b)c = ac + bc,\ a(b + c) = ab + ac$$

für alle $a, b, c \in R$.

*Das neutrale Element bezüglich „+“ bezeichnen wir mit 0, das neutrale Element bezüglich „$\cdot$“ bezeichnen wir mit 1. Der Ring heißt **kommutativ**, wenn die Multiplikation kommutativ ist, d.h. wenn $ab = ba$ für alle $a, b \in R$ gilt.*

Die Verknüpfungen lassen wir im Folgenden aus der Notation heraus und schreiben kurz: „R ist ein Ring“ anstelle von „$(R, +, \cdot)$ ist ein Ring“. Ab jetzt betrachten wir nur noch kommutative Ringe, d.h. der Ausdruck „Ring“ soll bis zum Ende des Skriptes stets für „kommutativer Ring“ stehen.

Beispiel 3.2. (a) *$\mathbb{Z}$ bildet zusammen mit der üblichen Addition und Multiplikation einen Ring.*

(b) *$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist mit der eingeschränkten Addition und Multiplikation von $\mathbb{C}$ ein Ring, der **Ring der ganzen Gaußschen Zahlen**.*

(c) *Ist R ein Ring, dann ist*

$$R[X] := \{a_n X^n + \ldots + a_1 X + a_0 \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in R\}$$

*zusammen mit der üblichen Addition und Multiplikation von Polynomen ein Ring, der **Polynomring** in einer Variablen über R.*

Definition 3.3. *Es sei R ein Ring und „$\equiv$“ eine Äquivalenzrelation auf R. Dann heisst „$\equiv$“ eine **Kongruenzrelation**, wenn für $a_1, a_2, b_1, b_2 \in R$ gilt:*
Aus $a_1 \equiv a_2$ und $b_1 \equiv b_2$ folgt stets $a_1 + b_1 \equiv a_2 + b_2$ und $a_1 b_1 \equiv a_2 b_2$.

Wir führen an dieser Stelle den Begriff des Ideals ein, den wir schon vom Ring der ganzen Zahlen kennen.

Definition 3.4. *Es sei R ein Ring und $\mathfrak{a} \subseteq R$. Dann heißt $\mathfrak{a}$ ein **Ideal** in R, wenn gilt:*

(a) $0 \in \mathfrak{a}$

(b) *Sind $a, b \in \mathfrak{a}$, dann ist auch $a + b \in \mathfrak{a}$*

(c) *Sind $a \in \mathfrak{a}$, $r \in R$, dann ist auch $ra \in \mathfrak{a}$.*

Beispiel 3.5. *Ideale im Ring $\mathbb{Z}$ haben wir bereits kennengelernt. Diese sind von der Form $n\mathbb{Z}$ mit einem eindeutig bestimmten $n \in \mathbb{N}_0$, vgl.1.11.*

In der nächsten Bemerkung sehen wir, dass Ideale in einem Ring R und Kongruenzrelationen auf R in einem sehr engen Zusammenhang stehen.

Proposition 3.6. *Es sei R ein Ring. Dann gilt:*

(a) *Ist „$\equiv$“ eine Kongruenzrelation auf R, dann ist*

$$\mathfrak{a} := \{a \in R \mid a \equiv 0\}$$

ein Ideal in R, und es gilt

$$a \equiv b \Leftrightarrow a - b \in \mathfrak{a}.$$

(b) *Ist $\mathfrak{a} \subseteq R$ ein Ideal und setzt man*

$$a \equiv b \overset{\text{Def}}{\Leftrightarrow} a - b \in \mathfrak{a},$$

dann ist „$\equiv$“ eine Kongruenzrelation auf R und es gilt

$$\mathfrak{a} = \{a \in R \mid a \equiv 0\}.$$

Die Äquivalenzklasse von $b \in R$ bezüglich „$\equiv$“ ist in diesen Fällen durch

$$\overline{b} := b + \mathfrak{a} := \{b + a \mid a \in \mathfrak{a}\}$$

*gegeben und heißt auch die **Restklasse** von b modulo „$\equiv$“ bzw. modulo $\mathfrak{a}$.*

Beweis. Wir zeigen zunächst Aussage (a). Sei dazu „$\equiv$“ eine Kongruenzrelation auf R. Wir rechnen nach, dass $\mathfrak{a} := \{a \in R \mid a \equiv 0\}$ die Eigenschaften eines Ideals aus 3.4 hat. Weil „$\equiv$“ als Äquivalenzrelation reflexiv ist, folgt $0 \equiv 0$ und deshalb $0 \in \mathfrak{a}$. Sind $a, b \in \mathfrak{a}$, dann gilt $a \equiv 0$ und $b \equiv 0$. Da „$\equiv$“ eine Kongruenzrelation ist, erhalten wir $a + b \equiv 0 + 0 = 0$ und aufgrunddessen $a + b \in \mathfrak{a}$. Ist $a \in \mathfrak{a}$ und $r \in R$, so gilt $a \equiv 0$, und weil „$\equiv$“ eine Kongruenzrelation ist, ergibt sich $ra \equiv r \cdot 0 = 0$, also $ra \in \mathfrak{a}$. Damit ist $\mathfrak{a}$ ein Ideal in R und es ist $a \equiv b \Leftrightarrow a - b \equiv 0 \Leftrightarrow a - b \in \mathfrak{a}$.

Zum Beweis von (b) sei $\mathfrak{a}$ ein Ideal in R, und wir setzen $a \equiv b \overset{\text{Def}}{\Leftrightarrow} a - b \in \mathfrak{a}$. Zunächst zeigen wir, dass „$\equiv$“ eine Äquivalenzrelation ist. Zum Nachweis der Reflexivität sei $a \in R$. Dann ist $a - a = 0 \in \mathfrak{a}$, denn $\mathfrak{a}$ ist ein Ideal. Wir erhalten $a \equiv a$. Für den Beweis der Symmetrie seien $a, b \in R$ mit $a \equiv b$. Wir finden $a - b \in \mathfrak{a}$, was aufgrund der Idealeigenschaft von a auch $b - a = (-1)(a - b) \in \mathfrak{a}$ liefert, also $b \equiv a$. Die Transitivität erkennen wir wie folgt: Sind $a, b, c \in R$ mit $a \equiv b$ und $b \equiv c$, so ergibt sich $a - b \in \mathfrak{a}$, $b - c \in \mathfrak{a}$. Weil $\mathfrak{a}$ ein Ideal ist, erhalten wir $a - c = (a - b) + (b - c) \in \mathfrak{a}$ und deshalb $a \equiv c$. Somit ist „$\equiv$“ eine Äquivalenzrelation. Wir weisen nun noch die restlichen Eigenschaften einer Kongruenzrelation nach. Dazu seien $a_1, a_2, b_1, b_2 \in R$ mit $a_1 \equiv a_2$, $b_1 \equiv b_2$. Das impliziert $a_1 - a_2 \in \mathfrak{a}$ und $b_1 - b_2 \in \mathfrak{a}$. Da $\mathfrak{a}$ ein Ideal ist, ergibt sich $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in \mathfrak{a}$ und aufgrunddessen $a_1 + b_1 \equiv a_2 + b_2$. Außerdem erhalten wir $b_1(a_1 - a_2) \in \mathfrak{a}$ sowie $a_2(b_1 - b_2) \in \mathfrak{a}$. Das liefert $a_1 b_1 - a_2 b_2 = b_1(a_1 - a_2) + a_2(b_1 - b_2) \in \mathfrak{a}$, also $a_1 b_1 \equiv a_2 b_2$. Wir haben somit gesehen, dass „$\equiv$“ eine Kongruenzrelation auf R ist.

In diesen Fällen ist die Äquivalenzklasse eines Elementes $b \in R$ bezüglich „$\equiv$“ durch

$$\begin{aligned} \{x \in R \mid x \equiv b\} &= \{x \in R \mid x - b \in \mathfrak{a}\} = \{x \in R \mid \text{Es gibt ein } a \in \mathfrak{a} \text{ mit } x - b = a\} \\ &= \{b + a \mid a \in \mathfrak{a}\} \\ &= b + \mathfrak{a} \end{aligned}$$

gegeben. □

Korollar 3.7. *Ist „$\equiv$“ eine Kongruenzrelation auf $\mathbb{Z}$, dann gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$, so dass gilt:*

$$a \equiv b \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n \mid (a - b)\,.$$

Umgekehrt ist für jedes $n \in \mathbb{N}_0$ durch

$$a \equiv b \overset{\text{Def}}{\Leftrightarrow} a - b \in n\mathbb{Z} \Leftrightarrow n \mid (a - b)$$

eine Kongruenzrelation auf $\mathbb{Z}$ gegeben. Für $a \equiv b$ schreiben wir in diesem Fall $a \equiv b \pmod{n}$. Die Äquivalenzklasse von $a \in \mathbb{Z}$ bezüglich „$\equiv \pmod{n}$“ ist durch

$$\overline{a} := a + n\mathbb{Z} = \{a + nr \mid r \in \mathbb{Z}\}$$

gegeben.

Beweis. Die Behauptungen folgen direkt aus 3.6, da die Ideale in $\mathbb{Z}$ nach 1.11 von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ sind. □

Beispiel 3.8. *Für $a, b \in \mathbb{Z}$ ist*

$$a \equiv b \pmod 3 \Leftrightarrow a - b \in 3\mathbb{Z} \Leftrightarrow 3 \mid (a-b).$$

Als Restklassen erhalten wir $\overline{0} = 3\mathbb{Z}$, $\overline{1} = 1 + 3\mathbb{Z}$, $\overline{2} = 2 + 3\mathbb{Z}$. Weitere, davon verschiedene Restklassen erhalten wir nicht, denn es ist $\overline{3} = \overline{0}$, da $3 \equiv 0 \pmod 3$, $\overline{4} = \overline{1}$, $\overline{-1} = \overline{2}$ usw. Die Menge der Restklassen modulo 3 ist also durch $\{\overline{0}, \overline{1}, \overline{2}\}$ gegeben.

Beispiel 3.9 (Dreierregel)**.** *Sei $n \in \mathbb{N}_0$. Wir entwickeln n im Dezimalsystem:*

$$n = a_r 10^r + \cdots + a_1 \cdot 10 + a_0$$

mit $0 \leq a_i \leq 9$ für $i = 0, \ldots, r$ $a_r \neq 0$. Es ist $10 \equiv 1 \pmod 3$. Da $\equiv \pmod 3$ eine Kongruenzrelation ist, folgt $10^2 = 10 \cdot 10 \equiv 1 \cdot 1 \pmod 3$, induktiv: $10^i \equiv 1 \pmod 3$ für $i \in \mathbb{N}_0$. Wir erhalten

$$n = a_r 10^r + \cdots + a_1 \cdot 10 + a_0 \equiv a_r \cdot 1 + \cdots + a_1 \cdot 1 + a_0 = a_r + \cdots + a_1 + a_0 \pmod 3.$$

Es folgt:

$$3 \mid n \Leftrightarrow n \equiv 0 \pmod 3 \Leftrightarrow a_r + \cdots + a_0 \equiv 0 \pmod 3 \Leftrightarrow 3 \mid (a_r + \cdots + a_0),$$

d.h. eine natürliche Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Proposition 3.10. *Es sei R ein Ring, „$\equiv$“ eine Kongruenzrelation auf R und $\mathfrak{a}$ das nach 3.6 zu „$\equiv$“ gehörige Ideal in R. $R/\equiv$ bzw. $R/\mathfrak{a}$ bezeichne die Menge aller Restklassen bezüglich „$\equiv$“. Dann ist $R/\mathfrak{a}$ ein Ring bezüglich der wie folgt erklärten Verknüpfungen:*

$$\overline{a} + \overline{b} := \overline{a+b},\ \overline{a} \cdot \overline{b} := \overline{a \cdot b}\,.$$

*und heißt **Restklassenring** („R modulo $\mathfrak{a}$“).*

Beweis. Wir müssen zeigen, dass die Verknüpfungen wohldefiniert sind. Seien dazu $a_1, a_2 \in \overline{a}$, $b_1, b_2 \in \overline{b}$. Dann ist $a_1 \equiv a_2$ und $b_1 \equiv b_2$, und weil „$\equiv$“ eine Kongruenzrelation ist, ergibt sich $a_1 + b_1 \equiv a_2 + b_2$ und somit $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Analog folgt $a_1 b_1 \equiv a_2 b_2$ und deshalb $\overline{a_1 b_1} = \overline{a_2 b_2}$. Addition und Multiplikation von Restklassen sind damit wohldefiniert. Die Ringeigenschaften übertragen sich von R auf $R/\mathfrak{a}$, da Addition und Multiplikation vertreterweise definiert sind. □

Beispiel 3.11. *Die Restklassenringe von $\mathbb{Z}$ sind nach 3.7 (bzw. 1.11) durch $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ gegeben. Explizit sehen diese wie folgt aus:*

- *$n = 0$: Es ist $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, denn für $a \in \mathbb{Z}$ ist $a + 0 \cdot \mathbb{Z} = \{a\}$ (hierbei identifizieren wir $\mathbb{Z}$ mit $\{\{a\} \mid a \in \mathbb{Z}\}$).*

- *$n = 1$: Es ist $\mathbb{Z}/\mathbb{Z} = 0$ der Nullring (hier sind Eins- und Nullelement gleich), denn für $a \in \mathbb{Z}$ ist $a + \mathbb{Z} = \mathbb{Z} = 0 + \mathbb{Z}$.*
- *$n > 1$: Es ist $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, denn für jedes $a \in \mathbb{Z}$ existieren $q, r \in \mathbb{Z}$, $0 \leq r \leq n-1$ mit $a = qn + r$, also $\overline{a} = \overline{qn + r} = \overline{qn} + \overline{r} = \overline{r}$. Für $a, b \in \mathbb{Z}$ mit $0 \leq a, b \leq n-1$, $a \neq b$ ist $a \not\equiv b (\mathrm{mod}\ n)$, d. h. $\overline{a} \neq \overline{b}$.*

Beispiel 3.12. *Für die Ringe $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ erhalten wir die folgenden Verknüpfungstafeln:*

$\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/4\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Im Ring $\mathbb{Z}/3\mathbb{Z}$ besitzt jede von $\overline{0}$ verschiedene Restklasse ein Inverses bezüglich der Multiplikation, während das im Ring $\mathbb{Z}/4\mathbb{Z}$ nicht gilt. Darüber hinaus treten im Falle des Ringes $\mathbb{Z}/4\mathbb{Z}$ sogenannte Nullteiler auf: Es ist $\overline{2} \cdot \overline{2} = \overline{0}$, obwohl $\overline{2} \neq \overline{0}$ ist. Damit werden wir uns im nächsten Abschnitt gründlicher beschäftigen.

§4 Prime Restklassen und der Satz von Euler-Fermat

Wir wiederholen zu Beginn des Abschnittes zunächst einige Begriffe, die bereits aus der Linearen Algebra bekannt sein sollten.

Definition 4.1. *Es sei R ein Ring. Ein Element $x \in R$ heißt ein **Nullteiler**, wenn es ein $y \in R$, $y \neq 0$ mit $xy = 0$ gibt. Der Ring R heißt **nullteilerfrei**, wenn $R \neq 0$ ist und 0 der einzige Nullteiler in R ist.*

Beispiel 4.2. *(vgl. 3.12)*

- *Nullteiler in $\mathbb{Z}/3\mathbb{Z}$: $\overline{0}$, also ist $\mathbb{Z}/3\mathbb{Z}$ nullteilerfrei.*
- *Nullteiler in $\mathbb{Z}/4\mathbb{Z}$: $\overline{0}, \overline{2}$ (denn: $\overline{2} \cdot \overline{2} = \overline{0}$), also ist $\mathbb{Z}/4\mathbb{Z}$ nicht nullteilerfrei.*

Definition 4.3. *Es sei R ein Ring. Ein Element $x \in R$ heißt eine **Einheit**, wenn es ein $y \in R$ mit $xy = 1$ gibt.*

Beispiel 4.4. *(vgl. 3.12)*

- *Einheiten in $\mathbb{Z}/3\mathbb{Z}$: $\overline{1}, \overline{2}$*

- *Einheiten in* $\mathbb{Z}/4\mathbb{Z}$: $\overline{1}, \overline{3}$

Proposition 4.5. *Es sei R ein Ring. Dann gilt:*

(a) $R^\times := \{x \in R \mid x \text{ ist eine Einheit}\}$ *ist eine abelsche Gruppe bezüglich der Multiplikation, die sogenannte* ***Einheitengruppe*** *von R. Insbesondere gibt es für jedes* $x \in R^\times$ *genau ein* $y \in R^\times$ *mit* $xy = 1$. *Dieses Element bezeichnen wir mit* x^{-1} *und nennen es das (multiplikativ)* ***Inverse*** *zu x.*

(b) *Ist* $x \in R^\times$, *dann ist x kein Nullteiler.*

(c) *Falls R endlich ist, dann gilt auch die Umkehrung von (b): Ist* $x \in R$ *kein Nullteiler, dann ist x eine Einheit.*

Insbesondere gilt im Fall $R = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, *für* $\overline{x} \in R$, *dass* $\overline{x}$ *genau dann eine Einheit ist, wenn* $\overline{x}$ *kein Nullteiler ist. Die Einheiten im Ring* $\mathbb{Z}/n\mathbb{Z}$ *nennt man* ***prime Restklassen modulo*** *n, die Gruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *dementsprechend die* ***Gruppe der primen Restklassen*** *modulo n.*

Beweis. (a) Sind $a, b \in R^\times$, dann ist auch $ab \in R^\times$, denn in diesem Fall existieren $c, d \in R$ mit $ac = 1$, $bd = 1$, weswegen $(ab)(cd) = (ac)(bd) = 1$ folgt. Das Assoziativgesetz und die Kommutativität folgen aus den entsprechenden Eigenschaften der Multiplikation in R, das neutrale Element ist durch 1 gegeben, was wegen $1 \cdot 1 = 1$ in $R^\times$ liegt. Ist $a \in R^\times$, dann existiert nach Definition ein $b \in R$ mit $ab = 1$. Das impliziert $ba = 1$ und deshalb ist $b \in R^\times$. Wir haben damit gezeigt, dass $R^\times$ eine abelsche Gruppe bezüglich der Multiplikation ist. Daraus folgt insbesondere die Eindeutigkeit des Inversen.
(b) Wir betrachten zunächst den Fall $R \neq 0$. Sei $x \in R^\times$ und $y \in R$ mit $xy = 0$. Wir erhalten $y = x^{-1}xy = 0$, also ist x kein Nullteiler. Im Fall $R = 0$ ist das Element 0 eine Einheit, aber kein Nullteiler.
(c) Wir setzen nun R als endlich voraus. Sei $x \in R$ kein Nullteiler. Wir betrachten die Abbildung $\tau : R \to R$, $a \mapsto xa$. Die Abbildung τ ist injektiv, denn aus $\tau(a) = \tau(b)$ folgt $xa = xb$, also $x(a - b) = 0$. Weil x kein Nullteiler ist, folgt $a - b = 0$ und somit $a = b$. Als injektive Selbstabbildung der endlichen Menge R ist τ auch surjektiv, insbesondere existiert ein $y \in R$ mit $\tau(y) = 1$, was $xy = 1$ und deshalb $x \in R^\times$ impliziert. □

Definition 4.6. *Ein Ring R heißt ein* ***Körper****, wenn* $R^\times = R \setminus \{0\}$ *ist.*

An dieser Stelle sei angemerkt, dass der Nullring $R = 0$ nach Definition offenbar kein Körper ist.

Beispiel 4.7. *(vgl. 4.4)* $\mathbb{Z}/3\mathbb{Z}$ *ist ein Körper,* $\mathbb{Z}/4\mathbb{Z}$ *ist kein Körper.*

Satz 4.8. *Es sei* $n \in \mathbb{N}$. *Dann sind äquivalent:*

(i) *n ist eine Primzahl.*

(ii) $\mathbb{Z}/n\mathbb{Z}$ *ist ein Körper.*

(iii) $\mathbb{Z}/n\mathbb{Z}$ *ist nullteilerfrei.*

Für Primzahlen p schreiben wir auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Beweis. (i)$\Longrightarrow$(ii): Sei n eine Primzahl, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \neq \overline{0}$. Zu zeigen ist $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, d.h. es existiert ein $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ mit $\overline{a}\overline{b} = \overline{1}$. Wegen $\overline{a} \neq \overline{0}$ folgt $n \nmid a$. Da n eine Primzahl ist, erhalten wir $\mathrm{ggT}(n, a) = 1$. Aufgrund des erweiterten Euklidischen Algorithmus 1.7(c) gibt es $u, v \in \mathbb{Z}$ mit $un + va = 1$. Das impliziert $\overline{un} + \overline{va} = \overline{1}$, also $\overline{v} \cdot \overline{a} = \overline{1}$. Wir setzen $\overline{b} := \overline{v}$ und erhalten die Behauptung.
(ii)$\Longrightarrow$(iii): Sei $\mathbb{Z}/n\mathbb{Z}$ ein Körper. Damit ist $\mathbb{Z}/n\mathbb{Z} \neq 0$ und $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. Wegen 4.5(b) ist dann $\overline{0}$ der einzige Nullteiler in $\mathbb{Z}/n\mathbb{Z}$, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei.
(iii)$\Longrightarrow$(i): Diese Implikation zeigen wir indirekt. Sei n keine Primzahl. Falls $n = 1$, dann ist $\mathbb{Z}/n\mathbb{Z} = 0$, also nicht nullteilerfrei. Falls $n > 1$ ist, dann gibt es $a, b \in \mathbb{N}$ mit $1 < a, b < n$, so dass $n = ab$ gilt. Es ergibt sich $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ mit $\overline{a}, \overline{b} \neq \overline{0}$, also sind $\overline{a}, \overline{b}$ Nullteiler, insbesondere ist $\mathbb{Z}/n\mathbb{Z}$ nicht nullteilerfrei. □

Der Beweis der Implikation (i)$\Longrightarrow$(ii) hat gezeigt, dass man für eine Primzahl p Inverse in $(\mathbb{Z}/p\mathbb{Z})^\times$ durch den erweiterten Euklidischen Algorithmus bestimmen kann. Es sei ferner angemerkt, dass es für Primzahlen p auch für $r > 1$ Körper mit p^r Elementen gibt. Diese sind aber von $\mathbb{Z}/p^r\mathbb{Z}$ verschieden, denn das sind nach 4.8 keine Körper.

Wir greifen die Idee aus dem obigen Beweis der Implikation (i)$\Longrightarrow$(ii) nochmal auf und verwenden diese, um die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ zu charakterisieren.

Proposition 4.9. *Es sei $n \in \mathbb{N}$, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Dann sind äquivalent:*

(i) $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

(ii) $\mathrm{ggT}(a, n) = 1$

Beweis. (i)$\Longrightarrow$(ii): Sei $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dann existiert ein $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{a}\overline{b} = \overline{1}$. Aufgrunddessen gibt es ein $k \in \mathbb{Z}$ mit $ab = 1 + kn$. Sei $d \in \mathbb{Z}$ mit $d|a$, $d|n$. Es folgt $d|(ab - kn) = 1$ und deshalb $\mathrm{ggT}(a, n) = 1$.
(ii)$\Longrightarrow$(i): Sei $\mathrm{ggT}(a, n) = 1$. Dann gibt es nach 1.7(c) Zahlen $u, v \in \mathbb{Z}$ mit $au + vn = 1$. Wir erhalten $\overline{a} \cdot \overline{u} = \overline{1}$, d.h. $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Der Beweis hat gezeigt, dass Inverse in $(\mathbb{Z}/n\mathbb{Z})^\times$ durch den erweiterten Euklidischen Algorithmus bestimmt werden können.

Korollar 4.10. *Es sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Dann sind äquivalent:*

(i) *Die Kongruenz $ax \equiv 1 \pmod{n}$ besitzt eine Lösung in $\mathbb{Z}$.*

(ii) $\mathrm{ggT}(a, n) = 1$.

Beweis. Die Kongruenz $ax \equiv 1 \pmod{n}$ entspricht der Gleichung $\overline{a} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$, welche genau dann lösbar ist, wenn $\overline{x}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist. □

Beispiel 4.11. *Gesucht ist eine Lösung der Kongruenz*

$$3x \equiv 1 \pmod{37}$$

Es ist $\mathrm{ggT}(3,37) = 1 = (-12)\cdot 3 + 37$, *also* $\overline{1} = \overline{-12}\cdot\overline{3} = \overline{25}\cdot\overline{3}$, *d.h.* $x = 25$ *ist eine Lösung der Kongruenz. Die Menge* L *aller Lösungen ist gegeben durch* $L = 25 + 37\mathbb{Z}$.

Proposition 4.12. *Es seien* $a, b \in \mathbb{Z},\ n \in \mathbb{N}$. *Dann sind äquivalent:*

(i) *Die Kongruenz* $ax \equiv b \pmod{n}$ *besitzt eine Lösung in* $\mathbb{Z}$.

(ii) $\mathrm{ggT}(a,n)|b$.

Beweis. (i)$\Longrightarrow$(ii): Sei $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{n}$. Dann existiert ein $k \in \mathbb{Z}$ mit $ax = b + kn$, also mit $b = ax - kn$. Wegen $\mathrm{ggT}(a,n)|a$ und $\mathrm{ggT}(a,n)|n$ folgt $\mathrm{ggT}(a,n)|b$.
(ii)$\Longrightarrow$(i): Es gelte $\mathrm{ggT}(a,n)|b$. Aus dem erweiterten Euklidischen Algorithmus 1.7(c) folgt die Existenz von $u, v \in \mathbb{Z}$ mit

$$ua + vn = \mathrm{ggT}(a,n).$$

Durch Multiplikation mit der nach Voraussetzung ganzen Zahl $\frac{b}{\mathrm{ggT}(a,n)}$ erhalten wir

$$ua\frac{b}{\mathrm{ggT}(a,n)} + vn\frac{b}{\mathrm{ggT}(a,n)} = b,$$

was die Kongruenz

$$a \cdot \frac{bu}{\mathrm{ggT}(a,n)} \equiv b \pmod{n}$$

und damit die Behauptung nach sich zieht. □

Beispiel 4.13. (a) *Die Kongruenz* $15x \equiv 7 \pmod{21}$ *hat wegen* $\mathrm{ggT}(15,21) = 3 \nmid 7$ *keine Lösung.*

(b) *Gesucht ist eine Lösung der Kongruenz* $15x \equiv 6 \pmod{21}$. *Es ist* $\mathrm{ggT}(15,21) = 3|6$, *d.h. die Kongruenz ist lösbar. Der erweiterte Euklidische Algorithmus liefert*

$$\mathrm{ggT}(15,21) = 3 = 3\cdot 15 + (-2)\cdot 21.$$

Wie im obigen Beweis ergibt sich daraus

$$6 = 6\cdot 15 + (-4)\cdot 21 \equiv 15\cdot 6 \pmod{21},$$

d.h. $x = 6$ *ist eine Lösung der Kongruenz.*

Definition 4.14. *Es sei* G *eine endliche Gruppe. Die* ***Ordnung*** *von* G *(Notation:* $|G|$*) ist definiert als die Anzahl der Elemente von* G.

Für die Anzahl der Elemente einer beliebigen Menge M werden wir im Unterschied dazu die Notation $\#M \in \mathbb{N}_0 \cup \{\infty\}$ verwenden.

Definition 4.15. *Die Abbildung*

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{N}\,, \\ n &\mapsto \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \underset{4.9}{=} \#\{a \in \mathbb{N}_0 \mid 0 \le a < n \text{ und } \operatorname{ggT}(a,n) = 1\} \end{aligned}$$

heißt die ***Eulersche φ-Funktion****.*

Beispiel 4.16. (a) *Es ist $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}$, also ist $\varphi(6) = 2$.*

(b) *Sei p eine Primzahl. Dann ist $\mathbb{Z}/p\mathbb{Z}$ nach 4.8 ein Körper, d.h.*

$$\varphi(p) = |(\mathbb{Z}/p\mathbb{Z})^\times| = \#(\mathbb{Z}/p\mathbb{Z}) - 1 = p - 1.$$

Proposition 4.17. *Es sei p eine Primzahl und $n \in \mathbb{N}$. Dann gilt:*

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

Beweis. Es gibt genau p^{n-1} Zahlen a mit $0 \le a < p^n$, die *nicht* teilerfremd zu p^n sind, nämlich: $0 \cdot p, 1 \cdot p, 2 \cdot p, \ldots, (p^{n-1}-1) \cdot p$. Wir erhalten $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

Im Folgenden werden wir öfters abstrakte Gruppen betrachten. Hierbei werden wir die Verknüpfung stets multiplikativ schreiben und das neutrale Element mit 1 bezeichnen (sofern nicht anders angegeben).

Proposition 4.18. *Es sei G eine endliche abelsche Gruppe und $g \in G$. Dann gilt:*

$$g^{|G|} = 1\,.$$

Beweis. Wir betrachten die Abbildung $\tau_g : G \to G$, $x \mapsto gx$. Diese ist injektiv, denn aus $\tau_g(x) = \tau_g(y)$ für $x, y \in G$ folgt $gx = gy$ und somit $g^{-1}gx = g^{-1}gy$, d.h. $x = y$. Die Abbildung τ_g ist auch surjektiv, denn für $y \in G$ gilt $\tau_g(g^{-1}y) = gg^{-1}y = y$. Also ist τ_g bijektiv, und weil die Gruppe G endlich und abelsch ist, ergibt sich

$$\prod_{x \in G} x = \prod_{x \in G} \tau_g(x) = \prod_{x \in G} gx = g^{|G|} \prod_{x \in G} x,$$

woraus $g^{|G|} = 1$ folgt. □

Die obige Aussage gilt im übrigen für jede endliche Gruppe (üblicherweise lernt man das in der Algebra-Vorlesung).

Satz 4.19 (Satz von Euler-Fermat)**.** *Es sei $n \in \mathbb{N}$ und $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dann gilt:*

$$\overline{a}^{\varphi(n)} = \overline{1}\,.$$

Beweis. Nach Definition ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Die Behauptung folgt direkt aus 4.18, angewendet auf $G = (\mathbb{Z}/n\mathbb{Z})^\times$. □

Beispiel 4.20. *Es ist* $3^{19} \equiv 10 \pmod{17}$*, denn:*

$$3^{16} = 3^{\varphi(17)} \equiv 1 \pmod{17},$$

also folgt

$$3^{19} = 3^3 \cdot 3^{16} \equiv 27 \cdot 1 \equiv 10 \pmod{17}.$$

Korollar 4.21 (Kleiner Satz von Fermat)**.** *Es sei p eine Primzahl. Dann gilt:*

(a) *Für jedes $\overline{a} \in \mathbb{F}_p^\times$ ist $\overline{a}^{p-1} = \overline{1}$.*

(b) *Für jedes $\overline{a} \in \mathbb{F}_p$ ist $\overline{a}^p = \overline{a}$.*

Beweis. (a) Es ist $\varphi(p) = p - 1$ nach 4.16, die Behauptung ergibt sich direkt aus dem Satz von Euler-Fermat 4.19.
(b) Ist $\overline{a} \in \mathbb{F}_p^\times$, dann ist $\overline{a}^{p-1} = \overline{1}$ und deshalb $\overline{a}^p = \overline{a} \cdot \overline{a}^{p-1} = \overline{a} \cdot \overline{1} = \overline{a}$. Für $\overline{a} = \overline{0}$ ist ebenfalls $\overline{a}^p = \overline{0}^p = \overline{0} = \overline{a}$. □

§5 Die Struktur der primen Restklassengruppen

Beispiel 5.1. *Es ist $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Es gilt: $\overline{1} = \overline{2}^0$, $\overline{2} = \overline{2}^1$, $\overline{3} = \overline{2}^3$, $\overline{4} = \overline{2}^2$, d.h. jedes Element von $(\mathbb{Z}/5\mathbb{Z})^\times$ lässt sich als $\overline{2}^n$ mit einem $n \in \mathbb{Z}$ schreiben. Man sagt dann auch, dass die Gruppe $(\mathbb{Z}/5\mathbb{Z})^\times$ zyklisch ist und vom Element $\overline{2}$ erzeugt wird.*

In diesem Abschnitt werden wir beweisen, dass die Gruppen $(\mathbb{Z}/p^n\mathbb{Z})^\times$ für jede ungerade Primzahl p zyklisch sind. Dafür müssen wir zunächst etwas mehr über zyklische Gruppen lernen.

Zyklische Gruppen

Definition 5.2. *Eine Gruppe G heißt **zyklisch**, wenn ein $g \in G$ existiert, so dass*

$$G = \{g^n \mid n \in \mathbb{Z}\} =: \langle g \rangle$$

*ist. In diesem Fall schreiben wir $G = \langle g \rangle$ und g heißt ein **Erzeuger** von G.*

Jede zyklische Gruppe ist offenbar abelsch, denn für $a, b \in \mathbb{Z}$ ist $g^a g^b = g^{a+b} = g^{b+a} = g^b g^a$.

Beispiel 5.3. (a) *Es ist $(\mathbb{Z}/5\mathbb{Z})^\times = \langle \overline{2} \rangle$ (vgl. Bsp. 5.1), insbesondere ist $(\mathbb{Z}/5\mathbb{Z})^\times$ zyklisch.*

(b) *Es ist $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Wir bestimmen $\langle g \rangle$ für alle $g \in (\mathbb{Z}/8\mathbb{Z})^\times$. Offensichtlich ist $\langle \overline{1} \rangle = \{\overline{1}\}$. Wegen $\overline{3}^2 = \overline{1}$ ist $\langle \overline{3} \rangle = \{\overline{1}, \overline{3}\}$ (denn: $\overline{3}^3 = \overline{3} \cdot \overline{3}^2 = \overline{3}, \ldots, \overline{3}^{-1} = \overline{3}$, da $\overline{3} \cdot \overline{3} = \overline{1}$, etc.). Analog ergibt sich $\langle \overline{5} \rangle = \{\overline{1}, \overline{5}\}$, $\langle \overline{7} \rangle = \{\overline{1}, \overline{7}\}$, da $\overline{5}^2 = \overline{7}^2 = \overline{1}$. Somit ist $(\mathbb{Z}/8\mathbb{Z})^\times$ nicht zyklisch.*

(c) *Wir betrachten die additive Gruppe* $\mathbb{Z}$. *Es ist* $\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$. *Man beachte, dass die Verknüpfung durch „+"gegeben ist, so dass* g^n *im Sinne der obigen Definition hier als* $\underbrace{g + \cdots + g}_{n-\text{mal}}$, *falls* $n \in \mathbb{N}_0$ *ist, bzw. als* $\underbrace{(-g) + \cdots + (-g)}_{(-n)-\text{mal}}$, *falls* $-n \in \mathbb{N}_0$ *ist, zu verstehen ist. Also ist* $\mathbb{Z}$ *zyklisch.*

(d) *Wir betrachten die additive Gruppe* $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. *Für jedes Element* $a \in \{0, \ldots, m-1\}$ *ist* $\overline{a} = \underbrace{\overline{1} + \cdots + \overline{1}}_{a-\text{mal}} \in \langle \overline{1} \rangle$, *woraus folgt, dass* $\mathbb{Z}/m\mathbb{Z}$ *zyklisch ist.*

Definition 5.4. *Es sei* G *eine endliche abelsche Gruppe und* $g \in G$. *Die* ***Ordnung*** *von* g *ist definiert als*

$$\operatorname{ord}(g) := \min\{n \in \mathbb{N} \mid g^n = 1\}.$$

Aufgrund von 4.18 ist $g^{|G|} = 1$, deswegen ist $\operatorname{ord}(g)$ wohldefiniert, und es gilt stets $\operatorname{ord}(g) \leq |G|$.

Beispiel 5.5. *Es sei* $G = (\mathbb{Z}/5\mathbb{Z})^\times$. *Für die Ordnungen der Elemente* $\overline{2}$ *bzw.* $\overline{4}$ *erhalten wir*

- $\operatorname{ord}(\overline{2}) = 4$, *denn:* $\overline{2}^1 = \overline{2}, \overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{3}, \overline{2}^4 = \overline{1}$,
- $\operatorname{ord}(\overline{4}) = 2$, *denn:* $\overline{4}^1 = \overline{4}, \overline{4}^2 = \overline{1}$.

Proposition 5.6. *Es sei* G *eine endliche abelsche Gruppe. Dann sind äquivalent:*

(i) G *ist zyklisch.*

(ii) *Es gibt ein* $g \in G$ *mit* $\operatorname{ord}(g) = |G|$.

In diesem Fall ist jedes Element $g \in G$ *mit* $\operatorname{ord}(g) = |G|$ *ein Erzeuger von* G, *und für jeden Erzeuger* g *von* G *gilt* $\operatorname{ord}(g) = |G|$.

Beweis. (i)$\Longrightarrow$(ii): Sei G zyklisch. Dann existiert ein $g \in G$ mit $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Wir behaupten, dass $\operatorname{ord}(g) = |G|$ gilt. Wir setzen $n := \operatorname{ord}(g)$. Ist $k \in \mathbb{Z}$, dann gibt es $q, r \in \mathbb{Z}$, $0 \leq r < n$ mit $k = qn + r$, insbesondere ist $g^k = g^{qn+r} = (g^n)^q g^r = g^r$. Für $r_1, r_2 \in \mathbb{Z}$ mit $0 \leq r_1 < r_2 < n$ ist $g^{r_1} \neq g^{r_2}$, sonst wäre $g^{r_2 - r_1} = 1$ im Widerspruch zur Minimalität von $\operatorname{ord}(g)$. Es ergibt sich $G = \langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\}$ und deshalb $|G| = n = \operatorname{ord}(g)$.
(ii)$\Longrightarrow$(i): Sei $g \in G$ mit $\operatorname{ord}(g) = |G| =: n$. Wie im Beweis der Implikation (i)$\Longrightarrow$(ii) erhalten wir $\langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\}$, also $|\langle g \rangle| = n = |G|$ und somit $\langle g \rangle = G$, d.h. G ist zyklisch. □

Der Beweis hat insbesondere gezeigt: $\langle g \rangle = \{1, g, \ldots g^{\operatorname{ord}(g)-1}\}$.

Proposition 5.7. *Es sei* G *eine endliche abelsche Gruppe und* $m \in \mathbb{Z}$. *Dann sind äquivalent:*

(i) $\operatorname{ord}(g) | m$.

(ii) $g^m = 1$.

Beweis. (i)$\Longrightarrow$(ii): Es gelte $\operatorname{ord}(g)|m$. Dann ist $m = q\operatorname{ord}(g)$ für ein $q \in \mathbb{Z}$, und wir erhalten $g^m = (g^{\operatorname{ord}(g)})^q = 1$.
(ii)$\Longrightarrow$(i): Es sei $g^m = 1$. Wir schreiben $m = q\operatorname{ord}(g) + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < \operatorname{ord}(g)$. Es ergibt sich $1 = g^m = (g^{\operatorname{ord}(g)})^q g^r = g^r$. Aus der Minimalität von $\operatorname{ord}(g)$ erhalten wir $r = 0$, was $\operatorname{ord}(g)|m$ impliziert. □

Korollar 5.8. *Es sei G eine endliche abelsche Gruppe und $g \in G$. Dann gilt:* $\operatorname{ord}(g)|\,|G|$.

Beweis. Das ergibt sich direkt aus 5.7 unter Beachtung von $g^{|G|} = 1$ (vgl. 4.18). □

Definition 5.9. *Es sei G eine endliche abelsche Gruppe. Der **Exponent** von G ist definiert als*

$$\exp(G) := \min\{n \in \mathbb{N} \mid g^n = 1 \text{ für alle } g \in G\}.$$

Beispiel 5.10. (a) *Es ist* $\exp((\mathbb{Z}/5\mathbb{Z})^\times) = 4$, *denn es ist* $\overline{a}^4 = \overline{1}$ *für alle* $\overline{a} \in (\mathbb{Z}/5\mathbb{Z})^\times$, *und* $\operatorname{ord}(\overline{2}) = 4$.

(b) *Es ist* $\exp((\mathbb{Z}/8\mathbb{Z})^\times) = 2$, *denn* $\operatorname{ord}(\overline{3}) = \operatorname{ord}(\overline{5}) = \operatorname{ord}(\overline{7}) = 2$.

Proposition 5.11. *Es sei G eine endliche abelsche Gruppe. Dann gilt:*

(a) $\exp(G)|\,|G|$

(b) $\exp(G) = \operatorname{kgV}\{\operatorname{ord}(g) \mid g \in G\}$.

Beweis. (a) Wir schreiben $|G| = q\exp(G) + r$ mit $0 \leq r < \exp(G)$, $q \in \mathbb{Z}$. Dann erhalten wir für alle $g \in G$:

$$1 = g^{|G|} = (g^{\exp(G)})^q g^r = g^r.$$

Aufgrund der Minimalität von $\exp(G)$ ist $r = 0$, was $\exp(G)|\,|G|$ impliziert.
(b) Wir rechnen nach, dass $\exp(G)$ die definierenden Eigenschaften von $\operatorname{kgV}\{\operatorname{ord}(g) \mid g \in G\}$ erfüllt (vgl. Übungen). Zunächst einmal ist $\exp(G)$ ein gemeinsames Vielfaches aller Ordnungen von Elementen von G, denn für $g \in G$ gilt $g^{\exp(G)} = 1$, was nach 5.7 $\operatorname{ord}(g)|\exp(G)$ impliziert. Sei nun $m \in \mathbb{Z}$ mit $\operatorname{ord}(g)|m$ für alle $g \in G$. Wir behaupten, dass dann $\exp(G)|m$ gilt. Dazu schreiben wir $m = q\exp(G) + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < \exp(G)$. Wegen $\operatorname{ord}(g)|m$ gilt für alle $g \in G$:

$$1 = g^m = (g^{\exp(G)})^q g^r = g^r,$$

was wegen der Minimalität von $\exp(G)$ zur Folge hat, dass $r = 0$ ist, was unsere Behauptung impliziert. □

Für das Weitere benötigen wir noch einige Begriffe aus der Gruppentheorie, die bereits aus der Linearen Algebra bekannt sein sollten. Wir stellen diese der Vollständigkeit halber im Folgenden zusammen.

Definition 5.12. *Es seien G, H Gruppen und $\psi : G \to H$ eine Abbildung. Die Abbildung ψ heißt ein **(Gruppen-)Homomorphismus**, wenn für alle Elemente $a, b \in G$ gilt, dass $\psi(ab) = \psi(a)\psi(b)$ ist. ψ heißt ein **(Gruppen-)Isomorphismus**, wenn ψ ein bijektiver Homomorphismus ist.*

Beispiel 5.13. *Sei K ein Körper. Dann ist* $\det : \mathrm{GL}_n(K) \to K^\times$ *ein Homomorphismus, denn* $\det(AB) = \det(A)\det(B)$ *für alle* $A, B \in \mathrm{GL}_n(K)$.

Proposition 5.14. *Es seinen G, H Gruppen und $\psi : G \to H$ ein Homomorphismus. Dann gilt:*

(a) *ψ ist genau dann injektiv, wenn* $\mathrm{Kern}(\psi) := \{g \in G \mid \psi(g) = 1\} = \{1\}$ *ist.*

(b) *Ist ψ ein Isomorphismus, dann ist $\psi^{-1} : H \to G$ ebenfalls ein Isomorphismus.*

Existiert ein Isomorphismus zwischen G und H, nennen wir G und H ***isomorph*** *(Notation: $G \cong H$).*

Beweis. (a) Wir bemerken zunächst, dass $\psi(1) = \psi(1 \cdot 1) = \psi(1)\psi(1)$ ist, woraus $\psi(1) = 1$ folgt. Sei nun ψ injektiv und $g \in \mathrm{Kern}(\psi)$. Es ergibt sich $\psi(g) = 1 = \psi(1)$, was wegen der Injektivität von ψ impliziert, dass $g = 1$ ist, d.h. $\mathrm{Kern}(\psi) = \{1\}$. Zum Beweis der Umkehrung sei $\mathrm{Kern}(\psi) = \{1\}$, und es seien $g_1, g_2 \in G$ mit $\psi(g_1) = \psi(g_2)$. Wegen $1 = \psi(1) = \psi(g_2 g_2^{-1}) = \psi(g_2)\psi(g_2^{-1})$ folgt $\psi(g_2^{-1}) = \psi(g_2)^{-1}$. Wir erhalten $\psi(g_1 g_2^{-1}) = \psi(g_1)\psi(g_2^{-1}) = \psi(g_1)\psi(g_2)^{-1} = 1$ und deswegen $g_1 g_2^{-1} \in \mathrm{Kern}(\psi) = \{1\}$. Das ergibt $g_1 = g_2$ und damit die Injektivität von ψ.
(b) Aufgrund der Bijektivität von ψ existiert ψ^{-1} und ist bijektiv. Wir müssen zeigen, dass ψ^{-1} ein Homomorphismus ist. Dazu seien $h_1, h_2 \in H$. Wir setzen $g_1 := \psi^{-1}(h_1)$, $g_2 := \psi^{-1}(h_2)$. Es ergibt sich $\psi(g_1 g_2) = \psi(g_1)\psi(g_2) = h_1 h_2$, also $\psi^{-1}(h_1 h_2) = g_1 g_2 = \psi^{-1}(h_1)\psi^{-1}(h_2)$. □

Der nächste Satz liefert eine Klassifikation zyklischer Gruppen bis auf Isomorphie.

Satz 5.15. *Es sei G eine zyklische Gruppe. Dann gilt:*

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } G \text{ unendlich,} \\ \mathbb{Z}/|G|\mathbb{Z} & \text{falls } G \text{ endlich.} \end{cases}$$

Beweis. Wir setzen $n := |G|$, falls G endlich ist, und $n := 0$, falls G unendlich ist. Sei $g \in G$ ein Erzeuger von G. Wir definieren

$$\psi : \mathbb{Z}/n\mathbb{Z} \to G, \overline{a} \mapsto g^a$$

Wir werden zeigen, dass ψ ein Isomorphismus ist, woraus sich dann die Behauptung ergibt. Zunächst zeigen wir, dass ψ wohldefiniert ist. Seien $a_1, a_2 \in \overline{a}$. Es folgt $a_1 - a_2 \in n\mathbb{Z}$, also existiert ein $k \in \mathbb{Z}$ mit $a_1 - a_2 = nk$, und wir erhalten

$$g^{a_1 - a_2} = g^{nk} = \begin{cases} (g^{|G|})^k & \text{falls } G \text{ endlich} \\ g^0 & \text{sonst} \end{cases} = 1,$$

also $g^{a_1} = g^{a_2}$. ψ ist ein Homomorphismus, denn für $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ ist

$$\psi(\overline{a} + \overline{b}) = \psi(\overline{a + b}) = g^{a+b} = g^a g^b = \psi(\overline{a})\psi(\overline{b}).$$

Als nächstes zeigen wir, dass ψ injektiv, d.h. $\mathrm{Kern}(\psi) = \{\overline{0}\}$ ist. Sei $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ mit $\psi(\overline{a}) = g^a = 1$. Falls G endlich ist, dann folgt $n = |G| \overset{5.6}{=} \mathrm{ord}(g) | a$ nach 5.7. Damit ist $\overline{a} = \overline{0}$. Ist G

unendlich, so nehmen wir an, dass $a \neq 0$ ist. Wir können dann o.E. $a > 0$ annehmen, denn $g^a = 1$ ist äquivalent zu $g^{-a} = 1$. Aus $g^a = 1$ folgt dann wie im Beweis zu 5.6, dass $\langle g \rangle = \{1, g, \ldots, g^{a-1}\}$ ist. Wegen $G = \langle g \rangle$ ist das ein Widerspruch zur Unendlichkeit von G. Also ist $a = 0$, und damit ist ψ injektiv. Die Abbildung ψ ist surjektiv, denn falls G endlich ist, ist $G = \{1, g, \ldots, g^{n-1}\} = \psi(\mathbb{Z}/n\mathbb{Z})$, und falls G unendlich ist, so ist $G = \{g^k \mid k \in \mathbb{Z}\} = \psi(\mathbb{Z})$. Somit ist ψ ein Isomorphismus. □

Beispiel 5.16. *In Beispiel 5.1 haben wir gesehen, dass $(\mathbb{Z}/5\mathbb{Z})^\times$ zyklisch ist. Wegen 5.15 ist $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$. Explizit ist ein Isomorphismus durch*

$$\psi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times,\ a \mapsto \overline{2}^a$$

gegeben, also $\psi(\overline{0}) = \overline{2}^0 = \overline{1}$, $\psi(\overline{1}) = \overline{2}^1 = \overline{2}$, $\psi(\overline{2}) = \overline{2}^2 = \overline{4}$, $\psi(\overline{3}) = \overline{2}^3 = \overline{3}$.

Satz 5.17. *Es sei G eine endliche abelsche Gruppe. Dann sind äquivalent:*

(i) *G ist zyklisch.*

(ii) $\exp(G) = |G|$.

Beweis. (i)$\Longrightarrow$(ii): Sei G zyklisch. Aufgrund von 5.11 gilt $\exp(G) \mid |G|$. Sei $g \in G$ ein Erzeuger von G. Dann folgt

$$|G| \overset{5.6}{=} \operatorname{ord}(g) \mid \operatorname{kgV}\{\operatorname{ord}(\tilde{g}) \mid \tilde{g} \in G\} = \exp(G)$$

und deshalb $\exp(G) = |G|$.
(ii)$\Longrightarrow$(i): Wir setzen $n := \exp(G) = |G|$ und schreiben $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, sowie $e_1, \ldots, e_r \in \mathbb{N}$. Im ersten Beweisschritt zeigen wir, dass es für jedes $i \in \{1, \ldots, r\}$ ein Element $g_i \in G$ mit $\operatorname{ord}(g_i) = p_i^{e_i}$ gibt. Sei dazu $i \in \{1, \ldots, r\}$ fixiert. Falls $p_i^{e_i} \nmid \operatorname{ord}(g)$ für alle $g \in G$ gilt, dann folgt

$$p_i^{e_i} \nmid \operatorname{kgV}\{\operatorname{ord}(g) \mid g \in G\} = \exp(G) = n,$$

was ein Widerspruch ist. Also gibt es ein $\tilde{g}_i \in G$ mit $p_i^{e_i} \mid \operatorname{ord}(\tilde{g}_i)$. Wir setzen

$$g_i := \tilde{g}_i^{\frac{\operatorname{ord}(\tilde{g}_i)}{p_i^{e_i}}}.$$

Es ergibt sich $g_i^{p_i^{e_i}} = \tilde{g}_i^{\operatorname{ord}(\tilde{g}_i)} = 1$ und deshalb $\operatorname{ord}(g_i) \mid p_i^{e_i}$ wegen 5.7. Wäre $\operatorname{ord}(g_i) < p_i^{e_i}$, etwa $\operatorname{ord}(g_i) = p_i^f$ mit $f < e_i$, dann wäre

$$1 = g_i^{p_i^f} = \tilde{g}_i^{\frac{\operatorname{ord}(\tilde{g}_i)}{p_i^{e_i - f}}},$$

was aufgrund von $\frac{\operatorname{ord}(\tilde{g}_i)}{p_i^{e_i-f}} < \operatorname{ord}(\tilde{g}_i)$ ein Widerspruch ist. Deshalb ist $\operatorname{ord}(g_i) = p_i^{e_i}$. Im zweiten Beweisschritt zeigen wir, dass $g := g_1 \cdot \ldots \cdot g_r$ ein Erzeuger von G ist, d.h. dass $\operatorname{ord}(g) = |G| =$

n ist. Wir nehmen an, dass $\operatorname{ord}(g) =: d < n$ ist. Aufgrund von 5.7 ergibt sich $d|n$. Wegen $d < n$ gibt es ein $j \in \{1, \ldots, r\}$ mit $d|\frac{n}{p_j}$, insbesondere folgt $g^{\frac{n}{p_j}} = 1$. Es ist dann

$$1 = g^{\frac{n}{p_j}} = g_1^{\frac{n}{p_j}} \cdot \ldots \cdot g_r^{\frac{n}{p_j}}.$$

Für $i \neq j$ gilt $p_i^{e_i}|\frac{n}{p_j}$ und somit $g_i^{\frac{n}{p_j}} = 1$. Wir erhalten $g_j^{\frac{n}{p_j}} = 1$, also

$$\operatorname{ord}(g_j) = p_j^{e_j}|\frac{n}{p_j} = p_1^{e_1} \cdot \ldots \cdot p_j^{e_j - 1} \cdot \ldots \cdot p_r^{e_r},$$

was ein Widerspruch ist. Aufgrunddessen ist $\operatorname{ord}(g) = n = |G|$, also ist G zyklisch. □

Die Zyklizität von $\mathbb{F}_p^\times$

Wir wollen als nächstes zeigen, dass für eine Primzahl p die Gruppe $\mathbb{F}_p^\times$ zyklisch ist. Dazu werden wir das Kriterium aus 5.17 verwenden. Dafür brauchen wir aber noch einige Vorbereitungen.

Definition 5.18. *Es sei R ein Ring, $f = a_n X^n + \ldots + a_1 X + a_0 \in R[X]$ mit $a_n \neq 0$. Der **Grad** von f ist definiert als $\deg(f) := n$, der **Leitkoeffizient** von f als $\ell(f) := a_n$. Wir setzen $\deg(0) := -\infty$, $\ell(0) := 0$.*

Proposition 5.19. *Es sei R ein Ring und $f, g \in R[X]$, wobei $\ell(f)$ oder $\ell(g)$ kein Nullteiler sei. Dann gilt: $\deg(fg) = \deg(f) + \deg(g)$.*

Beweis. Falls $f = 0$ oder $g = 0$ ist, dann ist $\deg(fg) = \deg(0) = -\infty = \deg(f) + \deg(g)$. Im Folgenden sei $f \neq 0$ und $g \neq 0$, etwa $f = a_n X^n + \ldots + a_0$, $g = b_m X^m + \ldots + b_0$ mit $a_n, b_m \neq 0$. Wir erhalten $fg = a_n b_m X^{n+m}$+Terme kleineren Grades. Da $\ell(f) = a_n$ oder $\ell(g) = b_m$ kein Nullteiler ist, folgt $a_n b_m \neq 0$ und somit $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Proposition 5.20 (Polynomdivision mit Rest)**.** *Es sei $R \neq 0$ ein Ring, $f, g \in R[X]$ mit $\ell(g) \in R^\times$. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.*

Beweis. Wir zeigen zuerst die Existenzaussage per Induktion nach $\deg(f)$. Falls $\deg(f) < \deg(g)$ ist, setzen wir $q := 0$, $r := f$. Sei nun $\deg(f) \geq \deg(g)$,

$$f = aX^{n+k} + \text{Terme kleineren Grades}, \quad g = bX^n + \text{Terme kleineren Grades},$$

wobei $a \in R, a \neq 0, b \in R^\times, n, j \in \mathbb{N}_0$. Es ist

$$\deg(f - \frac{a}{b} X^k g) < \deg(f),$$

nach Induktionsvoraussetzung existieren also $q_1, r_1 \in R[X]$ mit

$$f - \frac{a}{b} X^k g = q_1 g + r_1$$

und $\deg(r_1) < \deg(g)$. Daraus erhalten wir

$$f = \left(q_1 + \frac{a}{b}X^k\right) g + r_1.$$

Wir setzen $q := q_1 + \frac{a}{b}X^k$, $r := r_1$, und der Existenzbeweis ist beendet. Zum Nachweis der Eindeutigkeit sei $f = q_1 g + r_1 = q_2 g + r_2$ mit $\deg(r_1), \deg(r_2) < \deg(g)$. Es ergibt sich

$$(q_1 - q_2)g = r_2 - r_1.$$

Wäre $q_1 \neq q_2$, dann folgt aus 5.19:

$$\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g),$$

da $\ell(g) \in R^\times$ und damit wegen 4.5 kein Nullteiler ist. Andererseits ist

$$\deg((q_1 - q_2)g) = \deg(r_2 - r_1) < \deg(g),$$

was zum Widerspruch führt. Deshalb ist $q_1 = q_2$ und somit auch $r_1 = r_2$. □

Proposition 5.21. *Es sei R ein Ring, $f \in R[X]$ und $a \in R$ eine Nullstelle von f, d.h. $f(a) = 0$. Dann gibt es ein $q \in R[X]$ mit $f = (X - a)q$.*

Beweis. Nach 5.20 existieren $q, r \in R[X]$ mit $f = q(X - a) + r$ und $\deg(r) < \deg(X - a) = 1$. Also ist r ein konstantes Polynom, und es gilt

$$0 = f(a) = q(a)(a - a) + r(a) = r(a),$$

weswegen $r = 0$ ist. □

Korollar 5.22. *Es sei R ein nullteilerfreier Ring und $f \in R[X]$, $f \neq 0$ mit $\deg(f) = n$. Dann besitzt f in R höchstens n Nullstellen.*

Beweis. Wir zeigen die Aussage per Induktion nach n. Für $n = 0$ ist die Behauptung wahr, denn ein konstantes, von Null verschiedenes Polynom besitzt keine Nullstelle. Sei nun $n > 0$. Falls f keine Nullstelle besitzt, sind wir fertig. Wir nehmen im folgenden an, dass f eine Nullstelle $a \in R$ besitzt. Nach 5.21 existiert ein $q \in R[X]$ mit $f = (X - a)q$. Aufgrund von

$$n = \deg(f) = \deg((X - a)q) = 1 + \deg(q)$$

ist $\deg(q) = n - 1$. Ist $b \in R$ eine weitere Nullstelle von f, so gilt $0 = f(b) = (b - a)q(b)$. Da R nullteilerfrei ist, folgt: $b = a$ oder b ist eine Nullstelle von q. Nach Induktionsvoraussetzung hat q aber höchstens $n - 1$ Nullstellen, weswegen f höchstens n Nullstellen haben kann. □

Beispiel 5.23. *Lässt man in 5.22 die Voraussetzung, dass R ein nullteilerfreier Ring ist, weg, so kann man leicht Gegenbeispiele finden: Im Ring $R = \mathbb{Z}/8\mathbb{Z}$ hat das Polynom $f = X^2 - \overline{1}$ die Nullstellen $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.*

Proposition 5.24. *Es sei p eine Primzahl. Dann gilt in $\mathbb{F}_p[X]$ die Identität*

$$\prod_{\overline{a}\in\mathbb{F}_p^\times}(X-\overline{a}) = X^{p-1}-\overline{1}$$

Beweis. Wir setzen

$$f := \prod_{\overline{a}\in\mathbb{F}_p^\times}(X-\overline{a}).$$

Division mit Rest im Polynomring $\mathbb{F}_p[X]$ liefert

$$X^{p-1}-\overline{1} = qf + r$$

mit $q, r \in \mathbb{F}_p[X]$, $\deg(r) < \deg(f) = p-1$. Ist $\overline{a} \in \mathbb{F}_p^\times$, dann ergibt sich aus dem Kleinen Satz von Fermat 4.21 die Gleichung $\overline{a}^{p-1} = \overline{1}$, d.h. $\overline{a}$ ist eine Nullstelle von $X^{p-1}-\overline{1}$. Weil auch $f(\overline{a}) = \overline{0}$ ist, erhalten wir $r(\overline{a}) = \overline{0}$. Das Polynom r hat somit $p-1$ Nullstellen. Aufgrund von $\deg(r) < p-1$ ergibt sich aus 5.22, dass $r = \overline{0}$ ist. Wegen $\deg(X^{p-1}-\overline{1}) = p-1 = \deg(f)$ ist q ein konstantes Polynom. Aus $\ell(X^{p-1}-\overline{1}) = \overline{1} = \ell(f)$ erhalten wir $q = \overline{1}$ und damit die Behauptung. □

Korollar 5.25 (Satz von Wilson)**.** *Es sei $n \in \mathbb{N}$ mit $n > 1$. Dann sind äquivalent:*

(i) *n ist eine Primzahl.*

(ii) $(n-1)! \equiv -1 \pmod{n}$.

Beweis. (i)$\Longrightarrow$(ii): Sei $n = p$ eine Primzahl. Aus 5.24 ergibt sich

$$(X-\overline{1})(X-\overline{2})\cdot\ldots\cdot(X-\overline{p-1}) = X^{p-1}-\overline{1}$$

in $\mathbb{F}_p[X]$. Setzen wir $X = \overline{0} = \overline{p}$, so erhalten wir

$$\overline{p-1}\cdot\overline{p-2}\cdot\ldots\cdot\overline{1} = -\overline{1}.$$

und somit $(p-1)! \equiv -1 \pmod{p}$.
(ii)$\Longrightarrow$(i): Diese Implikation zeigen wir indirekt. Sei $n \in \mathbb{N}$, $n > 1$ keine Primzahl. Dann gibt es eine Primzahl $p < n$ mit $p|n$. Insbesondere folgt $p|(n-1)!$, also $\mathrm{ggT}((n-1)!, n) \neq 1$. Deswegen ist $\overline{(n-1)!}$ keine prime Restklasse modulo n. Weil $\overline{-1}$ aber eine prime Restklasse modulo n ist, erhalten wir $(n-1)! \not\equiv -1 \pmod{n}$. □

Satz 5.26. *Es sei R ein nullteilerfreier Ring und $G \subseteq R^\times$ eine endliche Gruppe (mit der eingeschränkten Multiplikation als Verknüpfung). Dann ist G zyklisch.*

Beweis. Wir setzen $n := \exp(G)$. Dann gilt für alle $g \in G$, dass $g^n = 1$ ist. Anders ausgedrückt: Alle $g \in G$ sind Nullstellen des Polynoms $X^n - 1 \in R[X]$. Dieses Polynom hat nach 5.22 höchstens n Nullstellen. Wir erhalten $|G| \leq n = \exp(G)$. Andererseits gilt nach 5.11: $\exp(G) \mid |G|$. Wir erhalten $\exp(G) = |G|$, was nach 5.17 impliziert, dass G zyklisch ist. □

Korollar 5.27. *Es sei p eine Primzahl. Dann ist $\mathbb{F}_p^\times$ eine zyklische Gruppe, insbesondere ist*

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

Beweis. Das ergibt sich direkt, wenn man in 5.26 $R = \mathbb{F}_p$ und $G = \mathbb{F}_p^\times$ setzt. □

Definition 5.28. *Es sei p eine Primzahl. Eine Zahl $w \in \mathbb{Z}$ heißt eine **primitive Wurzel** modulo p, wenn $\overline{w}$ ein Erzeuger von $\mathbb{F}_p^\times$ ist: $\mathbb{F}_p^\times = \langle \overline{w} \rangle$.*

Beispiel 5.29. (a) *2 ist eine primitive Wurzel modulo 5, denn $\mathbb{F}_5^\times = \langle \overline{2} \rangle$, siehe 5.1.*

(b) *Wir betrachten den Fall $p = 7$. Es ist $\mathbb{F}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Ordnungen von Elementen aus $\mathbb{F}_7^\times$ müssen Teiler von $|\mathbb{F}_7^\times| = 6$ sein, als Elementordnungen kommen also nur $1, 2, 3, 6$ in Frage. 2 ist keine primitive Wurzel modulo 7, denn $\overline{2}^2 = \overline{4} \neq \overline{1}$, $\overline{2}^3 = \overline{1}$, insbesondere ist $\operatorname{ord}(\overline{2}) = 3$. 3 ist eine primitive Wurzel modulo 7, denn wegen $\overline{3}^2 = \overline{2} \neq \overline{1}$, $\overline{3}^3 = \overline{6} \neq \overline{1}$ ist $\operatorname{ord}(\overline{3}) = 6$. Explizit erhalten wir als Potenzen von $\overline{3}$: $\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{4}$, $\overline{3}^5 = \overline{5}$, $\overline{3}^6 = \overline{1}$.*

Es ist keine allgemeingültige Formel bekannt, die für jede Primzahl p eine primitive Wurzel modulo p liefert.

Die Gruppen $(\mathbb{Z}/p^n\mathbb{Z})^\times$

Proposition 5.30. *Es sei G eine endliche abelsche Gruppe und es seien $m, n \in \mathbb{N}$ mit $\operatorname{ggT}(m,n) = 1$ und $|G| = mn$. Wir setzen weiterhin voraus, dass Elemente $g, h \in G$ existieren mit $\operatorname{ord}(g) = m$, $\operatorname{ord}(h) = n$. Dann gilt: G ist zyklisch und gh ist ein Erzeuger von G.*

Beweis. Wir zeigen $\operatorname{ord}(gh) = mn$, was die Behauptung dann impliziert. Sei $d \in \mathbb{N}$ mit $(gh)^d = 1$. Wir erhalten

$$1 = 1^m = ((gh)^d)^m = (g^m)^d h^{dm} = h^{dm}$$

und deswegen $\operatorname{ord}(h) = n | dm$, was aufgrund von $\operatorname{ggT}(m,n) = 1$ schließlich $n|d$ zur Folge hat. Analog ergibt sich $m|d$ und unter erneuter Verwendung von $\operatorname{ggT}(m,n) = 1$ somit $mn|d$, also $\operatorname{ord}(gh) \geq mn$. Wegen $\operatorname{ord}(gh) \leq |G| = mn$ folgt $\operatorname{ord}(gh) = mn$. □

Dass die Gruppe G unter den obigen Voraussetzungen zyklisch ist, folgt direkt aus 5.17, denn aus den Voraussetzungen folgt $m|\exp(G)$, $n|\exp(G)$, wegen $\operatorname{ggT}(m,n) = 1$ also $|G| = mn|\exp(G)$, und somit ist G nach 5.17 zyklisch. Der Sinn der obigen Proposition ist vor allem darin zu sehen, dass explizit ein Erzeuger angegeben wird.

Wir werden die eben bewiesene Proposition benutzen, um die Zyklizität von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ für ungerade Primzahlen p und $n \in \mathbb{N}$ nachzuweisen. Aufgrund von

$$|(\mathbb{Z}/p^n\mathbb{Z})^\times| = \varphi(p^n) = p^{n-1}(p-1)$$

genügt es nach 5.30, Elemente der Ordnung p^{n-1} bzw. $p-1$ zu konstruieren.

Definition 5.31. *Es sei $n \in \mathbb{Z}$ mit $n \neq 0$ und p eine Primzahl. Wir schreiben n in der Form $n = p^a m$ mit $a \in \mathbb{N}_0$, $m \in \mathbb{Z}$, $p \nmid m$. Wir setzen $v_p(n) := a$ und nennen $v_p(n)$ die **p-Bewertung** von n.*

Beispiel 5.32. *Es ist $v_3(45) = 2$, denn $45 = 3^2 \cdot 5$.*

Proposition 5.33. *Es sei p eine Primzahl, $n \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $1 \leq m \leq p^n$. Dann gilt:*

$$v_p(\binom{p^n}{m}) = n - v_p(m).$$

Beweis. Es ist

$$\binom{p^n}{m} = \frac{(p^n)!}{(p^n - m)!m!} = \frac{p^n(p^n-1)\cdot\ldots\cdot(p^n-(m-1))}{1\cdot 2\cdot\ldots\cdot(m-1)\cdot m}$$

und deshalb

$$\begin{aligned} v_p(\binom{p^n}{m}) &= v_p(p^n) + v_p(p^n-1) + \ldots + v_p(p^n-(m-1)) \\ &\quad -v_p(1) - \ldots - v_p(m-1) - v_p(m) \\ &= n + (v_p(p^n-1) - v_p(1)) + \ldots + (v_p(p^n-(m-1)) - v_p(m-1)) \\ &\quad -v_p(m) \end{aligned}$$

Sei $a \in \{1, \ldots, m-1\}$ mit $v_p(a) = k$, d.h. $a = p^k b$ mit $p \nmid b$. Es ergibt sich

$$p^n - a = p^n - p^k b = p^k(p^{n-k} - b)$$

mit $p \nmid (p^{n-k} - b)$, also $v_p(p^n - a) = v_p(a)$. Das impliziert

$$v_p(\binom{p^n}{m}) = n - v_p(m).$$

□

Proposition 5.34. *Es sei p eine Primzahl und $n \in \mathbb{N}$ mit $n > 1$. Dann gilt:*

(a) $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$,

(b) $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$, *falls $p \neq 2$.*

Beweis. (a) Es ist

$$(1+p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1}p + \binom{p^{n-1}}{2}p^2 + \ldots + \binom{p^{n-1}}{p^{n-1}}p^{(p^{n-1})}.$$

Sei $m \in \mathbb{N}$ mit $1 \leq m \leq p^{n-1}$. Wir erhalten

$$v_p(\binom{p^{n-1}}{m}p^m) \overset{5.33}{=} n - 1 - v_p(m) + m = n + (m - (v_p(m) + 1)).$$

Durch einen einfachen Induktionsbeweis sieht man, dass für $k \in \mathbb{N}_0$ stets $p^k \geq k+1$ gilt. Daraus ergibt sich

$$m \geq p^{v_p(m)} \geq v_p(m)+1$$

und deshalb

$$v_p(\binom{p^{n-1}}{m} p^m) \geq n,$$

woraus

$$(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$$

folgt.
(b) Es ist

$$\begin{aligned}(1+p)^{p^{n-2}} &= 1+\binom{p^{n-2}}{1}p+\binom{p^{n-2}}{2}p^2+\ldots+\binom{p^{n-2}}{p^{n-2}}p^{(p^{n-2})}\\ &= 1+p^{n-1}+\binom{p^{n-2}}{2}p^2+\ldots+\binom{p^{n-2}}{p^{n-2}}p^{(p^{n-2})}.\end{aligned}$$

Sei $m \in \mathbb{N}$ mit $2 \leq m \leq p^{n-2}$. Es ergibt sich

$$v_p(\binom{p^{n-2}}{m} p^m) \overset{5.33}{=} n-2-v_p(m)+m = n+(m-(v_p(m)+2)).$$

Ist $v_p(m)=0$, dann ist $m \geq 2 = v_p(m)+2$. Wir betrachten nun den Fall $v_p(m) \neq 0$. Durch eine einfache Induktion sieht man, dass für $k \in \mathbb{N}$ stets $p^k \geq k+2$ gilt. An dieser Stelle geht $p \neq 2$ ein, denn für $p=2$, $k=1$ ist die Aussage falsch. Wir erhalten

$$m \geq p^{v_p(m)} \geq v_p(m)+2,$$

also

$$v_p(\binom{p^{n-2}}{m} p^m) \geq n$$

und somit

$$(1+p)^{p^{n-2}} \equiv 1+p^{n-1} \not\equiv 1 \pmod{p^n}.$$

□

Satz 5.35. *Es sei p eine Primzahl mit $p \neq 2$. Dann gilt:*

(a) $(\mathbb{Z}/p^n\mathbb{Z})^\times$ *ist eine zyklische Gruppe.*

(b) *Ist $w \in \mathbb{Z}$ eine primitive Wurzel modulo p, dann ist $\overline{w^{p^{n-1}}(1+p)}$ ein Erzeuger von $(\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Beweis. Es genügt offenbar, Aussage (b) zu beweisen, denn diese impliziert (a). Sei $w \in \mathbb{Z}$ eine primitive Wurzel modulo p. Wir setzen $u := w^{p^{n-1}}$. Im ersten Beweisschritt zeigen wir, dass $\operatorname{ord}(\overline{u}) = p-1$ ist. Aufgrund von 4.21 ist $w^p \equiv w \pmod{p}$. Induktiv erhalten wir $u = w^{p^{n-1}} \equiv w \pmod{p}$, d.h. u ist eine primitive Wurzel modulo p. Damit sind $1, u, \ldots, u^{p-2}$ paarweise

inkongruent modulo p, also auch paarweise inkongruent modulo p^n, weshalb $\operatorname{ord}(\overline{u}) \geq p-1$ ist. Andererseits ist

$$u^{p-1} = w^{p^{n-1}(p-1)} = w^{\varphi(p^n)} \equiv 1 \pmod{p^n},$$

was $\operatorname{ord}(\overline{u}) | (p-1)$ impliziert. Zusammengenommen erhalten wir $\operatorname{ord}(\overline{u}) = p-1$.
Im zweiten Beweisschritt zeigen wir $\operatorname{ord}(\overline{1+p}) = p^{n-1}$. Aufgrund von 5.34(a) ist

$$(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n},$$

woraus $\operatorname{ord}(\overline{1+p}) | p^{n-1}$ folgt. Deshalb ist $\operatorname{ord}(\overline{1+p}) = p^k$ für ein $k \in \mathbb{N}$ mit $1 < k \leq n-1$. Nach 5.34(b) ist jedoch

$$(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$$

und deswegen $\operatorname{ord}(\overline{1+p}) = p^{n-1}$.
Aus 5.30 erhalten wir wegen $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = \varphi(p^n) = (p-1)p^{n-1}$ und $\operatorname{ord}(\overline{u}) = p-1$, $\operatorname{ord}(\overline{1+p}) = p^{n-1}$, dass $\overline{u} \cdot \overline{1+p}$ ein Erzeuger von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ist. □

Der Beweis hat gezeigt: Ist $w \in \mathbb{Z}$ eine primitive Wurzel modulo p mit $\operatorname{ord}(\overline{w}) = p-1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, dann ist $\overline{w(1+p)}$ ein Erzeuger von $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Definition 5.36. *Es sei p eine ungerade Primzahl. Eine Zahl $w \in \mathbb{Z}$ heißt eine **primitive Wurzel** modulo p^n, wenn $\overline{w}$ ein Erzeuger von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ ist.*

Beispiel 5.37. *Wir haben in 5.29 gesehen, dass 3 eine primitive Wurzel modulo 7 ist. Gesucht ist nun eine primitive Wurzel modulo 49. Nach 5.35 ist $\overline{3^7(1+7)} = \overline{31} \cdot \overline{8} = \overline{3}$ ein Erzeuger von $(\mathbb{Z}/49\mathbb{Z})^\times$, d.h. 3 ist eine primitive Wurzel modulo 49.*

Die Gruppen $(\mathbb{Z}/2^n\mathbb{Z})^\times$

Die Gruppen $(\mathbb{Z}/2\mathbb{Z})^\times$ und $(\mathbb{Z}/4\mathbb{Z})^\times$ sind beide offenbar zyklisch. In Beispiel 5.3 haben wir jedoch gesehen, dass dies für die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times$ nicht mehr gilt. In diesem Abschnitt werden wir Gruppen der Form $(\mathbb{Z}/2^n\mathbb{Z})^\times$ näher untersuchen.

Proposition 5.38. *Es sei $n \in \mathbb{N}$ mit $n > 1$. Dann gilt:*

(a) $5^{2^{n-2}} \equiv 1 \pmod{2^n}$,
(b) $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$.

Beweis. (a) Es ist

$$5^{2^{n-2}} = (1+2^2)^{2^{n-2}} = 1 + \binom{2^{n-2}}{1}2^2 + \binom{2^{n-2}}{2}2^4 + \ldots + \binom{2^{n-2}}{2^{n-2}}2^{2\cdot 2^{n-2}}.$$

Sei $m \in \mathbb{N}$ mit $1 \leq m \leq 2^{n-2}$. Wir erhalten

$$v_2\left(\binom{2^{n-2}}{m}2^{2m}\right) \overset{5.33}{=} n-2-v_2(m)+2m = n+(m-(v_2(m)+1))+m-1.$$

Wie im Beweis von 5.34 ist $m-(v_2(m)+1)\geq 0$ und deshalb

$$v_2(\binom{2^{n-2}}{m}2^{2m})\geq n,$$

woraus

$$5^{2^{n-2}}\equiv 1 \pmod{2^n}$$

folgt.
(b) Es ist

$$\begin{aligned} 5^{2^{n-3}} &= (1+2^2)^{2^{n-3}} = 1+\binom{2^{n-3}}{1}2^2+\binom{2^{n-3}}{2}2^4+\ldots+\binom{2^{n-3}}{2^{n-3}}2^{2\cdot 2^{n-3}} \\ &= 1+2^{n-1}+\binom{2^{n-3}}{2}2^4+\ldots+\binom{2^{n-3}}{2^{n-3}}2^{2\cdot 2^{n-3}}. \end{aligned}$$

Sei $m\in\mathbb{N}$ mit $2\leq m\leq 2^{n-3}$. Es ergibt sich

$$v_2(\binom{2^{n-3}}{m}2^{2m}) \overset{5.33}{=} n-3-v_2(m)+2m = n+(m-(v_2(m)+1))+m-2,$$

was mit analoger Arguemtation wie im Beweis von 5.34 zu

$$v_2(\binom{2^{n-3}}{m}2^{2m})\geq n$$

führt, was

$$5^{2^{n-3}}\equiv 1+2^{n-1}\not\equiv 1 \pmod{2^n}.$$

impliziert. □

Proposition 5.39. *Es sei $n\in\mathbb{N}$ mit $n>2$. Dann gilt:*

(a) *In $(\mathbb{Z}/2^n\mathbb{Z})^\times$ ist $\operatorname{ord}(\overline{5})=2^{n-2}$.*
(b) *Für jedes $\overline{a}\in(\mathbb{Z}/2^n\mathbb{Z})^\times$ gibt es eindeutig bestimmte Zahlen $i\in\{0,1\}$, $j\in\{0,\ldots,2^{n-2}-1\}$ mit*
$$\overline{a}=\overline{-1}^i\overline{5}^j.$$
(c) $\exp((\mathbb{Z}/2^n\mathbb{Z})^\times)=2^{n-2}<|(\mathbb{Z}/2^n\mathbb{Z})^\times|=2^{n-1}$, *insbesondere ist $(\mathbb{Z}/2^n\mathbb{Z})^\times$ nicht zyklisch.*

Beweis. (a) Aufgrund von 5.38 ist $\overline{5}^{2^{n-2}}=\overline{1}$. Daraus folgt

$$\operatorname{ord}(\overline{5})|2^{n-2},$$

und deshalb ist $\operatorname{ord}(\overline{5})=2^k$ für ein k mit $1\leq k\leq n-2$. Wegen 5.38 ist $\overline{5}^{2^{n-3}}\neq\overline{1}$. Das hat

$$\operatorname{ord}(\overline{5})=2^{n-2}$$

zur Folge.
(b) Wir bemerken zunächst, dass es offenbar $2 \cdot 2^{n-2} = 2^{n-1} = \varphi(2^n) = |(\mathbb{Z}/2^n\mathbb{Z})^\times|$ Paare (i,j) mit $i \in \{0,1\}$, $j \in \{0,\dots,2^{n-2}-1\}$ gibt. Seien nun $i,i' \in \{0,1\}$ und $j,j' \in \{0,\dots,2^{n-2}-1\}$ mit

$$\overline{-1}^i\overline{5}^j = \overline{-1}^{i'}\overline{5}^{j'}.$$

Dann erhalten wir $\overline{-1}^{i-i'} = \overline{5}^{j'-j}$. Wäre $i \neq i'$, so würde $\overline{-1} = \overline{5}^{j'-j}$ folgen und somit $-1 \equiv 5^{j'-j} \pmod{2^n}$. Wegen $n > 2$ wäre dann $-1 \equiv 1 \pmod 4$, was ein Widerspruch ist. Also ist $i = i'$ und deshalb $\overline{5}^{j'-j} = \overline{1}$. Das liefert $2^{n-2} = \operatorname{ord}(\overline{5}) | (j'-j)$. Da $-(2^{n-2}-1) \leq j'-j \leq 2^{n-2}-1$ ist, erhalten wir $j'-j = 0$, also $j = j'$. Damit gibt es genau $|(\mathbb{Z}/2^n\mathbb{Z})^\times|$ verschiedene Produkte der Form $\overline{-1}^i\overline{5}^j$ mit $i \in \{0,1\}$, $j \in \{0,\dots,2^{n-2}-1\}$. Dies impliziert die Behauptung.
(c) Wegen $\operatorname{ord}(\overline{5}) = 2^{n-2}$ und 5.11 ergibt sich $2^{n-2} | \exp((\mathbb{Z}/2^n\mathbb{Z})^\times)$. Ist $\overline{a} \in (\mathbb{Z}/2^n\mathbb{Z})^\times$, dann gibt es nach (b) Zahlen $i \in \{0,1\}$, $j \in \{0,\dots,2^{n-2}-1\}$ mit $\overline{a} = \overline{-1}^i\overline{5}^j$. Insbesondere ist

$$\overline{a}^{2^{n-2}} = \overline{-1}^{2^{n-2}i}\overline{5}^{2^{n-2}j} = (\overline{-1}^2)^{2^{n-3}i}(\overline{5}^{2^{n-2}})^j = \overline{1},$$

also ist $\exp((\mathbb{Z}/2^n\mathbb{Z})^\times) \leq 2^{n-2}$. Insgesamt erhalten wir $\exp((\mathbb{Z}/2^n\mathbb{Z})^\times) = 2^{n-2}$. Aufgrund von

$$|(\mathbb{Z}/2^n\mathbb{Z})^\times| = \varphi(2^n) = 2^{n-1} \neq 2^{n-2} = \exp((\mathbb{Z}/2^n\mathbb{Z})^\times)$$

und 5.17 ist die Gruppe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ nicht zyklisch. □

Nachdem wir festgestellt haben, dass die Gruppen $(\mathbb{Z}/2^n\mathbb{Z})^\times$ für $n > 2$ nicht zyklisch sind, würden wir natürlich trotzdem gerne ihre Struktur beschreiben. Dazu führen wir das direkte Produkt von Gruppen ein.

Proposition 5.40. *Es seien $G_1,\dots,G_n$ Gruppen. Dann ist*

$$G_1 \times \dots \times G_n := \{(g_1,\dots,g_n) \mid g_1 \in G_1,\dots,g_n \in G_n\}$$

zusammen mit der komponentenweisen Verknüpfung

$$(g_1,\dots,g_n)\cdot(g_1',\dots,g_n') := (g_1g_1',\dots,g_ng_n')$$

*eine Gruppe, das sogenannte **direkte Produkt** der Gruppen $G_1,\dots,G_n$. Sind alle Gruppen $G_1,\dots,G_n$ abelsch, dann ist auch $G_1 \times \dots \times G_n$ abelsch.*

Beweis. Die Behauptung ergibt sich unmittelbar aus der Definition: Das Assoziativgesetz folgt aus dem Assoziativgesetz auf jeder Komponente, das neutrale Element ist durch $(1_{G_1},\dots,1_{G_n})$ gegeben, wobei 1_{G_i} das neutrale Element in G_i bezeichne, und das zu $(g_1,\dots,g_n)$ inverse Element ist durch $(g_1^{-1},\dots,g_n^{-1})$ gegeben. □

Satz 5.41. *Es sei $n \in \mathbb{N}$ mit $n > 1$. Dann ist die Abbildung*

$$\begin{aligned}\psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} &\to (\mathbb{Z}/2^n\mathbb{Z})^\times \\ (i+2\mathbb{Z}, j+2^{n-2}\mathbb{Z}) &\mapsto \overline{-1}^i\overline{5}^j\end{aligned}$$

ein Isomorphismus. Es gilt also:

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

Beweis. Die Abbildung ψ ist wohldefiniert,

denn: Seien $i_1, i_2 \in i + 2\mathbb{Z}$ und $j_1, j_2 \in j + 2^{n-2}\mathbb{Z}$. Dann ist $i_1 - i_2 \in 2\mathbb{Z}$ und $j_1 - j_2 \in 2^{n-2}\mathbb{Z}$. Wegen $\operatorname{ord}(\overline{-1}) = 2$ und $\operatorname{ord}(\overline{5}) = 2^{n-2}$ erhalten wir $\overline{-1}^{i_1-i_2} = \overline{1}$ und $\overline{5}^{j_1-j_2} = \overline{1}$. Das liefert $\overline{-1}^{i_1} = \overline{-1}^{i_2}$ und $\overline{5}^{j_1} = \overline{5}^{j_2}$ und deshalb $\psi(i_1 + 2\mathbb{Z}, j_1 + 2^{n-2}\mathbb{Z}) = \psi(i_2 + 2\mathbb{Z}, j_2 + 2^{n-2}\mathbb{Z})$. #

Die Abbildung ψ ist ein Homomorphismus,

denn: Seien $i_1 + 2\mathbb{Z}, i_2 + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$ und $j_1 + 2^{n-2}\mathbb{Z}, j_2 + 2^{n-2}\mathbb{Z} \in \mathbb{Z}/2^{n-2}\mathbb{Z}$. Wir erhalten

$$\begin{aligned}&\psi((i_1 + 2\mathbb{Z}, j_1 + 2^{n-2}\mathbb{Z}) + (i_2 + 2\mathbb{Z}, j_2 + 2^{n-2}\mathbb{Z})) = \psi(i_1 + i_2 + 2\mathbb{Z}, j_1 + j_2 + 2^{n-2}\mathbb{Z})\\ &= \overline{-1}^{i_1+i_2}\overline{5}^{j_1+j_2} = \overline{-1}^{i_1}\overline{5}^{j_1}\overline{-1}^{i_2}\overline{5}^{j_2} = \psi(i_1 + 2\mathbb{Z}, j_1 + 2^{n-2}\mathbb{Z}) \cdot \psi(i_2 + 2\mathbb{Z}, j_2 + 2^{n-2}\mathbb{Z}).\end{aligned}$$

#

Die Bijektivität von ψ ergibt sich unmittelbar aus 5.39. □

§6 Der Chinesische Restsatz

Beispiel 6.1. *Heute ist Montag. Angenommen, heute ist Neumond. In wievielen Tagen fällt der Vollmond auf einen Mittwoch? Wir gehen davon aus, dass die Mondphasen eine Periode von 29 Tagen haben und nummerieren die Wochentage mit* $0, \ldots, 6$*, beginnend bei Montag. Zu lösen ist also das folgende System von Kongruenzen:*

$$x \equiv 2 \pmod 7,\ x \equiv 15 \pmod{29}$$

Wir werden uns in diesem Abschnitt mit der Frage der Lösbarkeit von Systemen von Kongruenzen beschäftigen.

Proposition 6.2. *Es seien* $R_1, \ldots, R_n$ *Ringe. Dann ist*

$$R_1 \times \ldots \times R_n := \{(r_1, \ldots, r_n) \mid r_1 \in R_1, \ldots, r_n \in R_n\}$$

zusammen mit den komponentenweisen Verknüpfungen

$$\begin{aligned}(r_1, \ldots, r_n) + (r'_1, \ldots, r'_n) &:= (r_1 + r'_1, \ldots, r_n + r'_n),\\ (r_1, \ldots, r_n) \cdot (r'_1, \ldots, r'_n) &:= (r_1 r'_1, \ldots, r_n r'_n).\end{aligned}$$

ein Ring, das sogenannte ***direkte Produkt*** *von* $R_1, \ldots, R_n$*.*

Beweis. Offenbar ist $R_1 \times \cdots \times R_n$ eine additive Gruppe mit neutralem Element $(0_{R_1}, \ldots, 0_{R_n})$ nach 5.40. Das Assoziativgesetz der Multiplikation und die Distributivgesetze werden von den Komponenten vererbt. Das neutrales Element der Multiplikation ist durch $(1_{R_1}, \ldots, 1_{R_n})$ gegeben. □

Definition 6.3. *Es seien R, S Ringe und $\psi : R \to S$ eine Abbildung. Die Abbildung ψ heißt ein **(Ring-)Homomorphismus**, wenn gilt: Für alle $a, b \in R$ ist*

$$\begin{aligned} \psi(a+b) &= \psi(a)+\psi(b), \\ \psi(ab) &= \psi(a)\psi(b), \\ \psi(1_R) &= 1_S\,. \end{aligned}$$

*ψ heißt ein **(Ring-)Isomorphismus**, wenn ψ ein bijektiver Ringhomomorphismus ist.*

Die folgende Aussage ergibt sich analog zu 5.14.

Proposition 6.4. *Es seien R, S Ringe und $\psi : R \to S$ ein Ringhomomorphismus. Dann gilt:*

(a) *ψ ist genau dann injektiv, wenn* $\operatorname{Kern}\psi := \{a \in R \mid \psi(a) = 0_S\} = \{0_R\}$ *ist.*

(b) *Ist ψ ein Ringisomorphismus, dann ist auch $\psi^{-1} : S \to R$ ein Ringisomorphismus.*

*Existiert ein Isomorphismus zwischen R und S, nennen wir R und S **isomorph** (Notation: $R \cong S$).*

Satz 6.5 (Chinesischer Restsatz)**.** *Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, $m := m_1 \cdot \ldots \cdot m_r$. Dann gilt: Die Abbildung*

$$\begin{aligned} \Psi = \Psi_{m_1,\ldots,m_r} : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \\ a + m\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) \end{aligned}$$

ist ein Ringisomorphismus mit Umkehrabbildung

$$\begin{aligned} \Psi^{-1} =: \Phi_{m_1,\ldots,m_r} : \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ (a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z}) &\mapsto a_1e_1 + \ldots + a_re_r + m\mathbb{Z}\,. \end{aligned}$$

Hierbei ist

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \text{ für } i = 1, \ldots, r\,.$$

Beweis. Die Abbildung Ψ ist wohldefiniert,

denn: Seien $a, b \in \mathbb{Z}$ mit $a + m\mathbb{Z} = b + m\mathbb{Z}$. Dann ist $a - b \in m\mathbb{Z} \subseteq m_i\mathbb{Z}$ für alle $i \in \{1, \ldots, r\}$, denn $m_i \mid m$. Wir erhalten $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$ für alle $i \in \{1, \ldots, r\}$. #

Die Abbildung Ψ ist ein Ringhomomorphismus,

denn: Es seien $a, b \in \mathbb{Z}$. Dann ist

$$\begin{aligned} \Psi((a + m\mathbb{Z}) + (b + m\mathbb{Z})) &= \Psi(a + b + m\mathbb{Z}) \\ &= (a + b + m_1\mathbb{Z}, \ldots, a + b + m_r\mathbb{Z}) \\ &= (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) + (b + m_1\mathbb{Z}, \ldots, b + m_r\mathbb{Z}) \\ &= \Psi(a + m\mathbb{Z}) + \Psi(b + m\mathbb{Z}) \end{aligned}$$

Die Rechnung für die für die Multiplikation verläuft analog. Darüber hinaus ist

$$\Psi(1+m\mathbb{Z}) = (1+m_1\mathbb{Z},\ldots,1+m_r\mathbb{Z}).$$

#

Die Abbildung Ψ ist injektiv, denn:

denn: Sei $a \in \mathbb{Z}$ mit $\Psi(a+m\mathbb{Z}) = (a+m_1\mathbb{Z},\ldots,a+m_r\mathbb{Z}) = (0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z})$. Wir erhalten $m_1 \mid a,\ldots,m_r \mid a$. Da die m_i paarweise teilerfremd sind, erhalten wir aus 1.9, dass auch $m_1\cdot\ldots\cdot m_r \mid a$ gilt. Somit ist $a+m\mathbb{Z} = 0+m\mathbb{Z}$. #

Die Abbildung Ψ is surjektiv, denn es ist

$$|\mathbb{Z}/m\mathbb{Z}| = m = m_1\cdot\ldots\cdot m_r = |\mathbb{Z}/m_1\mathbb{Z}\times\ldots\times\mathbb{Z}/m_r\mathbb{Z}|,$$

die Surjektivität von Ψ folgt deshalb aus der Injektivität von Ψ. Damit ist die Abbildung Ψ ein Ringisomorphismus, und wir müssen nur noch nachrechnen, dass die Umkehrabbildung von Ψ tatsächlich so aussieht, wie oben behauptet wird. Wir setzen

$$\begin{aligned}\Phi : \mathbb{Z}/m_1\mathbb{Z}\times\ldots\times\mathbb{Z}/m_r\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z}\\ (a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z}) &\mapsto a_1e_1+\ldots+a_re_r+m\mathbb{Z}.\end{aligned}$$

mit

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \text{ für } i=1,\ldots,r.$$

Die Abbildung Φ ist wohldefiniert,

denn: Seien $a_1\ldots,a_r,b_1,\ldots,b_r \in \mathbb{Z}$ mit $a_i+m_i\mathbb{Z} = b_i+m_i\mathbb{Z}$ für $i=1,\ldots,r$. Das liefert $a_i-b_i \in m_i\mathbb{Z}$, also ist

$$(a_i-b_i)e_i = \underbrace{(a_i-b_i)}_{\in m_i\mathbb{Z}}\underbrace{\left(\frac{m}{m_i}\right)^{\varphi(m_i)}}_{\in \frac{m}{m_i}\mathbb{Z}} \in m\mathbb{Z} \text{ für } i=1,\ldots,r$$

Es ergibt sich

$$(a_1-b_1)e_1+\ldots+(a_r-b_r)e_r \in m\mathbb{Z},$$

und deshalb ist

$$a_1e_1+\ldots+a_re_r+m\mathbb{Z} = b_1e_1+\ldots+b_re_r+m\mathbb{Z}.$$

#

Es ist $\Psi\circ\Phi = id_{\mathbb{Z}/m_1\mathbb{Z}\times\ldots\times\mathbb{Z}/m_r\mathbb{Z}}$,

denn: Für $a_1,\ldots,a_r \in \mathbb{Z}$ ist

$$\Psi(\Phi((a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z}))) = \Psi(a_1e_1+\ldots+a_re_r+m\mathbb{Z}).$$

Wegen $e_i = (\frac{m}{m_i})^{\varphi(m_i)}$ und $m_j \mid \frac{m}{m_i}$ für $j\neq i$ folgt $e_i \in m_j\mathbb{Z}$ für $j\neq i$. Daraus ergibt sich

$$\begin{aligned}\Psi(a_1e_1+\ldots a_re_r+m\mathbb{Z}) &= (a_1e_1+\ldots+a_re_r+m_1\mathbb{Z},\ldots,a_1e_1+\ldots+a_re_r+m_r\mathbb{Z})\\ &= (a_1e_1+m_1\mathbb{Z},\ldots,a_re_r+m_r\mathbb{Z}).\end{aligned}$$

Es ist $\frac{m}{m_i} = m_1 \cdot \dots \cdot m_{i-1} m_{i+1} \cdot \dots \cdot m_r$. Da die m_j nach Voraussetzung paarweise teilerfremd sind, ist $\mathrm{ggT}(\frac{m}{m_i}, m_i) = 1$. Der Satz von Euler-Fermat 4.19 liefert

$$e_i = \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \equiv 1 \pmod{m_i}.$$

Wir erhalten

$$\begin{aligned}\Psi(\Phi((a_1 + m_1\mathbb{Z}, \dots, a_r + m_r\mathbb{Z}))) &= (a_1 e_1 + m_1\mathbb{Z}, \dots, a_r e_r + m_r\mathbb{Z}) \\ &= (a_1 + m_1\mathbb{Z}, \dots, a_r + m_r\mathbb{Z}),\end{aligned}$$

was die Behauptung zeigt. #

Da die Abbildung Ψ bijektiv ist, ist die Abbildung Φ die Umkehrabbildung von Ψ. □

Korollar 6.6. *Es seien $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd, und es seien $a_1, \dots, a_r \in \mathbb{Z}$. Dann gilt: Das System von Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

besitzt eine Lösung $x \in \mathbb{Z}$. Diese ist eindeutig bestimmt modulo $m_1 \cdot \dots \cdot m_r$.

Beweis. Aufgrund der Surjektivität der Abbildung $\Psi = \Psi_{m_1,\dots,m_r}$ existiert ein $x \in \mathbb{Z}$ mit

$$\Psi(x + m_1 \cdot \dots \cdot m_r\mathbb{Z}) = (x + m_1\mathbb{Z}, \dots, x + m_r\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \dots, a_r + m_r\mathbb{Z}),$$

d.h.mit

$$x \equiv a_1 \pmod{m_1}, \quad \dots \quad , x \equiv a_r \pmod{m_r}.$$

Ist $y \in \mathbb{Z}$ mit $y \equiv a_1 \pmod{m_1}, \dots, y \equiv a_r \pmod{m_r}$, dann folgt

$$\Psi(x + m_1 \cdot \dots \cdot m_r\mathbb{Z}) = \Psi(y + m_1 \cdot \dots \cdot m_r\mathbb{Z})$$

und wegen der Injektivität von Ψ somit

$$x + m_1 \cdot \dots \cdot m_r\mathbb{Z} = y + m_1 \cdot \dots \cdot m_r\mathbb{Z},$$

also $y \equiv x \pmod{m_1 \cdot \dots \cdot m_r}$. □

Beispiel 6.7 (vgl. Bsp. 6.1)**.** *Gesucht sind die Lösungen des Systems von Kongruenzen*

$$x \equiv 2 \pmod{7}, \quad x \equiv 15 \pmod{29}.$$

Aufgrund von 6.5 haben wir einen Ringisomorphismus

$$\begin{aligned}\Phi_{7,29} : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z} &\to \mathbb{Z}/(7 \cdot 29)\mathbb{Z} = \mathbb{Z}/203\mathbb{Z}, \\ (a_1 + 7\mathbb{Z}, a_2 + 29\mathbb{Z}) &\mapsto a_1 e_1 + a_2 e_2 + 203\mathbb{Z}\end{aligned}$$

mit

$$e_1 = \left(\frac{7 \cdot 29}{7}\right)^{\varphi(7)} = 29^6 \equiv 29 \pmod{203},$$

$$e_2 = \left(\frac{7 \cdot 29}{29}\right)^{\varphi(29)} = 7^{28} \equiv 175 \pmod{203}.$$

Es ist also

$$\Phi_{7,29}(a_1 + 7\mathbb{Z}, a_2 + 29\mathbb{Z}) = 29a_1 + 175a_2 + 203\mathbb{Z}.$$

Insbesondere ist

$$\Phi_{7,29}(2 + 7\mathbb{Z}, 15 + 29\mathbb{Z}) = 29 \cdot 2 + 175 \cdot 15 + 203\mathbb{Z} = 44 + 203\mathbb{Z},$$

d.h.

$$\{x \in \mathbb{Z} \mid x \equiv 2 \pmod{7},\ x \equiv 15 \pmod{29}\} = \{44 + 203k \mid k \in \mathbb{Z}\}.$$

Proposition 6.8. *Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, und es sei $m := m_1 \cdot \ldots \cdot m_r$. Ferner sei*

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \text{ für } i = 1, \ldots, r\,.$$

Dann gilt:

(a) $\Psi_{m_1,\ldots,m_r}(e_i + m\mathbb{Z}) = (0 + m_1\mathbb{Z}, \ldots, 1 + m_i\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z})$.

(b) *In $\mathbb{Z}/m\mathbb{Z}$ gilt*

- $\overline{e_i} \cdot \overline{e_j} = \overline{0}$ *für* $i \neq j$
- $\overline{e_i} \cdot \overline{e_i} = \overline{e_i}$ *für* $i = 1, \ldots, r$.
- $\overline{e_1} + \ldots + \overline{e_r} = \overline{1}$.

*Man sagt auch: Die $\overline{e_i}$ bilden eine **Zerlegung der Eins in paarweise orthogonale Idempotente**.*

Beweis. (a) Im Beweis von 6.5 haben wir gesehen: $e_i \in m_j\mathbb{Z}$ für $j \neq i$, sowie $e_i \equiv 1 \pmod{mi}$. Das impliziert die Behauptung.
(b) Aus (a) folgt für $i \neq j$:

$$\Psi_{m_1,\ldots,m_r}(\overline{e_i} \cdot \overline{e_j}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i})\Psi_{m_1,\ldots,m_r}(\overline{e_j}) = (0 + m_1\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{0}),$$

was wegen der Injektivität von $\Psi_{m_1,\ldots,m_r}$ zu $\overline{e_i} \cdot \overline{e_j} = \overline{0}$ führt. Die anderen Aussagen folgen analog unter Verwendung von

$$\Psi_{m_1,\ldots,m_r}(\overline{e_i})\Psi_{m_1,\ldots,m_r}(\overline{e_i}) = (0 + m_1\mathbb{Z}, \ldots, 1 + m_i\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i}),$$

und

$$\Psi_{m_1,\ldots,m_r}(\overline{e_1}) + \ldots + \Psi_{m_1,\ldots,m_r}(\overline{e_r}) = (1 + m_1\mathbb{Z}, \ldots, 1 + m_r\mathbb{Z}) = \Psi_{m_1,\ldots,m_r}(\overline{1}).$$

□

Proposition 6.9. *Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, und es sei $m := m_1 \cdot \ldots \cdot m_r$. Ferner sei*

$$e_i := \left(\frac{m}{m_i}\right)^{\varphi(m_i)} \quad \text{für } i = 1, \ldots, r\,.$$

Es seien $u_1, \ldots, u_r \in \mathbb{Z}$ mit

$$u_1 \frac{m}{m_1} + \ldots + u_r \frac{m}{m_r} = 1.$$

Dann gilt in $\mathbb{Z}/m\mathbb{Z}$:

$$\overline{e_i} = \overline{u_i \frac{m}{m_i}}$$

für $i = 1, \ldots, r$.

Beweis. Da $m_1 \ldots, m_r$ paarweise teilerfremd sind, ist $\mathrm{ggT}(\frac{m}{m_1}, \ldots, \frac{m}{m_r}) = 1$, damit existieren $u_1, \ldots, u_r$ wie oben. Offenbar ist $u_i \frac{m}{m_i} \equiv 0 \pmod{m_j}$ für $j \neq i$, und es ist

$$u_i \frac{m}{m_i} = 1 - u_1 \frac{m}{m_1} - \ldots - u_{i-1} \frac{m}{m_{i-1}} - u_{i+1} \frac{m}{m_{i+1}} - \ldots - u_r \frac{m}{m_r} \equiv 1 \pmod{m_i}.$$

Somit ist

$$\Psi_{m_1,\ldots,m_r}(\overline{u_i \frac{m}{m_i}}) = \Psi_{m_1,\ldots,m_r}(\overline{e_i}).$$

Aufgrund der Injektivität von $\Psi_{m_1,\ldots,m_r}$ folgt $\overline{e_i} = \overline{u_i \frac{m}{m_i}}$. □

Beispiel 6.10 (vgl. Bsp. 6.7)**.** *Wir wollen $\overline{e_1}, \overline{e_2}$ für $m_1 = 7$, $m_2 = 29$ mittels 6.9 berechnen. Es ist*

$$\mathrm{ggT}(7, 29) = 1 = (-4) \cdot 7 + 1 \cdot 29$$

und deshalb $\overline{e_1} = \overline{1 \cdot 29} = \overline{29}$, $\overline{e_2} = \overline{(-4) \cdot 7} = \overline{-28} = \overline{175}$.

Wir wollen den Chinesischen Restsatz benutzen, um einen Struktursatz über die primen Restklassengruppen zu erhalten. Dazu brauchen wir noch eine kleine algebraische Vorüberlegung.

Proposition 6.11. *Es seien R, S Ringe und $\psi : R \to S$ ein Ringisomorphismus. Dann induziert ψ einen Gruppenisomorphismus*

$$\psi^\times := \psi|_{R^\times} : R^\times \to S^\times.$$

Beweis. Die Abbildung $\psi^\times$ ist wohldefiniert, denn ist $a \in R^\times$, dann existiert ein $b \in R^\times$ mit $ab = 1$. Das liefert

$$\psi^\times(a)\psi^\times(b) = \psi^\times(ab) = \psi^\times(1) = 1,$$

weswegen $\psi^\times(a)$ in $S^\times$ liegt. Da ψ ein Ringhomomorphismus ist, ist die Abbildung $\psi^\times$ ein Gruppenhomomorphismus. Die Injektivität von ψ vererbt sich auf $\psi^\times$. Zum Nachweis der Surjektivität sei $\tilde{a} \in S^\times$. Dann gibt es ein $\tilde{b} \in S^\times$ mit $\tilde{a}\tilde{b} = 1$. Aufgrund der Surjektivität von ψ existieren $a, b \in R$ mit $\psi(a) = \tilde{a}$ und $\psi(b) = \tilde{b}$. Damit erhalten wir

$$\psi(ab) = \psi(a)\psi(b) = \tilde{a}\tilde{b} = 1 = \psi(1),$$

was $ab = 1$ und damit $a \in R^\times$ zur Folge hat. □

Die nächste Aussage ergibt sich direkt aus der komponentenweisen Erklärung der Multiplikation in direkten Produkten von Ringen.

Proposition 6.12. *Es seien $R_1, \ldots, R_n$ Ringe. Dann gilt:*

$$(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times.$$

Aus diesen Vorüberlegungen und dem Chinesischen Restsatz ergibt sich unmittelbar:

Korollar 6.13. *Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, und es sei $m := m_1 \cdot \ldots m_r$. Dann ist die Abbildung*

$$\begin{aligned} \Psi^\times_{m_1,\ldots,m_r} : (\mathbb{Z}/m\mathbb{Z})^\times &\to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times, \\ a + m\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}) \end{aligned}$$

ein Gruppenisomorphismus.

Korollar 6.14. *Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd. Dann gilt:*

$$\varphi(m_1 \cdot \ldots \cdot m_r) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_r).$$

*Man sagt auch, die Eulersche φ-Funktion ist **schwach multiplikativ**.*

Beweis. Es ist

$$\begin{aligned} \varphi(m_1 \cdot \ldots \cdot m_r) &= \left|(\mathbb{Z}/m_1 \cdot \ldots \cdot m_r\mathbb{Z})^\times\right| \\ &\overset{6.13}{=} \left|(\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times\right| \\ &= \left|(\mathbb{Z}/m_1\mathbb{Z})^\times\right| \cdot \ldots \cdot \left|(\mathbb{Z}/m_r\mathbb{Z})^\times\right| \\ &= \varphi(m_1) \cdot \ldots \cdot \varphi(m_r) \end{aligned}$$

□

Beispiel 6.15. *(a) Es ist*

$$\varphi(140) = \varphi(4 \cdot 5 \cdot 7) = \varphi(4) \cdot \varphi(5) \cdot \varphi(7) = 2 \cdot (5-1) \cdot (7-1) = 2 \cdot 4 \cdot 6 = 48.$$

(b) Ohne die Voraussetzung der Teilerfremdheit von $m_1, \ldots, m_r$ wird Aussage 6.14 falsch: Zum Beispiel ist $\varphi(2 \cdot 2) = \varphi(4) = 2$, aber $\varphi(2)\varphi(2) = 1 \cdot 1 = 1$.

Korollar 6.16. *Es sei $m \in \mathbb{N}$. Dann gilt:*

$$\varphi(m) = m \prod_{p \in \mathbb{P}, p \mid m} \left(1 - \frac{1}{p}\right).$$

Beweis. Sei $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ sowie $e_1, \ldots, e_r \in \mathbb{N}$. Wir erhalten

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1}) \cdot \ldots \cdot \varphi(p_r^{e_r}) \\ &= p_1^{e_1-1}(p_1-1) \cdot \ldots \cdot p_r^{e_r-1}(p_r-1) \\ &= p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \left(1-\frac{1}{p_1}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_r}\right) \\ &= m \prod_{p \in \mathbb{P}, p \mid m} \left(1-\frac{1}{p}\right).\end{aligned}$$

□

Wir wollen uns nun der Frage zuwenden, für welche Werte von m die primen Restklassengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ zyklisch sind.

Proposition 6.17. *Es seien $G_1, \ldots, G_r$ endliche zyklische Gruppen, und es sei $G := G_1 \times \ldots \times G_r$. Dann gilt:*

$$\exp(G) = \mathrm{kgV}(|G_1|, \ldots, |G_r|).$$

Insbesondere ist die Gruppe G genau dann zyklisch, wenn die Ordnungen $|G_1|, \ldots, |G_r|$ paarweise teilerfremd sind.

Beweis. Wir rechnen nach, dass $\exp(G)$ die definierenden Eigenschaften des kleinsten gemeinsamen Vielfachen $\mathrm{kgV}(|G_1|, \ldots, |G_r|)$ erfüllt. Offenbar gilt $|G_i| \mid \exp(G)$ für $i = 1, \ldots, r$, denn

$$\exp(G) = \mathrm{kgV}(\mathrm{ord}(g) \mid g \in G),$$

und für das Element $\tilde{g}_i := (1, \ldots, 1, g_i, 1, \ldots, 1) \in G$ mit einem Erzeuger g_i von G_i ist $\mathrm{ord}(\tilde{g}_i) = |G_i|$. Sei nun $m \in \mathbb{Z}$ mit $|G_1| \mid m, \ldots |G_r| \mid m$. Dann folgt $\exp(G) | m$,

denn: Für alle $i \in \{1, \ldots, r\}$ existiert ein $q_i \in \mathbb{Z}$ mit $m = q_i |G_i|$. Für $x = (x_1, \ldots, x_r) \in G$ ist dann

$$x^m = (x_1^m, \ldots, x_r^m) = (x_1^{q_1|G_1|}, \ldots, x_r^{q_r|G_r|}) = (1, \ldots, 1).$$

Wir schreiben m in der Form $m = q \exp(G) + s$ mit $0 \leq s < \exp(G)$. Wir erhalten

$$1 = x^m = x^{q \exp(G)} x^s = x^s$$

für alle $x \in G$. Aufgrund der Minimalität von $\exp(G)$ ergibt sich $s = 0$. Das impliziert $\exp(G) \mid m$. #

Die Gruppe G ist nach 5.17 genau dann zyklisch, wenn $\exp(G) = |G| = |G_1| \cdot \ldots \cdot |G_r|$ ist. Das ist nach dem eben Gezeigten genau dann der Fall, wenn $\mathrm{kgV}(|G_1|, \ldots, |G_r|) = |G_1| \cdot \ldots \cdot |G_r|$ ist. Dies ist wiederum äquivalent dazu, dass die Ordnungen $|G_1|, \ldots, |G_r|$ paarweise teilerfremd sind (vgl. Übungen). □

Satz 6.18. *Es sei $m \in \mathbb{N}$ mit $m > 1$. Dann sind äquivalent:*

(i) *Die Gruppe* $(\mathbb{Z}/m\mathbb{Z})^\times$ *ist zyklisch.*

(ii) *Einer der folgenden Fälle liegt vor:*

$$m = \begin{cases} 2 \\ 4 \\ p^e, \text{ wobei } p \text{ eine ungerade Primzahl und } e \in \mathbb{N} \text{ ist} \\ 2p^e, \text{ wobei } p \text{ eine ungerade Primzahl und } e \in \mathbb{N} \text{ ist} \end{cases}$$

Beweis. (i)$\Longrightarrow$(ii): Sei $(\mathbb{Z}/m\mathbb{Z})^\times$ zyklisch. Wir schreiben m in der Form $m = 2^a p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \in \mathbb{N}$ sowie $a, r \in \mathbb{N}_0$. Aufgrund von 6.13 erhalten wir

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/2^a\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times.$$

Die Gruppen $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ sind hierbei alle zyklisch der Ordnung

$$|(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times| = \varphi(p_i^{e_i}) = (p_i - 1)p_i^{e_i - 1}.$$

Wäre $a > 2$, so würde aufgrund von 5.41 folgen, dass

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z} \times (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$$

ist. Da die Gruppen $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/2^{a-2}\mathbb{Z}$ beide gerade Ordnung haben, stünde dies wegen 6.17 im Widerspruch zur Zyklizität von $(\mathbb{Z}/m\mathbb{Z})^\times$. Somit ist $a \leq 2$, insbesondere ist die Gruppe $(\mathbb{Z}/2^a\mathbb{Z})^\times$ zyklisch. Da die Primzahlen p_i alle ungerade sind, sind die Ordnungen der Gruppen $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ für $i = 1, \ldots, r$ alle gerade. Wiederum mittels 6.17 folgt, dass $r \in \{0, 1\}$ ist. Ist $r = 0$, so erhalten wir die Fälle $m = 2$ und $m = 4$. Ist $r = 1$, so ergeben sich die Fälle $m = p_1^{e_1}$, $m = 2p_1^{e_1}$ und $m = 4p_1^{e_1}$. Der Fall $m = 4p_1^{e_1}$ scheidet wegen 6.17 aus, da die Gruppen $(\mathbb{Z}/4\mathbb{Z})^\times$ und $(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times$ beide gerade Ordnung haben. Somit verbleiben genau die angegebenen Fälle.

(ii)$\Longrightarrow$(i): Die Gruppen $(\mathbb{Z}/2\mathbb{Z})^\times$ sowie $(\mathbb{Z}/4\mathbb{Z})^\times$ sind offenbar zyklisch. Gruppen der Form $(\mathbb{Z}/p^e\mathbb{Z})^\times$ sind zyklisch nach 5.35. Darüber hinaus ist

$$(\mathbb{Z}/2p^e\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^e\mathbb{Z})^\times = \{\overline{1}\} \times (\mathbb{Z}/p^e\mathbb{Z})^\times \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$$

und somit ebenfalls zyklisch. □

Beispiel 6.19. (a) *Die Gruppe* $(\mathbb{Z}/35\mathbb{Z})^\times$ *ist wegen* $35 = 5 \cdot 7$ *nach 6.18 nicht zyklisch. In der Tat ist*

$$(\mathbb{Z}/35\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

und somit $\exp((\mathbb{Z}/35\mathbb{Z})^\times) = \mathrm{kgV}(4, 6) = 12 < \varphi(35) = 4 \cdot 6 = 24$.

(b) *Die Gruppe* $(\mathbb{Z}/18\mathbb{Z})^\times$ *ist wegen* $18 = 2 \cdot 3^2$ *nach 6.18 zyklisch. In der Tat ist*

$$(\mathbb{Z}/18\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \cong \{\overline{1}\} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

Definition 6.20. *Sei* $m \in \mathbb{N}$, $m > 1$ *von der Form wie in 6.18(ii). Ist* $w \in \mathbb{Z}$ *ein Erzeuger von* $(\mathbb{Z}/m\mathbb{Z})^\times$, *dann heißt* w *eine* ***primitive Wurzel modulo*** m.

Beispiel 6.21. *Nach 6.18 ist die Gruppe* $(\mathbb{Z}/10\mathbb{Z})^\times$ *zyklisch. Offenbar ist* 3 *eine primitive Wurzel modulo* 10, *denn*

$$\langle\overline{3}\rangle = \{\overline{1}, \overline{3}, \overline{9}, \overline{7}\} = (\mathbb{Z}/10\mathbb{Z})^\times.$$

§7 Das RSA-Verfahren

Wir werden in diesem Abschnitt eine Anwendung des bisher behandelten Stoffes, das sogenannte RSA-Verschlüsselungsverfahren, kennenlernen. Wir werden uns dabei auf die wesentlichen mathematischen Grundlagen beschränken, für alles weitere sei auf die entsprechende Literatur zur Kryptographie verwiesen.

Problemstellung: Man möchte eine Nachricht verschlüsselt übertragen, ohne dass Absender und Empfänger vorher gemeinsam auf sichere Weise einen Schlüssel austauschen.

Im Folgenden möchte Person A (Absender) eine Nachricht an Person E (Empfänger) übermitteln.

Idee: Person E erzeugt einen öffentlichen Schlüssel (zur Verschlüsselung) und einen privaten Schlüssel (zur Entschlüsselung). Der öffentliche Schlüssel wir öffentlich bekanntgegeben, den privaten Schlüssel behält Person E für sich. Person A verwendet den öffentlichen Schlüssel, um die Nachricht zu verschlüsseln und sendet die Nachricht an Person E. Person E benutzt den privaten Schlüssel, um die Nachricht zu entschlüsseln.

Problem: Das Erzeugen des öffentlichen und privaten Schlüssels muß schnell gehen, ebenso das Verschlüsseln mit dem öffentlichen Schlüssel und das Entschlüsseln, wenn der private Schlüssel bekannt ist. Das Bestimmen des privaten Schlüssels aus dem öffentlichen Schlüssel darf in angemessener Zeit nicht machbar sein.

Das ***RSA-Verfahren*** (nach Rivest, Shamir und Adleman, 1977) basiert auf dem aktuellen Wissensstand, dass das Faktorisieren einer Zahl in ihre Primfaktoren sehr aufwändig ist, wo hingegen das Erzeugen einer Zahl durch Multiplikation von Primzahlen sehr einfach ist.

Algorithmus 7.1 (Schlüsselerzeugung beim RSA-Verfahren)**.** *Person E möchte ein Paar von Schlüsseln erzeugen, so dass sie künftig als Empfänger von verschlüsselten Nachrichten in Frage kommt.*

(1) Person E bestimmt zufällig zwei große voneinander verschiedene Primzahlen p, q (groß heißt hier mehrere Hundert Stellen). Das kann etwa dadurch geschehen, dass er solange zufällig natürliche Zahlen auswählt und auf ihre Primzahleigenschaft hin testet, bis zwei Primzahlen gefunden sind. Effiziente Primzahltests werden wir im weiteren Verlauf der Vorlesung kennenlernen.

(2) Person E berechnet den RSA-Modul $n = pq$.

(3) Person E berechnet $\varphi(n) = (p-1)(q-1)$.

(4) Person E wählt zufällig eine Zahl $e \in \mathbb{N}$ mit $1 < e < \varphi(n)$und $\mathrm{ggT}(e, \varphi(n)) = 1$.

(5) Person E bestimmt die eindeutig bestimmte Lösung $d \in \mathbb{N}$ mit $1 < d < \varphi(n)$ der Kongruenz

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

Das kann z.B. mit dem erweiterten Euklidischen Algorithmus geschehen.

(6) Person E setzt

$$\textit{öffentlicher Schlüssel} := (n, e), \quad \textit{privater Schlüssel} := (n, d).$$

Den öffentlichen Schlüssel gibt Person E bekannt, den privaten Schlüssel behält sie für sich.

Beispiel 7.2. *Um die Schlüsselerzeugung zu veranschaulichen, schauen wir uns ein Beispiel mit (natürlich für die Praxis viel zu kleinen) $p = 17$, $q = 19$ an. Wir erhalten*

$$n = 17 \cdot 19 = 323, \quad \varphi(n) = (17-1) \cdot (19-1) = 16 \cdot 18 = 288.$$

Wir wählen $e = 95$. Es ist $\mathrm{ggT}(95, 288) = 1 = 32 \cdot 288 - 97 \cdot 95$. *Insbesondere ist* $(-97) \cdot 95 \equiv 1 \pmod{288}$ *und deshalb* $191 \cdot 95 \equiv 1 \pmod{288}$. *Somit ist $d = 191$. Der öffentliche Schlüssel ist durch* $(323, 95)$, *der private Schlüssel durch* $(323, 191)$ *gegeben.*

Ist der öffentliche Schlüssel durch (n, e) gegeben, so geht das weitere Verfahren davon aus, dass die zu übermittelnde Nachricht als eine Folge von Elementen aus $\mathbb{Z}/n\mathbb{Z}$ vorliegt. Wie man eine Umwandlung von üblichen Nachrichten (etwa Text) in eine Folge von Elementen von $\mathbb{Z}/n\mathbb{Z}$ und zurück vornimmt, werden wir an dieser Stelle nicht behandeln (vgl. Übungen). Es sollte jedoch klar sein, dass man auch hier geschickt vorgehen muss, sonst ist das ganze Verfahren angreifbar.

Algorithmus 7.3 (Verschlüsselung mit dem RSA-Verfahren)**.** *Person A möchte eine Nachricht verschlüsselt an Person E senden.*

(1) Person A besorgt sich den öffentlichen Schlüssel (n, e) von Person E.

(2) Person A schreibt ihre Nachricht als Folge von Elementen $\overline{x_1}, \ldots, \overline{x_r} \in \mathbb{Z}/n\mathbb{Z}$.

(3) Mit Hilfe der Verschlüsselungsfunktion

$$V : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \overline{x} \mapsto \overline{x}^e$$

verschlüsselt Person A die Nachricht zu $V(\overline{x_1}), \ldots, V(\overline{x_r})$.

(4) Person A übermittelt $V(\overline{x_1}), \ldots, V(\overline{x_r})$.

Algorithmus 7.4 (Entschlüsselung mit dem RSA-Verfahren)**.** *Person E möchte eine empfangene Nachricht entschlüsseln.*

(1) Person E empfängt eine Folge von Elementen $\overline{y_1}, \ldots, \overline{y_r}$ aus $\mathbb{Z}/n\mathbb{Z}$ als verschlüsselte Nachricht.

(2) Mit Hilfe des privaten Schlüssels (n, d) und der Entschlüsselungsfunktion

$$E : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \overline{y} \mapsto \overline{y}^d$$

entschlüsselt Person E die Nachricht als $E(\overline{y_1}), \ldots, E(\overline{y_r})$.

Wir müssen uns an dieser Stelle überlegen, dass die Entschlüsselung tatsächlich funktioniert, d.h. wir müsen zeigen, dass für alle $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ tatsächlich $E(V(\overline{x})) = \overline{x}$ ist. Dies folgt jedoch recht schnell aus der folgenen Überlegung:

Proposition 7.5. *Es sei $n \in \mathbb{N}$ quadratfrei, es sei $k \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann gilt:*

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

Beweis. Sei $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Dann ist

$$\varphi(n) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1).$$

Sei $i \in \{1, \ldots, r\}$. Falls $p_i \nmid a$ gilt, so ist $a^{p_i - 1} \equiv 1 \pmod{p_i}$ und deshalb $a^{k\varphi(n)} \equiv 1 \pmod{p_i}$. Das liefert $a^{k\varphi(n)+1} \equiv a \pmod{p_i}$. Gilt $p_i \mid a$, so ist offenbar $a^{k\varphi(n)+1} \equiv 0 \equiv a \pmod{p_i}$. Somit ergibt sich $a^{k\varphi(n)+1} \equiv a \pmod{p_1 \cdot \ldots \cdot p_r}$ und damit die Behauptung. □

Es ist nun $E(V(\overline{x})) = E(\overline{x}^e) = \overline{x}^{ed}$. Nach Konstruktion von e, d ist $ed \equiv 1 \pmod{\varphi(n)}$. Wegen $ed > 1$ existiert also ein $k \in \mathbb{N}$, so dass $ed = k\varphi(n) + 1$ ist. Es ergibt sich

$$E(V(\overline{x})) = \overline{x}^{ed} = \overline{x}^{k\varphi(n)+1} = \overline{x}$$

nach der obigen Bemerkung. Damit ist gezeigt, dass das RSA-Verfahren korrekt arbeitet.

Wieso sieht man das RSA-Verfahren als sicher an? Das „naive“ Argument dazu könnte wohl wie folgt lauten: Um zu entschlüsseln, muß man den privaten Schlüssel (n, d) aus dem öffentlichen Schlüssel (n, e) bestimmen. Dazu muß man die Kongruenz $ed \equiv 1 \pmod{\varphi(n)}$ lösen. Dafür benötigt man $\varphi(n) = (p-1) \cdot (q-1)$, und dafür benötigt man wiederum p, q, also die Primfaktoren von n. Für große Zahlen n ist die Faktorisierung jedoch mit den heute gängigen Verfahren praktisch nicht durchführbar. Leider ist dieses naive Argument nicht wirklich tragfähig, denn es könnte ja andere Möglichkeiten geben, den privaten Schlüssel aus dem öffentlichen Schlüssel zu bestimmen, oder vielleicht kommt man auch ohne Kenntnis des privaten Schlüssels zum Ziel der Entschlüsselung. Aus diesem Grund wollen wir das an dieser Stelle doch nochmal ein klein wenig differenzierter anschauen. Für eine wirklich ernsthafte Betrachtung sei jedoch auf die entsprechende Literatur aus der Kryptographie verwiesen. Wir betrachten im weiteren Verlauf die folgenden Probleme:

- *RSA*: Gegeben ist der öffentliche Schlüssel (n, e) sowie eine verschlüsselte Nachricht $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$. Gesucht wird die Ausgangsnachricht, d.h. ein $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ mit $V(\overline{x}) = \overline{x}^e = \overline{y}$.
- *RSA-Schlüssel*: Gegeben ist der öffentliche Schlüssel (n, e). Gesucht wird der private Schüssel (n, d), d.h. dasjenige $d \in \mathbb{N}$ mit $1 < d < \varphi(n)$ und $ed \equiv 1 \pmod{\varphi(n)}$.
- *Faktorisierung*: Gegeben ist eine Zahl $n \in \mathbb{N}$, welche genau zwei Primfaktoren p, q hat. Gesucht sind p und q.

Wir wollen diese Probleme von ihrer Schwierigkeit her vergleichen. Im Folgenden bedeute Problem A $\underset{p}{\leq}$ Problem B, dass nach Lösung von Problem B das Problem A durch einen Algorithmus von polynomialer Laufzeit gelöst werden kann. Anschaulich heißt dass in etwa, dass Problem A leichter als oder gleichschwer wie Problem B ist. Problem A $\underset{p}{=}$ Problem B stehe für Problem A $\underset{p}{\leq}$ Problem B und Problem B $\underset{p}{\leq}$ Problem A. Offenbar gilt

$$\textit{RSA} \underset{p}{\leq} \textit{RSA-Schlüssel} \underset{p}{\leq} \textit{Faktorisierung},$$

denn: Ist die Faktorisierung von n bekannt, also Primzahlen p, q mit $n = pq$, kann man $\varphi(n) = (p-1) \cdot (q-1)$ berechnen. Über den erweiterten Euklidischen Algorithmus bestimmt man dann (n, d) aus (n, e), d.h. man kann RSA-Schlüssel lösen. Das liefert $\overline{x} = E(\overline{y}) = \overline{y}^d$, d.h. die Lösung von RSA. Man kann sogar zeigen:

$$\textit{RSA-Schlüssel} \underset{p}{=} \textit{Faktorisierung}$$

Momentan ist kein effizienter Algorithmus bekannt, der das Faktorisierungsproblem löst. Dasselbe gilt somit auch für *RSA-Schlüssel*. Es ist allerdings unbekannt, ob *RSA*$\underset{p}{=}$*RSA-Schlüssel* ist. Es könnte also effiziente Möglichkeiten geben, Nachrichten zu entschlüsseln, ohne den privaten Schlüssel zu finden. Da das Verfahren in der realen Welt auf real existierenden Computern durchgeführt wird, gibt es auch darüber hinaus eine nicht unbeträchtliche Zahl von Angriffsmöglichkeiten auf das RSA-Verfahren.

KAPITEL II

Das Quadratische Reziprozitätsgesetz und seine Anwendungen

§8 Das Quadratische Reziprozitätsgesetz

Definition 8.1. *Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$. Die Zahl a (bzw. die Restklasse $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$) heißt ein **quadratischer Rest** modulo p, falls $p \nmid a$ gilt und es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{p}$ gibt. Die Zahl a (bzw. die Restklasse $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$) heißt ein **quadratischer Nichtrest** modulo p, falls $p \nmid a$ gilt und es kein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{p}$ gibt. Wir setzen*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest modulo } p \\ 0 & \text{falls } p|a \\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p \end{cases}$$

*$\left(\frac{\cdot}{p}\right)$ heißt das **Legendre-Symbol** modulo p.*

Offenbar hängt das Legendre-Symbol $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab.

Beispiel 8.2. *In $(\mathbb{Z}/5\mathbb{Z})^\times$ ist $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{4}$ und $\overline{4}^2 = \overline{1}$. Dementsprechend erhalten wir als*

- *quadratische Reste modulo 5: $\overline{1}, \overline{4}$*
- *quadratische Nichtreste modulo 5: $\overline{2}, \overline{3}$.*

Für $a \in \mathbb{Z}$ ist also

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & \text{falls } a \equiv 1 \pmod 5 \text{ oder } a \equiv 4 \pmod 5 \\ 0 & \text{falls } a \equiv 0 \pmod 5 \\ -1 & \text{falls } a \equiv 2 \pmod 5 \text{ oder } a \equiv 3 \pmod 5. \end{cases}$$

Proposition 8.3. *Es sei p eine ungerade Primzahl, es sei w eine primitive Wurzel modulo p, und es sei $r \in \mathbb{N}_0$. Dann gilt:*

$$\left(\frac{w^r}{p}\right) = (-1)^r.$$

Beweis. Die Behauptung ist offenbar äquivalent zur Aussage, dass w^r genau dann quadratischer Rest modulo p ist, wenn $2|r$ gilt. Dies zeigen wir im Folgenden.

„$\Longrightarrow$“: Sei w^r quadratischer Rest modulo p. Dann gibt es ein $x \in \mathbb{Z}$ mit $\overline{w}^r = \overline{x}^2$ in $\mathbb{Z}/p\mathbb{Z}$. Da w eine primitive Wurzel modulo p ist, existiert ein $n \in \mathbb{N}_0$ mit $\overline{x} = \overline{w}^n$. Wir erhalten $\overline{w}^r = \overline{w}^{2n}$ und somit $\overline{w}^{r-2n} = \overline{1}$. Aus 5.7 ergibt sich $p-1 = \mathrm{ord}(\overline{w})|(r-2n)$. Wegen $2|(p-1)$ folgt $2|(r-2n)$ und somit $2|r$.

„$\Longleftarrow$“: Es gelte $2|r$. Dann gibt es ein $q \in \mathbb{N}_0$ mit $r = 2q$. Das liefert $\overline{w}^r = (\overline{w}^q)^2$, weswegen $\overline{w}^r$ ein quadratischer Rest modulo p ist. □

Es ist $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{w}, \ldots, \overline{w}^{p-2}\}$. In dieser Darstellung sind die quadratischen Reste modulo p also genau diejenigen Restklassen mit geradem Exponenten, die quadratischen Nichtreste diejenigen mit ungeradem Exponenten.

Satz 8.4. *Es sei p eine ungerade Primzahl, und es seien $a, b \in \mathbb{Z}$. Dann gilt:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Insbesondere induziert das Legendre-Symbol einen Gruppenhomomorphismus

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad \overline{a} \mapsto \left(\frac{a}{p}\right).$$

Beweis. Da p eine Primzahl ist, gilt die Äquivalenz $p|ab \iff p|a$ oder $p|b$. Damit ist die linke Seite genau dann Null, wenn die rechte Seite Null ist. Im Folgenden seien a, b und somit auch ab nicht durch p teilbar. Sei w eine primitive Wurzel modulo p. Dann existieren $r, s \in \mathbb{N}_0$ mit $\overline{a} = \overline{w}^r$ und $\overline{b} = \overline{w}^s$. Es ergibt sich

$$\left(\frac{ab}{p}\right) = \left(\frac{w^{r+s}}{p}\right) = (-1)^{r+s} = (-1)^r(-1)^s = \left(\frac{w^r}{p}\right)\left(\frac{w^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Satz 8.5 (Satz von Euler)**.** *Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$. Dann gilt:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Beweis. Falls $p|a$ gilt, so ist

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Im Folgenden gelte $p \nmid a$. Aufgrund des Kleinen Satzes von Fermat erhalten wir in $\mathbb{F}_p$ die Gleichung

$$(\overline{a}^{\frac{p-1}{2}})^2 = \overline{a}^{p-1} = \overline{1}.$$

Das Polynom $X^2 - \overline{1} \in \mathbb{F}_p[X]$ hat wegen 5.22 höchstens zwei Nullstellen. Daher sind $\overline{1}, \overline{-1}$ die einzigen Nullstellen dieses Polynoms. Somit ist $\overline{a}^{\frac{p-1}{2}} \in \{\overline{1}, \overline{-1}\}$. Zu zeigen ist damit die folgende Aussage:

$$\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

„$\Longrightarrow$“: Sei $\left(\frac{a}{p}\right) = 1$. Dann gibt es ein $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $\overline{a} = \overline{x}^2$, woraus wiederum

$$\overline{a}^{\frac{p-1}{2}} = \overline{x}^{p-1} = \overline{1}$$

folgt.

„$\Longleftarrow$“: Sei $w \in \mathbb{Z}$ eine primitive Wurzel modulo p, und sei $r \in \mathbb{N}_0$ mit $\overline{a} = \overline{w}^r$. Wir erhalten

$$(\overline{w}^r)^{\frac{p-1}{2}} = \overline{a}^{\frac{p-1}{2}} = \overline{1}.$$

Mittels 5.7 ergibt sich $(p-1) | r\frac{p-1}{2}$, weswegen r gerade ist. Somit ist

$$\left(\frac{a}{p}\right) = (-1)^r = 1.$$

□

Wegen $p > 2$ sind die Restklassen von $-1, 0, 1$ modulo p paarweise verschieden. Daher ist das Legendre-Symbol durch seine Restklasse modulo p eindeutig bestimmt.

Proposition 8.6 (Lemma von Gauß)**.** *Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$ mit $p \nmid a$. Wir setzen*

$$H := \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\} \subseteq \mathbb{Z}/p\mathbb{Z}.$$

Es seien $\overline{h_1}, \ldots, \overline{h_{\frac{p-1}{2}}} \in H$ und $\varepsilon_1, \ldots, \varepsilon_{\frac{p-1}{2}} \in \{\pm 1\}$ mit

$$\overline{a} \cdot \overline{1} = \overline{\varepsilon_1} \cdot \overline{h_1}, \ \ldots, \ \overline{a} \cdot \overline{\frac{p-1}{2}} = \overline{\varepsilon_{\frac{p-1}{2}}} \cdot \overline{h_{\frac{p-1}{2}}}.$$

Dann gilt:

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}.$$

Beweis. Die Restklassen $\overline{h_1}, \ldots, \overline{h_{\frac{p-1}{2}}}$ sind paarweise verschieden,

denn: Seien $i, j \in \{1, \ldots, \frac{p-1}{2}\}$ mit $\overline{h_i} = \overline{h_j}$. Dann ist $\overline{h_i}^2 = \overline{h_j}^2$ und deshalb $\overline{a}^2\overline{i}^2 = \overline{a}^2\overline{j}^2$. Das liefert $\overline{i}^2 = \overline{j}^2$ und deshalb $(\overline{i} \cdot \overline{j}^{-1})^2 = \overline{1}$. Da wir in $\mathbb{Z}/p\mathbb{Z}$ rechnen, folgt $\overline{i} \cdot \overline{j}^{-1} \in \{\overline{1}, \overline{-1}\}$ und somit $\overline{i} = \pm\overline{j}$. Wegen $\overline{i}, \overline{j} \in H$ folgt $\overline{i} = \overline{j}$. #

Aufgrund der eben getätigten Überlegung taucht jedes Element aus H genau einmal als ein Element der Form $\overline{h_i}$ auf. Wir erhalten

$$\overline{a}^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} \bar{i} = \prod_{i=1}^{\frac{p-1}{2}} (\overline{a} \cdot \bar{i}) = \prod_{i=1}^{\frac{p-1}{2}} (\overline{\varepsilon_i} \cdot \overline{h_i}) = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}} \prod_{i=1}^{\frac{p-1}{2}} \overline{h_i} = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}} \prod_{i=1}^{\frac{p-1}{2}} \bar{i}$$

und deshalb

$$\overline{a}^{\frac{p-1}{2}} = \overline{\varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}}.$$

Aufgrund von 8.5 ergibt sich

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}} \pmod{p}.$$

Da das Produkt auf der rechten Seite in der Menge $\{\pm 1\}$ liegt, folgt sogar

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}.$$

□

Beispiel 8.7. *Es sei $p = 5$ und $a = 2$. Dann ist $H = \{\overline{1}, \overline{2}\}$. Wir erhalten*

- $\overline{a} \cdot \overline{1} = \overline{2} \cdot \overline{1} = \overline{1} \cdot \overline{2}$, *also ist $\varepsilon_1 = 1$, $\overline{h_1} = \overline{2}$.*
- $\overline{a} \cdot \overline{2} = \overline{2} \cdot \overline{2} = \overline{4} = \overline{-1} = \overline{-1} \cdot \overline{1}$, *also ist $\varepsilon_2 = -1$, $\overline{h_2} = \overline{1}$.*

Es ergibt sich

$$\left(\frac{2}{5}\right) = \varepsilon_1 \cdot \varepsilon_2 = 1 \cdot (-1) = -1.$$

Satz 8.8 (Quadratisches Reziprozitätsgesetz)**.** *Es seien p, q ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Ist also eine der beiden Primzahlen p, q kongruent 1 modulo 4, dann ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Andernfalls ist

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Satz 8.9 (Erster Ergänzungssatz zum QRG)**.** *Es sei p eine ungerade Primzahl. Dann gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Die Zahl -1 ist also genau dann quadratischer Rest modulo p, wenn $p \equiv 1 \pmod{4}$ ist.

Satz 8.10 (Zweiter Ergänzungssatz zum QRG). *Es sei p eine ungerade Primzahl. Dann gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Die Zahl 2 ist also genau dann quadratischer Rest modulo p, wenn $p \equiv \pm 1 \pmod 8$ ist.

Beweis. (von 8.8, 8.9, 8.10) Wir bemerken zunächst, dass der Satz von Euler 8.5 für $a = -1$ den Ersten Ergänzungssatz zum QRG liefert. Im Folgenden sei $a \in \mathbb{Z}$ mit $p \nmid a$. Wir schreiben für $1 \leq i \leq \frac{p-1}{2}$:

$$a \cdot i = \varepsilon_i \cdot h_i + e_i \cdot p$$

mit $h_i \in \{1, \ldots, \frac{p-1}{2}\}$, $\varepsilon_i \in \{\pm 1\}$, $e_i \in \mathbb{Z}$. Sei $i \in \{1, \ldots, \frac{p-1}{2}\}$. Dann ist

$$\varepsilon_i = (-1)^{\left\lfloor \frac{2ai}{p} \right\rfloor},$$

denn:

Fall 1: $\varepsilon_i = 1$**.** Dann ist $ai = h_i + e_i p$ und deshalb

$$\frac{2ai}{p} = \frac{2h_i}{p} + 2e_i.$$

Es ist $0 < \frac{2h_i}{p} < 1$ und somit $\left\lfloor \frac{2ai}{p} \right\rfloor = 2e_i$, insbesondere ist $\left\lfloor \frac{2ai}{p} \right\rfloor$ gerade.

Fall 2: $\varepsilon_i = -1$**.** Dann ist $ai = -h_i + e_i p$ und somit

$$\frac{2ai}{p} = \frac{p - 2h_i}{p} + 2e_i - 1.$$

Wegen $0 < \frac{p-2h_i}{p} < 1$ ist $\left\lfloor \frac{2ai}{p} \right\rfloor = 2e_i - 1$, insbesondere ist $\left\lfloor \frac{2ai}{p} \right\rfloor$ ungerade. #

Aufgrund von 8.6 erhalten wir

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ai}{p} \right\rfloor}.$$

Als zusätzliche Voraussetzung an a fordern wir ab jetzt, dass a ungerade ist. Dann ist $a + p$ gerade, und wir erhalten

$$\left(\frac{2a}{p}\right) = \left(\frac{2a + 2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right).$$

Hierbei haben wir verwendet, dass 4 offensichtlich ein Quadrat modulo p ist. Es ergibt sich

$$\begin{aligned}\left(\frac{2a}{p}\right) &= (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)i}{p} \right\rfloor} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} + i \right\rfloor} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} i + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor} \\ &= (-1)^{\frac{1}{2} \cdot \frac{p-1}{2} \cdot (\frac{p-1}{2}+1)} (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor} \\ &= (-1)^{\frac{p^2-1}{8}} (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor}\end{aligned}$$

Für $a = 1$ ist $\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor = 0$ und deshalb

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

womit wir 8.10 gezeigt haben. Es verbleibt der Beweis von 8.8. Wir bemerken dafür zunächst, dass nach der obigen Rechnung gilt:

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor} = \left(\frac{2}{p}\right)(-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor},$$

woraus sich

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor}$$

ergibt. Diese Beschreibung des Legendre-Symbols werden wir im weiteren Verlauf benutzen, um die gewünschte Identität zu zeigen. Sei q eine ungerade Primzahl. Im Fall $p = q$ ist die Aussage aus 8.8 offensichtlich, denn dann steht auf beiden Seiten 0. Im Folgenden sei $q \neq p$. Wir setzen

$$\ell_1 := \#\{(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} \mid qi > pj\}$$
$$\ell_2 := \#\{(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\} \mid qi < pj\}$$

Wegen $qi \neq pj$ für $(i,j) \in \{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\}$ folgt für festes $i \in \{1,\dots,\frac{p-1}{2}\}$:

$$qi > pj \iff j < \frac{qi}{p} \iff j \leq \left\lfloor \frac{qi}{p} \right\rfloor.$$

Das liefert

$$\ell_1 = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor.$$

Analog ist

$$\ell_2 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor.$$

Außerdem ist

$$\ell_1 + \ell_2 = \#(\{1,\dots,\frac{p-1}{2}\} \times \{1,\dots,\frac{q-1}{2}\}) = \frac{p-1}{2}\frac{q-1}{2}.$$

Wir erhalten

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor}(-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor} = (-1)^{\ell_2+\ell_1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Wegen $\left(\frac{q}{p}\right)^2 = 1$ ergibt sich

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

□

Beispiel 8.11. *Das Reziprozitätsgesetz kann benutzt werden, um Legendre-Symbole auszurechnen: Es soll das Legendre-Symbol* $\left(\frac{273}{307}\right)$ *bestimmt werden. Unter Verwendung von 8.4 erhalten wir*

$$\left(\frac{273}{307}\right) = \left(\frac{3 \cdot 7 \cdot 13}{307}\right) = \left(\frac{3}{307}\right)\left(\frac{7}{307}\right)\left(\frac{13}{307}\right).$$

Wegen $3 \equiv 3 \pmod 4$, $7 \equiv 3 \pmod 4$, $13 \equiv 1 \pmod 4$, $307 \equiv 3 \pmod 4$ *ergibt sich durch Anwendung des QRG:*

$$\left(\frac{273}{307}\right) = (-1)\left(\frac{307}{3}\right)(-1)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right) = \left(\frac{307}{3}\right)\left(\frac{307}{7}\right)\left(\frac{307}{13}\right).$$

Aufgrund von $307 \equiv 1 \pmod 3$, $307 \equiv -1 \pmod 7$, $307 \equiv 8 \pmod{13}$ *erhalten wir*

$$\left(\frac{273}{307}\right) = \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{8}{13}\right)$$

Der erste Faktor ist offenbar 1, *der zweite Faktor ist wegen* $7 \equiv 3 \pmod 4$ *nach 8.9 durch* -1 *gegeben. Somit ist*

$$\left(\frac{273}{307}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)^3 = -\left(\frac{2}{13}\right),$$

wobei wir für die letzte Gleichung verwendet haben, dass das Legendresymbol den Wert 1 *oder* -1 *hat. Aus dem zweiten Ergänzungssatz zum QRG erhalten wir wegen* $13 \equiv 5 \pmod 8$, *dass*

$$\left(\frac{273}{307}\right) = (-1) \cdot (-1) = 1$$

ist.

Eine Verallgemeinerung des Legendre-Symbols ist durch das Jacobi-Symbol gegeben, welches wir im Folgenden studieren werden.

Definition 8.12. *Es sei* $a \in \mathbb{Z}$ *und* $n \in \mathbb{N}$ *ungerade mit Primfaktorzerlegung* $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$. *Wir setzen*

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}.$$

$\left(\frac{\cdot}{n}\right)$ *heißt das* ***Jacobi-Symbol*** *modulo* n.

Ist n eine Primzahl, so stimmen das Jacobi- und das Legendre-Symbol modulo n offenbar überein, unsere Notation ist also konsistent. Ist a ein quadratischer Rest modulo $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$,

so ist a auch quadratischer Rest modulo $p_1, \ldots, p_r$, d.h. $\left(\frac{a}{p_1}\right) = \ldots = \left(\frac{a}{p_r}\right) = 1$. Somit ist dann $\left(\frac{a}{n}\right) = 1$. Die Umkehrung ist jedoch falsch: Es ist etwa

$$\left(\frac{5}{9}\right) = \left(\frac{5}{3^2}\right) = \left(\frac{5}{3}\right)^2 = (-1)^2 = 1,$$

aber 5 ist kein quadratischer Rest modulo 9 (sonst wäre 2 quadratischer Rest modulo 3).
Wir merken an, dass das Jacobi-Symbol offenbar multiplikativ in beiden Argumenten ist. Darüber hinaus ist genau dann $\left(\frac{a}{n}\right) = 0$, wenn a und n nicht teilerfremd sind.

Wir wollen im Folgenden ein Reziprozitätsgesetz für das Jacobi-Symbol zeigen. Wir starten dazu mit einer Vorbemerkung.

Proposition 8.13. *Es seien $n_1, n_2 \in \mathbb{N}$ ungerade. Dann gilt:*

(a)
$$\frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \equiv \frac{n_1 n_2 - 1}{2} \pmod 2,$$

(b)
$$\frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \equiv \frac{(n_1 n_2)^2 - 1}{8} \pmod 2.$$

Beweis. (a) Es ist $n_1 - 1 \equiv 0 \equiv n_2 - 1 \pmod 2$, und deshalb ist $(n_1 - 1)(n_2 - 1) \equiv 0 \pmod 4$. Das liefert $n_1 n_2 - n_1 - n_2 + 1 \equiv 0 \pmod 4$ und somit $n_1 n_2 - 1 \equiv n_1 - 1 + n_2 - 1 \pmod 4$. Wir erhalten
$$\frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \equiv \frac{n_1 n_2 - 1}{2} \pmod 2.$$
(b) Es ist $n_1 - 1 \equiv n_1 + 1 \equiv n_2 - 1 \equiv n_2 + 1 \pmod 2$. Somit ist

$$(n_1^2 - 1)(n_2^2 - 1) = (n_1 - 1)(n_1 + 1)(n_2 - 1)(n_2 + 1) \equiv 0 \pmod{16}.$$

Es ergibt sich
$$n_1^2 n_2^2 - 1 \equiv n_1^2 - 1 + n_2^2 - 1 \pmod{16}$$
und schließlich
$$\frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \equiv \frac{(n_1 n_2)^2 - 1}{8} \pmod 2.$$

□

Satz 8.14 (Reziprozitätsgesetz für das Jacobi-Symbol)**.** *Es seien m, n ungerade natürliche Zahlen mit $m, n \geq 3$. Dann gilt:*

(a)
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

(b)

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

(c)

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$$

Beweis. Die Primfaktorzerlegungen von n bzw. m seien gegeben durch $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, $m = q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}$.
(a) Es ist

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{-1}{p_r}\right)^{e_r} = (-1)^{\frac{p_1-1}{2}e_1} \cdot \ldots \cdot (-1)^{\frac{p_r-1}{2}e_r} \\ &\overset{8.13}{=} (-1)^{\frac{p_1^{e_1}-1}{2}} \cdot \ldots \cdot (-1)^{\frac{p_r^{e_r}-1}{2}} \overset{8.13}{=} (-1)^{\frac{p_1^{e_1}\cdot\ldots\cdot p_r^{e_r}-1}{2}} \\ &= (-1)^{\frac{n-1}{2}}.\end{aligned}$$

(b) Es ist

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{2}{p_r}\right)^{e_r} = (-1)^{\frac{p_1^2-1}{8}e_1} \cdot \ldots \cdot (-1)^{\frac{p_r^2-1}{8}e_r} \\ &\overset{8.13}{=} (-1)^{\frac{p_1^{2e_1}-1}{8}} \cdot \ldots \cdot (-1)^{\frac{p_r^{2e_r}-1}{8}} \overset{8.13}{=} (-1)^{\frac{p_1^{2e_1}\cdot\ldots\cdot p_r^{2e_r}-1}{8}} \\ &= (-1)^{\frac{n^2-1}{8}}.\end{aligned}$$

(c) Ist $\mathrm{ggT}(m,n) \neq 1$, dann ist $\left(\frac{m}{n}\right) = 0 = \left(\frac{n}{m}\right)$. Im Folgenden sei $\mathrm{ggT}(m,n) = 1$, d.h. $\{p_1,\ldots,p_r\} \cap \{q_1,\ldots,q_s\} = \varnothing$. Wir erhalten

$$\begin{aligned}\left(\frac{m}{n}\right) &= \left(\frac{m}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{m}{p_r}\right)^{e_r} = \prod_{i,j} \left(\frac{q_i}{p_j}\right)^{f_i e_j} \overset{8.8}{=} \prod_{i,j} ((-1)^{\frac{q_i-1}{2}\frac{p_j-1}{2}} \left(\frac{p_j}{q_i}\right))^{f_i e_j} \\ &\overset{8.13}{=} \prod_{i,j} (-1)^{\frac{q_i^{f_i}-1}{2}\frac{p_j^{e_j}-1}{2}} \left(\frac{p_j}{q_i}\right)^{e_j f_i} \\ &\overset{8.13}{=} (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).\end{aligned}$$

□

Beispiel 8.15. *(vgl. Bsp. 8.11) Wir wollen erneut das Legendre-Symbol $\left(\frac{273}{307}\right)$ berechnen, diesmal unter Verwendung des Reziprozitätsgesetzes für das Jacobi-Symbol. Wegen $273 \equiv 1 \pmod 4$ erhalten wir*

$$\left(\frac{273}{307}\right) \overset{8.14}{=} \left(\frac{307}{273}\right) = \left(\frac{34}{273}\right) = \left(\frac{2}{273}\right)\left(\frac{17}{273}\right).$$

Da $273 \equiv 1 \pmod 8$ ist, liefert der zweite Ergänzungssatz zum QRG

$$\left(\frac{273}{307}\right) = \left(\frac{17}{273}\right).$$

Durch erneute Anwendung des Reziprozitätsgesetzes für das Jacobi-Symbol und Beachtung von $17 \equiv 1 \pmod 4$ *erhalten wir*

$$\left(\frac{273}{307}\right) = \left(\frac{273}{17}\right) = \left(\frac{1}{17}\right) = 1.$$

Im Gegensatz zur Rechnung in Beispiel 8.15 brauchten wir hier nicht die Primfaktorzerlegung von 273 *zu bestimmen.*

§9 Primzahlen mit vorgegebener Restklasse

Proposition 9.1. (a) *Es gibt unendlich viele Primzahlen* p *mit* $p \equiv -1 \pmod 3$.

(b) *Es gibt unendlich viele Primzahlen* p *mit* $p \equiv -1 \pmod 4$.

Beweis. (a) Angenommen, es gibt nur endlich viele Primzahlen p mit $p \equiv -1 \pmod 3$, etwa $p_1, \ldots, p_n$. Wir setzen

$$m := 3p_1 \cdot \ldots \cdot p_n - 1.$$

Dann gilt $3 \nmid m$, $p_1 \nmid m, \ldots, p_n \nmid m$. Somit gilt für jeden Primteiler q von m, dass $q \equiv 1 \pmod 3$ ist. Das liefert $m \equiv 1 \pmod 3$, was ein Widerspruch ist.
(b) Angenommen, es gibt nur endlich viele Primzahlen p mit $p \equiv -1 \pmod 4$, etwa $p_1, \ldots, p_n$. Wir setzen

$$m := 4p_1 \cdot \ldots \cdot p_n - 1.$$

Dann gilt $2 \nmid m$, $p_1 \nmid m, \ldots, p_n \nmid m$. Aus diesem Grund gilt für jeden Primteiler q von m, dass $q \equiv 1 \pmod 4$ ist. Daraus ergibt sich $m \equiv 1 \pmod 4$, was ein Widerspruch ist. □

Proposition 9.2. *Es gibt unendlich viele Primzahlen* p *mit* $p \equiv 1 \pmod 4$.

Beweis. Wir nehmen an, dass es nur endlich viele Primzahlen p mit $p \equiv 1 \pmod 4$ gibt, etwa $p_1, \ldots, p_n$. Wir setzen

$$m := (2p_1 \cdot \ldots \cdot p_n)^2 + 1.$$

Ist q ein Primteiler von m, so ist q ungerade, und es gilt $(2p_1 \cdot \ldots \cdot p_n)^2 \equiv -1 \pmod q$. Somit ist

$$\left(\frac{-1}{q}\right) = 1,$$

was nach dem Ersten Ergänzungssatz zum QRG $q \equiv 1 \pmod 4$ zur Folge hat. Insbesondere ist $q \in \{p_1, \ldots, p_n\}$. Wegen $q|m$ erhalten wir $q|1$, was ein Widerspruch ist. □

Satz 9.3. *Es sei* $a \in \mathbb{Z}$, $a \neq 0$. *Dann gibt es unendlich viele ungerade Primzahlen* p, *so dass* $\left(\frac{a}{p}\right) = 1$ *ist.*

Beweis. Wir nehmen an, dass es nur endlich viele Primzahlen p gibt, so dass $\left(\frac{a}{p}\right) = 1$ ist, etwa $p_1, \ldots, p_n$. Wir wählen $A \in \mathbb{Z}$ so, dass gilt:

- $\mathrm{ggT}(a, A) = 1$,
- A gerade $\iff$ a ungerade,
- $N := (p_1 \cdot \ldots \cdot p_n A)^2 - a > 1$.

Sei q ein Primteiler von N. Da N ungerade ist, ist q ungerade, und wegen $p_i \nmid a$ für $i = 1, \ldots, n$ ist $q \neq p_1, \ldots, p_n$.

Fall 1: $q|a$**.** Es ergibt sich $q|(N + a) = (p_1 \cdot \ldots \cdot p_n A)^2$ und deshalb $q|A^2$. Da q eine Primzahl ist, folgt $q|A$, im Widerspruch zu $\mathrm{ggT}(a, A) = 1$.

Fall 2: $q \nmid a$**.** Aufgrund von $(p_1 \cdot \ldots \cdot p_n A)^2 \equiv a \pmod{q}$ folgt $\left(\frac{a}{q}\right) = 1$. Somit ist $q \in \{p_1, \ldots, p_n\}$, was ein Widerspruch ist. □

Proposition 9.4. *Es gibt unendlich viele Primzahlen p mit $p \equiv 1 \pmod 3$.*

Beweis. Sei p eine ungerade Primzahl. Dann ist

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Insbesondere gilt für ungerade Primzahlen p die Äquivalenz

$$p \equiv 1 \pmod 3 \iff \left(\frac{p}{3}\right) = 1 \iff \left(\frac{-3}{p}\right) = 1.$$

Aufgrund von 9.3 gibt es unendlich viele Primzahlen p mit $\left(\frac{-3}{p}\right) = 1$. Das liefert die Behauptung. □

Satz 9.5. *Es sei $a \in \mathbb{Z}$ kein Quadrat. Dann gibt es unendlich viele Primzahlen p, so dass $\left(\frac{a}{p}\right) = -1$ ist.*

Beweis. **Fall 1:** $a = -1$**.** Nach dem Ersten Ergänzungssatz zum QRG ist

$$\left(\frac{-1}{p}\right) = -1 \iff p \equiv -1 \pmod 4.$$

Aufgrund von 9.1 gibt es unendlich viele Primzahlen p mit $p \equiv -1 \pmod 4$, und damit ergibt sich die Behauptung.

Fall 2: $a = 2$**.** Nach dem Zweiten Ergänzungssatz zum QRG ist

$$\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod 8.$$

Wir nehmen an, dass es nur endlich viele Primzahlen p mit $p \equiv \pm 3 \pmod 8$ gibt, etwa $p_1 = 3, p_2, \ldots, p_n$. Wir setzen

$$N := 8p_2 \cdot \ldots \cdot p_n + 3.$$

Die Zahl N ist größer als 1, ungerade und durch keine der Primzahlen $p_1, \ldots, p_n$ teilbar. Somit hat N nur Primteiler, welche $\equiv \pm 1 \pmod 8$ sind. Das impliziert jedoch $N \equiv \pm 1 \pmod 8$, was ein Widerspruch zu $N \equiv 3 \pmod 8$ ist. Somit gibt es unendlich viele Primzahlen p mit $p \equiv 3 \pmod 8$, was die Behauptung liefert.

Fall 3: $a = -2$**.** Mit den Ergänzungssätzen zum QRG gilt

$$\begin{aligned}\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = -1 \quad &\Longleftrightarrow \quad (p \equiv 1 \pmod 4 \text{ und } p \equiv \pm 3 \pmod 8)\\ &\quad \text{oder } (p \equiv 3 \pmod 4 \text{ und } p \equiv \pm 1 \pmod 8)\\ &\Longleftrightarrow \quad p \equiv 5 \pmod 8 \text{ oder } p \equiv 7 \pmod 8.\end{aligned}$$

Wir nehmen an, dass es nur endlich viele Primzahlen p mit $p \equiv 5 \pmod 8$ oder $p \equiv 7 \pmod 8$ gibt, etwa $p_1 = 5, p_2, \ldots, p_n$. Wir setzen

$$N := 8p_2 \ldots p_n + 5.$$

Die Zahl N ist größer als 1, ungerade und durch keine der Primzahlen $p_1, \ldots, p_n$ teilbar. Aufgrunddessen hat N nur Primteiler, welche $\equiv 1 \pmod 8$ oder $\equiv 3 \pmod 8$ sind. Damit gilt $N \equiv 1 \pmod 8$ oder $N \equiv 3 \pmod 8$, im Widerspruch zu $N \equiv 5 \pmod 8$. Damit gibt es unendlich viele Primzahlen p mit $p \equiv 3 \pmod 8$ oder $p \equiv 7 \pmod 8$, was die Behauptung liefert.

Fall 4: $a \neq -1, \pm 2$**.** Da sich $\left(\frac{a}{p}\right)$ sich bei Abänderung von a um Quadrate höchstens bei endlich vielen Primzahlen p ändert (nämlich bei den Primteilern von a), können wir ohne Einschränkung annehmen:

$$a = (-1)^{\varepsilon} 2^e q_1 \cdot \ldots \cdot q_n$$

mit paarweise verschiedenen ungeraden Primzahlen $q_1, \ldots, q_n$, $n \geq 1$, sowie $e, \varepsilon \in \{0, 1\}$. Wir nehmen an, dass es nur endlich viele Primzahlen p mit $\left(\frac{a}{p}\right) = -1$ gibt, etwa $p_1, \ldots, p_m$. Insbesondere ist dann $\{q_1, \ldots, q_n\} \cap \{p_1, \ldots, p_m\} = \varnothing$. Sei $\alpha \in \mathbb{Z}$ ein quadratischer Nichtrest modulo q_n. Nach dem Chinesischen Resatz existiert ein $N \in \mathbb{N}$ mit

$$\begin{aligned}&N \equiv 1 \pmod 8,\ N \equiv 1 \pmod{p_1}, \ldots,\ N \equiv 1 \pmod{p_m}\\ &N \equiv 1 \pmod{q_1}, \ldots,\ N \equiv 1 \pmod{q_{n-1}},\ N \equiv \alpha \pmod{q_n}.\end{aligned}$$

Wir schreiben N in der Form $N = l_1 \cdot \ldots \cdot l_r$ mit ungeraden, nicht notwendig paarweise verschiedenen Primzahlen $l_1, \ldots, l_r$. Offenbar ist $\{l_1, \ldots, l_r\} \cap \{2, p_1, \ldots, p_m, q_1, \ldots, q_n\} = \varnothing$. Unter Verwendung von $N \equiv 1 \pmod 8$ erhalten wir aus 8.14:

$$\begin{aligned}\prod_{i=1}^{r}\left(\frac{a}{l_i}\right) = \left(\frac{a}{N}\right) &= \left(\frac{-1}{N}\right)^{\varepsilon}\left(\frac{2}{N}\right)^{e}\left(\frac{q_1 \cdot \ldots \cdot q_n}{N}\right) = (-1)^{\frac{N-1}{2}\varepsilon}(-1)^{\frac{N^2-1}{8}e}\left(\frac{N}{q_1 \cdot \ldots \cdot q_n}\right)\\ &= \left(\frac{N}{q_1}\right) \cdot \ldots \cdot \left(\frac{N}{q_n}\right) = \left(\frac{1}{q_n}\right) \cdot \ldots \cdot \left(\frac{1}{q_{n-1}}\right)\left(\frac{\alpha}{q_n}\right) = \left(\frac{\alpha}{q_n}\right) = -1\end{aligned}$$

Aus diesem Grund existiert ein $i \in \{1, \ldots, r\}$ mit $\left(\frac{a}{l_i}\right) = -1$. Wegen $l_i \notin \{p_1, \ldots, p_m\}$ ist das ein Widerspruch. □

Die in diesem Abschnitt bewiesenen Sätze über Primzahlen mit vorgegebener Restklasse sind Spezialfälle des Satzes von Dirichlet über Primzahlen in arithmetischen Progressionen: Sind $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$, so gibt es unendlich viele Primzahlen p mit $p \equiv a \pmod{n}$.

§10 Summen von Quadraten

In diesem Abschnitt wollen wir uns mit der Frage beschäftigen, welche natürlichen Zahlen sich als Summe von zwei bzw. vier Quadratzahlen schreiben lassen.

Beispiel 10.1. *Es ist* $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 1^2 + 2^2$, *während sich die Zahl* 3 *nicht als Summe von zwei Quadraten ganzer Zahlen schreiben lässt.*

Proposition 10.2 (Lemma von Thue)**.** *Es sei p eine Primzahl, und es seien $e, f \in \mathbb{N}$ mit $ef > p$. Dann gilt: Für jedes $r \in \mathbb{Z}$ gibt es $x, y \in \mathbb{Z}$ mit $0 \leq x < e$, $1 \leq y < f$, $p \nmid y$ und*

$$r \equiv \pm\frac{x}{y} \pmod{p}.$$

Beweis. Sei $r \in \mathbb{Z}$.

Fall 1: $e \geq p$**.** Wir setzen $y := 1$, und x sei der Rest, den r bei Division durch p lässt. Dann ist $r \equiv x \equiv \frac{x}{y} \pmod{p}$.

Fall 2: $f \geq p$**.** Gilt $p|r$, so setzen wir $x := 0$, $y := 1$. Dann ist $r \equiv 0 \equiv \frac{x}{y} \pmod{p}$. Gilt $p \nmid r$, so setzen wir $x := 1$, und y sei ein Vertreter aus $\{1, \ldots, p-1\}$ der Restklasse $\overline{r}^{-1}$. Dann ist $r \equiv \frac{1}{\overline{r}} \equiv \frac{x}{y} \pmod{p}$.

Fall 3: $e, f < p$**.** Wir betrachten die Menge

$$M := \{1, \ldots, e\} \times \{1, \ldots, f\}.$$

Es ist $\#M = ef > p$, deswegen gibt es $(x_1, y_1) \neq (x_2, y_2) \in M$ mit

$$y_1 r - x_1 \equiv y_2 r - x_2 \pmod{p}.$$

Wäre $y_1 \equiv y_2 \pmod{p}$, so folgte $x_1 - x_2 \equiv r(y_1 - y_2) \equiv 0 \pmod{p}$. Wegen $e, f < p$ ergäbe sich dann $x_1 = x_2$ und $y_1 = y_2$, was ein Widerspruch ist. Also ist $y_1 - y_2 \not\equiv 0 \pmod{p}$ und deshalb

$$r \equiv \frac{x_1 - x_2}{y_1 - y_2} \equiv \pm\frac{|x_1 - x_2|}{|y_1 - y_2|} \pmod{p}.$$

Setzen wir $x := |x_1 - x_2|$ und $y := |y_1 - y_2|$, so folgt die Behauptung. □

Satz 10.3 (Euler)**.** *Es sei p eine ungerade Primzahl. Dann sind äquivalent:*

(i) *Die Zahl p lässt sich als Summe von zwei Quadraten schreiben, d.h. es existieren $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$.*

(ii) $p \equiv 1 \pmod 4$.

Beweis. „(i)$\Longrightarrow$(ii)“: Ist $p = x^2 + y^2$, dann ist $p \equiv x^2 + y^2 \pmod 4$. Wegen $x^2 \equiv 0, 1 \pmod 4$ und $y^2 \equiv 0, 1 \pmod 4$ folgt $p \equiv 0, 1, 2 \pmod 4$. Da p eine ungerade Primzahl ist, ergibt sich $p \equiv 1 \pmod 4$.

„(ii)$\Longrightarrow$(i)“: Wegen $p \equiv 1 \pmod 4$ ist -1 quadratischer Rest modulo p. Somit gibt es ein $r \in \mathbb{Z}$ mit $r^2 \equiv -1 \pmod p$. Wir setzen

$$e := f := \lfloor \sqrt{p} \rfloor + 1.$$

Offenbar ist $ef > p$. Aufgrund von 10.2 existieren $x, y \in \mathbb{Z}$ mit $0 \leq x < e$, $1 \leq y < f$, $p \nmid y$ und

$$r \equiv \pm \frac{x}{y} \pmod p.$$

Das liefert

$$-1 \equiv r^2 \equiv \frac{x^2}{y^2} \pmod p$$

und deshalb $x^2 + y^2 \equiv 0 \pmod p$. Aufgrund von $x < e = \lfloor \sqrt{p} \rfloor + 1$ folgt $x < \sqrt{p}$, also $x^2 < p$. Analog ist $y^2 < p$. Wegen $0 < x^2 + y^2 < 2p$ folgt $x^2 + y^2 = p$. □

Satz 10.4. *Es sei $n \in \mathbb{N}$. Dann sind äquivalent:*

(i) *Die Zahl n lässt sich als Summe von zwei Quadraten schreiben.*

(ii) *In der Primfaktorzerlegung von n kommen die Primzahlen p mit $p \equiv 3 \pmod 4$ nur mit geradem Exponenten vor.*

Beweis. „(i)$\Longrightarrow$(ii)“: Diese Implikation zeigen wir indirekt. Wir gehen davon aus, dass (ii) verletzt ist, und dass $n = x^2 + y^2$ für geeignete $x, y \in \mathbb{Z}$ ist. Insbesondere gibt es eine Primzahl p mit $p \equiv 3 \pmod 4$, so dass $n = mp^{2k+1}$ mit $p \nmid m$ ist. Aus $x^2 + y^2 = mp^{2k+1}$ ergibt sich $x^2 \equiv -y^2 \pmod p$. Gilt $p|y$, so folgt $p|x^2 = mp^{2k+1} - y^2$, und weil p eine Primzahl ist, folgt $p|x$. Es ergibt sich $p^2|x^2 + y^2 = n$ und

$$\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = \frac{n}{p^2} = mp^{2(k-1)+1}.$$

Wir ersetzen dann x durch $\frac{x}{p}$, y durch $\frac{y}{p}$, n durch $\frac{n}{p^2}$ und k durch $k - 1$. Indem wir dieses Argument gegebenfalls mehrfach anwenden, können wir schließlich erreichen, dass zuätzlich $p \nmid y$ gilt (das Verfahren bricht ab, weil spätestens bei $k = 0$ der Fall $p|y$ zum Widerspruch $p^2|n$ führt). Aus $x^2 \equiv -y^2 \pmod p$ folgt dann

$$\left(\frac{x}{y}\right)^2 \equiv -1 \pmod p,$$

was einen Widerspruch zu $p \equiv 3 \pmod 4$ darstellt.

„(ii)$\Longrightarrow$(i)“: Wir bemerken zunächst, dass sich mit zwei Zahlen $m_1 = a^2 + b^2$, $m_2 = c^2 + d^2$ mit $a, b, c, d \in \mathbb{Z}$ auch deren Produkt $m_1 m_2$ als Summe von zwei Quadraten darstellen lässt:

$$m_1 m_2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Nach Voraussetzung ist

$$n = 2^e p_1^{2f_1} \cdot \ldots \cdot p_r^{2f_r} q_1^{g_1} \cdot \ldots \cdot q_s^{g_s},$$

wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen mit $p_i \equiv 3 \pmod 4$ sind, und $q_1, \ldots, q_s$ sind paarweise verschiedene Primzahlen mit $q_i \equiv 1 \pmod 4$. Wir setzen $n_1 := 2^e q_1^{g_1} \cdot \ldots \cdot q_s^{e_s}$. Wegen $2 = 1^2 + 1^2$ und 10.3, zusammen mit unserer Vorüberlegung, ist $n_1 = a^2 + b^2$ für geeignete $a, b \in \mathbb{Z}$.Wir setzen $n_2 := p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$. Es ergibt sich

$$n = n_1 n_2^2 = (a^2 + b^2) n_2^2 = (n_2 a)^2 + (n_2 b)^2.$$

□

Satz 10.5 (Lagrange). *Jede natürliche Zahl lässt sich als Summe von vier Quadraten schreiben.*

Beweis. Wir bemerken zunächst, dass für $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ die Gleichung

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =& (x_1 y_1 - x_2 y_2 + x_3 y_3 - x_4 y_4)^2 \\ &+ (x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)^2 \\ &+ (x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2)^2 \\ &+ (x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2)^2\end{aligned}$$

gilt. Aufgrunddessen und wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ genügt es zu zeigen, dass sich jede ungerade Primzahl als Summe von vier Quadraten schreiben lässt.
Die Gleichung $x^2 + y^2 \equiv -1 \pmod p$ besitzt eine Lösung,

denn: Es ist

$$x^2 + y^2 \equiv -1 \pmod p \quad \Longleftrightarrow \quad y^2 \equiv -1 - x^2 \pmod p.$$

Wegen 8.3 gibt es (zusammen mit 0) genau $\frac{p+1}{2}$ Quadrate modulo p und genausoviel Restklassen der Form $-1 - x^2$ modulo p. Da es nur $\frac{p-1}{2}$ Nichtquadrate modulo p gibt, ist unter den $\frac{p+1}{2}$ Restklassen der Form $-1 - x^2$ modulo p mindestens ein Quadrat modulo p. Somit existieren $x, y \in \mathbb{Z}$ mit $y^2 \equiv 1 - x^2 \pmod p$. #

Aufgrunddessen besitzt die Gleichung

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 \equiv 0 \pmod p$$

eine Lösung des Typs $(x, y, 1, 0)$ mit $x, y \in \mathbb{Z}$. Hierbei können x, y so gewählt werden, dass $|x|, |y| \leq \frac{p}{2}$ sind. Dann ist

$$x^2 + y^2 + 1^2 + 0^2 \leq \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2.$$

Zusammenfassend stellen wir fest, dass es $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ und $k \in \mathbb{N}$ mit $k < p$ gibt, so dass

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$$

ist. Ist $k = 1$, so sind wir fertig. Ist $k > 1$, so werden wir zeigen, dass man $x_1, \ldots, x_4$ so verändern kann, dass die Gleichung auch mit kleinerem k gilt. Durch endliche Wiederholung dieses Schrittes kann man schließlich $k = 1$ erreichen, was die Behauptung liefert.

Es seien also $k \in \mathbb{N}$ mit $1 < k < p$ und $x_1, \ldots, x_4 \in \mathbb{Z}$ mit

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp.$$

Fall 1: k ist gerade. Dann ist auch $kp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ gerade. Somit ist eine gerade Anzahl der x_i gerade. Wir nummerieren die x_i so um, dass x_1 und x_2 bzw. x_3 und x_4 entweder beide ungerade oder beide gerade sind. Dann ist

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{k}{2}p.$$

Fall 2: k ist ungerade. Wir wählen $y_1, \ldots, y_4 \in \mathbb{Z}$ mit

$$y_1 \equiv -x_1 \pmod{k},\ y_2 \equiv x_2 \pmod{k},\ y_3 \equiv x_3 \pmod{k},\ y_4 \equiv x_4 \pmod{k}$$

und $|y_i| < \frac{k}{2}$ für $i = 1, \ldots, 4$. Es ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\frac{k^2}{4} = k^2.$$

Darüber hinaus ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{k},$$

weswegen ein $\tilde{k} \in \mathbb{N}_0$ mit $0 \leq \tilde{k} < k$ und

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = \tilde{k}k$$

existiert. Es ist $\tilde{k} \neq 0$,

denn: Wir nehmen an, dass $\tilde{k} = 0$ ist. Dann ist $y_1 = y_2 = y_3 = y_4 = 0$, also ist $x_i \equiv 0 \pmod{k}$ für $i = 1, \ldots, 4$. Das liefert $x_i^2 \equiv 0 \pmod{k^2}$ für $i = 1, \ldots, 4$, was

$$0 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv kp \pmod{k^2}$$

zur Folge hat. Das liefert $k|p$, im Widerspruch zu $1 < k < p$. #

Aufgrund unserer Vorüberlegung ist

$$k^2\tilde{k}p = kp\tilde{k}k = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

mit

$$\begin{aligned}
a_1 &= x_1y_1 - x_2y_2 + x_3y_3 - x_4y_4,\\
a_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 + x_2(-x_1) + x_3x_4 - x_4x_3 \equiv 0 \pmod{k},\\
a_3 &= x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2 \equiv x_1x_3 + x_3(-x_1) - x_2x_4 + x_4x_2 \equiv 0 \pmod{k},\\
a_4 &= x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2 \equiv x_1x_4 + x_4(-x_1) + x_2x_3 - x_3x_2 \equiv 0 \pmod{k}.
\end{aligned}$$

Daraus ergibt sich $k^2 \mid (k^2\tilde{k}p - a_2^2 - a_3^2 - a_4^2) = a_1^2$. Wir erhalten

$$\left(\frac{a_1}{k}\right)^2 + \left(\frac{a_2}{k}\right)^2 + \left(\frac{a_3}{k}\right)^2 + \left(\frac{a_4}{k}\right)^2 = \tilde{k}p$$

mit $1 \leq \tilde{k} < k$. □

§11 Primzahltests

In diesem Abschnitt werden wir uns mit effizienten Algorithmen beschäftigen, die testen, ob eine vorgegebene Zahl eine Primzahl ist. Die naive Methode – die Methode der Probedivisionen – geht von der Definition einer Primzahl aus und testet bei Vorgabe einer Zahl n für alle (Prim-) Zahlen $x \leq \sqrt{n}$, ob $x \mid n$ gilt. Es ist offensichtlich, dass diese Methode für große Zahlen n in der Praxis nicht durchführbar ist. Um effizientere Verfahren zu erhalten, benötigen wir geeignete Primzahlkriterien. Um wiederum solche zu erhalten, kann man sich die bisher bewiesenen Sätze für Primzahlen anschauen und fragen, ob sich diese in geeigneter Weise umkehren und zur Charakterisierung von Primzahlen verwenden lassen.

Der erste Satz, mit dessen Umkehrung wir uns beschäftigen werden, ist der Kleine Satz von Fermat: Ist p eine Primzahl, so gilt für alle $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, dass $\overline{a}^{p-1} = \overline{1}$ ist. Kann man diese Eigenschaft zur Charakterisierung von Primzahlen verwenden? Es stellt sich leider heraus, dass dies nicht der Fall ist. Trotzdem ist es von Interesse und für uns auch im weiteren Verlauf von Bedeutung, für welche welche Zahlen die Umkehrung schiefgeht.

Definition 11.1. *Es sei n eine natürliche Zahl mit $n > 1$. Die Zahl n heißt eine **Carmichael-Zahl**, wenn n keine Primzahl ist und für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ die Gleichung $\overline{a}^{n-1} = \overline{1}$ gilt.*

Proposition 11.2. *Es sei $n \in \mathbb{N}$ mit $n > 1$. Dann sind äquivalent:*

(i) *Die Zahl n ist eine Carmichael-Zahl.*

(ii) *Die Zahl n ist von der Form $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$, $r \geq 3$, mit $(p_i - 1) | (n-1)$ für $i = 1, \ldots, r$.*

Beweis. „(i)$\Longrightarrow$(ii)“: Sei n eine Carmichael-Zahl, d.h. es gelte $\overline{a}^{n-1} = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere gilt dann $\mathrm{ord}(\overline{a}) | (n-1)$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Das liefert

$$\exp((\mathbb{Z}/n\mathbb{Z})^\times) = \mathrm{kgV}(\mathrm{ord}(\overline{a})\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times) | (n-1).$$

Wir schreiben n in der Form $n = 2^a p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$, $r \in \mathbb{N}_0$, und $e_1, \ldots, e_r \in \mathbb{N}$, $a \in \mathbb{N}_0$. Dann ist

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p_1^{e_1-1}(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{e_r-1}(p_r-1)\mathbb{Z}, & \text{falls } a = 0,1 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z} \times \mathbb{Z}/p_1^{e_1-1}(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{e_r-1}(p_r-1)\mathbb{Z}, & \text{falls } a \geq 2. \end{cases}$$

Die Zahl n ist ungerade,

denn: Wir nehmen an, dass n gerade ist. Ist $a = 1$, so ist $r \geq 1$, denn $n = 2$ ist keine Carmichael-Zahl. Aufgrund von 6.17 gilt $p_1^{e_1-1}(p_1-1) | \exp((\mathbb{Z}/n\mathbb{Z})^\times)$ und deshalb $p_1^{e_1-1}(p_1-1) \mid (n-1)$. Weil p_1 ungerade ist, folgt, dass n ungerade ist, was ein Widerspruch ist. Ist $a \geq 2$, so ergibt sich mittels 6.17, dass $2 \mid \exp((\mathbb{Z}/n\mathbb{Z})^\times)$ und deshalb $2 \mid (n-1)$ gilt, im Widerspruch dazu, dass n gerade ist. #

Es gilt $e_i = 1$ und $(p_i - 1) \mid (n-1)$ für $i = 1, \ldots, r$,

denn: Sei $i \in \{1, \ldots, r\}$. Aufgrund von 6.17 gilt $p_i^{e_i-1}(p_i-1) \mid (n-1)$. Wäre $e_i > 1$, so folgte $p_i \mid (n-1)$, was wegen $p_i \mid n$ zu $p_i \mid 1$ führen würde. #

Es ist $r \geq 3$,

denn: Da n als Carmichael-Zahl keine Primzahl ist, ist $r \geq 2$. Nehmen wir an, dass $r = 2$ ist, also n von der Form $n = p_1 p_2$ mit ungeraden Primzahlen p_1, p_2, wobei wir ohne Einschränkung $p_1 < p_2$ annehmen. Wie wir uns bereits überlegt haben, gilt $n - 1 \equiv 0 \pmod{p_2 - 1}$. Darüber hinaus ist

$$n - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) + p_1 - 1 \equiv p_1 - 1 \pmod{p_2 - 1}.$$

Das liefert $p_1 - 1 \equiv 0 \pmod{p_2 - 1}$, also $(p_2 - 1) | (p_1 - 1)$, im Widerspruch zu $1 < p_1 - 1 < p_2 - 1$. #

Damit ist die Behauptung gezeigt.

„(ii)$\Longrightarrow$(i)“: Sei $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$, $r \geq 3$, und $(p_i - 1)(n-1)$ für $i = 1, \ldots, r$. Es ergibt sich

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r\mathbb{Z})^\times \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/(p_r-1)\mathbb{Z}.$$

Mittels 6.17 erhalten wir

$$\exp((\mathbb{Z}/n\mathbb{Z})^\times) = \mathrm{kgV}(p_i - 1 \mid i = 1, \ldots, r) \mid (n-1).$$

Das liefert $\overline{a}^{n-1} = \overline{1}$ für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, weswegen n eine Carmichael-Zahl ist. □

Beispiel 11.3. *Die kleinsten Carmichael-Zahlen sind* $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$.

Man kann zeigen, dass es unendlich viele Carmichael-Zahlen gibt (Satz von Alford-Granville-Pomerance, 1994). Genauer gilt: Für $x \gg 0$ ist

$$\#\{n \in \mathbb{N} \mid n \leq x,\ n \text{ ist Carmichael-Zahl}\} > x^{\frac{2}{7}}.$$

Der nächste Satz, mit dessen Umkehrung wir uns beschäftigen, ist der Satz von Euler (Satz 8.5). Wie sich herausstellt, kann dieser zur Charakterisierung von Primzahlen verwendet werden.

Satz 11.4. *Es sei $n \in \mathbb{N}$ ungerade mit $n > 1$. Dann sind äquivalent:*

(i) *n ist eine Primzahl.*

(ii) *Für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ist*
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

Beweis. „(i)$\Longrightarrow$(ii)“: Das ist die Aussage von Satz 8.5.

„(ii)$\Longrightarrow$(i)“: Wir setzen voraus, dass
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$
für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt. Durch Quadrieren ergibt sich, dass für alle $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ die Gleichung
$$\overline{a}^{n-1} = \overline{1}$$
gilt. Somit ist n eine Primzahl oder eine Carmichael-Zahl. Die Zahl n ist jedoch keine Carmichael-Zahl,

denn: Nehmen wir an, dass n eine Carmichael-Zahl ist. Aufgrund von 11.2 ist n dann von der Form
$$n = p_1 \cdot \ldots \cdot p_r$$
mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$, $r \geq 3$. Sei $\alpha \in \mathbb{Z}$ ein Nichtquadrat modulo p_1. Nach dem Chinesischen Restsatz existiert ein $b \in \mathbb{Z}$ mit
$$b \equiv \alpha \pmod{p_1},\ b \equiv 1 \pmod{p_2}, \ldots,\ b \equiv 1 \pmod{p_r}.$$
Es ist
$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right) \cdot \ldots \cdot \left(\frac{b}{p_n}\right) = (-1) \cdot 1 \cdot \ldots \cdot 1 = -1.$$
Nach Konstruktion ist $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, und nach Voraussetzung ist
$$\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \pmod{n}.$$
Das liefert
$$b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$
und somit insbesondere
$$b^{\frac{n-1}{2}} \equiv -1 \pmod{p_2},$$
was im Widerspruch zu
$$b^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$$
steht. #

Damit haben wir gezeigt, dass n eine Primzahl ist. □

Definition 11.5. *Es sei $n \in \mathbb{N}$ ungerade mit $n > 1$, und es sei $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl a heißt ein **Eulerscher Zeuge für die Zerlegbarkeit** von n, wenn*

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}$$

ist. Wir setzen

$$E_n := \{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a \text{ ist ein Eulerscher Zeuge für die Zerlegbarkeit von } n\}.$$

Aufgrund von 11.4 ist eine ungerade Zahl $n \in \mathbb{N}$ mit $n > 1$ genau dann eine Primzahl, wenn $E_n = \varnothing$ ist.

Proposition 11.6. *Es sei $n \in \mathbb{N}$, $n > 1$ ungerade und keine Primzahl. Dann gilt:*

$$|E_n| \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{1}{2}\varphi(n),$$

d.h. mindestens die Hälfte aller Restklassen aus $(\mathbb{Z}/n\mathbb{Z})^\times$ liefert Eulersche Zeugen für die Zerlegbarkeit von n.

Beweis. Da n keine Primzahl ist, existiert nach 11.4 ein $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\overline{a} \in E_n$. Wir setzen

$$\widehat{E_n} := (\mathbb{Z}/n\mathbb{Z})^\times \setminus E_n.$$

und

$$M := \{\overline{a}\overline{b} \mid \overline{b} \in \widehat{E_n}\}.$$

Es ist $\#M = \#\widehat{E_n}$, denn für $\overline{b_1}, \overline{b_2} \in \widehat{E_n}$ gilt $\overline{a}\overline{b_1} = \overline{a}\overline{b_2}$ genau dann, wenn $\overline{b_1} = \overline{b_2}$ ist. Darüber hinaus ist $M \cap \widehat{E_n} = \varnothing$,

denn: Sei $\overline{c} \in M \cap \widehat{E_n}$. Dann ist $\overline{c}$ von der Form $\overline{c} = \overline{a}\overline{b}$ für ein $\overline{b} \in \widehat{E_n}$. Das liefert

$$\overline{a} = \overline{c}\overline{b}^{-1} = \overline{c}\overline{b}^{\varphi(n)-1} = \overline{cb^{\varphi(n)-1}}$$

und deshalb wegen $\overline{c}, \overline{b} \in \widehat{E_n}$

$$\left(\frac{a}{n}\right) = \left(\frac{cb^{\varphi(n)-1}}{n}\right) = \left(\frac{c}{n}\right)\left(\frac{b}{n}\right)^{\varphi(n)-1} \equiv c^{\frac{n-1}{2}}(b^{\frac{n-1}{2}})^{\varphi(n)-1} \equiv (cb^{\varphi(n)-1})^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} \pmod{n},$$

was $a \in \widehat{E_n}$ zur Folge hätte, was ein Widerspruch ist. #

Wir erhalten

$$\#\widehat{E_n} = \frac{1}{2}\#(\widehat{E_n} \cup M) \leq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{1}{2}\varphi(n)$$

und somit

$$\#E_n \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{1}{2}\varphi(n).$$

□

Algorithmus 11.7 (Primzahltest von Solovay-Strassen, 1977)**.** *Es soll getestet werden, ob die ungerade natürliche Zahl $n > 1$ eine Primzahl ist.*

(1) Wähle zufällig Zahlen $a_1, \dots, a_r$ mit $\mathrm{ggT}(a_i, n) = 1$ für $i = 1, \dots, r$.

(2) Bestimme für $i = 1, \dots, r$, ob a_i ein Eulerscher Zeuge für die Zerlegbarkeit von n ist.

(3) Falls eines der a_i ein Eulerscher Zeuge für die Zerlegbarkeit von n ist, so gib aus: „n ist keine Primzahl". Andernfalls gib aus: „n ist vermutlich eine Primzahl".

Ist n keine Primzahl, so gilt für die Wahrscheinlichkeit W, dass die Ausgabe „n ist vermutlich eine Primzahl" lautet, die Abschätzung $W \leq \frac{1}{2^r}$.

Die Korrektheit des Algorithmus, falls die Ausgabe „n ist keine Primzahl" lautet, ergibt sich aus 11.4; die Abschätzung für die Wahrscheinlickeit W folgt unmittelbar aus 11.6.

Bei dem Primzahltest von Solovay-Strassen handelt es sich um einen *probabilistischen* Primzahltest. Für die Praxis ist das durchaus akzeptabel; denn selbst ein deterministischer Primzahltest wird, wenn er auf einem Computer implementiert ist, aufgrund der Möglichkeit von Hardware- und Softwarefehlern eine gewisse Fehlerwahrscheinlichkeit aufweisen. In der Praxis wählt man den Parameter r „hinreichend groß".

Beispiel 11.8. *Es sei $n = 73$. Wir wählen $r = 2$, $a_1 = 3$, $a_2 = 5$. Es ist*

$$a_1^{\frac{n-1}{2}} = 3^{36} \equiv 1 \pmod{73}, \quad \left(\frac{a_1}{n}\right) = \left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1,$$
$$a_2^{\frac{n-1}{2}} = 5^{36} \equiv -1 \pmod{73}, \quad \left(\frac{a_2}{n}\right) = \left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Somit sind $a_1 = 3$, $a_2 = 5$ keine Eulerschen Zeugen für die Zerlegbarkeit von n. Die Ausgabe des Solovay-Strassen-Tests lautet: $n = 73$ ist vermutlich eine Primzahl.

Wir werden als weiteren Algorithmus in diesem Kontext noch den Primzahltest von Miller-Rabin behandeln. Er verwendet ein ähnliches Konzept wie der Algorithmus von Solovay-Strassen.

Definition 11.9. *Es sei $n \in \mathbb{N}$ ungerade mit $n > 1$. Wir schreiben $n - 1 = 2^t u$ mit $t \geq 1$, $2 \nmid u$. Weiterhin sei $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl a heißt ein **Zeuge für die Zerlegbarkeit** von n, wenn gilt:*

$$\overline{a}^u \neq \overline{1} \quad \textit{und} \quad \overline{a}^{2^s u} \neq \overline{-1} \textit{ für alle } s = 0, \dots, t-1.$$

Wir setzen

$$R_n := \{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a \textit{ ist ein Zeuge für die Zerlegbarkeit von } n\}.$$

Proposition 11.10. *Es sei p eine ungerade Primzahl. Dann gilt:*

$$R_p = \varnothing.$$

Beweis. Wir schreiben p in der Form $p-1 = 2^t u$ mit $t \geq 1$, $2 \nmid u$. Wir nehmen an, dass $R_p \neq \varnothing$ ist. Dann gibt es einen Zeugen a für die Zerlegbarkeit von p. Wegen $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ist

$$\overline{1} = \overline{a}^{p-1} = \overline{a}^{2^t u}.$$

Nach Voraussetzung ist $\overline{a}^u \neq \overline{1}$, es existiert also ein maximales Element $s \in \mathbb{N}_0$ mit $0 \leq s < t$, so dass

$$\overline{b} := \overline{a}^{2^s u} \neq \overline{1}$$

ist. Dann ist $\overline{b}^2 = \overline{a}^{2^{s+1}u} = \overline{1}$. Das Polynom $X^2 - \overline{1} \in \mathbb{F}_p[X]$ hat nur die beiden Nullstellen $\overline{\pm 1}$, weswegen $\overline{b} = \overline{-1}$ ist. Das liefert

$$\overline{a}^{2^s u} = \overline{-1},$$

im Widerspruch zu $\overline{a} \in R_p$. □

Satz 11.11. *Es sei $n \in \mathbb{N}$ ungerade mit $n > 1$. Dann gilt:*

$$E_n \subseteq R_n.$$

Beweis. Wir setzen $\widehat{E_n} := (\mathbb{Z}/n\mathbb{Z})^\times \smallsetminus E_n$, $\widehat{R_n} := (\mathbb{Z}/n\mathbb{Z})^\times \smallsetminus R_n$ und zeigen $\widehat{R_n} \subseteq \widehat{E_n}$. Wir schreiben n in der Form $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \in \mathbb{N}$, und wir schreiben $n - 1 = 2^t u$ mit $t, u \in \mathbb{N}$ und $2 \nmid u$. Sei $\overline{a} \in \widehat{R_n}$.

Fall 1: $\overline{a}^u = \overline{1}$. Dann ist

$$\left(\frac{a}{n}\right)^u = \left(\frac{a^u}{n}\right) = \left(\frac{1}{n}\right) = 1.$$

Da u ungerade ist, folgt $\left(\frac{a}{n}\right) = 1$. Ebenso ist

$$\overline{a}^{\frac{n-1}{2}} = \overline{a}^{2^{t-1}u} = (\overline{a}^u)^{2^{t-1}} = \overline{1},$$

weswegen $\overline{a} \in \widehat{E_n}$ ist.

Fall 2: Es gibt ein $s \in \mathbb{N}_0$ mit $0 \leq s < t$ und $\overline{a}^{2^s u} = \overline{-1}$. Sei $i \in \{1, \ldots, r\}$. Wir setzen

$$d_i := \operatorname{ord}_{(\mathbb{Z}/p_i\mathbb{Z})^\times}(a + p_i\mathbb{Z}).$$

Es ist $a^{2^s u} \equiv -1 \pmod{p_i}$, also $a^{2^{s+1}u} \equiv 1 \pmod{p_i}$. Das liefert $d_i \nmid 2^s u$, $d_i | 2^{s+1}u$. Somit ist d_i von der Form $d_i = 2^{s+1}v_i$ für ein $v_i \in \mathbb{Z}$ mit $2 \nmid v_i$. Wegen 5.8 gilt $d_i | (p_i - 1)$ und deshalb $2^{s+1} | (p_i - 1)$. Somit existiert ein $k_i \in \mathbb{N}$ mit $p_i - 1 = 2^{s+1}k_i$, also mit $p_i = 1 + 2^{s+1}k_i$. Es ergibt sich

$$\begin{aligned} n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} &= (1 + 2^{s+1}k_1)^{e_1} \cdot \ldots \cdot (1 + 2^{s+1}k_r)^{e_r} \\ &\equiv (1 + e_1 2^{s+1}k_1) \cdot \ldots \cdot (1 + e_r 2^{s+1}k_r) \pmod{2^{s+2}} \\ &\equiv 1 + 2^{s+1}(e_1k_1 + \ldots + e_rk_r) \pmod{2^{s+2}} \end{aligned}$$

Das liefert

$$2^{t-1}u = \frac{n-1}{2} \equiv 2^s(e_1k_1 + \ldots + e_rk_r) \pmod{2^{s+1}}.$$

und somit

$$2^{t-s-1}u \equiv e_1k_1 + \ldots + e_rk_r \pmod 2.$$

Wir erhalten

$$a^{\frac{n-1}{2}} = a^{2^{t-1}u} = (a^{2^s u})^{2^{t-1-s}} \equiv (-1)^{2^{t-1-s}} \overset{2\nmid u}{=} (-1)^{2^{t-1-s}u} \equiv (-1)^{e_1k_1+\ldots+e_rk_r} \pmod n$$

Andererseits erhalten wir aus $(a^{\frac{d_i}{2}})^2 = a^{d_i} \equiv 1 \pmod{p_i}$, dass $a^{\frac{d_i}{2}} \equiv -1 \pmod{p_i}$ ist. Das impliziert

$$\left(\frac{a}{p_i}\right) \overset{8.5}{\equiv} a^{\frac{p_i-1}{2}} = a^{\frac{d_i}{2}\frac{p_i-1}{d_i}} \equiv (-1)^{\frac{p_i-1}{d_i}} = (-1)^{\frac{p_i-1}{2^{s+1}}v_i} \overset{2\nmid v_i}{=} (-1)^{\frac{p_i-1}{2^{s+1}}} = (-1)^{k_i} \pmod{p_i}.$$

Daraus ergibt sich

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{e_r} = (-1)^{k_1e_1} \cdot \ldots \cdot (-1)^{k_re_r} = (-1)^{e_1k_1+\ldots+e_rk_r} \equiv a^{\frac{n-1}{2}} \pmod n,$$

was $\overline{a} \in \widehat{E_n}$ zur Folge hat. □

Korollar 11.12. *Es sei $n \in \mathbb{N}$ ungerade mit $n > 1$. Dann sind äquivalent:*

(i) *n ist eine Primzahl.*

(ii) *$R_n = \varnothing$.*

Beweis. „(i)$\Longrightarrow$(ii)“ ist die Aussage von 11.10.

„(ii)$\Longrightarrow$(i)“: Ist $R_n = \varnothing$, so ist wegen 11.11 auch $E_n = \varnothing$. Aufgrund von 11.4 ist die Zahl n eine Primzahl. □

Korollar 11.13. *Es sei $n \in \mathbb{N}$, $n > 1$, ungerade und keine Primzahl. Dann gilt:*

$$|R_n| \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{1}{2}\varphi(n),$$

d.h. mindestens die Hälfte aller Restklassen aus $(\mathbb{Z}/n\mathbb{Z})^\times$ liefert Zeugen für die Zerlegbarkeit von n.

Beweis. Die Aussage ergibt sich unmittelbar aus 11.6 und 11.11. □

Tatsächlich gilt sogar eine stärkere Aussage:

Satz 11.14 (Satz von Rabin)**.** *Es sei $n \in \mathbb{N}$, $n \geq 15$ ungerade und keine Primzahl. Dann gilt:*

$$|R_n| \geq \frac{3}{4}\varphi(n).$$

Für den Beweis siehe etwa das Buch von Müller-Stach/Piontkowski.

Algorithmus 11.15 (Primzahltest von Miller-Rabin, 1980)**.** *Es soll getestet werden, ob die ungerade natürliche Zahl $n \geq 15$ eine Primzahl ist.*

(1) Wähle zufällig Zahlen $a_1, \ldots, a_r$ mit $\mathrm{ggT}(a_i, n) = 1$ für $i = 1, \ldots, r$.

(2) Bestimme für $i = 1, \ldots, r$, ob a_i ein Zeuge für die Zerlegbarkeit von n ist.

(3) Falls eines der a_i ein Zeuge für die Zerlegbarkeit von n ist, so gib aus: „n ist keine Primzahl". Andernfalls gib aus: „n ist vermutlich eine Primzahl".

Ist n keine Primzahl, so gilt für die Wahrscheinlichkeit W, dass die Ausgabe „n ist vermutlich eine Primzahl" lautet, die Abschätzung $W \leq \frac{1}{4^r}$.

Die Korrektheit des Algorithmus, falls die Ausgabe „n ist keine Primzahl" lautet, ergibt sich aus 11.12; die Abschätzung für die Wahrscheinlickeit W folgt unmittelbar aus 11.14.

Beispiel 11.16. *Es sei $n = 437$. Wir wählen $a_1 = 2$. Es ist $n - 1 = 436 = 2^2 \cdot 109$, also ist $t = 2$ und $u = 109$. Wir erhalten $a_1^u = 2^{109} \equiv 173 \not\equiv \pm 1 \pmod{437}$, $a_1^{2u} = 2^{2 \cdot 109} \equiv 213 \not\equiv -1 \pmod{437}$, d.h. $a_1 = 2$ ist ein Zeuge für die Zerlegbarkeit von $n = 437$. Der Miller-Rabin-Test liefert: $n = 437$ ist keine Primzahl.*

Für alle natürlichen Zahlen $n < 2.152.302.898.747$, die ungerade und keine Primzahlen sind, ist eine der Zahlen $2, 3, 5, 7, 11$ ein Zeuge für die Zerlegbarkeit von n. Unter Anahme der (unbewiesenen) erweiterten Riemannschen Vermutung kann man zeigen: Ist $n \in \mathbb{N}$, $n > 1$ ungerade und keine Primzahl, dann gibt es einen Zeugen a für die Zerlegbarkeit von n mit $0 < a < 2(\log n)^2$ und a Primzahl (Satz von Ankeny-Montgomery-Bach, 1980-1994). Das liefert einen deterministischen Primzahltest, der in polynomialer Zeit läuft. Im Jahr 2002 haben Agrawal, Kayal und Saxena einen deterministischen Algorithmus gefunden, der ohne Annahme von zusätzlichen Hypothesen in polynomialer Zeit testet, ob eine Zahl eine Primzahl ist. In der Praxis ist dieser jedoch langsamer als der Miller-Rabin-Test.

KAPITEL III

Kettenbrüche und quadratische Zahlkörper

§12 Die Kettenbruchentwicklung reeller Zahlen

Die Darstellung reeller Zahlen im Dezimalsystem ist aus mathematischer Sicht insofern unkanonisch, als das dass die Wahl der Basis 10 hier eingeht. In diesem Abschnitt werden wir die Kettenbruchentwicklung reeller Zahlen behandeln. Diese kommt ohne Basiswahl aus und weist darüber hinaus zahlreiche weitere bemerkenswerte Eigenschaften auf.

Definition 12.1. *Es seien $a_0, \ldots, a_m \in \mathbb{R}$ mit $a_1 \ldots, a_m > 0$. Wir setzen*

$$[a_0, a_1, \ldots, a_m] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}$$

*und nennen das Tupel $((a_0, \ldots, a_m), [a_0, \ldots, a_m])$ einen **endlichen Kettenbruch** mit Wert $[a_0, \ldots, a_m]$. Ist $(a_n)_{n\in\mathbb{N}_0}$ eine Folge reeller Zahlen mit $a_n > 0$ für $n \geq 1$ und existiert der Grenzwert $\lim_{n\to\infty}[a_0, \ldots, a_n]$, dann setzen wir*

$$[a_0, a_1, \ldots] := \lim_{n\to\infty}[a_0, \ldots, a_n]$$

*und nennen das Tupel $((a_n)_{n\in\mathbb{N}_0}, [a_0, a_1, \ldots])$ einen **unendlichen Kettenbruch** mit Wert $[a_0, a_1, \ldots]$. Unter einer **Kettenbruchdarstellung** einer reellen Zahl x verstehen wir einen Kettenbruch, dessen Wert durch x gegeben ist, also einen Kettenbruch der Form $((a_0, \ldots, a_m), x)$ oder $((a_n)_{n\in\mathbb{N}_0}, x)$. Eine solche Kettenbruchdarstellung von x heißt eine **Kettenbruchentwicklung** von x, wenn $a_0 \in \mathbb{Z}$ ist und $a_n \in \mathbb{N}$ für $n \geq 1$, sowie $a_m \neq 1$, falls die Kettenbruchdarstellung endlich ist.*

Die obige Definition des Wertes endlicher Kettenbrüche lässt sich auch induktiv aufschreiben. Es ist dann $[a_0] := a_0$ sowie

$$[a_0, \ldots, a_i, a_{i+1}] := [a_0, \ldots, a_{i-1}, a_i + \frac{1}{a_{i+1}}].$$

Beispiel 12.2. (a) *Es ist*

$$\frac{65}{27} = 2 + \frac{11}{27} = 2 + \frac{1}{\frac{27}{11}} = 2 + \frac{1}{2 + \frac{5}{11}} = 2 + \frac{1}{2 + \frac{1}{\frac{11}{5}}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{5}}} = [2, 2, 2, 5],$$

d.h. $((2, 2, 2, 5), \frac{65}{27})$ *ist eine endliche Kettenbruchentwicklung von* $\frac{65}{27}$.

(b) *Falls der Grenzwert* $\phi = \lim_{n\to\infty}[\underbrace{1, 1, \ldots, 1}_{n-\text{mal}}]$ *existiert, dann ist*

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \ldots}} = 1 + \frac{1}{\phi},$$

d.h. $\phi^2 - \phi - 1 = 0$. *Die einzige positive Lösung dieser Gleichung ist* $\phi = \frac{1+\sqrt{5}}{2}$, *der* Goldene Schnitt. *Somit ist vorbehaltlich der Existenz des obigen Grenzwertes* $([1, 1, \ldots], \phi)$ *eine unendliche Kettenbruchentwicklung des Goldenen Schnittes.*

Ziel dieses Abschnittes wird es sein, zu zeigen, dass jede reelle Zahl eine eindeutig bestimmte Kettenbruchentwicklung hat. Im Folgenden geben wir den Kettenbruchalgorithmus an. Dieser dient dazu, zu einer gegebenen reellen Zahl x die Kettenbruchentwicklung zu bestimmen.

Algorithmus 12.3 (Kettenbruchalgorithmus)**.** *Es soll die Kettenbruchentwicklung von* $x \in \mathbb{R}$ *bestimmt werden.*

(1) $a_0 := \lfloor x \rfloor \in \mathbb{Z}$, $t_0 := x - a_0 \in [0, 1)$, $m := 0$.

(2) Solange $t_m \neq 0$ *ist, wiederhole (3)-(6)*

(3) $\xi_m := \frac{1}{t_m}$

(4) $a_{m+1} := \lfloor \xi_m \rfloor \in \mathbb{N}$

(5) $t_{m+1} := \xi_m - a_{m+1} \in [0, 1)$

(6) $m := m + 1$

Falls die Schleife (2)-(6) terminiert, d.h. falls nach endlich vielen Schritten $t_m = 0$ *erreicht wird, dann ist* $((a_0, \ldots, a_m), x)$ *die Kettenbruchentwicklung von* x. *Falls die Schleife nicht terminiert, dann ist* $((a_n)_{n\in\mathbb{N}_0}, x)$ *die Kettenbruchentwicklung von* x.

Wir werden im Laufe dieses Abschnittes sehen, dass der Kettenbruchalgorithmus ein korrektes Ergebnis liefert. Er terminiert nur für rationales x und gibt in diesem Fall eine endliche Kettenbruchentwicklung als Ergebnis aus, für irrationales x erhalten wir eine unendliche Kettenbruchentwicklung.

Satz 12.4. *Sei $x \in \mathbb{R}$. Dann gilt:*

(a) *Die Zahl x besitzt eine eindeutig bestimmte Kettenbruchentwicklung. Diese wird durch den Kettenbruchalgorithmus geliefert.*

(b) *Ist x rational, dann ist die Kettenbruchentwicklung von x endlich. Ist x irrational, dann ist die Kettenbruchentwicklung von x unendlich.*

Ist die Kettenbruchentwicklung von x durch $((a_0, \ldots, a_m), x)$ bzw. $((a_n)_{n\in\mathbb{N}_0}, x)$ gegeben, dann heißen rationalen Zahlen $[a_0, \ldots, a_n]$ mit $n \in \mathbb{N}_0$ (und $n \leq m$, falls $x \in \mathbb{Q}$ ist) die ***Näherungsbrüche*** *von x.*

Den Beweis schieben wir an dieser Stelle auf, er benötigt einige Hilfsresultate, die wir im Laufe dieses Abschnitts bereitstellen werden. Wir studieren zunächst einige Beispiele zur Anwendung des Kettenbruchalgorithmus auf rationale Zahlen.

Beispiel 12.5. *Wie in Beispiel 12.2(a) gesehen, ist*

$$\frac{65}{27} = 2 + \frac{11}{27} = 2 + \frac{1}{\frac{27}{11}} = 2 + \frac{1}{2 + \frac{5}{11}} = 2 + \frac{1}{2 + \frac{1}{\frac{11}{5}}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{5}}} = [2, 2, 2, 5].$$

Mit den Bezeichnungen aus dem Kettenbruchalgorithmus 12.3 stellt sich diese Rechnung wie folgt dar: $a_0 = 2$, $t_0 = \frac{11}{27}$, $\xi_0 = \frac{27}{11}$, $a_1 = 2$, $t_1 = \frac{5}{11}$, $\xi_1 = \frac{11}{5}$, $a_2 = 2$, $t_2 = \frac{1}{5}$, $\xi_2 = 5$, $a_3 = 5$, $t_3 = 0$.

Beispiel 12.6. *Kettenbruchentwicklungen treten auch in einigen Anwendungen auf:*

(a) *Die Umlaufzeit der Erde um die Sonne beträgt in guter Näherung*

$$365d\ 5h\ 48min\ 45,8s = \left(365 + \frac{104.629}{432.000}\right) d.$$

Der Kettenbruchalgorithmus liefert

$$\frac{104.629}{432.000} = [0, 4, 7, 1, 3, 6, 2, 1, 170].$$

Näherungsbrüche dafür lassen sich in klassischen Kalendersystemen finden:

- *Der nullte Näherungsbruch für $\frac{104.629}{432.000}$ ist $[0] = 0$. Diese Näherung wurde beispielsweise im alten Ägypten vorgenommen: Es gibt keine Schaltjahre, dafür wird gelegentlich ein Jahr um ein paar Tage verlängert.*
- *Der erste Näherungsbruch für $\frac{104.629}{432.000}$ lautet $[0, 4] = \frac{1}{4}$. Dies entspricht dem Vorgehen im julianischen Kalender: Alle 4 Jahre wird ein Schaltjahr eingefügt.*

- *Der fünfte Näherungsbruch für $\frac{104.629}{432.000}$ ist durch $[0,4,7,1,3,6] = \frac{194}{801}$ gegeben. Das kommt der Gestaltung des gregorianischen Kalenders sehr nahe: In Modifikation des julianischen Kalenders fallen hier in 800 Jahren 6 Schaltjahre weg, nämlich diejenigen Jahre, deren Jahreszahl durch 100, aber nicht durch 400 teilbar ist.*

(b) *HUYGENS wollte 1682 ein Zahnradmodell des Planetensystems bauen. Das Verhältnis der Umlaufzeiten von Saturn und Erde ist in guter Näherung*

$$x = \frac{77.708.431}{2.640.858}.$$

Dieses Verhältnis soll durch Zahnräder mit möglichst wenig Zähnen möglichst exakt realisiert werden.
Eine naive Idee, das zu tun, wäre folgende Rundung vorzunehmen:

$$x \approx \frac{77.700.000}{2.600.000} = \frac{777}{26}.$$

Allerdings beträgt der Fehler hier bereits etwa 1,6%, und man benötigt ein Zahnrad mit 777 Zähnen.
Der Kettenbruchalgorithmus liefert

$$x = [29,2,2,1,5,1,4,1,1,2,1,6,1,10,2,2,3].$$

Der vierte Näherungsbruch ist durch $[29,2,2,1] = \frac{206}{7}$ gegeben. Der Fehler liegt hier nur bei ca. 0,01%, man benötigt ein Zahnrad mit 206 Zähnen und eines mit 7 Zähnen. Genau ein solches baute HUYGENS.

(c) *Bei der Einteilung des Jahres in Monate muss man das Verhältnis einer Mondperiode zur Jahreslänge berechnen. Dieses ist ziemlich genau*

$$x = \frac{2.953.059}{36.524.220}.$$

Über den Kettenbruchalgorithmus erhält man

$$x = [0,12,2,1,2,1,1,17,3,6,2,1,2,1,1,7].$$

Auch hier lassen sich Näherungsbrüche in klassischen Kalendersystemen finden:

- *Der erste Näherungsbruch für x lautet $[0,12] = \frac{1}{12}$. Das entspricht der Kalendereinteilung im alten Ägypten: Ein Jahr besteht aus 12 Monaten mit je 30 Tagen, dazu kommen 5 Feiertage.*
- *Der sechste Näherungsbruch für x ist durch $[0,12,2,1,2,1,1] = \frac{19}{235}$ gegeben. Dieses Verhältnis wird im jüdischen Kalender verwendet („Meton-Zyklus"): 19 Jahre werden zu einer Zeitperiode von 235 Monaten zusammengefasst.*

Proposition 12.7. *Sei $x \in \mathbb{R}$. Mit den Notationen aus dem Kettenbruchalgorithmus 12.3 gilt:*

(a) *Ist $m \in \mathbb{N}_0$ mit $t_m \neq 0$, dann ist $x = [a_0, \ldots, a_m, \xi_m]$.*

(b) *Ist $m \in \mathbb{N}_0$ mit $t_m = 0$, dann ist $x = [a_0, \ldots, a_m]$. Im Falle $m \geq 1$ ist dabei $a_m > 1$.*

Insbesondere gibt der Kettenbruchalgorithmus, falls er nach endlich vielen Schritten terminiert, eine endliche Kettenbruchentwicklung $((a_0, \ldots, a_m), x)$ von x aus.

Beweis. (a) Wir zeigen die Aussage per Induktion nach m. Sei $m = 0$, $t_0 \neq 0$. Es ist

$$\xi_0 = \frac{1}{t_0} = \frac{1}{x - a_0}$$

und deshalb

$$x = a_0 + \frac{1}{\xi_0} = [a_0, \xi_0].$$

Es sei nun $t_{m+1} \neq 0$. Wir erhalten

$$\begin{aligned} x &= [a_0, \ldots, a_m, \xi_m] = [a_0, \ldots, a_m, a_{m+1} + t_{m+1}] = [a_0, \ldots, a_m, a_{m+1} + \frac{1}{\xi_{m+1}}] \\ &= [a_0, \ldots, a_m, a_{m+1}, \xi_{m+1}]. \end{aligned}$$

(b) Ist $t_0 = 0$, dann ist offenbar $x = [a_0]$. Ist $m \geq 1$ mit $t_m = 0$, so ist $t_{m-1} \neq 0$, weshalb sich aus (a) unmittelbar $x = [a_0, \ldots, a_{m-1}, \xi_{m-1}]$ ergibt. Aufgrund von $0 = t_m = \xi_{m-1} - a_m$ folgt $x = [a_0, \ldots, a_m]$. In diesem Fall ist $a_m = \xi_{m-1} = \frac{1}{t_{m-1}} > 1$ wegen $t_{m-1} \in (0, 1)$. □

Proposition 12.8. *Sei $x \in \mathbb{R}$. Dann sind äquivalent:*

(i) *Der Kettenbruchalgorithmus terminiert bei Eingabe von x nach endlich vielen Schritten.*

(ii) $x \in \mathbb{Q}$.

Insbesondere gibt der Kettenbruchalgorithmus bei Eingabe einer rationalen Zahl eine endliche Kettenbruchentwicklung derselben aus.

Beweis. (i)$\Longrightarrow$(ii): Wir verwenden die Notation aus 12.3. Ist $t_0 = 0$, dann ist $x = [a_0] \in \mathbb{Z}$. Ist $m \in \mathbb{N}_0$ maximal mit $t_m \neq 0$, so ergibt sich aus 12.7

$$x = [a_0, \ldots, a_m, \xi_m] = [a_0, \ldots, a_m, a_{m+1}]$$

mit $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_{m+1} \in \mathbb{N}$ und damit sofort $x \in \mathbb{Q}$.
(ii)$\Longrightarrow$(i): Sei $x \in \mathbb{Q}$, etwa $x = \frac{p}{q}$ mit $p \in \mathbb{Z}$, $q \in \mathbb{N}$. Für $x = 0$ ist die Behauptung klar, so dass wir im Folgenden $x \neq 0$ voraussetzen. Wir setzen $r_0 := p$, $r_1 := q$ und führen den Euklidischen Algorithmus aus:

$$\begin{array}{rcll} r_0 & = & a_0' r_1 + r_2 & \text{mit } a_0' \in \mathbb{Z}, \quad 0 < r_2 < r_1, \\ r_1 & = & a_1' r_2 + r_3 & \text{mit } a_1' \in \mathbb{N}, \quad 0 < r_3 < r_2, \\ & \vdots & & \\ r_i & = & a_i' r_{i+1} + r_{i+2} & \text{mit } a_i' \in \mathbb{N}, \quad 0 < r_{i+2} < r_{i+1}, \\ & \vdots & & \\ r_{m-1} & = & a_{m-1}' r_m + r_{m+1} & \text{mit } a_{m-1}' \in \mathbb{N}, \quad 0 < r_{m+1} < r_m, \\ r_m & = & a_m' r_{m+1} & \text{mit } a_m' \in \mathbb{N}. \end{array}$$

Wir erhalten

$$\begin{aligned} \frac{r_i}{r_{i+1}} &= a_i' + \frac{r_{i+2}}{r_{i+1}} \quad \text{mit } \frac{r_{i+2}}{r_{i+1}} \in (0,1) \text{ für } i = 0, \dots, m-1, \\ \frac{r_m}{r_{m+1}} &= a_m'. \end{aligned}$$

Wir setzen

$$t_i' := \frac{r_{i+2}}{r_{i+1}} \quad \text{für } i = -1, \dots, m-1, \quad t_m' := 0,$$

und erhalten

$$\frac{1}{t_{i-1}'} = a_i' + t_i' \quad \text{für } i = 0, \dots, m,$$

wobei $t_i' \in (0,1)$ für $i = 0, \dots, m-1$ ist. Wir vergleichen dies mit den Formeln aus dem Kettenbruchalgorithmus 12.3. Es bezeichne $((a_i)_{i\in I}, x)$ das Resultat des Kettenbruchalgorithmus bei Eingabe von x, wobei $I = \{0, \dots, n\}$ sei, falls der Algorithmus nach endlich vielen Schritten abbricht, und $I = \mathbb{N}_0$ sonst. Die Folge $(t_i)_{i\in I}$ sei wie im Kettenbruchalgorithmus definiert. Wir zeigen induktiv, dass $a_i = a_i'$ und $t_i = t_i'$ für $i = 0, \dots, m$ ist. Insbesondere ist dann $t_m = t_m' = 0$, d.h. der Kettenbruchalgorithmus bricht nach endlich vielen Schritten ab. Sei zunächst $i = 0$. Es ist

$$a_0 = \lfloor x \rfloor = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{1}{t_{-1}'} \right\rfloor = a_0'$$

und

$$t_0 = x - a_0 = \frac{1}{t_{-1}'} - a_0' = t_0'.$$

Sei nun $0 < i \leq m$. Aus der Induktionsvoraussetzung ergibt sich $t_{i-1} = t_{i-1}' \neq 0$ und deshalb

$$a_i = \left\lfloor \frac{1}{t_{i-1}} \right\rfloor = \left\lfloor \frac{1}{t_{i-1}'} \right\rfloor = a_i'$$

sowie

$$t_i = \frac{1}{t_{i-1}} - a_i = \frac{1}{t_{i-1}'} - a_i' = t_i'.$$

□

Der Beweis hat gezeigt, dass man den Kettenbruchalgorithmus für rationale Zahlen als Variante des Euklidischen Algorithmus ansehen kann.

Beispiel 12.9. *Der Vergleich zwischen Euklidischen Algorithmus und Kettenbruchalgorithmus sieht in Beispiel 12.2(a) wie folgt aus:*

$$\begin{aligned} 65 &= 2 \cdot 27 + 11 \implies \frac{65}{27} = 2 + \frac{11}{27} \\ 27 &= 2 \cdot 11 + 5 \implies \frac{27}{11} = 2 + \frac{5}{11} \\ 11 &= 2 \cdot 5 + 1 \implies \frac{11}{5} = 2 + \frac{1}{5} \\ 5 &= 5 \cdot 1 + 0 \implies \frac{5}{1} = 5 + 0 \end{aligned}$$

Als Kettenbruchentwicklung von $\frac{65}{27}$ ergibt sich wie gehabt $((2,2,2,5),\frac{65}{27})$.

Die nächste Bemerkung zeigt insbesondere, dass es für jede rationale Zahl x genau eine endliche Kettenbruchentwicklung gibt.

Proposition 12.10. *Es seien $a_0, b_0 \in \mathbb{Z}$, $a_1, \ldots, a_n, b_1, \ldots, b_m \in \mathbb{N}$ mit $a_n, b_m \neq 1$ und $[a_0, \ldots, a_n] = [b_0, \ldots, b_m]$. Dann gilt: $n = m$ und $a_i = b_i$ für $i = 0, \ldots, n$.*

Beweis. Es sei o.E. $n \leq m$. Wir beweisen die Behauptung per Induktion nach n. Sei zunächst $n = 0$. Falls $m \geq 1$ wäre, dann ist

$$a_0 = b_0 + \frac{1}{[b_1, \ldots, b_m]},$$

wobei aufgrund von $b_m \neq 1$ die Ungleichung

$$0 < \frac{1}{[b_1, \ldots, b_m]} < 1$$

gilt, weshalb die linke Seite der vorigen Gleichung eine ganze Zahl ist, die rechte Seite dagegegen nicht. Somit ist $m = 0 = n$ und demzufolge $a_0 = [a_0] = [b_0] = b_0$. Im Folgenden sei $n \geq 1$. Es sei

$$x = [a_0, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = b_0 + \frac{1}{[b_1, \ldots, b_m]} = [b_0, \ldots, b_m]$$

Hierbei ist zu beachten, dass mit demselben Argument wie oben aus $n \geq 1$ auch $m \geq 1$ folgt. Aufgrund von $a_n \neq 1$ und $b_m \neq 1$ erhalten wir

$$0 < \frac{1}{[a_1, \ldots, a_n]} < 1 \text{ sowie } 0 < \frac{1}{[b_1, \ldots, b_m]} < 1,$$

und deshalb $a_0 = \lfloor x \rfloor = b_0$ und schließlich $[a_1, \ldots, a_n] = [b_1, \ldots, b_m]$. Aus der Induktionsannahme folgern wir $n = m$ und $a_i = b_i$ für $i = 1, \ldots, n$. □

Lässt man in 12.10 die Voraussetzung $a_n, b_m \neq 1$ weg, gilt die Eindeutigkeitsaussage nicht mehr:

$$[a_0, \ldots, a_{n-1}, a_n] = \begin{cases} [a_0, \ldots, a_n - 1, 1] & \text{für } a_n > 1 \text{ oder } n = 0, \\ [a_0, \ldots, a_{n-1} + 1] & \text{für } a_n = 1 \text{ und } n \geq 1 \end{cases}$$

Im Folgenden werden wir uns mit der Kettenbruchentwicklung irrationaler Zahlen beschäftigen. Dazu starten wir mit einer Folge ganzer Zahlen $(a_n)_{n\in\mathbb{N}_0}$ mit $a_n \geq 1$ für $n \geq 1$ und werden folgendes beweisen:

- Die Folge $([a_0, \ldots, a_n])_{n\in\mathbb{N}_0}$ konvergiert.
- Stammt die Folge $(a_n)_{n\in\mathbb{N}_0}$ aus der Ausgabe des Kettenbruchalgorithmus für eine irrationale Zahl x, dann konvergiert die Folge $([a_0, \ldots, a_n])_{n\in\mathbb{N}_0}$ gegen x, d.h. der Kettenbruchalgorithmus liefert als Ausgabe eine unendliche Kettenbruchentwicklung von x.

Die nächste Bemerkung hat einen sehr technischen Charakter, wird sich aber im weiteren Verlauf des Kapitels als nützlich herausstellen und an vielerlei Stellen Anwendung finden.

Proposition 12.11. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Wir setzen*

$$\begin{array}{llll} p_{-2} := 0, & p_{-1} := 1, & p_n := a_n p_{n-1} + p_{n-2} & \text{für } n \geq 0 \quad (\text{insb. } p_0 = a_0), \\ q_{-2} := 1, & q_{-1} := 0, & q_n := a_n q_{n-1} + q_{n-2} & \text{für } n \geq 0 \quad (\text{insb. } q_0 = 1), \end{array}$$

(bzw. in Matrixschreibweise:

$$\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \text{ für } n \geq 0).$$

Dann gilt:

(a)
$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{für alle } n \in \mathbb{N}_0,$$

(b)
$$[a_0, \ldots, a_n] = \frac{p_n}{q_n}$$
für alle $n \in \mathbb{N}_0$,

(c)
$$[a_0, \ldots, a_n, \xi] = \frac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}}$$
für alle $n \in \mathbb{N}_0$, $\xi \in \mathbb{R}_{>0}$,

(d) $q_{n+1} > q_n$ *für alle $n \in \mathbb{N}$, insbesondere $q_n \geq n$,*

(e) $q_1 \geq q_0$, *wobei Gleichheit genau dann besteht, wenn $a_1 = 1$ ist,*

(f)
$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$
für alle $n \in \mathbb{N}_0$,

(g)
$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$
für alle $n \in \mathbb{N}_0$,

(h) $\mathrm{ggT}(p_n, q_n) = 1$ *für alle $n \in \mathbb{N}_0$.*

Beweis. (a) Die Behauptung folgt aus der Rekursionsformel in Matrixschreibweise.
(c) Wir zeigen die Aussage per Induktion nach n. Im Fall $n = 0$ ist

$$[a_0, \xi] = a_0 + \frac{1}{\xi} = \frac{\xi a_0 + 1}{\xi} = \frac{\xi p_0 + p_{-1}}{\xi q_0 + q_{-1}}.$$

Sei $n \geq 1$. Nach Induktionsvoraussetzung erhalten wir

$$\begin{aligned}[a_0,\ldots,a_n,\xi] &= [a_0,\ldots,a_{n-1},a_n+\frac{1}{\xi}] = \frac{(a_n+\frac{1}{\xi})p_{n-1}+p_{n-2}}{(a_n+\frac{1}{\xi})q_{n-1}+q_{n-2}} \\ &= \frac{(a_n\xi+1)p_{n-1}+\xi p_{n-2}}{(a_n\xi+1)q_{n-1}+\xi q_{n-2}} = \frac{\xi(a_np_{n-1}+p_{n-2})+p_{n-1}}{\xi(a_nq_{n-1}+q_{n-2})+q_{n-1}} \\ &= \frac{\xi p_n+p_{n-1}}{\xi q_n+q_{n-1}}.\end{aligned}$$

(b) Nach (c) ist

$$[a_0,\ldots,a_n] = \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}} = \frac{p_n}{q_n}.$$

(d), (e) Es ist $q_0 = 1$, $q_1 = a_1q_0 = a_1 \geq 1$, $q_{n+1} = a_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1}$. Induktiv ergibt sich $q_{n+1} > q_n \geq n$ für $n \in \mathbb{N}$.
(f) Es ist

$$\begin{aligned}p_nq_{n-1}-p_{n-1}q_n &= \det\begin{pmatrix}p_n & p_{n-1}\\ q_n & q_{n-1}\end{pmatrix} = \det\Big(\begin{pmatrix}a_0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a_1 & 1\\ 1 & 0\end{pmatrix}\cdot\ldots\cdot\begin{pmatrix}a_n & 1\\ 1 & 0\end{pmatrix}\Big) \\ &= \det\begin{pmatrix}a_0 & 1\\ 1 & 0\end{pmatrix}\cdot\ldots\cdot\det\begin{pmatrix}a_n & 1\\ 1 & 0\end{pmatrix} = (-1)^{n+1}.\end{aligned}$$

(g) Wir berechnen

$$\begin{aligned}p_nq_{n-2}-p_{n-2}q_n &= (a_np_{n-1}+p_{n-2})q_{n-2}-p_{n-2}(a_nq_{n-1}+q_{n-2}) \\ &= a_n(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}) \overset{\text{(f)}}{=} (-1)^na_n.\end{aligned}$$

(h) Ist $d \in \mathbb{Z}$ mit $d|p_n$ und $d|q_n$, dann folgt $d|(p_nq_{n-1}-p_{n-1}q_n) = (-1)^n$, also $d = \pm 1$. Das impliziert $\mathrm{ggT}(p_n,q_n) = 1$. □

Da wir im weiteren Verlauf des Kapitels gelegentlich die Indexmenge $\{-2,-1,0,1,2,\ldots\}$ benötigen werden, führen wir an dieser Stelle dafür die Bezeichnung $\mathbb{N}_{-2}$ ein.

Satz 12.12. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Dann gilt:*

(a) *Die Brüche $[a_0,\ldots,a_n] = \frac{p_n}{q_n}$ (vgl. 12.11) bilden eine konvergente Folge.*

(b) *Die Teilfolge $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\in\mathbb{N}_0}$ ist streng monoton wachsend, die Teilfolge $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\in\mathbb{N}_0}$ ist streng monoton fallend. Insbesondere gilt: Ist $x = \lim_{n\to\infty}\frac{p_n}{q_n} = [a_0,a_1,\ldots]$, dann ist*

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < x < \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

(c) *Die Zahl $[a_0,a_1,\ldots]$ ist irrational.*

Ist $x = [a_0,\ldots,a_m] \in \mathbb{Q}$, und sind $\frac{p_0}{q_0},\ldots,\frac{p_m}{q_m}$ die zugehörigen Näherungsbrüche, dann gilt Aussage (b) entsprechend mit $\ldots \leq x \leq \ldots$.

Beweis. (a) Wegen 12.11 gilt für $i \in \mathbb{N}$:

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{p_i q_{i-1} - p_{i-1} q_i}{q_i q_{i-1}} = \frac{(-1)^{i+1}}{q_i q_{i-1}}.$$

Es folgt

$$\frac{p_n}{q_n} = \frac{p_0}{q_0} + \sum_{i=1}^{n} \left(\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \right) = a_0 + \sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_i q_{i-1}}.$$

Die Folge $\left(\frac{1}{q_i q_{i-1}} \right)_{i \in \mathbb{N}}$ ist aufgrund von 12.11(d),(e) eine streng monoton fallende Nullfolge, weswegen aus dem Leibniz-Kriterium die Konvergenz von $\sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_i q_{i-1}}$ folgt. Somit ist die Folge $(\frac{p_n}{q_n})_{n \in \mathbb{N}}$ konvergent.
(b) Aufgrund von 12.11(g) gilt für alle $n \in \mathbb{N}_0$:

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = (-1)^n \frac{a_n}{q_n q_{n-2}}$$

Demzufolge gilt für alle $n \geq 2$ wegen $a_n, q_n, q_{n-2} \geq 1$:

$$\frac{p_n}{q_n} > \frac{p_{n-2}}{q_{n-2}}, \text{ falls } n \text{ gerade},$$

$$\frac{p_n}{q_n} < \frac{p_{n-2}}{q_{n-2}}, \text{ falls } n \text{ ungerade}.$$

(c) Wir nehmen an, dass $x = [a_0, a_1, \ldots]$ rational ist. Der Kettenbruchalgorithmus liefert in diesem Fall eine endliche Kettenbruchentwicklung $((b_0, \ldots, b_m), x)$ von x. Wir zeigen zunächst induktiv, dass $a_k = b_k$ für $k = 0, \ldots, m$ ist. Es ist $a_0 = \lfloor x \rfloor = b_0$. Sei nun $[a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_{k-1}, b_k, \ldots, b_m]$. Wir setzen $\xi_{k-1} := [a_k, a_{k+1}, \ldots]$. Das ist aufgrund von (a) wohldefiniert, und es gilt

$$[a_0, a_1, \ldots, a_{k-1}, \xi_{k-1}] = [a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_{k-1}, b_k, \ldots, b_m]$$

Durch Termumformung ergibt sich $\xi_{k-1} = [b_k, \ldots, b_m]$, was $a_k = \lfloor \xi_{k-1} \rfloor = b_k$ zur Folge hat und die Induktion beendet. Mit $\xi_m = [a_{m+1}, a_{m+2}, \ldots]$ ergibt sich die Gleichung $[a_0, \ldots, a_m] = [a_0, \ldots, a_m, \xi_m]$, was zum Widerspruch führt. □

Beispiel 12.13. *(vgl. Bsp. 12.2(b)) Es sei $a_n = 1$ für alle $n \in \mathbb{N}_0$. Es ergibt sich für $n \geq 0$:*

$$p_n = p_{n-1} + p_{n-2}, \quad q_n = q_{n-1} + q_{n-2},$$

insbesondere $p_0 = 1$, $p_1 = 2$, $q_0 = 1$, q_1=1. Bezeichnet $(F_n)_{n \in \mathbb{N}_0}$ die Folge der Fibonaccizahlen, dann ist $p_n = F_{n+1}$, $q_n = F_n$ für alle $n \in \mathbb{N}_0$. Die Folge $\frac{p_n}{q_n} = \frac{F_{n+1}}{F_n}$ ist aufgrund von 12.12 konvergent, aus der Überlegung in 12.2 erhalten wir

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \lim_{n \to \infty} \frac{F_{n+1}}{F_n} = [1, 1, \ldots] = \frac{1 + \sqrt{5}}{2}.$$

Aus Satz 12.12 folgt insbesondere, dass die Folge der Näherungsbrüche, die man über den Kettenbruchalgorithmus zu einer irrationalen Zahl x bestimmt, konvergiert. Im nächsten Satz werden wir zeigen, dass der Grenzwert durch x selbst gegeben ist.

Satz 12.14. *Sei $x \in \mathbb{R} \setminus \mathbb{Q}$ und $((a_n)_{n\in\mathbb{N}_0}, x)$ die Ausgabe des Kettenbruchalgorithmus bei Eingabe von x, $(\frac{p_n}{q_n})_{n\in\mathbb{N}_0}$ bezeichne die Folge der Näherungsbrüche (vgl. 12.11). Dann gilt:*

(a) *Die Folge der Näherungsbrüche $[a_0, \ldots, a_n] = \frac{p_n}{q_n}$ konvergiert gegen x, es ist also $x = [a_0, a_1, \ldots]$.*

(b) *Für alle $n \in \mathbb{N}_0$ ist*
$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}},$$
für $n \geq 1$ ist insbesondere
$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{n(n+1)}.$$

(c) *Für alle $n \in \mathbb{N}_0$ ist*
$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(q_n + q_{n+1})},$$

Somit liefert der Kettenbruchalgorithmus eine unendliche Kettenbruchentwicklung von x als Ergebnis.

Beweis. Wir beginnen mit dem Beweis von Aussage (b), denn diese impliziert Aussage (a). Die Folge $(\xi_n)_{n\in\mathbb{N}_0}$ sei definiert wie im Kettenbruchalgorithmus. Aufgrund von 12.7 und 12.11(c) erhalten wir für jedes $n \in \mathbb{N}_0$:
$$x = [a_0, \ldots, a_n, \xi_n] = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}$$
und deshalb
$$x - \frac{p_n}{q_n} = \frac{(\xi_n p_n + p_{n-1})q_n - p_n(\xi_n q_n + q_{n-1})}{q_n(\xi_n q_n + q_{n-1})} = \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(\xi_n q_n + q_{n-1})} \overset{12.11(f)}{=} \frac{(-1)^n}{q_n(\xi_n q_n + q_{n-1})}.$$
Wegen $a_{n+1} = \lfloor \xi_n \rfloor < \xi_n$ (andernfalls würde der Kettenbruchalgorithmus an dieser Stelle terminieren) erhalten wir
$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\xi_n q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1} q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}}.$$
Für $n \geq 1$ ist nach 12.11(d) $q_n \geq n$, was
$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}$$
zur Folge hat.
(c) Wegen $\xi_n < \lfloor \xi_n \rfloor + 1 = a_{n+1} + 1$ ist
$$\begin{aligned} \left| x - \frac{p_n}{q_n} \right| &= \frac{1}{q_n(\xi_n q_n + q_{n-1})} > \frac{1}{q_n((a_{n+1}+1)q_n + q_{n-1})} = \frac{1}{q_n(a_{n+1}q_n + q_{n-1} + q_n)} \\ &= \frac{1}{q_n(q_{n+1} + q_n)}. \end{aligned}$$

□

Proposition 12.15. *Sei $x = [a_0, \ldots, a_m] \in \mathbb{Q}$, $a_m \neq 1$. Dann gilt:*

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} \quad \text{und} \quad \left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(q_n + q_{n+1})}$$

für alle $n \in \{0, \ldots, m-1\}$, wobei bei der ersten Ungleichung Gleichheit nur im Fall $n = m-1$ auftritt.

Beweis. Der Beweis verläuft analog zum Beweis von 12.14. □

Es verbleibt zum Beweis von Satz 12.4 noch zu zeigen, dass jede reelle Zahl eine eindeutig bestimmte Kettenbruchentwicklung besitzt. In Verbindung mit 12.10 und 12.12(c) genügt dafür die folgende Bemerkung.

Proposition 12.16. *Es seien $(a_n)_{n\in\mathbb{N}_0}$, $(b_n)_{n\in\mathbb{N}_0}$ Folgen ganzer Zahlen mit $a_n, b_n \geq 1$ für $n \geq 1$ und $[a_0, a_1, \ldots] = [b_0, b_1, \ldots]$. Dann gilt: Für alle $n \in \mathbb{N}_0$ ist $a_n = b_n$.*

Beweis. Wir zeigen die Aussage per Induktion nach n. Wir setzen $x = [a_0, a_1, \ldots] = [b_0, b_1, \ldots]$. Es ist $a_0 = \lfloor x \rfloor = b_0$. Es sei nun $a_0 = b_0, \ldots, a_n = b_n$. Setzen wir $\xi = [a_{n+1}, a_{n+2}, \ldots]$, $\xi' = [b_{n+1}, b_{n+2}, \ldots]$, so ergibt sich $[a_0, \ldots, a_n, \xi] = [b_0, \ldots, b_n, \xi'] = [a_0, \ldots, a_n, \xi']$ und daraus $\xi = \xi'$. Aufgrunddessen ist $a_{n+1} = \lfloor \xi \rfloor = \lfloor \xi' \rfloor = b_{n+1}$. □

Beispiel 12.17. (a) *Der Kettenbruchalgorithmus liefert für $x = \sqrt{2}$*

$$\begin{aligned}
\sqrt{2} = 1 + (\sqrt{2} - 1) &= 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)}} = 1 + \frac{1}{\sqrt{2}+1} \\
&= 1 + \frac{1}{2 + (\sqrt{2} - 1)} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} \\
&= 1 + \frac{1}{2 + \frac{1}{2 + (\sqrt{2} - 1)}}
\end{aligned}$$

Aus Satz 12.14 folgt, dass $((1, 2, 2, 2, \ldots), \sqrt{2})$ die Kettenbruchentwicklung von $\sqrt{2}$ ist.

(b) *Man kann zeigen: $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots]$.*

(c) *Der Kettenbruchalgorithmus liefert*

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, \ldots],$$

es ist kein Muster bekannt. Der dritte Näherungsbruch für π ist durch $[3, 7, 15, 1] = \frac{355}{113} \approx 3,1415929$ gegeben. Dieser Näherungsbruch für π war dem Chinesen TSU-CHUNG-CHI bereits im dritten Jahrhundert v.Chr. bekannt. PTOLEMÄUS verwendete den Näherungsbruch $\frac{333}{106} = [3, 7, 15] \approx 3,1415094$.

§13 Periodische Kettenbrüche

Definition 13.1. *Es sei $(a_n)_{n\in\mathbb{N}_0}$ eine Folge ganzer Zahlen mit $a_n \geq 1$ für $n \geq 1$. Der Kettenbruch $((a_n)_{n\in\mathbb{N}_0}, [a_0, a_1, \ldots])$ heißt **periodisch**, wenn es ein $h \in \mathbb{N}$ und ein $n \in \mathbb{Z}_{\geq -1}$ mit $a_{m+h} = a_m$ für alle $m \geq n+1$ gibt. In diesem Fall nennen wir das minimale h mit dieser Eigenschaft die **Periodenlänge**, für den Kettenbruch verwenden wir die Notation*

$$((a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), [a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}]).$$

*Der Kettenbruch heißt **reinperiodisch**, wenn $n = -1$ gewählt werden kann, d.h. wenn es keine Vorperiode gibt.*

Beispiel 13.2. (a) *Der Goldene Schnitt $\phi = \frac{1+\sqrt{5}}{2} \overset{12.13}{=} [\overline{1}]$ hat eine reinperiodische Kettenbruchentwicklung mit Periodenlänge 1.*

(b) *$\sqrt{2} = [1, \overline{2}]$ (vgl. 12.17) hat eine periodische Kettenbruchentwicklung mit Periodenlänge 1.*

Satz 13.3 (Euler-Lagrange)**.** *Sei $x \in \mathbb{R}$. Dann sind äquivalent:*

(i) *Die Kettenbruchentwicklung von x ist periodisch.*

(ii) *Die Zahl x ist eine **quadratische Irrationalzahl**, d.h. x ist irrational und x erfüllt eine quadratische Gleichung der Form $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{Z}$.*

Beweis. (i)$\Longrightarrow$(ii) (Euler): Die Kettenbruchentwicklung von x sei periodisch. Damit ist sie insbesondere unendlich, weswegen x nach 12.4 irrational ist. Sei die Kettenbruchentwicklung von x explizit durch $((a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), x)$ gegeben. Wir setzen $\xi = [\overline{a_{n+1}, \ldots, a_{n+h}}]$. Es ergibt sich $\xi = [a_{n+1}, \ldots, a_{n+h}, \xi]$. Die Folge der Näherungszähler bzw. -nenner zu ξ gemäß 12.11 bezeichnen wir im Folgenden mit $(p'_i)_{i\in\mathbb{N}_{-2}}$ bzw. $(q'_i)_{i\in\mathbb{N}_{-2}}$. Aus 12.11(c) erhalten wir

$$\xi = \frac{\xi p'_{h-1} + p'_{h-2}}{\xi q'_{h-1} + q'_{h-2}}$$

und daraus

$$\xi^2 q'_{h-1} + (q'_{h-2} - p'_{h-1})\xi - p'_{h-2} = 0.$$

Wir bezeichen die Folge der Näherungszähler bzw. -nenner zu x gemäß mit $(p_i)_{i\in\mathbb{N}_{-2}}$ bzw. $(q_i)_{i\in\mathbb{N}_{-2}}$. Dann gilt

$$x = [a_0, \ldots, a_n, \xi] = \frac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}}$$

und aufgrunddessen

$$\xi = -\frac{q_{n-1}x - p_{n-1}}{q_n x - p_n}.$$

Das Einsetzen von ξ in die obige quadratische Gleichung für ξ und anschließendes Multiplizieren mit $(q_n x - p_n)^2$ liefert eine quadratische Gleichung für x mit Koeffizienten in $\mathbb{Z}$.
(ii)$\Longrightarrow$(i) (Lagrange): Sei x eine quadratische Irrationalzahl mit $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Z}$. Nach 12.4 ist die Kettenbruchentwicklung von x unendlich, etwa $((a_0, a_1, \ldots), x)$. Sei $(\xi_n)_{n\in\mathbb{N}_0}$

wie im Kettenbruchalgorithmus definiert, $(p_n)_{n\in\mathbb{N}_{-2}}$ bzw. $(q_n)_{n\in\mathbb{N}_{-2}}$ bezeichne die Folge der Näherungszähler bzw. -nenner. Dann ist insbesondere

$$x = [a_0, \dots, a_n, \xi_n] = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}$$

für alle $n \in \mathbb{N}_0$. Durch Einsetzen dieses Ausdrucks in die quadratische Gleichung für x erhalten wir

$$a\left(\frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}}\right)^2 + b\frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}} + c = 0$$

und deshalb

$$\begin{aligned} 0 &= a(\xi_n p_n + p_{n-1})^2 + b(\xi_n p_n + p_{n-1})(\xi_n q_n + q_{n-1}) + c(\xi_n q_n + q_{n-1})^2 \\ &= \xi_n^2(ap_n^2 + bp_n q_n + cq_n^2) + \xi_n(2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1}q_n) + 2cq_n q_{n-1}) \\ &\quad + ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \end{aligned}$$

Wir setzen für $n \in \mathbb{N}_0$

$$\begin{aligned} A_n &:= ap_n^2 + bp_n q_n + cq_n^2, \\ B_n &:= 2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1}q_n) + 2cq_n q_{n-1}, \\ C_n &:= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2, \end{aligned}$$

so dass also $A_n\xi_n^2 + b_n\xi_n + C_n = 0$ gilt. Wir bemerken zudem, dass offenbar $C_{n+1} = A_n$ ist. Eine längere Rechnung ergibt

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)(p_n q_{n-1} - q_n p_{n-1})^2 \overset{12.11}{=} b^2 - 4ac.$$

Aufgrund von 12.14(b) und 12.11 ist

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \le \frac{1}{q_n^2},$$

d.h. es existiert ein $\delta_n \in \mathbb{R}$ mit $|\delta_n| < 1$ und

$$x - \frac{p_n}{q_n} = -\delta_n \frac{1}{q_n^2}.$$

Das impliziert

$$p_n = xq_n + \frac{\delta_n}{q_n}$$

und deswegen

$$\begin{aligned} |A_n| &= |ap_n^2 + bp_n q_n + cq_n^2| \\ &= \left|a\left(xq_n + \frac{\delta_n}{q_n}\right)^2 + bq_n\left(xq_n + \frac{\delta_n}{q_n}\right) + cq_n^2\right| \\ &= \left|q_n^2(ax^2 + bx + c) + 2ax\delta_n + b\delta_n + a\frac{\delta_n^2}{q_n^2}\right| \\ &= \left|2ax\delta_n + b\delta_n + a\frac{\delta_n^2}{q_n^2}\right| \\ &< 2|ax| + |b| + |a|. \end{aligned}$$

Die rechte Seite ist unabhängig von n, also treten in der Folge $(A_n)_{n\in\mathbb{N}_0}$ nur endlich viele verschiedene Werte auf. Wegen $C_{n+1} = A_n$ gilt dies auch für die Folge $(C_n)_{n\in\mathbb{N}_0}$, und aufgrund von $B_n^2 - 4A_nC_n = b^2 - 4ac$ ebenso für die Folge $(B_n)_{n\in\mathbb{N}_0}$. Da $A_n\xi_n^2 + B_n\xi_n + C_n = 0$ ist, können auch in der Folge $(\xi_n)_{n\in\mathbb{N}_0}$ nur endlich viele verschiedene Werte auftreten. Demzufolge gibt es ein $h \in \mathbb{N}$ und ein $m \in \mathbb{N}_0$ mit $\xi_{m+h} = \xi_m$. Das hat zur Folge, dass die Kettenbruchentwicklung von x periodisch ist. □

Proposition 13.4. *Es sei $d \in \mathbb{Z}$, d kein Quadrat. Wir setzen*

$$\mathbb{Q}(\sqrt{d}) := \{u + v\sqrt{d} \mid u, v \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Dann gilt:

(a) *$(1, \sqrt{d})$ ist eine Basis von $\mathbb{Q}(\sqrt{d})$ als $\mathbb{Q}$-Vektorraum, d.h. für jedes $x \in \mathbb{Q}(\sqrt{d})$ gibt es eindeutig bestimmte $u, v \in \mathbb{Q}$ mit $x = u + v\sqrt{d}$.*

(b) *$\mathbb{Q}(\sqrt{d})$ ist (mit der eingeschränkten Addition und Multiplikation von $\mathbb{C}$) ein Körper.*

(c) *Die Abbildung*

$$\overline{\ } : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}),\ u + v\sqrt{d} \mapsto u - v\sqrt{d}$$

ist ein Körperautomorphismus von $\mathbb{Q}(\sqrt{d})$, d.h. $\overline{\ }$ ist bijektiv und für alle $x_1, x_2 \in \mathbb{Q}(\sqrt{d})$ gilt: $\overline{x_1 + x_2} = \overline{x_1} + \overline{x_2}$, $\overline{x_1 \cdot x_2} = \overline{x_1} \cdot \overline{x_2}$.

(d) *Ein Element $x \in \mathbb{Q}(\sqrt{d})$ liegt genau dann in $\mathbb{Q}$, wenn $\overline{x} = x$ ist.*

(e) *Erfüllt $x \in \mathbb{Q}(\sqrt{d})$ die quadratische Gleichung $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{Q}$, so ist $a\overline{x}^2 + b\overline{x} + c = 0$. Ist insbesondere $x \notin \mathbb{Q}$, dann ist $\overline{x}$ die zweite Lösung dieser Gleichung.*

Beweis. (a) Nach Definition ist $(1, \sqrt{d})$ ein Erzeugendensystem von $\mathbb{Q}(\sqrt{d})$ als $\mathbb{Q}$-Vektorraum. $(1, \sqrt{d})$ ist linear unabhängig über $\mathbb{Q}$, denn wäre $u \cdot 1 + v\sqrt{d} = 0$ mit $(u, v) \in \mathbb{Q}^2$, $(u, v) \neq (0, 0)$, dann wäre $v \neq 0$ und $\sqrt{d} = -\frac{u}{v} \in \mathbb{Q}$, was ein Widerspruch ist, denn d ist kein Quadrat.
(b) Die Abgeschlossenheit unter Addition und Multiplikation rechnet man leicht nach, ebenso wie die Ringaxiome. Interessantester Punkt dürfte wohl die Existenz von Inversen bzgl. der Multiplikation sein, welche wir kurz demonstrieren. Dazu seien $u, v \in \mathbb{Q}$ mit $u + v\sqrt{d} \neq 0$. In $\mathbb{C}$ berechnen wir

$$\frac{1}{u + v\sqrt{d}} = \frac{u - v\sqrt{d}}{(u + v\sqrt{d})(u - v\sqrt{d})} = \frac{u - v\sqrt{d}}{u^2 - v^2d} = \frac{u}{u^2 - v^2d} - \frac{v}{u^2 - v^2d}\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

(c) Es seien $u_1, u_2, v_1, v_2 \in \mathbb{Q}$. Wir berechnen

$$\begin{aligned}\overline{(u_1 + v_1\sqrt{d}) + (u_2 + v_2\sqrt{d})} &= \overline{(u_1 + u_2) + (v_1 + v_2\sqrt{d})} = u_1 + u_2 - (v_1 + v_2)\sqrt{d} \\ &= (u_1 - v_1\sqrt{d}) + (u_2 - v_2)\sqrt{d} = \overline{u_1 + v_1\sqrt{d}} + \overline{u_2 + v_2\sqrt{d}}\end{aligned}$$

sowie

$$\begin{aligned}\overline{(u_1 + v_1\sqrt{d})(u_2 + v_2\sqrt{d})} &= \overline{u_1u_2 + v_1v_2d + (u_1v_2 + u_2v_1)\sqrt{d}} \\ &= u_1u_2 + v_1v_2d - (u_1v_2 + u_2v_1)\sqrt{d} \\ &= (u_1 - v_1\sqrt{d})(u_2 - v_2\sqrt{d}) \\ &= \overline{u_1 + v_1\sqrt{d}} \cdot \overline{u_2 + v_2\sqrt{d}}.\end{aligned}$$

Die Bijektivität der Abbildung ergibt sich daraus, dass es sich sich offenbar um eine Involution handelt, d.h. zweimaliges Anwenden liefert die Identität auf $\mathbb{Q}(\sqrt{d})$.
(d) ist klar.
(e) Wegen (c) folgt aus $ax^2 + bx + c = 0$ durch Anwenden von $\overline{\ }$, dass

$$0 = \overline{0} = \overline{ax^2 + bx + c} = a\overline{x}^2 + b\overline{x} + c$$

ist. □

Proposition 13.5. *Es sei x eine quadratische Irrationalzahl. Dann gilt:*

(a) *Es gibt ein eindeutig bestimmtes quadratfreies $d \in \mathbb{N} \setminus \{1\}$ mit $x \in \mathbb{Q}(\sqrt{d})$. Damit existieren nach 13.4 eindeutig bestimmte $u, v \in \mathbb{Q}$ mit $x = u + v\sqrt{d}$. Anwendung von $\overline{\ }$ in $\mathbb{Q}(\sqrt{d})$ liefert $\overline{x} = u - v\sqrt{d}$. $\overline{x}$ heißt die zu x **konjugierte Zahl**.*

(b) *$\overline{x}$ ist eine quadratische Irrationalzahl.*

Beweis. (a) Wir zeigen zunächst die Existenzaussage. Seien $a, b, c \in \mathbb{Z}$ mit $ax^2 + bx + c = 0$. Da x irrational ist, ist $a \neq 0$. In $\mathbb{R}$ erhalten wir

$$x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}.$$

Wir schreiben $b^2 - 4ac = r^2 d$ mit $d \in \mathbb{N} \setminus \{1\}$ quadratfrei und $r \in \mathbb{N}$. Das impliziert

$$x = -\frac{b}{2a} \pm \frac{r}{2a}\sqrt{d}.$$

Setzen wir $u := -\frac{b}{2a}$, $v := \pm\frac{r}{2a}$, so ist $x = u + v\sqrt{d}$. Zum Nachweis der Eindeutigkeitsaussage sei $x \in \mathbb{Q}(\sqrt{d_1}) \cap \mathbb{Q}(\sqrt{d_2})$, $x \notin \mathbb{Q}$, wobei $d_1, d_2 \in \mathbb{N} \setminus \{1\}$ quadratfrei sind. Somit existieren $u_1, u_2, v_1, v_2 \in \mathbb{Q}$ mit $x = u_1 + v_1\sqrt{d_1} = u_2 + v_2\sqrt{d_2}$. Nach Multiplikation mit den auftretenden Nennern können wir o.E. $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ annehmen. Es ist dann

$$(u_1 - u_2)^2 = (v_2\sqrt{d_2} - v_1\sqrt{d_1})^2 = v_1^2 d_1 + v_2^2 d_2 - 2v_1 v_2\sqrt{d_1 d_2},$$

also

$$(u_1 - u_2)^2 - v_1^2 d_1 - v_2^2 d_2 + 2v_1 v_2\sqrt{d_1 d_2} = 0$$

Aufgrund von $x \notin \mathbb{Q}$ sind $v_1, v_2 \neq 0$. Wegen 13.4(a) ist $d_1 d_2$ ein Quadrat und deshalb $d_1 = d_2$.
(b) folgt direkt aus 13.4(e). □

Schwächt man die Forderung der Quadratfreiheit von d ab, indem man nur noch fordert, dass d kein Quadrat ist, so gilt die Existenzaussage in (a) natürlich immer noch, die Eindeutigkeit geht allerdings verloren. Die nächste Bemerkung zeigt jedoch, dass das Berechnen des Konjugierten davon unbeschadet bleibt.

Proposition 13.6. *Sei x eine quadratische Irrationalzahl der Form $x = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$, wobei $d \in \mathbb{N}$ kein Quadrat ist. Dann gilt: $\overline{x} = u - v\sqrt{d}$.*

Beweis. Wir schreiben d in der Form $d = r^2 d'$, wobei $d' \in \mathbb{N} \setminus \{1\}$ quadratfrei ist und $r \in \mathbb{N}$ ist. Es ergibt sich

$$\overline{x} = \overline{u + v\sqrt{d}} = \overline{u + v\sqrt{r^2 d'}} = \overline{u + vr\sqrt{d'}} = u - vr\sqrt{d'} = u - v\sqrt{d}.$$

□

Beispiel 13.7. *Sei $x \in \mathbb{R}$ die positive reelle Nullstelle von $2X^2 - 6X - 1$. Dann ist $x = \frac{3}{2} + \frac{1}{4}\sqrt{44} = \frac{3}{2} + \frac{1}{2}\sqrt{11}$, also $\overline{x} = \frac{3}{2} - \frac{1}{2}\sqrt{11}$.*

Proposition 13.8. *Es sei $x \in \mathbb{R}$ eine quadratische Irrationalzahl mit reinperiodischer Kettenbruchentwicklung $((\overline{a_0, a_1, \ldots, a_{h-1}}), x)$. Dann gilt:*

$$-\frac{1}{\overline{x}} = [\overline{a_{h-1}, \ldots, a_1, a_0}].$$

Beweis. Wir setzen $y := [\overline{a_{h-1}, \ldots, a_1, a_0}]$. Es seien $(p_n)_{n\in\mathbb{N}_{-2}}$, $(q_n)_{n\in\mathbb{N}_{-2}}$ bzw. $(p'_n)_{n\in\mathbb{N}_{-2}}$, $(q'_n)_{n\in\mathbb{N}_{-2}}$ die Folgen der Näherungsbruchzähler und -nenner zu x bzw. y. Es ist

$$x = [a_0, a_1, \ldots, a_{h-1}, x], \quad y = [a_{h-1}, \ldots, a_1, a_0, y],$$

woraus sich mittels 12.11

$$x = \frac{xp_{h-1} + p_{h-2}}{xq_{h-1} + q_{h-2}}, \quad y = \frac{yp'_{h-1} + p'_{h-2}}{qq'_{h-1} + q'_{h-2}}$$

ergibt. Das liefert

$$\begin{aligned} q_{h-1}x^2 + (q_{h-2} - p_{h-1})x - p_{h-2} &= 0 \\ q'_{h-1}y^2 + (q'_{h-2} - p'_{h-1})y - p'_{h-2} &= 0. \end{aligned}$$

Durch Multiplikation der letzten Gleichung mit $-\frac{1}{y^2}$ finden wir

$$p'_{h-2}\left(-\frac{1}{y}\right)^2 + (q'_{h-2} - p'_{h-1})\left(-\frac{1}{y}\right) - q'_{h-1} = 0.$$

Nach 12.11 ist

$$\begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_{h-1} & 1 \\ 1 & 0 \end{pmatrix},$$

was

$$\begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix}^t = \begin{pmatrix} a_{h-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \overset{12.11}{=} \begin{pmatrix} p'_{h-1} & p'_{h-2} \\ q'_{h-1} & q'_{h-2} \end{pmatrix}$$

zur Folge hat. Das impliziert

$$p_{h-1} = p'_{h-1},\ p_{h-2} = q'_{h-1},\ q_{h-1} = p'_{h-2},\ q_{h-2} = q'_{h-2},$$

und somit erfüllt $-\frac{1}{y}$ dieselbe quadratische Gleichung wie x. Aus 13.4(e) erhalten wir $x = -\frac{1}{y}$ oder $\overline{x} = -\frac{1}{y}$. Aus $a_0 = a_h \geq 1$ folgt $x, y > 0$ und deshalb $-\frac{1}{y} < 0$, so dass der Fall $x = -\frac{1}{y}$ nicht auftritt. Demzufolge ist $\overline{x} = -\frac{1}{y}$, also $y = -\frac{1}{\overline{x}}$. □

Beispiel 13.9. *Für* $x = \frac{3+\sqrt{11}}{2}$ *berechnen wir* $x = [\overline{3,6}]$. *Aus 13.8 ergibt sich* $-\frac{1}{\overline{x}} = [\overline{6,3}]$, *also*

$$[\overline{6,3}] = -\frac{1}{\frac{3-\sqrt{11}}{2}} = \frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{2} = 3+\sqrt{11}.$$

Definition 13.10. *Es sei x eine quadratische Irrationalzahl. Die Zahl x heißt* ***reduziert****, wenn* $x > 1$ *ist und* $-1 < \overline{x} < 0$ *gilt.*

Beispiel 13.11. $\frac{3+\sqrt{11}}{2}$ *ist reduziert, denn* $\frac{3+\sqrt{11}}{2} > 1$ *und* $-1 < \frac{3-\sqrt{11}}{2} < 0$.

Satz 13.12. *Es sei x eine quadratische Irrationalzahl. Dann sind äquivalent:*

(i) *x ist reduziert.*

(ii) *Die Kettenbruchentwicklung von x ist reinperiodisch.*

Beweis. (ii)$\Longrightarrow$(i): Die Kettenbruchentwicklung von x sei durch $((\overline{a_0, a_1, \ldots, a_{h-1}}), x)$ gegeben. Dann ist $x > a_0 = a_h \geq 1$, und aufgrund von 13.8 ist

$$-\frac{1}{\overline{x}} = [\overline{a_{h-1}, \ldots, a_0}] > 1.$$

Damit ist $\frac{1}{\overline{x}} < -1$ und deshalb $-1 < \overline{x} < 0$, d.h. x ist reduziert.
(i)$\Longrightarrow$(ii): Sei x reduziert, und sei $(\xi_i)_{i\in\mathbb{N}_0}$ die zugehörige Hilfsfolge aus dem Kettenbruchalgorithmus 12.3. Wir bemerken zunächst, dass ξ_0 eine quadratische Irrationalzahl ist. Dies ergibt sich daraus, dass mit der Kettenbruchentwicklung der quadratischen Irrationalzahl x auch die Kettenbruchentwicklung von ξ_0 periodisch ist. Wir zeigen nun, dass ξ_0 reduziert ist. Nach Definition ist

$$\xi_0 = \frac{1}{x - \lfloor x \rfloor} > 1,$$

denn $x - \lfloor x \rfloor \in (0,1)$. Sei $d \in \mathbb{N}$ mit $x \in \mathbb{Q}(\sqrt{d})$. Wegen 13.4$(b)$ ist auch $\xi_0 = \frac{1}{x-\lfloor x \rfloor} \in \mathbb{Q}(\sqrt{d})$, und es ist

$$\overline{\xi_0} = \frac{1}{\overline{x - \lfloor x \rfloor}} \overset{13.4}{=} \frac{1}{\overline{x} - \lfloor x \rfloor}.$$

Aufgrund von $-1 < \overline{x} < 0$ und $\lfloor x \rfloor \geq 1$ folgt $\overline{x} - \lfloor x \rfloor < -1$ und somit $-1 < \overline{\xi_0} < 0$, d.h. ξ_0 ist reduziert. Induktiv folgt mit dergleichen Argumentation, dass ξ_i für jedes $i \in \mathbb{N}_0$ eine reduzierte quadratische Irrationalzahl ist (im Beweis spielt ξ_{i-1} die Rolle von x). Da x quadratische Irrationalzahl ist, besitzt x nach 13.3 eine periodische Kettenbruchentwicklung $((a_0, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}), x)$. Wir werden im Folgenden zeigen, dass $a_n = a_{n+h}$ ist. Die wiederholte Anwendung dieses Resultats liefert schließlich, dass die Kettenbruchentwicklung von x reinperiodisch ist, und der Beweis ist beendet. Nach den obigen Überlegungen ist ξ_{n-1} reduziert, also $0 < -\overline{\xi_{n-1}} < 1$ (im Fall $n = 0$ setzen wir hierbei $\xi_{-1} := x$). Aufgrund von

$$\xi_{n-1} = a_n + \frac{1}{\xi_n}$$

ist

$$-\frac{1}{\overline{\xi_n}} = a_n - \xi_{n-1},$$

woraus

$$-\frac{1}{\overline{\xi_n}} = a_n + (-\overline{\xi_{n-1}})$$

mit $-\overline{\xi_{n-1}} \in (0,1)$ folgt. Insbesondere ist

$$\lfloor -\frac{1}{\overline{\xi_n}} \rfloor = a_n.$$

Außerdem folgt mit 13.8:

$$-\frac{1}{\overline{\xi_n}} = [\overline{a_{n+h}, \ldots, a_{n+1}}]$$

und deshalb

$$a_{n+h} = \lfloor -\frac{1}{\overline{\xi_n}} \rfloor = a_n.$$

□

Zum Ende dieses Abschnittes werden wir uns mit der Kettenbruchentwicklung von Quadratwurzeln beschäftigen.

Beispiel 13.13.

$$\begin{aligned}
\sqrt{2} &= [1, \overline{2}] \\
\sqrt{3} &= [1, \overline{1,2}] \\
\sqrt{5} &= [2, \overline{4}] \\
\sqrt{7} &= [2, \overline{1,1,1,4}] \\
\sqrt{19} &= [4, \overline{2,1,3,1,2,8}]
\end{aligned}$$

Proposition 13.14. *Es sei $d \in \mathbb{N}$ kein Quadrat. Dann gilt: Die Kettenbruchentwicklung von $\sqrt{d}$ ist vom Typ $((a_0, \overline{a_1, \ldots, a_{h-1}, 2a_0}), \sqrt{d})$ mit $a_{h-i} = a_i$ für $i = 1, \ldots, h-1$.*

Beweis. Die Kettenbruchentwicklung von $\sqrt{d}$ sei durch $((a_n)_{n\in\mathbb{N}_0}, \sqrt{d})$ gegeben. Es ist $a_0 = \left\lfloor \sqrt{d} \right\rfloor$. Wir setzen $x := a_0 + \sqrt{d}$. Die Kettenbruchentwicklungen von $\sqrt{d}$ und x unterscheiden sich nur an der nullten Stelle: dort steht a_0 bei $\sqrt{d}$ sowie $2a_0$ bei x. Die quadratische Irrationalzahl x ist reduziert, denn $x > 1$ und

$$\overline{x} = a_0 - \sqrt{d} = \lfloor \sqrt{d} \rfloor - \sqrt{d} \in (-1, 0).$$

Aufgrund von 13.12 hat x eine reinperiodische Kettenbruchentwicklung der Form

$$((\overline{2a_0, a_1, \ldots, a_{h-1}}), x),$$

weswegen wir $((a_0, \overline{a_1, \ldots, a_{h-1}, 2a_0}), \sqrt{d})$ als Kettenbruchentwicklung von $\sqrt{d}$ erhalten. Es verbleibt der Nachweis der Symmetrieeigenschaft. Mit

$$\xi_0 = \frac{1}{x - 2a_0} = [\overline{a_1, \ldots, a_{h-1}, 2a_o}]$$

ergibt sich

$$-\frac{1}{\overline{\xi_0}} = [\overline{2a_0, a_{h-1}, \ldots, a_1}],$$

andererseits ist

$$-\frac{1}{\overline{\xi_0}} = -\frac{1}{\frac{1}{\overline{x} - 2a_0}} = -(\overline{x} - 2a_0) = -(a_0 - \sqrt{d} - 2a_0) = a_0 + \sqrt{d} = x.$$

Das impliziert

$$[\overline{2a_0, a_1, \ldots, a_{h-1}}] = [\overline{2a_0, a_{h-1}, \ldots, a_1}].$$

In Verbindung mit 13.8 folgt daraus: $a_{h-i} = a_i$ für $i = 1, \ldots, h-1$. □

§14 Die Pellsche Gleichung und diophantische Approximation

In diesem Abschnitt studieren wir die ***Pellsche Gleichung***

$$x^2 - dy^2 = 1, \quad d \in \mathbb{N} \text{ kein Quadrat}$$

und ihre ganzzahligen Lösungen bzw. allgemeiner Gleichungen der Form

$$x^2 - dy^2 = c, \quad d \in \mathbb{N} \text{ kein Quadrat}, \ c \in \mathbb{Z}.$$

Wir führen die folgende Bezeichnung ein:

$$L_d := \{(x, y) \in \mathbb{Z}^2 \mid x^2 - dy^2 = 1\},$$

d.h. L_d ist die Lösungsmenge der Pellschen Gleichung zum Parameter d. In jedem Fall enthält L_d die beiden Lösungen $(\pm 1, 0)$, die sogenannten trivialen Lösungen. Die Frage ist, ob L_d darüber hinaus weitere Elemente enthält. Wir werden als erstes zeigen, dass L_d unter der Annahme der Existenz einer nichttrivialen Lösung aus unendlich vielen Elementen besteht, und wir werden eine Beschreibung von L_d angeben. Wichtig dafür ist die folgende Beobachtung: Die Pellsche Gleichung $x^2 - dy^2 = 1$ kann man auch in der Form $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$ schreiben. Jedes Element aus L_d korrespondiert also zu einem Element $x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $x, y \in \mathbb{Z}$ und $(x + y\sqrt{d})(\overline{x + y\sqrt{d}}) = 1$.

Satz 14.1. *Es sei $d \in \mathbb{N}$ kein Quadrat. Dann gilt: Falls die Pellsche Gleichung $x^2 - dy^2 = 1$ eine nichttriviale ganzzahlige Lösung besitzt, so gibt es unter den Lösungen (x, y) in $L_d \cap \mathbb{N}^2$ eine eindeutig bestimmte Lösung mit minimalem x. Diese heißt die **Fundamentallösung** in L_d. Ist (a, b) die Fundamentallösung, so ist*

$$L_d = \{\pm(x_n, y_n) \in \mathbb{Z}^2 \mid x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n, \ n \in \mathbb{Z}\}.$$

Beweis. Aufgrund der vorausgesetzten Existenz einer nichttrivialen Lösung in L_d ist auch $L_d \cap \mathbb{N}^2 \neq \varnothing$. Da für eine Lösung $(x,y) \in L_d \cap \mathbb{N}^2$ der Wert von y durch den Wert von x eindeutig festgelegt ist, gibt es unter den Lösungen (x,y) in $L_d \cap \mathbb{N}^2$ eine eindeutig bestimmte Lösung mit minimalem x. Damit ist die Existenz und Eindeutigkeit der Fundamentallösung bereits gezeigt. Sei (a,b) im Folgenden die Fundamentallösung. Wir bemerken, dass für $(x_1,y_1),(x_2,y_2) \in L_d \cap \mathbb{N}^2$ mit $x_1 < x_2$ auch $y_1 < y_2$ gilt, denn es ist

$$y_2^2 = \frac{x_2^2 - 1}{d} > \frac{x_1^2 - 1}{d} = y_1^2.$$

Damit gilt offenbar für von (a,b) verschiedenes $(x,y) \in L_d \cap \mathbb{N}^2$ die Ungleichung

$$1 < a + b\sqrt{d} < x + y\sqrt{d}.$$

Sei nun $(x,y) \in L_d$. Wir bemerken, dass $x = 0$ zu $dy^2 = 1$ und damit zum Widerspruch führt, während $y = 0$ zu $x = \pm 1$ führt. Es ergeben sich daher die folgenden Fälle.

Fall 1: $x = \pm 1, y = 0$**.** Dann ist $x + y\sqrt{d} = \pm 1 = \pm(a + b\sqrt{d})^0$.

Fall 2: $x > 0$**,** $y > 0$**.** Dann existiert ein $n \in \mathbb{N}$ mit $x + y\sqrt{d} = (a + b\sqrt{d})^n$,

denn: Nehmen wir an, dies wäre nicht der Fall. Dann existiert ein $n \in \mathbb{N}$ mit

$$(a + b\sqrt{d})^n < x + y\sqrt{d} < (a + b\sqrt{d})^{n+1}.$$

Es ist $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = 1$ und somit

$$1 = (a + b\sqrt{d})^n(a - b\sqrt{d})^n < (x + y\sqrt{d})(a - b\sqrt{d})^n < (a + b\sqrt{d})^{n+1}(a - b\sqrt{d})^n = a + b\sqrt{d}.$$

Es gibt $\tilde{a}, \tilde{b} \in \mathbb{Z}$ mit $(x + y\sqrt{d})(a - b\sqrt{d})^n = \tilde{a} + \tilde{b}\sqrt{d}$. Wir erhalten

$$(x - y\sqrt{d})(a + b\sqrt{d})^n = \overline{x + y\sqrt{d}} \cdot \overline{(a - b\sqrt{d})^n} = \overline{(x + y\sqrt{d})(a - b\sqrt{d})^n} = \overline{\tilde{a} + \tilde{b}\sqrt{d}} = \tilde{a} - \tilde{b}\sqrt{d}.$$

Das liefert

$$\begin{aligned} \tilde{a}^2 - d\tilde{b}^2 =& (\tilde{a} + \tilde{b}\sqrt{d})(\tilde{a} - \tilde{b}\sqrt{d}) = (x + y\sqrt{d})(a - b\sqrt{d})^n(x - y\sqrt{d})(a + b\sqrt{d})^n \\ =& (x^2 - dy^2)(a^2 - db^2)^n = 1, \end{aligned}$$

und somit ist $(\tilde{a}, \tilde{b}) \in L_d$. Wegen $\tilde{a} + \tilde{b}\sqrt{d} < a + b\sqrt{d}$ kann $(\tilde{a}, \tilde{b})$ nicht in $L_d \cap \mathbb{N}^2$ liegen. Wäre $\tilde{a} \leq 0$ und $\tilde{b} > 0$, dann wäre

$$0 > -\frac{1}{\tilde{a} + \tilde{b}\sqrt{d}} = -(\tilde{a} - \tilde{b}\sqrt{d}) = -\tilde{a} + \tilde{b}\sqrt{d} > 0.$$

Wäre $\tilde{a} > 0$ und $\tilde{b} \leq 0$, dann wäre

$$1 > \frac{1}{\tilde{a} + \tilde{b}\sqrt{d}} = \tilde{a} - \tilde{b}\sqrt{d} \geq \tilde{a} + \tilde{b}\sqrt{d} > 1.$$

Folglich ist sowohl $\tilde{a} \leq 0$ als auch $\tilde{b} \leq 0$, im Widerspruch zu $\tilde{a} + \tilde{b}\sqrt{d} > 1$. #

Fall 3: $x < 0, y < 0$**.** Dann ist

$$x + y\sqrt{d} = -(-x - y\sqrt{d}) = -(a + b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2.

Fall 4: $x > 0, y < 0$**.** Dann ist

$$\frac{1}{x + y\sqrt{d}} = x - y\sqrt{d} = (a + b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2 und deshalb $x + y\sqrt{d} = (a + b\sqrt{d})^{-n}$.

Fall 5: $x < 0, y > 0$**.** Dann ist

$$-\frac{1}{x + y\sqrt{d}} = -x + y\sqrt{d} = (a + b\sqrt{d})^n$$

für ein $n \in \mathbb{N}$ nach Fall 2 und deshalb $x + y\sqrt{d} = -(a + b\sqrt{d})^{-n}$.

Seien nun umgekehrt $n \in \mathbb{Z}$ und $x_n, y_n \in \mathbb{Z}$ mit $x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n$. Dann ist

$$x_n - y_n\sqrt{d} = \overline{x_n + y_n\sqrt{d}} = \overline{(a + b\sqrt{d})^n} = (a - b\sqrt{d})^n.$$

und somit

$$x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (a + b\sqrt{d})^n(a - b\sqrt{d})^n = (a^2 - db^2)^n = 1,$$

d.h. $(x_n, y_n) \in L_d$. Damit ist auch $(-x_n, -y_n) \in L_d$. □

Der vorangegangene Satz sagt leider nichts über die Existenz einer nichttrivialen Lösung der Pellschen Gleichung aus. Unser Ziel im weiteren Verlauf des Abschnittes wird es sein, nichttriviale Lösungen der Pellschen Gleichung zu konstruieren. Die Theorie der Kettenbrüche kommt dabei wie folgt ins Spiel: Ist $(x, y) \in \mathbb{N}^2$ eine Lösung von $x^2 - dy^2 = 1$, dann ist

$$\frac{x}{y} = \sqrt{d + \frac{1}{y^2}}$$

eine sehr gute rationale Näherung von $\sqrt{d}$. Wir werden zeigen, dass es sich um eine sogenannte diophantische Approximation von $\sqrt{d}$ handelt. Wie sich herausstellt, sind diophantische Approximationen einer reellen Zahl durch Näherungsbrüche dieser reellen Zahl gegeben. Somit werden uns Näherungsbruche $\frac{p_n}{q_n}$ von $\sqrt{d}$ nichttriviale Lösungen (p_n, q_n) der Pellschen Gleichung liefern.

Definition 14.2. *Es sei $\alpha \in \mathbb{R}$, und es sei $z = \frac{p}{q} \in \mathbb{Q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$ und $\mathrm{ggT}(p, q) = 1$. Die rationale Zahl z heißt eine **diophantische Approximation** von α, wenn für alle $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}$ mit $\tilde{q} \leq q$ und $\frac{\tilde{p}}{\tilde{q}} \neq \frac{p}{q}$ die Ungleichung*

$$|\alpha q - p| < |\alpha\tilde{q} - \tilde{p}|$$

gilt.

Ist $z = \frac{p}{q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$ und $\mathrm{ggT}(p,q) = 1$ eine diophantische Approximation von α, dann gibt es keine rationale Zahl $\frac{\tilde{p}}{\tilde{q}}$ mit $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}, \tilde{q} \leq q$ und

$$\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| \leq \left|\alpha - \frac{p}{q}\right|,$$

denn andernfalls wäre

$$|\alpha\tilde{q} - \tilde{p}| = \tilde{q}\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| \leq q\left|\alpha - \frac{p}{q}\right| = |\alpha q - p|.$$

Die Umkehrung hiervon ist falsch: Es gibt etwa keine rationale Zahl $\frac{\tilde{p}}{\tilde{q}} \neq \frac{1}{3}$ mit $\tilde{p} \in \mathbb{Z}, \tilde{q} \in \mathbb{N}$, $\tilde{q} \leq 3$ und

$$\left|\frac{1}{5} - \frac{\tilde{p}}{\tilde{q}}\right| \leq \left|\frac{1}{5} - \frac{1}{3}\right| = \frac{2}{15},$$

aber $\frac{1}{3}$ ist keine diophantische Approximation von $\frac{1}{5}$, denn es ist $\frac{0}{1} \neq \frac{1}{3}$, $1 < 3$ und

$$\left|\frac{1}{5} \cdot 1 - 0\right| = \frac{1}{5} < \left|\frac{1}{5} \cdot 3 - 1\right| = \frac{2}{5}.$$

Satz 14.3. *Es sei $\alpha \in \mathbb{R}$, und $\left(\frac{p_n}{q_n}\right)_{n \in I}$ mit $I = \mathbb{N}_0$, falls $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist und $I = \{0, \ldots, k\}$, falls $\alpha \in \mathbb{Q}$ ist, bezeichne die Folge der Näherungsbrüche von α. Sei $z \in \mathbb{Q}$ eine diophantische Approximation von α. Dann gibt es ein $n \in I$ mit $z = \frac{p_n}{q_n}$, d.h. z ist ein Näherungsbruch von α.*

Beweis. Wir schreiben $z = \frac{p}{q}$ mit $p \in \mathbb{Z}$, $q \in \mathbb{N}$ und $\mathrm{ggT}(p,q) = 1$. Ist $\alpha = a_0 \in \mathbb{Z}$, so folgt $|\alpha \cdot 1 - a_0| = 0$, d.h. $\frac{a_0}{1} = \alpha$ ist die einzige diophantische Approximation von α, also ist $z = \frac{a_0}{1} = \frac{p_0}{q_0}$. Im Folgenden sei $\alpha \notin \mathbb{Z}$. Insbesondere ist $k \geq 1$, falls $\alpha \in \mathbb{Q}$ ist. Nach 12.12 gilt

$$a_0 = \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots \leq \alpha \leq \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Ist z nicht von der Form $\frac{p_n}{q_n}$ für ein $n \in \mathbb{N}_0$, dann liegt z in einem der Intervalle $(-\infty, \frac{p_0}{q_0})$, $(\frac{p_1}{q_1}, \infty)$ oder in einem Intervall zwischen zwei Näherungsbrüchen.

Fall 1: $z < \frac{p_0}{q_0}$**.** Wegen $\frac{p_0}{q_0} = a_0 \leq \alpha$ folgt $|\alpha - a_0| < |\alpha - z|$, d.h. die rationale Zahl $\frac{a_0}{1}$ liegt näher an α als z, weswegen z keine diophantische Approximation von α sein kann.

Fall 2: $z > \frac{p_1}{q_1}$**.** Wegen $\frac{p_1}{q_1} \geq \alpha$ folgt

$$|\alpha - z| = \left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_1}{q_1} - \frac{p}{q}\right| = \frac{|p_1 q - p q_1|}{q_1 q} \geq \frac{1}{q_1 q}$$

und deshalb

$$|\alpha q - p| \geq \frac{1}{q_1} = \frac{1}{q_1 q_0} \overset{12.14,12.15}{\geq} \left|\alpha - \frac{p_0}{q_0}\right| = |\alpha \cdot 1 - a_0|.$$

Weil $z = \frac{p}{q}$ eine diophantische Approximation von α ist, folgt $\frac{a_0}{1} = \frac{p}{q}$ und deshalb

$$\frac{p_0}{q_0} = \frac{a_0}{1} = \frac{p}{q} = z > \frac{p_1}{q_1}$$

im Widerspruch zu 12.12.

Fall 3: $\frac{p_{n-1}}{q_{n-1}} < \frac{p}{q} < \frac{p_{n+1}}{q_{n+1}}$ **für ein ungerades** $n \in \mathbb{N}$ **mit** $n+1 \leq k$**, falls** $\alpha \in \mathbb{Q}$**.** Wir erhalten

$$\frac{1}{qq_{n-1}} \leq \frac{|pq_{n-1} - p_{n-1}q|}{qq_{n-1}} = \left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_{n-1}}{q_{n-1}}\right| \leq \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \overset{12.14,12.15}{\leq} \frac{1}{q_{n-1}q_n}$$

und somit $q_n < q$. Außerdem ist

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}},$$

woraus sich

$$|\alpha q - p| \geq \frac{1}{q_{n+1}} = q_n \frac{1}{q_n q_{n+1}} \overset{12.14,12.15}{\geq} q_n \left|\alpha - \frac{p_n}{q_n}\right| = |\alpha q_n - p_n|$$

ergibt. Da $z = \frac{p}{q}$ eine diophantische Approximation von α ist, folgt wegen $q_n < q$, dass $\frac{p}{q} = \frac{p_n}{q_n}$ ist, was ein Widerspruch zu $\mathrm{ggT}(p,q) = 1$ ist.

Fall 4: $\frac{p_{n+1}}{q_{n+1}} < \frac{p}{q} < \frac{p_{n-1}}{q_{n-1}}$ **für ein gerades** $n \in \mathbb{N}$ **mit** $n+1 \leq k$**, falls** $\alpha \in \mathbb{Q}$**.** Dieser Fall wird analog zu Fall 3 behandelt.

Fall 5: $\alpha = \frac{p_k}{q_k} < \frac{p}{q} < \frac{p_{k-1}}{q_{k-1}}$ **für** $\alpha \in \mathbb{Q}$ **und** k **gerade.** Dieser Fall wird analog zu Fall 3 behandelt.

Fall 6: $\frac{p_{k-1}}{q_{k-1}} < \frac{p}{q} < \frac{p_k}{q_k} = \alpha$ **für** $\alpha \in \mathbb{Q}$ **und** k **ungerade.** Dieser Fall wird analog zu Fall 3 behandelt.

Da alle Fälle zum Widerspruch führen, ist z von der Form $\frac{p_n}{q_n}$ für ein $n \in \mathbb{N}_0$. □

Satz 14.4. *Es sei* $\alpha \in \mathbb{R}$*, und* $\left(\frac{p_n}{q_n}\right)_{n\in I}$ *mit* $I = \mathbb{N}_0$*, falls* $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ *ist und* $I = \{0, \ldots, k\}$*, falls* $\alpha \in \mathbb{Q}$ *ist, bezeichne die Folge der Näherungsbrüche aus der Kettenbruchentwicklung von* α*. Dann ist* $\frac{p_n}{q_n}$ *eine diophantische Approximation von* α *für alle* $n \in I$ *mit* $n \geq 1$*.*

Beweis. Im Folgenden sei $n \in I$ mit $n \geq 1$. Wir setzen

$$B_n := \{(p,q) \in \mathbb{Z} \times \mathbb{N} \mid q \leq q_n \text{ und } |\alpha q - p| \text{ minimal}\}.$$

B_n ist wohldefiniert und nichtleer, denn die zweite Komponente kann nur endlich viele Werte annehmen, und für festes q gilt $|\alpha q - p| \to \infty$ für $p \to \infty$ und $p \to -\infty$. Darüber hinaus setzen wir

$$q^* := \min\{q \in \mathbb{N} \mid \text{Es existiert ein } p \in \mathbb{Z} \text{ mit } (p,q) \in B_n\}.$$

Es gibt genau ein $p^* \in \mathbb{Z}$ mit $(p^*, q^*) \in B_n$,

denn: Wir nehmen an, dass es $p^*, \tilde{p}$ mit $(p^*, q^*), (\tilde{p}, q^*) \in B_n$ und $p^* \neq \tilde{p}$ gibt. Wir erhalten

$$|\alpha q^* - p^*| = |\alpha q^* - \tilde{p}|$$

und deshalb

$$\left|\alpha - \frac{p^*}{q^*}\right| = \left|\alpha - \frac{\tilde{p}}{q^*}\right|.$$

Wegen $p^* \neq \tilde{p}$ ist $\frac{p^*}{q^*} \neq \frac{\tilde{p}}{q^*}$ und deshalb

$$\alpha = \frac{p^* + \tilde{p}}{2q^*}.$$

Das liefert

$$|\alpha q^* - p^*| = \left|\frac{p^* + \tilde{p}}{2} - p^*\right| = \left|\frac{\tilde{p} - p^*}{2}\right| \geq \frac{1}{2}.$$

Fall 1: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ oder $\alpha \in \mathbb{Q}$ mit $k \geq 2$, jeweils mit $a_1 > 1$. Dann ist $q_2 > q_1 > q_0 = 1$, also $q_2 \geq 3$ und somit

$$|\alpha q_1 - p_1| = q_1 \left|\alpha - \frac{p_1}{q_1}\right| \leq q_1 \frac{1}{q_1 q_2} = \frac{1}{q_2} \leq \frac{1}{3},$$

was ein Widerspruch zur Minimalität von $|\alpha q^* - p^*| \geq \frac{1}{2}$ ist.

Fall 2: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ oder $\alpha \in \mathbb{Q}$ mit $k \geq 2$, jeweils mit $a_1 = 1$. Es ergibt sich $q_1 = q_0 = 1$, $\frac{p_0}{q_0} = a_0$, $\frac{p_1}{q_1} = a_0 + 1$. Wegen $\alpha \neq [a_0, 2]$ ist $|\alpha - a_0| < \frac{1}{2}$ oder $|\alpha - (a_0 + 1)| < \frac{1}{2}$. Es ist jedoch $|\alpha - a_0| = |\alpha q_0 - p_0|$ und $|\alpha - (a_0 + 1)| = |\alpha q_1 - p_1|$. Das liefert $|\alpha q_0 - p_0| < \frac{1}{2}$ oder $|\alpha q_1 - p_1| < \frac{1}{2}$, im Widerspruch zur Minimalität von $|\alpha q^* - p^*| \geq \frac{1}{2}$.

Fall 3: $\alpha \in \mathbb{Q}$ mit $k = 1$. Dann ist $\alpha = \frac{p_1}{q_1}$, also $|\alpha q_1 - p_1| = 0$, was wiederum zum Widerspruch führt. #

Es ist $\mathrm{ggT}(p^*, q^*) = 1$, andernfalls wären p^*, q^* von der Form $p^* = d\tilde{p}, q^* = d\tilde{q}$ mit einem $d > 1$. Das hätte

$$|\alpha\tilde{q} - \tilde{p}| < d\,|\alpha\tilde{q} - \tilde{p}| = |\alpha q^* - p^*|$$

zur Folge, was ein Widerspruch ist. Nach Konstruktion ist $\frac{p^*}{q^*}$ eine diophantische Approximation von α. Aufgrund von 14.3 gibt es ein $m \in \mathbb{N}_0$ mit $\frac{p^*}{q^*} = \frac{p_m}{q_m}$. Wegen $q^* \leq q_n$ folgt $m \leq n$ (hier geht $n \geq 1$ ein; für $n = 0$ wäre auch $m = 1$ möglich). Weil $\mathrm{ggT}(p^*, q^*) = 1$ ist, erhalten wir $p^* = p_m$, $q^* = q_m$. Es ist $m = n$,

denn: Wir nehmen an, dass $m < n$ ist. Aufgrund von 12.14 ist

$$|\alpha q_m - p_m| = q_m \left|\alpha - \frac{p_m}{q_m}\right| > \frac{1}{q_m + q_{m+1}} \geq \frac{1}{q_{n-1} + q_n}.$$

Nach Konstruktion von $p^* = p_m$, $q^* = q_m$ ist

$$|\alpha q_m - p_m| \leq |\alpha q_n - p_n| = q_n \left|\alpha - \frac{p_n}{q_n}\right| \overset{12.14}{\leq} q_n \frac{1}{q_n q_{n+1}} = \frac{1}{q_{n+1}}.$$

Damit erhalten wir

$$\frac{1}{q_{n-1}+q_n} < \frac{1}{q_{n+1}},$$

also $q_{n+1} < q_n + q_{n-1}$, was ein Widerspruch ist, denn $q_{n+1} = a_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1}$. #

Somit ist $\frac{p_n}{q_n} = \frac{p^*}{q^*}$ eine diophantische Approximation von α. □

Eine genaue Analyse des Beweises zeigt, dass die Aussage von Satz 14.4 auch im Fall $n = 0$ gültig ist, allerdings mit folgenden Ausnahmen:

- $\alpha = [a_0, 2]$,
- $\alpha = [a_0, 1, \ldots, a_k]$ mit $k \geq 2$,
- $\alpha = [a_0, 1, a_2, \ldots]$,

bei denen $\frac{p_0}{q_0}$ keine diophantische Approximation von α ist.

Satz 14.5. *Es sei $\alpha \in \mathbb{R}$, und es seien $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit $\mathrm{ggT}(p,q) = 1$ und*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Dann ist $\frac{p}{q}$ eine diophantische Approximation von α, insbesondere ist $\frac{p}{q}$ ein Näherungsbruch von α.

Beweis. Es seien $\tilde{p} \in \mathbb{Z}$, $\tilde{q} \in \mathbb{N}$ mit $\tilde{q} \leq q$, $\frac{\tilde{p}}{\tilde{q}} \neq \frac{p}{q}$ und $|\alpha\tilde{q} - \tilde{p}| \leq |\alpha q - p|$. Es ergibt sich

$$\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| = \frac{1}{\tilde{q}}\,|\alpha\tilde{q} - \tilde{p}| \leq \frac{1}{\tilde{q}}\,|\alpha q - p| = \frac{q}{\tilde{q}}\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q\tilde{q}}.$$

Das liefert

$$\left|\frac{\tilde{p}}{\tilde{q}} - \frac{p}{q}\right| \leq \left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{2q\tilde{q}} + \frac{1}{2q^2} = \frac{q+\tilde{q}}{2q^2\tilde{q}}.$$

Andererseits ist

$$\left|\frac{p}{q} - \frac{\tilde{p}}{\tilde{q}}\right| = \frac{|\tilde{p}q - p\tilde{q}|}{q\tilde{q}} \geq \frac{1}{q\tilde{q}}.$$

Wir erhalten

$$\frac{1}{q\tilde{q}} < \frac{q+\tilde{q}}{2q^2\tilde{q}}$$

und deshalb

$$2q < q + \tilde{q},$$

also

$$q < \tilde{q},$$

was ein Widerspruch ist. Somit ist $\frac{p}{q}$ eine diophantische Approximation von α. Aufgrund von 14.3 ist $\frac{p}{q}$ ein Näherungsbruch von α. □

Satz 14.6. *Es sei $d \in \mathbb{N}$ kein Quadrat, und es sei $c \in \mathbb{Z}$ mit $|c| < \frac{1}{2}(\sqrt{f} + \sqrt{d})$, wobei*

$$f = \begin{cases} d & \text{falls } c \geq 0 \\ \max\{c+d, 0\} & \text{falls } c < 0. \end{cases}$$

Es bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$.
Dann gibt es für jede Lösung $(p,q) \in \mathbb{N}^2$ der Gleichung $x^2 - dy^2 = c$ ein $n \in \mathbb{N}_0$, so dass $\frac{p}{q} = \frac{p_n}{q_n}$ ist. Ist insbesondere $\mathrm{ggT}(p,q) = 1$, so ist $p = p_n$ und $q = q_n$.

Beweis. Es seien $p, q \in \mathbb{N}$ mit $p^2 - dq^2 = c$, und es seien $\tilde{p}, \tilde{q} \in \mathbb{N}$ mit $\mathrm{ggT}(\tilde{p}, \tilde{q}) = 1$ und $\frac{p}{q} = \frac{\tilde{p}}{\tilde{q}}$. Dann ist

$$p - q\sqrt{d} = \frac{c}{p + q\sqrt{d}},$$

und es ist

$$p = \sqrt{c + dq^2}.$$

Das liefert

$$\left|\sqrt{d} - \frac{\tilde{p}}{\tilde{q}}\right| = \left|\sqrt{d} - \frac{p}{q}\right| = \frac{|c|}{q(p + q\sqrt{d})} = \frac{|c|}{q(\sqrt{c + dq^2} + q\sqrt{d})} = \frac{|c|}{q^2(\sqrt{\frac{c}{q^2} + d} + \sqrt{d})}$$
$$\leq \frac{|c|}{q^2(\sqrt{f} + \sqrt{d})} < \frac{1}{2q^2} \leq \frac{1}{2\tilde{q}^2},$$

weswegen $\frac{p}{q} = \frac{\tilde{p}}{\tilde{q}}$ nach 14.5 eine diophantische Approximation von $\sqrt{d}$ und somit ein Näherungsbruch von $\sqrt{d}$ ist. □

Korollar 14.7. *Es sei $d \in \mathbb{N}$ kein Quadrat. Es bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$. Dann gilt:*

$$L_d \cap \mathbb{N}^2 \subseteq \{(p_n, q_n) \mid n \in \mathbb{N}_0\},$$

d.h. für jede Lösung $(p,q) \in \mathbb{N}^2$ der Pellschen Gleichung $x^2 - dy^2 = 1$ ist $\frac{p}{q}$ ein Näherungsbruch von $\sqrt{d}$.

Beweis. Wir bemerken zum Beweis, dass für $c = 1$ die Abschätzung aus 14.6 trivialerweise erfüllt ist, und dass für jede Lösung $(p,q) \in \mathbb{N}^2$ der Pellschen Gleichung $x^2 - dy^2 = 1$ stets $\mathrm{ggT}(p,q) = 1$ gilt, denn jeder gemeinsame Teiler von p, q teilt auch $p^2 - dq^2 = 1$. □

Die Aussage des Korollars impliziert jedoch noch nicht, dass unter den Näherungsbrüchen wie oben auch tatsächlich Lösungen der Pellschen Gleichung auftreten. Davon müssen wir uns im weiteren Verlauf noch überzeugen.

Beispiel 14.8. *Es sei $d = 3$. Es ist $\sqrt{3} = [1, \overline{1,2}]$ und demzufolge*

$$\frac{p_0}{q_0} = \frac{1}{1}, \frac{p_1}{q_1} = \frac{2}{1}, \frac{p_2}{q_2} = \frac{5}{3}, \frac{p_3}{q_3} = \frac{7}{4}, \frac{p_4}{q_4} = \frac{19}{11}.$$

Das liefert

$$p_0^2 - 3q_0^2 = -2, \quad p_1^2 - 3q_1^2 = 1, \quad p_2^2 - 3q_2^2 = -2, \quad p_3^2 - 3q_3^2 = 1, \quad p_4^2 - 3q_4^2 = -2.$$

Unter den ersten fünf Näherungsbrüchen liefern also $\frac{p_1}{q_1}$ und $\frac{p_3}{q_3}$ Lösungen der Pellschen Gleichung $x^2 - 3y^2 = 1$. Die Fundamentallösung ist offenbar durch $(p_1, q_1) = (2, 1)$ gegeben.

Satz 14.9. *Es sei $d \in \mathbb{N}$ kein Quadrat. Die Kettenbruchentwicklung von $\sqrt{d}$ sei durch*

$$((a_0, \overline{a_1, \ldots, a_h}), \sqrt{d})$$

mit Periodenlänge h gegeben. Es bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$, die Folge $(\xi_n)_{n\in\mathbb{N}_0}$ sei wie im Kettenbruchalgorithmus 12.3 definiert. Wir setzen $b_0 := \left\lfloor \sqrt{d} \right\rfloor$, $c_{-1} := 1$, $c_0 := d - b_0^2$,

$$b_{n+1} := a_n c_n - b_n,$$
$$c_{n+1} := c_{n-1} + 2a_n b_n - a_n^2 c_n$$

für $n \geq 0$. Dann gilt für alle $n \in \mathbb{N}_0$:

(a) $\xi_n = \frac{b_n + \sqrt{d}}{c_n}$,
(b) $p_n^2 - dq_n^2 = (-1)^{n+1} c_n$,
(c) $0 < c_n < 2\sqrt{d}$,
(d) $c_n = 1 \iff n \equiv -1 \pmod{h}$.

Beweis. Wir zeigen zunächst die Gleichung

$$d - b_{n+1}^2 = c_n c_{n+1}$$

für $n \geq -1$ per Induktion. Für $n = -1$ ist $d - b_0^2 = c_0 = c_0 c_{-1}$. Für $n > -1$ ist

$$\begin{aligned} d - b_{n+1}^2 &= d - (a_n c_n - b_n)^2 = (d - b_n^2) + (2a_n c_n b_n - a_n^2 c_n^2) = d - b_n^2 + c_n(c_{n+1} - c_{n-1}) \\ &= c_{n-1} c_n + c_n c_{n+1} - c_n c_{n-1} = c_n c_{n+1}. \end{aligned}$$

Da d kein Quadrat ist, impliziert dies insbesondere, dass $c_n \neq 0$ für alle $n \in \mathbb{N}_0$ ist.
(a) Wir zeigen die Behauptung per Induktion. Für $n = 0$ ist $a_0 = \left\lfloor \sqrt{d} \right\rfloor$,

$$\xi_0 = \frac{1}{\sqrt{d} - \left\lfloor \sqrt{d} \right\rfloor} = \frac{1}{\sqrt{d} - b_0} = \frac{b_0 + \sqrt{d}}{d - b_0^2} = \frac{b_0 + \sqrt{d}}{c_0}.$$

Für $n > 1$ erhalten wir

$$\xi_{n+1} = \frac{1}{\xi_n - a_n} = \frac{c_n}{b_n + \sqrt{d} - a_n c_n} = \frac{c_n}{\sqrt{d} - b_{n+1}} = \frac{c_n(b_{n+1} + \sqrt{d})}{d - b_{n+1}^2} = \frac{c_n(b_{n+1} + \sqrt{d})}{c_n c_{n+1}}$$
$$= \frac{b_{n+1} + \sqrt{d}}{c_{n+1}}.$$

(b) Sei $n \in \mathbb{N}_0$. Aufgrund von 12.11 ist

$$\sqrt{d} = \frac{\xi_n p_n + p_{n-1}}{\xi_n q_n + q_{n-1}} = \frac{(b_n + \sqrt{d})p_n + c_n p_{n-1}}{(b_n + \sqrt{d})q_n + c_n q_{n-1}}.$$

und somit

$$((b_n + \sqrt{d})q_n + c_n q_{n-1})\sqrt{d} = (b_n + \sqrt{d})p_n + c_n p_{n-1}.$$

Das liefert

$$(b_n p_n + c_n p_{n-1} - d q_n) + (p_n - b_n q_n - c_n q_{n-1})\sqrt{d} = 0,$$

was wegen 13.5

$$b_n p_n + c_n p_{n-1} - d q_n = 0 \text{ und } p_n - b_n q_n - c_n q_{n-1} = 0$$

zur Folge hat. Wir erhalten

$$q_n(b_n p_n + c_n p_{n-1} - d q_n) + p_n(p_n - b_n q_n - c_n q_{n-1}) = 0$$

und damit

$$p_n^2 + c_n(p_{n-1}q_n - p_n q_{n-1}) - d q_n^2 = 0.$$

Unter Verwendung von 12.11 ergibt sich

$$p_n^2 - d q_n^2 = (-1)^{n+1} c_n.$$

(c) Wir zeigen die Aussage per Induktion nach n. Für $n = 0$ ist

$$c_0 = d - \left\lfloor \sqrt{d} \right\rfloor^2 = (\sqrt{d} - \left\lfloor \sqrt{d} \right\rfloor)(\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor),$$

woraus sich $0 < c_0 < 2\sqrt{d}$ ergibt. Sei nun $n \geq 1$. Aufgrund von 13.14 besitzt ξ_n eine reinperiodische Kettenbruchentwicklung. Wegen 13.12 ist ξ_n reduziert, es ist also $\xi_n > 1$ und $-1 < \overline{\xi_n} < 0$. Wir erhalten

$$0 < \xi_n - \overline{\xi_n} = \frac{b_n + \sqrt{d}}{c_n} - \frac{b_n - \sqrt{d}}{c_n} = \frac{2\sqrt{d}}{c_n},$$

was $c_n > 0$ zur Folge hat. Das liefert

$$|b_n| = \sqrt{d - c_{n-1}c_n} < \sqrt{d}.$$

Aufgrund von $\xi_n > 1$ ergibt sich $c_n < c_n \xi_n = b_n + \sqrt{d} \leq |b_n| + \sqrt{d} < 2\sqrt{d}$.

(d) Sei zunächst $n \in \mathbb{N}_0$ mit $n \equiv -1 \pmod{h}$, d.h. es gibt ein $k \in \mathbb{N}$ mit $n = kh - 1$. Es ist

$$\begin{aligned}\xi_n &= [a_{n+1}, a_{n+2}, \ldots] = [a_{kh}, a_{kh+1}, \ldots] = [\overline{a_h, a_1, \ldots, a_{h-1}}] = [a_h, \overline{a_1, \ldots, a_h}] \overset{13.14}{=} [2a_0, \overline{a_1, \ldots, a_h}] \\ &= a_0 + [a_0, \overline{a_1, \ldots, a_h}] = a_0 + \sqrt{d}\end{aligned}$$

und damit $c_n = 1$. Sei nun umgekehrt $n \in \mathbb{N}_0$ mit $c_n = 1$. Dann ist $\xi_n = b_n + \sqrt{d}$, deshalb ist ξ_n von der Form

$$\xi_n = [\tilde{a}_0, a_1, a_2, \ldots]$$

mit einem $\tilde{a}_0 \in \mathbb{Z}$. Da ξ_n reduziert ist (siehe Beweis von (c); das gilt auch für $n = 0$), ist $\xi_n > 1$ und deshalb $\tilde{a}_0 \in \mathbb{N}$. Wegen $\sqrt{d} = [a_0, a_1, \ldots, a_n, \xi_n]$ erhalten wir

$$[a_0, a_1, \ldots] = \sqrt{d} = [a_0, a_1, \ldots, a_n, \tilde{a}_0, a_1, a_2, \ldots].$$

Aus der Eindeutigkeit der Kettenbruchentwicklung ergibt sich $a_{i+(n+1)} = a_i$ für alle $i \geq 1$. Andererseits gilt ebenfalls $a_{i+h} = a_i$ für alle $i \geq 1$. Wir schreiben $n + 1 = qh + r$ mit einem $r \in \mathbb{N}_0$ mit $0 \leq r < h$. Dann erhalten wir für alle $i \geq 1$ die Identität

$$a_i = a_{i+(n+1)} = a_{i+qh+r} = a_{i+r},$$

was wegen der Minimalität von h zu $r = 0$ führt. Deshalb folgt $h|(n+1)$ und somit $n \equiv -1 \pmod{h}$. □

Korollar 14.10 (Legendre). *Es sei $d \in \mathbb{N}$ kein Quadrat. Es bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$, und h sei die Periodenlänge von $\sqrt{d}$. Ferner sei*

$$\tilde{h} := \begin{cases} h, & \text{falls } h \text{ gerade,} \\ 2h, & \text{falls } h \text{ ungerade.} \end{cases}$$

Dann gilt:

$$L_d \cap \mathbb{N}^2 = \{(p_{k\tilde{h}-1}, q_{k\tilde{h}-1}) \mid k \in \mathbb{N}\}$$

Die Fundamentallösung in L_d ist durch $(p_{\tilde{h}-1}, q_{\tilde{h}-1})$ gegeben.

Beweis. Sei zunächst $(p, q) \in L_d \cap \mathbb{N}^2$. Aufgrund von 14.7 gibt es ein $n \in \mathbb{N}_0$ mit $p = p_n, q = q_n$. Wegen 14.9 ist

$$1 = p^2 - dq^2 = p_n^2 - dq_n^2 = (-1)^{n+1} c_n$$

mit c_n wie in 14.9, insbesondere ist $c_n > 0$. Somit ist n ungerade und $c_n = 1$. Aus 14.9 folgt $n \equiv -1 \pmod{h}$, d.h. es gibt ein $\tilde{k} \in \mathbb{N}$ mit $n = \tilde{k}h - 1$, wobei $\tilde{k}$ genau dann gerade ist, wenn h ungerade ist. Somit existiert ein $k \in \mathbb{N}$ mit $n = k\tilde{h} - 1$, d.h. es ist $(p, q) = (p_{k\tilde{h}-1}, q_{k\tilde{h}-1})$.

Ist umgekehrt $n = k\tilde{h} - 1$ mit einem $k \in \mathbb{N}$, dann ist

$$p_n^2 - dq_n^2 = p_{k\tilde{h}-1}^2 - dq_{k\tilde{h}-1}^2 \overset{14.9}{=} (-1)^{k\tilde{h}} c_{k\tilde{h}-1} \overset{14.9}{=} 1,$$

d.h. $(p_n, q_n) \in L_d \cap \mathbb{N}^2$.

Aufgrund von 12.11 ist $q_{\tilde{h}-1} < q_{2\tilde{h}-1} < \ldots$, und wegen $p_{\tilde{k}h-1} = \sqrt{1 + dq_{\tilde{k}h-1}^2}$ folgt $p_{\tilde{h}-1} < p_{2\tilde{h}-1} < \ldots$. Somit ist $(p_{\tilde{h}-1}, q_{\tilde{h}-1})$ die Fundamentallösung in L_d. □

Beispiel 14.11. *Es sei $d = 23$. Es ist $\sqrt{23} = [4, \overline{1,3,1,8}]$ und somit $h = 4$, $\tilde{h} = 4$. Aus diesem Grund ist (p_3, q_3) die Fundamentallösung der Pellschen Gleichung $x^2 - 23y^2 = 1$. Wir berechnen*

$$\begin{pmatrix} p_3 & p_2 \\ q_3 & q_2 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 24 & 19 \\ 5 & 4 \end{pmatrix},$$

d.h. $(24, 5)$ ist die Fundamentallösung der Pellschen Gleichung $x^2 - 23y^2 = 1$.

Korollar 14.12. *Es sei $d \in \mathbb{N}$ kein Quadrat. Es bezeichne $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$, und h sei die Periodenlänge von $\sqrt{d}$. Dann gilt:*

(a) *Ist h gerade, dann hat die Gleichung $x^2 - dy^2 = -1$ keine Lösung $(p, q) \in \mathbb{Z}^2$.*

(b) *Ist h ungerade, dann sind die Lösungen $(p, q) \in \mathbb{N}^2$ der Gleichung $x^2 - dy^2 = -1$ durch (p_{kh-1}, q_{kh-1}), $k \in \mathbb{N}$ ungerade, gegeben.*

Beweis. Offenbar hat die Gleichung $x^2 - dy^2 = -1$ keine ganzzahligen Lösungen mit $x = 0$ oder $y = 0$. Aufgrund von 14.6 mit $c = -1$ und unter Verwendung von

$$|-1| = 1 < \frac{1}{2}(1 + \sqrt{2}) \leq \frac{1}{2}(\sqrt{d-1} + \sqrt{d})$$

folgt, dass es für jede Lösung $(p, q) \in \mathbb{N}^2$ von $x^2 - dy^2 = -1$ ein $n \in \mathbb{N}_0$ mit $p = p_n$, $q = q_n$ gibt. Hierbei verwenden wir, dass $\mathrm{ggT}(p, q) = 1$ ist, denn jeder gemeinsame Teiler von p und q teilt auch $p^2 - dq^2 = -1$. Wegen 14.9 ist

$$p_n^2 - dq_n^2 = (-1)^{n+1} c_n$$

mit $c_n > 0$. Im Folgenden nehmen wir an, dass (p_n, q_n) eine Lösung ist. Dann folgt $c_n = 1$, nach 14.9 also $n \equiv -1 \pmod{h}$, d.h. es gibt ein $k \in \mathbb{N}$ mit $n = kh - 1$.

(a) Falls h gerade ist, so ist $n = kh - 1$ ungerade und demzufolge

$$p_n^2 - dq_n^2 = (-1)^{n+1} = 1,$$

was ein Widerspruch ist. Unter dieser Voraussetzung kann es also keine Lösungen in $\mathbb{N}^2$ und demzufolge auch keine in $\mathbb{Z}^2$ geben.
(b) Ist h ungerade, $n = kh - 1$, so folgt

$$p_n^2 - dq_n^2 = (-1)^{kh}$$

Die Lösungen $(p, q) \in \mathbb{N}^2$ sind in diesem Fall genau durch die (p_{kh-1}, q_{kh-1}) mit $k \in \mathbb{N}$ ungerade gegeben. □

Beispiel 14.13. (a) *Es sei $d = 23$. Dann ist $h = 4$, siehe 14.11, d.h. die Gleichung $x^2 - 23y^2 = -1$ hat keine ganzzahligen Lösungen. Das kann man natürlich auch dadurch sehen, dass man die Gleichung modulo 23 betrachtet und feststellt, dass $\left(\frac{-1}{23}\right) = -1$ ist.*

(b) *Es sei* $d = 5$. *Es ist* $\sqrt{5} = [2, \overline{4}]$, *d.h.* $h = 1$. *Somit sind die Lösungen* $(p, q) \in \mathbb{N}^2$ *von* $x^2 - 5y^2 = -1$ *durch* (p_{k-1}, q_{k-1}) *mit* $k \in \mathbb{N}$ *ungerade, also genau durch* (p_{2k}, q_{2k}) *mit* $k \in \mathbb{N}_0$ *gegeben:* $(p_0, q_0) = (2, 1)$, $(p_2, q_2) = (38, 17), \ldots$
Die Lösungen von $x^2 - 5y^2 = 1$ *in* $\mathbb{N}^2$ *sind durch* (p_{2k-1}, q_{2k-1}), $k \in \mathbb{N}$, *gegeben.*

§15 Die Einheitengruppe des Ganzheitsringes quadratischer Zahlkörper

Definition 15.1. *Es sei K ein Körper mit* $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ *(mit den von* $\mathbb{C}$ *eingeschränkten Verknüpfungen). Insbesondere kann man K mit der skalaren Multiplikation* $\mathbb{Q} \times K \to K$, $(\alpha, x) \mapsto \alpha x$ *als* $\mathbb{Q}$*-Vektorraum auffassen. K heißt ein* ***quadratischer Zahlkörper****, wenn* $\dim_{\mathbb{Q}} K = 2$ *ist.*

Proposition 15.2. *Es sei K ein Körper mit* $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ *(mit den von* $\mathbb{C}$ *eingeschränkten Verknüpfungen). Dann sind äquivalent:*

(i) *K ist ein quadratischer Zahlkörper.*

(ii) *Es gibt ein eindeutig bestimmtes quadratfreies* $d \in \mathbb{Z}$, $d \neq 0, 1$ *mit* $K = \mathbb{Q}(\sqrt{d})$.

Ist $\tilde{d} \in \mathbb{Z}$ *mit* $\tilde{d} = r^2 d$ *mit* $r \in \mathbb{N}$, $d \in \mathbb{Z}$ *quadratfrei,* $d \neq 0, 1$, *dann ist* $\mathbb{Q}(\sqrt{\tilde{d}}) = \mathbb{Q}(\sqrt{d})$.
Im Fall $d > 0$ *heißt K ein* ***reellquadratischer Zahlkörper****, im Fall* $d < 0$ *ein* ***imaginärquadratischer Zahlkörper****.*

Beweis. „(i)$\Longrightarrow$(ii)“: Wir zeigen zunächst die Existenzaussage. Sei $x \in K \setminus \mathbb{Q}$. Dann ist das System $(1, x)$ offenbar $\mathbb{Q}$-linear unabhängig, wegen $\dim_{\mathbb{Q}} K = 2$ ist $(1, x)$ also eine $\mathbb{Q}$-Basis von K. Das System $(1, x, x^2)$ ist wegen $\dim_{\mathbb{Q}} K = 2$ linear abhängig über $\mathbb{Q}$, d.h. es existieren $a, b, c \in \mathbb{Q}$ mit $ax^2 + bx + c = 0$, $a \neq 0$. Wir können ohne Einschränkung $a, b, c \in \mathbb{Z}$ annehmen. In $\mathbb{C}$ erhalten wir die Gleichung

$$x = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}.$$

Wir schreiben $b^2 - 4ac = r^2 d$ mit $r \in \mathbb{N}$, $d \in \mathbb{Z}$ quadratfrei. Wegen $x \notin \mathbb{Q}$ ist $d \neq 0, 1$. Das liefert $x = -\frac{b}{2a} \pm \frac{r}{2a}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ und somit $K = \mathbb{Q} + \mathbb{Q}x \subseteq \mathbb{Q}(\sqrt{d})$. Aufgrund von 13.4 ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2 = \dim_{\mathbb{Q}} K$ und deshalb $K = \mathbb{Q}(\sqrt{d})$. Es verbleibt der Nachweis der Eindeutigkeit. Sei $K = \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ mit $d_1, d_2 \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Insbesondere ist dann $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_2})$, d.h. es gibt $u, v \in \mathbb{Q}$ mit $\sqrt{d_1} = u + v\sqrt{d_2}$. Das liedert $d_1 = u^2 + v^2 d_2 + 2uv\sqrt{d_2}$. As 13.4 erhalten wir $uv = 0$. Wäre $v = 0$, dann wäre $\sqrt{d_1} = u \in \mathbb{Z}$, was ein Widerspruch ist. Also ist $u = 0$ und damit $d_1 = v^2 d_2$. Da d_1 quadratfrei ist, ist $v = 1$ und deshalb $d_1 = d_2$.

„(ii)$\Longrightarrow$(i)“: Nach 13.4 ist $\mathbb{Q}(\sqrt{d})$ ein Körper, und $(1, \sqrt{d})$ ist eine Basis von $\mathbb{Q}(\sqrt{d})$ als $\mathbb{Q}$-Vektorraum. Insbesondere ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$.

Sei nun $\tilde{d} = r^2 d$ mit $r \in \mathbb{N}$ und $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$. Offenbar ist $(1, \sqrt{\tilde{d}}) = (1, r\sqrt{d})$ und damit aber auch $(1, \sqrt{d})$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{\tilde{d}})$. Es folgt $\mathbb{Q}(\sqrt{\tilde{d}}) = \mathbb{Q}(\sqrt{d})$. □

Wir erinnern an dieser Stelle daran, dass wir nach 13.4 auf dem Körper $\mathbb{Q}(\sqrt{d})$ den Körperautomorphismus

$$\overline{\ } : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}),\ u + v\sqrt{d} \mapsto u - v\sqrt{d}$$

haben.

Definition 15.3. *Es sei K ein quadratischer Zahlkörper und $d \in \mathbb{Z}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Wir definieren die Abbildungen **Norm** und **Spur** als*

$$\mathrm{N}\colon K \to \mathbb{Q}, \quad x = u + v\sqrt{d} \mapsto x\overline{x} = u^2 - v^2 d,$$
$$\mathrm{Sp}\colon K \to \mathbb{Q}, \quad x = u - v\sqrt{d} \mapsto x + \overline{x} = 2u.$$

Proposition 15.4. *Es sei K ein quadratischer Zahlkörper, und es seien $x, y \in K$. Dann gilt:*

(a) $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$,
(b) $\mathrm{Sp}(x+y) = \mathrm{Sp}(x) + \mathrm{Sp}(y)$,
(c) $\mathrm{N}(x) = \mathrm{N}(\overline{x})$,
(d) $\mathrm{Sp}(x) = \mathrm{Sp}(\overline{x})$,
(e) $x^2 - \mathrm{Sp}(x)x + \mathrm{N}(x) = 0$.

Beweis. (a) Es ist

$$\mathrm{N}(xy) = xy\overline{xy} = xy\overline{x}\,\overline{y} = x\overline{x}y\overline{y} = \mathrm{N}(x)\,\mathrm{N}(y).$$

(b) Es ergibt sich

$$\mathrm{Sp}(x+y) = x + y + \overline{x+y} = x + y + \overline{x} + \overline{y} = x + \overline{x} + y + \overline{y} = \mathrm{Sp}(x) + \mathrm{Sp}(y).$$

(c),(d) ergeben sich unmittelbar aus der Definition.
(e) Es ist

$$x^2 - \mathrm{Sp}(x)x + \mathrm{N}(x)x = x^2 - (x + \overline{x})x + x\overline{x} = 0.$$

□

Definition 15.5. *Es sei K ein quadratischer Zahlkörper und $x \in K$. Das Element x heißt **ganz**, wenn $\mathrm{Sp}(x) \in \mathbb{Z}$ und $\mathrm{N}(x) \in \mathbb{Z}$ ist. Wir setzen*

$$\mathcal{O}_K := \{x \in K \mid x \text{ ist ganz}\}.$$

Proposition 15.6. *Es sei K ein quadratischer Zahlkörper, und es sei $x \in K$. Dann gilt:*

(a) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.
(b) $x \in \mathcal{O}_K \iff \overline{x} \in \mathcal{O}_K$.

Beweis. (a) Es ist

$$\mathcal{O}_K \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid x \text{ ist ganz}\} = \{x \in \mathbb{Q} \mid \mathrm{Sp}(x) = 2x \in \mathbb{Z} \text{ und } \mathrm{N}(x) = x^2 \in \mathbb{Z}\} = \mathbb{Z}.$$

(b) Dies ergibt sich aus 15.4 (c),(d). □

Wir werden im weiteren Verlauf sehen, dass $\mathcal{O}_K$ ein Ring ist. Dieser wird im Körper K eine vergleichbare Rolle zum Ring der ganzen Zahlen im Körper $\mathbb{Q}$ spielen.

Beispiel 15.7. *Es sei* $K = \mathbb{Q}(\sqrt{5})$.

- $x = 2 - \sqrt{5}$: $\mathrm{Sp}(x) = 4, \mathrm{N}(x) = (2-\sqrt{5})(2+\sqrt{5}) = 4 - 5 = -1$, *d.h.* $x \in \mathcal{O}_K$.
- $x = 1 + \frac{1}{2}\sqrt{5}$: $\mathrm{Sp}(x) = 2, \mathrm{N}(x) = (1+\frac{1}{2}\sqrt{5})(1-\frac{1}{2}\sqrt{5}) = 1 - \frac{5}{4} = -\frac{1}{4}$, *d.h.* $x \notin \mathcal{O}_K$.
- $x = \frac{3}{2} + \frac{1}{2}\sqrt{5}$: $\mathrm{Sp}(x) = 3, \mathrm{N}(x) = (\frac{3}{2}+\frac{1}{2}\sqrt{5})(\frac{3}{2}-\frac{1}{2}\sqrt{5}) = \frac{9}{4} - \frac{5}{4} = 1$, *d.h.* $x \in \mathcal{O}_K$.

Wie man im obigen Beispiel sieht, können bei ganzen Elementen in quadratischen Zahlkörpern sehr wohl Nenner auftreten.

Proposition 15.8. *Es sei K ein quadratischer Zahlkörper, und es sei $x \in K \setminus \mathbb{Q}$. Dann sind äquivalent:*

(i) $x \in \mathcal{O}_K$.

(ii) *Es gibt ein normiertes quadratisches Polynom $f = X^2 + aX + b \in \mathbb{Z}[X]$ mit $f(x) = 0$.*

Beweis. „(i)$\Longrightarrow$(ii)“: Es sei $x \in \mathcal{O}_K$. Dann sind $\mathrm{N}(x) \in \mathbb{Z}$ und $\mathrm{Sp}(x) \in \mathbb{Z}$, weswegen das Polynom $f := X^2 - \mathrm{Sp}(x)X + \mathrm{N}(x)$ in $\mathbb{Z}[X]$ liegt. Nach 15.4 ist $f(x) = 0$.

„(ii)$\Longrightarrow$(i)“: Sei $f(x) = x^2 + ax + b = 0$. Wegen $x \in K \setminus \mathbb{Q}$ ist $x \neq \overline{x}$, und aufgrund von 13.4 ist $\overline{x}^2 + a\overline{x} + b = 0$, d.h. $x, \overline{x}$ sind die zwei Nullstellen von f. Es folgt

$$f = (X - x)(X - \overline{x}) = X^2 - \mathrm{Sp}(x)X + \mathrm{N}(x).$$

Wegen $f \in \mathbb{Z}[X]$ ist $\mathrm{Sp}(x) = -a \in \mathbb{Z}$ und $\mathrm{N}(x) = b \in \mathbb{Z}$, d.h. x ist ganz. □

Der nächste Satz liefert eine explizite Beschreibung der ganzen Elemente eines quadratischen Zahlkörpers. Als Nebenprodukt erhalten wir, dass diese einen Ring bilden.

Satz 15.9. *Es sei K ein quadratischer Zahlkörper, es sei $d \in \mathbb{Z}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Dann gilt:*

(a)
$$\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}, \text{ wobei } \omega = \begin{cases} \frac{1}{2}(1+\sqrt{d}) & \text{falls } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls } d \equiv 2, 3 \pmod 4. \end{cases}$$

(b) $\mathcal{O}_K$ *ist ein Ring, der sogennante* ***Ganzheitsring*** *von K.*

(c) $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid \mathrm{N}(x) = \pm 1\}$.

Beweis. (a) Sei zunächst $x \in \mathcal{O}_K$. Wir schreiben x in der Form $x = u + v\sqrt{d}$ mit $u, v \in \mathbb{Q}$. Es ist $\mathrm{Sp}(x) = 2u \in \mathbb{Z}$, d.h. es gibt ein $p \in \mathbb{Z}$ mit $u = \frac{p}{2}$. Somit ist $x = \frac{p}{2} + v\sqrt{d}$ und

$$\mathrm{N}(x) = \frac{p^2}{4} - v^2 d \in \mathbb{Z}.$$

Es gibt demzufolge ein $a \in \mathbb{Z}$ mit $v^2 d = \frac{a}{4}$. Weil d quadratfrei ist, existiert ein $q \in \mathbb{Z}$ mit $v = \frac{q}{2}$. Wir erhalten $x = \frac{p}{2} + \frac{q}{2}\sqrt{d}$ und deshalb

$$\mathrm{N}(x) = \frac{p^2 - q^2 d}{4} \in \mathbb{Z},$$

also $p^2 \equiv q^2 d \pmod 4$.

Fall 1: $d \equiv 2, 3 \pmod 4$**.** Falls $q^2 \equiv 1 \pmod 4$ wäre, dann wäre $p^2 \equiv q^2 d \equiv d \equiv 2, 3 \pmod 4$, was ein Widerspruch ist. Es ist also $q^2 \equiv 0 \pmod 4$ und folglich $p^2 \equiv 0 \pmod 4$. Das liefert $2|p$ und $2|q$ und somit $u, v \in \mathbb{Z}$, also $x = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Fall 2: $d \equiv 1 \pmod 4$**.** Dann ist $p^2 \equiv q^2 \pmod 4$ und deshalb $p \equiv q \pmod 2$. Wir erhalten

$$x = \frac{p}{2} + \frac{q}{2}\sqrt{d} = \frac{p-q}{2} + q\frac{1}{2}(1 + \sqrt{d}) = \frac{p-q}{2} + q\omega \in \mathbb{Z}[\omega].$$

Damit ist die Inklusion $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$ gezeigt. Sei nun $x \in \mathbb{Z}[\omega]$.

Fall 1: $d \equiv 2, 3 \pmod 4$**.** Dann existieren $a, b \in \mathbb{Z}$ mit $x = a + b\sqrt{d}$. Demzufolge ist

$$\mathrm{Sp}(x) = \mathrm{Sp}(a + b\sqrt{d}) = 2a \in \mathbb{Z}, \quad \mathrm{N}(x) = \mathrm{N}(a + b\sqrt{d}) = a^2 - b^2 d \in \mathbb{Z},$$

d.h. $x \in \mathcal{O}_K$.

Fall 2: $d \equiv 1 \pmod 4$**.** In diesem Fall existieren $a, b \in \mathbb{Z}$ mit

$$x = a + b\omega = a + b\frac{1 + \sqrt{d}}{2} = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}.$$

Es ergibt sich

$$\mathrm{Sp}(x) = \mathrm{Sp}(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}) = 2a + b \in \mathbb{Z}$$

sowie

$$\mathrm{N}(x) = \mathrm{N}(a + \frac{b}{2} + \frac{b}{2}\sqrt{d}) = (a + \frac{b}{2})^2 - \frac{b^2}{4}d = a^2 + ab + \frac{b^2}{4}(1 - d),$$

was wegen $d \equiv 1 \pmod 4$ ebenfalls in $\mathbb{Z}$ liegt. Somit ist $x \in \mathcal{O}_K$.

(b) Wegen $\mathcal{O}_K \subseteq \mathbb{C}$ und $0, 1 \in \mathcal{O}_K$ müssen wir nur nachrechnen, dass $\mathcal{O}_K$ abgeschlossen unter Addition und Multiplikation ist. Aufgrund von (a) ist $\mathcal{O}_K = \mathbb{Z}[\omega]$ für ω wie in (a) angegeben. Es seien $x = a_1 + b_1\omega$, $y = a_2 + b_2\omega \in \mathcal{O}_K$ mit $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Wir erhalten

$$x + y = (a_1 + a_2) + (b_1 + b_2)\omega \in \mathbb{Z}[\omega] = \mathcal{O}_K$$

und

$$xy = (a_1 + b_1\omega)(x_2 + y_2\omega) = a_1 a_2 + (a_1 b_2 + b_1 a_2)\omega + b_1 b_2 \omega^2.$$

Um $xy \in \mathcal{O}_K$ zu folgern, genügt es zu zeigen, dass $\omega^2 \in \mathbb{Z}[\omega]$ ist. Falls $d \equiv 2, 3 \pmod 4$ ist, so ist $\omega^2 = (\sqrt{d})^2 = d \in \mathbb{Z}[\omega]$. Ist $d \equiv 1 \pmod 4$, so ist

$$\omega^2 = \left(\frac{1 + \sqrt{d}}{2}\right)^2 = \frac{1 + 2\sqrt{d} + d}{4} = \frac{2 + 2\sqrt{d} + d - 1}{4} = \frac{d-1}{4} + \omega \in \mathbb{Z}[\omega].$$

(c) Sei $x \in \mathcal{O}_K^\times$. Dann ist $x^{-1} \in \mathcal{O}_K^\times$, und wir erhalten

$$1 = \mathrm{N}(1) = \mathrm{N}(xx^{-1}) = \mathrm{N}(x)\,\mathrm{N}(x^{-1})$$

mit $\mathrm{N}(x), \mathrm{N}(x^{-1}) \in \mathbb{Z}$. Das liefert $\mathrm{N}(x) \in \{\pm 1\}$.
Sei nun $x \in \mathcal{O}_K$ mit $\mathrm{N}(x) \in \{\pm 1\}$. Dann ist $x \neq 0$, und in $\mathbb{Q}(\sqrt{d})$ gilt die Identität

$$\frac{1}{x} = \frac{\overline{x}}{x\overline{x}} = \frac{\overline{x}}{\mathrm{N}(x)} = \pm\overline{x} \in \mathcal{O}_K,$$

weswegen $x \in \mathcal{O}_K^\times$ ist. □

Für einen quadratischen Zahlkörper $K = Q(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei, $d \equiv 1 \pmod 4$, ist also $\mathbb{Z}[\sqrt{d}]$ eine echte Teilmenge von $\mathcal{O}_K$.

Satz 15.10. *Es sei K ein imaginärquadratischer Zahlkörper, und es sei $d \in \mathbb{Z}$, $d < 0$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Dann gilt:*

(a) *Falls $d \neq -1, -3$ ist, so ist $\mathcal{O}_K^\times = \{\pm 1\} = \langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.*
(b) *Falls $d = -1$ ist, so ist $\mathcal{O}_K^\times = \{\pm 1, \pm i\} = \langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}$.*
(c) *Falls $d = -3$ ist, so ist $\mathcal{O}_K^\times = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} = \langle \frac{1+\sqrt{-3}}{2} \rangle \cong \mathbb{Z}/6\mathbb{Z}$.*

Beweis. (a) **Fall 1:** $d \equiv 2, 3 \pmod 4$**.** In diesem Fall ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Wegen $d < 0, d \neq -1$ folgt $d \leq -2$. Es sei $x = u + v\sqrt{d} \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$. Nach 15.9 gilt:

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 - v^2 d = \pm 1.$$

Die Gleichung $u^2 - v^2 d = -1$ hat wegen $d < 0$ keine Lösung, die Gleichung $u^2 - v^2 d = 1$ hat wegen $d \leq -2$ nur die Lösungen $(u, v) = (\pm 1, 0)$. Das liefert

$$\mathcal{O}_K^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Fall 2: $d \equiv 1 \pmod 4$**.** In diesem Fall ist $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$. Sei $x = u + v\frac{1}{2}(1 + \sqrt{d}) \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$. Wir setzen $\tilde{u} := 2u + v$, $\tilde{v} := v$, dann ist $x = \frac{1}{2}(\tilde{u} + \tilde{v}\sqrt{d})$. Aufgrund von 15.9 gilt:

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff \mathrm{N}(\frac{1}{2})\,\mathrm{N}(\tilde{u} + \tilde{v}\sqrt{d}) = \pm 1 \iff \tilde{u}^2 - \tilde{v}^2 d = \pm 4.$$

Wegen $d < 0$ und $d \equiv 1 \pmod 4$ ist $d \leq -7$. Daher hat die Gleichung $\tilde{u}^2 - \tilde{v}^2 d = \pm 4$ nur die Lösungen $(\tilde{u}, \tilde{v}) = (\pm 2, 0)$. Es ergibt sich

$$\mathcal{O}_K^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

(b) Sei $d = -1$. Es ergibt sich $\mathcal{O}_K = \mathbb{Z}[i]$. Sei $x = u + vi \in \mathcal{O}_K$ mit $u, v \in \mathbb{Z}$. Wir erhalten

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 + v^2 = \pm 1.$$

Diese Gleichung hat die Lösungen $(u,v) = (\pm 1, 0), (0, \pm 1)$. Das liefert

$$\mathcal{O}_K^\times = \{\pm 1, \pm i\} = \langle i \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

(c) Sei $d = -3$. Dann ist $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Wie im Beweis von (a) ergibt sich für $x = u + v\frac{1}{2}(1 + \sqrt{-3})$ mit $\tilde{u} := 2u + v$, $\tilde{v} := v$ die Äquivalenz

$$x \in \mathcal{O}_K^\times \iff \tilde{u}^2 + 3\tilde{v}^2 = \pm 4.$$

Diese Gleichung besitzt die Lösungen $(\tilde{u}, \tilde{v}) = (\pm 2, 0), (\pm 1, \pm 1)$, also $\mathcal{O}_K^\times = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$. Wegen $\frac{1+\sqrt{-3}}{2} = e^{\frac{2\pi i}{6}}$ ist $\operatorname{ord}(\frac{1+\sqrt{-3}}{2}) = 6$, also

$$\mathcal{O}_K^\times = \langle \frac{1+\sqrt{-3}}{2} \rangle \cong \mathbb{Z}/6\mathbb{Z}.$$

□

Aufgrund von 15.10 ist die Einheitengruppe des Ganzheitsringes eines imaginärquadratischen Zahlkörpers endlich. Für reellquadratische Zahlkörper sieht die Situation anders aus: Für $K = \mathbb{Q}(\sqrt{d})$ mit $d > 1$ quadratfrei ist stets $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, und für $x = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ ist

$$x \in \mathcal{O}_K^\times \iff \mathrm{N}(x) = \pm 1 \iff u^2 - dv^2 = \pm 1.$$

Diese Gleichung hat nach den Ergebnissen des vorangegangenen Abschnitts unendlich viele Lösungen, d.h. die Einheitengruppe eines reellquadratischen Zahlkörpers ist unendlich.

Satz 15.11. *Es sei K ein reellquadratischer Zahlkörper. Dann gibt es eine eindeutig bestimmte minimale Einheit > 1 in $\mathcal{O}_K$, die sogenannte **Fundamentaleinheit** η. Jedes Element $x \in \mathcal{O}_K^\times$ lässt sich in der Form $x = \pm\eta^n$ mit einem eindeutig bestimmten $n \in \mathbb{Z}$ schreiben. Insbesondere ist $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Beweis. Im Folgenden sei $K = \mathbb{Q}(\sqrt{d})$ mit $d > 1$ quadratfrei. Die Gleichung $x^2 - dy^2 = 1$ hat nach den Ergebnissen des letzten Abschnitts eine Lösung $(p,q) \in \mathbb{N}^2$. Es ist dann $\mathrm{N}(p + q\sqrt{d}) = p^2 - dq^2 = 1$, d.h. $p + q\sqrt{d} \in \mathcal{O}_K^\times$. Wir setzen $N := \left\lfloor p + q\sqrt{d} \right\rfloor + 1$. Dann ist $(1, N] \cap \mathcal{O}_K^\times \neq \varnothing$. Die Menge $(1, N] \cap \mathcal{O}_K^\times$ ist endlich,

denn: Wir nehmen an, dass die Menge $(1, N] \cap \mathcal{O}_K^\times$ unendlich ist. Dann ist auch die Menge $[1, N] \cap \mathcal{O}_K^\times$ unendlich. Insbesondere existiert eine Folge $(x_n)_{n\in\mathbb{N}}$ mit paarweise verschiedenen Folgegliedern aus $[1, N] \cap \mathcal{O}_K^\times$. Wegen der Kompaktheit von $[1, N]$ besitzt diese Folge eine Teilfolge, die gegen ein $x \in [1, N]$ konvergiert. Wir können ohne Einschränkung annehmen, dass die Folge $(x_n)_{n\in\mathbb{N}}$ gegen x konvergiert. Wegen 15.9 gibt es für alle $n \in \mathbb{N}$ Elemente $a_n, b_n \in \mathbb{Z}$ mit $x_n = \frac{a_n + b_n\sqrt{d}}{2}$. Die Folge $(a_n)_{n\in\mathbb{N}}$ kann nicht beschränkt sein, sonst wäre wegen

$$\pm 1 = \mathrm{N}(x_n) = x_n\overline{x_n} = \frac{a_n^2 - b_n^2 d}{4},$$

also

$$b_n^2 = \frac{a_n^2 \pm 4}{d}$$

auch die Folge $(b_n)_{n\in\mathbb{N}}$ beschränkt. Damit würden nur endlich viele Werte in der Folge $(x_n)_{n\in\mathbb{N}}$ auftreten, im Widerspruch dazu, dass die Werte x_n, $n \in \mathbb{N}$, paarweise verschieden sind. Es existiert deshalb eine Teilfolge (a_{n_i}) von (a_n) mit $a_{n_i} \to \infty$ für $n_i \to \infty$ oder mit $a_{n_i} \to -\infty$ für $n_i \to \infty$. Wir betrachten hier nur den Fall $a_{n_i} \to \infty$, im anderen Fall kann man analog argumentieren. Die entsprechende Teilfolge (b_{n_i}) von (b_n) erfüllt $b_{n_i} \to -\infty$, denn

$$x_{n_i} = \frac{a_{n_i} + b_{n_i}\sqrt{d}}{2} \to x \text{ für } n_i \to \infty.$$

Die Folge $(\overline{x_{n_i}})$ mit

$$\overline{x_{n_i}} = \frac{a_{n_i} - b_{n_i}\sqrt{d}}{2}$$

erfüllt deshalb $\overline{x_{n_i}} \to \infty$ für $n_i \to \infty$. Andererseits gilt:

$$|\overline{x_{n_i}}| = \left|\frac{x_{n_i}\overline{x_{n_i}}}{x_{n_i}}\right| = \left|\frac{\mathrm{N}(x_{n_i})}{x_{n_i}}\right| = \frac{1}{|x_{n_i}|} \to \frac{1}{x}$$

für $n_i \to \infty$, was zum Widerspruch führt #

Somit existiert ein minimales $\eta \in \mathcal{O}_K^\times$ mit $\eta > 1$. Jedes Element aus $\mathcal{O}_K^\times$ lässt sich in der Form $\pm\eta^n$ mit einem eindeutig bestimmten Element $n \in \mathbb{Z}$ schreiben,

denn: Wir zeigen zunächst die Existenzaussage. Sei $x \in \mathcal{O}_K^\times$, ohne Einschränkung $x > 0$. Für $n \to -\infty$ gilt $\eta^n \to 0$, für $n \to \infty$ gilt $\eta^n \to \infty$. Es existiert folglich ein $n \in \mathbb{Z}$ mit $\eta^n \le x < \eta^{n+1}$. Das liefert $1 \le x\eta^{-n} < \eta$. Aus $x\eta^{-n} \in \mathcal{O}_K^\times$ ergibt sich $x\eta^{-n} = 1$ wegen der Minimalität von η. Somit folgt $x = \eta^n$. Zum Nachweis der Eindeutigkeitsaussage bemerken wir, dass die Elemente $\pm\eta^n$, $n \in \mathbb{Z}$, wegen $\eta > 1$ paarweise verschieden sind. #

Wir betrachten die Abbildung

$$\psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \to \mathcal{O}_K^\times, \quad (\bar{i}, n) \mapsto (-1)^i\eta^n.$$

Die Abbildung ψ ist wohldefiniert wegen $(-1)^2 = 1$ und bijektiv aufgrunddessen, was wir bereits gezeigt haben. Darüber hinaus ist ψ ein Gruppenhomomorphismus, denn für $\overline{i_1}, \overline{i_2} \in \mathbb{Z}/2\mathbb{Z}$, $n_1, n_2 \in \mathbb{Z}$ ist

$$\begin{aligned}\psi((\overline{i_1}, n_1) + (\overline{i_2}, n_2)) &= \psi(\overline{i_1 + i_2}, n_1 + n_2) = (-1)^{i_1+i_2}\eta^{n_1+n_2} = (-1)^{i_1}\eta^{n_1}(-1)^{i_2}\eta^{n_2} \\ &= \psi(\overline{i_1}, n_1)\psi(\overline{i_2}, n_2).\end{aligned}$$

□

Im Rest des Abschnittes werden wir daran arbeiten, einen Algorithmus zur Berechnung der Fundamentaleinheit des Ganzheitsringes reellquadratischer Zahlkörper zu finden.

Proposition 15.12. *Es sei K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es seien $a, b \in \mathbb{Z}$, so dass $\varepsilon := \frac{a+b\sqrt{d}}{2} \in \mathcal{O}_K^\times$ ist. Dann sind äquivalent:*

(i) $\varepsilon > 1$,

(ii) $a, b \geq 1$.

Beweis. „(i)$\Longrightarrow$(ii)“: Sei $\varepsilon > 1$. Dann sind die Elemente $\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ paarweise verschieden, von diesen vier Elementen ist ε das größte. Es ist

$$\varepsilon^{-1} = \frac{\overline{\varepsilon}}{\varepsilon\overline{\varepsilon}} = \frac{\overline{\varepsilon}}{\mathrm{N}(\varepsilon)} = \pm\overline{\varepsilon} = \pm\frac{a - b\sqrt{d}}{2}$$

Aus diesem Grund ist $a \geq 1$, denn eines der beiden Elemente $\varepsilon^{-1}, -\varepsilon^{-1}$ ist von der Form $\frac{-a+b\sqrt{d}}{2}$ und wäre im Falle $a \leq 0$ größer als ε oder gleich ε. Ebenso ist $b \geq 1$, denn eines der beiden Elemente $\varepsilon^{-1}, -\varepsilon^{-1}$ ist von der Form $\frac{a-b\sqrt{d}}{2}$ und wäre im Falle $b \leq 0$ größer als ε oder gleich ε.

„(ii)$\Longrightarrow$(i)“: Sind $a, b \geq 1$, dann ist

$$\varepsilon = \frac{a + b\sqrt{d}}{2} \geq \frac{1 + \sqrt{d}}{2} > 1.$$

□

Proposition 15.13. *Es sei K ein quadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$. Dann gilt: Ist $d \not\equiv 5 \pmod 8$, dann ist $\eta \in \mathbb{Z}[\sqrt{d}]$.*

Beweis. Falls $d \not\equiv 1 \pmod 4$ ist, dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ und deshalb $\eta \in \mathbb{Z}[\sqrt{d}]$. Sei im Folgenden $d \equiv 1 \pmod 4$, und es sei $\eta \notin \mathbb{Z}[\sqrt{d}]$. Nach 15.9 gibt es $u, v \in \mathbb{Z}$ mit

$$\eta = u + v\frac{1}{2}(1 + \sqrt{d}) = \frac{a + b\sqrt{d}}{2},$$

wobei wir $a := 2u + v$ und $b := v$ gesetzt haben. Wegen $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $b = v$ ungerade, also ist auch a ungerade. Aufgrund von $\eta \in \mathcal{O}_K^\times$ ist $\mathrm{N}(\eta^2) = \mathrm{N}(\eta)^2 = (\pm 1)^2 = 1$. Es ist

$$\eta^2 = \frac{a^2 + db^2 + 2ab\sqrt{d}}{4}.$$

Weil ab ungerade ist, ist $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$. Wir schreiben analog zu oben $\eta^2 = \frac{x+y\sqrt{d}}{2}$ mit $x, y \in \mathbb{Z}$ ungerade. Aufgrund von $\mathrm{N}(\eta^2) = 1$ ergibt sich $x^2 - y^2 d = 4$. Da x, y ungerade sind, folgt $x^2, y^2 \equiv 1 \pmod 8$ und damit $1 - d \equiv 4 \pmod 8$, d.h. $d \equiv 5 \pmod 8$. □

Proposition 15.14. *Es sei K ein quadratischer Zahlkörper, und es sei $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$, diese liege in $\mathbb{Z}[\sqrt{d}]$. Für $n \in \mathbb{N}$ sei $\eta^n = a_n + b_n\sqrt{d}$ mit $a_n, b_n \in \mathbb{N}$ (vgl. 15.12). Es seien $m, n \in \mathbb{N}$. Dann sind äquivalent:*

(i) $n < m$,

(ii) $\eta^n < \eta^m$,

(iii) $a_n < a_m$,

(iv) $b_n < b_m$.

Beweis. Wegen $\eta > 1$ ist die Folge $(\eta^n)_{n\in\mathbb{N}}$ streng monoton wachsend, es gilt also (i)$\Longleftrightarrow$(ii). Zum Nachweis der restlichen Äquivalenzen genügt es zu zeigen, dass $a_n < a_{n+1}$ und $b_n < b_{n+1}$ für alle $n \in \mathbb{N}$ gilt. Es ist

$$\eta^{n+1} = \eta^n \cdot \eta = (a_n + b_n\sqrt{d})(a_1 + b_1\sqrt{d}) = a_n a_1 + b_n b_1 d + (a_n b_1 + b_n a_1)\sqrt{d}$$

und deshalb $a_{n+1} = a_n a_1 + b_n b_1 d$, $b_{n+1} = a_n b_1 + b_n a_1$. Wegen $a_n, b_n, a_1, b_1 \in \mathbb{N}$ ergibt sich

$$a_{n+1} \geq a_n + d > a_n, \quad b_{n+1} \geq b_n + 1 > b_n.$$

□

Proposition 15.15. *Es sei K ein quadratischer Zahlkörper, und es sei $d \in \mathbb{N}$ quadratfrei, $d \neq 5, 13$, mit $K = \mathbb{Q}(\sqrt{d})$. Es bezeichne η die Fundamentaleinheit von $\mathcal{O}_K$, diese liege nicht in $\mathbb{Z}[\sqrt{d}]$. Für $n \in \mathbb{N}$ sei $\eta^n = \frac{a_n + b_n\sqrt{d}}{c_n}$ mit $a_n, b_n \in \mathbb{N}$, $c_n \in \{1, 2\}$, $\mathrm{ggT}(a_n, b_n, c_n) = 1$ (vgl. 15.12). Es seien $m, n \in \mathbb{N}$. Dann sind äquivalent:*

(i) $n < m$,
(ii) $\eta^n < \eta^m$,
(iii) $a_n < a_m$,
(iv) $b_n < b_m$.

Beweis. Wegen $\eta > 1$ ist die Folge $(\eta^n)_{n\in\mathbb{N}}$ streng monoton wachsend, woraus sich (i)$\Longleftrightarrow$(ii) ergibt. Zum Nachweis der restlichen Äquivalenzen genügt es zu zeigen, dass $a_n < a_{n+1}$ und $b_n < b_{n+1}$ für alle $n \in \mathbb{N}$ gilt. Aufgrund von $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $c_1 = 2$ und demzufolge

$$\frac{a_{n+1}}{c_{n+1}} + \frac{b_{n+1}}{c_{n+1}}\sqrt{d} = \eta^{n+1} = \eta^n \cdot \eta = \frac{a_n + b_n\sqrt{d}}{c_n}\frac{a_1 + b_1\sqrt{d}}{2} = \frac{a_n a_1 + b_n b_1 d}{2c_n} + \frac{a_n b_1 + b_n a_1}{2c_n}\sqrt{d}.$$

Dies impliziert

$$a_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n a_1 + b_n b_1 d}{2}, \quad b_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n b_1 + b_n a_1}{2}.$$

Wie wir im Beweis von 15.13 gesehen haben, ist darüberhinaus a_1 ungerade. Es ergeben sich die folgenden Fälle:

Fall 1: $a_1 = 1$**.** Dann ist $db_1^2 = -3$ oder $db_1^2 = 5$. Wegen $d > 0$, $d \neq 5$ haben diese Gleichungen jedoch keine Lösung, d.h. es kommt zum Widerspruch.

Fall 2: $a_1 = 3$**.** Es ergibt sich $db_1^2 = 5$ oder $db_1^2 = 13$. Aufgrund von $d \neq 5, 13$ haben diese Gleichungen keine Lösungen, somit führt auch dieser Fall zum Widerspruch.

Fall 3: $a_1 \geq 5$**.** Wir erhalten

$$a_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n a_1 + b_n b_1 d}{2} \geq \frac{1}{2}\frac{5a_n + b_n b_1 d}{2} > a_n$$

sowie

$$b_{n+1} = \frac{c_{n+1}}{c_n}\frac{a_n b_1 + b_n a_1}{2} \geq \frac{1}{2}\frac{a_n b_1 + 5b_n}{2} > b_n.$$

□

Algorithmus 15.16 (Bestimmung der Fundamentaleinheit)**.** *Es sei K ein reellquadratischer Zahlkörper und $d \in \mathbb{N}$ quadratfrei mit $K = \mathbb{Q}(\sqrt{d})$. Es soll die Fundamentaleinheit η von $\mathcal{O}_K$ bestimmt werden.*

(1) Falls $d = 5$ ist, dann ist $\eta = \frac{1+\sqrt{5}}{2}$.

(2) Falls $d \neq 5$ ist, berechne solange Näherungsbrüche $\frac{p_n}{q_n}$, $n \in \mathbb{N}_0$, von $\sqrt{d}$, bis erstmalig

$$p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$$

gilt. Es ist dann

$$\eta = \begin{cases} p_n + q_n\sqrt{d} & \text{falls } p_n^2 - dq_n^2 \in \{\pm 1\}, \\ \frac{p_n+q_n\sqrt{d}}{2} & \text{falls } p_n^2 - dq_n^2 \in \{\pm 4\}. \end{cases}$$

Ist $d \not\equiv 5 \pmod 8$, dann ist $\eta = p_{h-1} + q_{h-1}\sqrt{d}$, wobei h die Periodenlänge von $\sqrt{d}$ ist.

Beweis. Im Folgenden bezeichne $(\frac{p_n}{q_n})_{n\in\mathbb{N}_0}$ die Folge der Näherungsbrüche von $\sqrt{d}$. Wir nehmen eine Fallunterscheidung vor.

Fall 1: $\eta \in \mathbb{Z}[\sqrt{d}]$**.** Aufgrund von 15.12 ist η von der Form $\eta = a + b\sqrt{d}$ mit $a, b \in \mathbb{N}$, und es ist $\mathrm{N}(\eta) = a^2 - b^2 d = \pm 1$. Wegen 14.6 gibt es ein $n \in \mathbb{N}_0$, so dass $\frac{a}{b} = \frac{p_n}{q_n}$ ist. Setzen wir $t := \mathrm{ggT}(a, b)$, so gilt $t | a^2 - b^2 d = \pm 1$ und deshalb $t = 1$. Es folgt $(a, b) = (p_n, q_n)$. Es gibt kein $k \in \mathbb{N}_0$, $k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 1, \pm 4\}$,

denn: Sei zunächst $k \in \mathbb{N}_0$, $k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 1\}$. Dann ist $\alpha := p_k + q_k\sqrt{d} \in \mathcal{O}_K^\times$, und es ist $\alpha > 1$. Wegen $\alpha > 1$ gibt es ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wenn $m = 1$ ist, so ist $\alpha = \eta$, also $p_k = p_n$ und $q_k = q_n$, im Widerspruch zu $k < n$. Also ist $m > 1$, was nach 15.14 jedoch $q_k > q_n$ und damit $k > n$ liefert, was ein Widerspruch ist. Sei nun $k \in \mathbb{N}_0$, $k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 4\}$. Dann ist $\alpha := \frac{p_k+q_k\sqrt{d}}{2} \in \mathcal{O}_K^\times$, denn $\mathrm{N}(\alpha) = \frac{1}{4}(p_k^2 - dq_k^2) = \pm 1, \mathrm{Sp}(\alpha) = p_k \in \mathbb{Z}$. Wegen $\eta \in \mathbb{Z}[\sqrt{d}]$ ist $\mathcal{O}_K^\times \subseteq \mathbb{Z}[\sqrt{d}]$, weswegen $\alpha \in \mathbb{Z}[\sqrt{d}]$ ist. Somit sind sowohl p_k als auch q_k gerade, im Widerspruch zu $\mathrm{ggT}(p_k, q_k) = 1$. #

Folglich ist $\eta = p_n + q_n\sqrt{d}$, wobei n minimal mit der Eigenschaft $p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$ ist (wobei der Fall $p_n^2 - dq_n^2 = \pm 4$ nach den obigen Überlegungen niemals eintreten kann.)

Fall 2: $\eta \notin \mathbb{Z}[\sqrt{d}]$**,** $d \neq 5, 13$**.** Wie im Beweis zu 15.15 erhalten wir, dass η von der Form $\eta = \frac{a+b\sqrt{d}}{2}$ mit $a, b \in \mathbb{N}$ ungerade ist. Wegen $\mathrm{N}(\eta) = \pm 1$ erhalten wir $a^2 - db^2 = \pm 4$. Da $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist, ergibt sich aus 15.13, dass $d \equiv 5 \pmod 8$ ist. Insbesondere ist $d \geq 21$ und deshalb $4 < \frac{1}{2}(\sqrt{d-4} + \sqrt{d})$. Aus 14.6 erhalten wir, dass es ein $n \in \mathbb{N}_0$ gibt, so dass $\frac{a}{b} = \frac{p_n}{q_n}$ ist. Setzen wir $t := \mathrm{ggT}(a, b)$, so gilt $t^2 | a^2 - b^2 d = \pm 4$ und deshalb $t \in \{1, 2\}$. Weil a, b beide ungerade sind, ist $t = 1$ und deshalb $(a, b) = (p_n, q_n)$. Es gibt kein $k \in \mathbb{N}_0$, $k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 1, \pm 4\}$,

denn: Sei zunächst $k \in \mathbb{N}_0$, $k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 1\}$. Wie in Fall 1 ist $\alpha := p_k + q_k\sqrt{d} \in \mathcal{O}_K^\times$, und es ist $\alpha > 1$. Aus diesem Grund gibt es ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wegen $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $\alpha \neq \eta$, d.h. $m > 1$. Aus 15.15 ergibt sich $q_k > q_n$ und deshalb $k > n$, was ein Widerspruch ist. Sei nun

$k \in \mathbb{N}_0, k < n$ mit $p_k^2 - dq_k^2 \in \{\pm 4\}$. Wie in Fall 1 ist $\alpha := \frac{p_k + q_k\sqrt{d}}{2} \in \mathcal{O}_K^\times$, und es gibt ein $m \in \mathbb{N}$ mit $\alpha = \eta^m$. Wäre $m = 1$, so folgte $\alpha = \eta$, also $p_k = p_n$ und $q_k = q_n$, im Widerspruch zu $k < n$. Also ist $m > 1$, was nach 15.14 wegen $\mathrm{ggT}(p_k, q_k, 2) = 1$ und $d \geq 21$ jedoch $q_k > q_n$ und damit $k > n$ liefert, was ein Widerspruch ist. #

Folglich ist $\eta = \frac{p_n + q_n\sqrt{d}}{2}$, wobei n minimal mit der Eigenschaft $p_n^2 - dq_n^2 \in \{\pm 1, \pm 4\}$ ist.

Fall 3: $d = 5$. Offensichtlich ist $\frac{1+\sqrt{5}}{2} \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathcal{O}_K$, und wegen $\mathrm{N}(\frac{1+\sqrt{5}}{2}) = -1$ handelt es sich um eine Einheit in $\mathcal{O}_K$. Darüber hinaus ist $\frac{1+\sqrt{5}}{2}$ minimal unter allen Elementen $\frac{a+b\sqrt{5}}{2} \in \mathcal{O}_K^\times$ mit $a, b \in \mathbb{N}$. Wir schließen, dass $\eta = \frac{1+\sqrt{5}}{2}$ die Fundamentaleinheit von $\mathcal{O}_K$ ist. (Die Kettenbruchentwicklung von $\sqrt{5}$ ist $\sqrt{5} = [2, \overline{4}]$, was $p_0 = 2$ und $q_0 = 1$ zur Folge hat. Es ist $p_0^2 - 5q_0^2 = -1$, dies liefert die Einheit $\varepsilon = 2 + \sqrt{5} = \eta^3$, jedoch nicht die Fundamentaleinheit. Aus diesem Grund ist bei unserem Algorithmus die Fallunterscheidung notwendig.)

Fall 4: $d = 13$. Offenbar ist $\frac{3+\sqrt{13}}{2} = 1 + \frac{1+\sqrt{13}}{2} \in \mathbb{Z}[\frac{1+\sqrt{13}}{2}] = \mathcal{O}_K$, und wegen $\mathrm{N}(\frac{3+\sqrt{13}}{2}) = -1$ handelt es sich um eine Einheit in $\mathcal{O}_K$. Man rechnet leicht nach, dass $\frac{3+\sqrt{13}}{2}$ minimal unter den Elementen $\frac{a+b\sqrt{13}}{2} \in \mathcal{O}_K^\times$ mit $a, b \in \mathbb{N}$ ist. Das impliziert, dass $\eta = \frac{3+\sqrt{13}}{2}$ die Fundamentaleinheit von $\mathcal{O}_K$ ist. Wegen $\sqrt{13} = [3, \overline{1, 1, 1, 6}]$ ist $p_0 = 3$, $q_0 = 1$ und $p_0^2 - 13q_0^2 = -4$. Der Algorithmus liefert daher das korrekte Resultat $\eta = \frac{3+\sqrt{13}}{2}$.

Falls $d \not\equiv 5 \pmod 8$ ist, dann liegt die Fundamentaleinheit η nach 15.13 in $\mathbb{Z}[\sqrt{d}]$. Nach den obigen Überlegungen ist $\eta = p_n + q_n\sqrt{d}$, wobei n minimal mit $p_n^2 - dq_n^2 \in \{\pm 1\}$ ist. Falls h gerade ist, hat die Gleichung $x^2 - dy^2 = -1$ nach 14.12 keine Lösung, die Fundamentallösung von $x^2 - dy^2 = 1$ ist durch (p_{h-1}, q_{h-1}) gegeben. Falls h ungerade ist, so ist (p_{h-1}, q_{h-1}) nach 14.12 diejenige Lösung von $x^2 - dy^2 = -1$ in $\mathbb{N}^2$ mit minimalem y, die Fundamentallösung von $x^2 - dy^2 = 1$ ist durch (p_{2h-1}, q_{2h-1}) gegeben. Wir erhalten $\eta = p_{h-1} + q_{h-1}\sqrt{d}$. □

Beispiel 15.17. (a) *Es sei* $d = 53$. *Es ist* $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$ *und demzufolge* $p_0 = 7$, $q_0 = 1$. *Wir erhalten* $p_0^2 - 53q_0^2 = -4$ *und deshalb* $\eta = \frac{7+\sqrt{53}}{2}$. *Es ist* $\mathrm{N}(\eta) = -1$.

(b) *Es sei* $d = 31$. *Es ist* $\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$. *Wegen* $31 \not\equiv 5 \pmod 8$ *ist* $\eta = p_{h-1} + q_{h-1}\sqrt{31}$. *Es ist* $h = 8$ *und* $\frac{p_7}{q_7} = \frac{1520}{273}$, *also* $\eta = 1520 + 273\sqrt{31}$. *Da* h *gerade ist, ist* (p_7, q_7) *die Fundamentallösung von* $x^2 - 31y^2 = 1$, *d.h.* $\mathrm{N}(\eta) = 1$.

Satz 15.18. *Es sei* K *ein reellquadratischer Zahlkörper und* $d \in \mathbb{N}$ *quadratfrei mit* $K = \mathbb{Q}(\sqrt{d})$. *Es bezeichne* η *die Fundamentaleinheit von* $\mathcal{O}_K$, *und es sei* (a, b) *die Fundamentallösung der Pellschen Gleichung* $x^2 - dy^2 = 1$. *Dann gilt:*

$$a + b\sqrt{d} = \begin{cases} \eta, & \text{falls } \eta \in \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = 1 \\ \eta^2, & \text{falls } \eta \in \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = -1 \\ \eta^3, & \text{falls } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = 1 \\ \eta^6, & \text{falls } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ und } \mathrm{N}(\eta) = -1 \end{cases}$$

Beweis. Die Fundamentallösung (a, b) von $x^2 - dy^2 = 1$ korrespondiert nach Definition zu einer Einheit $\varepsilon = a + b\sqrt{d} \in \mathcal{O}_K^\times$ mit $\mathrm{N}(\varepsilon) = a^2 - db^2 = 1$, so dass a minimal ist. Wie wir

im Beweis von 14.1 gesehen haben, ist die Minimalität von a äquivalent zur Minimalität von $\varepsilon = a + b\sqrt{d}$. Gesucht ist somit das minimale $n \in \mathbb{N}$ mit $\eta^n \in \mathbb{Z}[\sqrt{d}]$ und $\mathrm{N}(\eta^n) = 1$.

Fall 1: $\eta \in \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = 1$**.** Dann ist $n = 1$.

Fall 2: $\eta \in \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = -1$**.** Dann ist $\mathrm{N}(\eta^2) = 1$ und $\eta^2 \in \mathbb{Z}[\sqrt{d}]$, also $n = 2$.

Fall 3: $\eta \notin \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = 1$**.** Wir schreiben $\eta = \frac{a+b\sqrt{d}}{2}$ mit $a, b \in \mathbb{N}$ ungerade. Wir erhalten

$$\eta^2 = \frac{a^2 + db^2 + 2ab\sqrt{d}}{4}, \quad \eta^3 = \frac{a^3 + 3dab^2 + (3ba^2 + db^3)\sqrt{d}}{8}.$$

Wegen $4 \nmid 2ab$ ist $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$. Aufgrund von $\eta \notin \mathbb{Z}[\sqrt{d}]$ ist $d \equiv 5 \pmod 8$. Unter Verwendung von $a^2 \equiv b^2 \equiv 1 \pmod 8$ liefert dies

$$a^3 + 3dab^2 \equiv a + 3da = a(1 + 3d) \equiv 0 \pmod 8$$

sowie

$$3ba^2 + db^3 \equiv 3b + db \equiv b(3 + d) \equiv 0 \pmod 8.$$

Somit ist $\eta^3 \in \mathbb{Z}[\sqrt{d}]$. Da außerdem $\mathrm{N}(\eta^3) = \mathrm{N}(\eta)^3 = 1$ ist, ist $n = 3$.

Fall 4: $\eta \notin \mathbb{Z}[\sqrt{d}]$ **und** $\mathrm{N}(\eta) = -1$**.** Wie in Fall 3 ist $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$, $\mathrm{N}(\eta^3) = -1$ und $\mathrm{N}(\eta^5) = -1$. Darüber hinaus ist $\eta^3 \in \mathbb{Z}[\sqrt{d}]$ und damit auch $\eta^{-3} = \frac{\overline{\eta^3}}{\mathrm{N}(\eta)^3} = -\overline{\eta^3}$. Folglich ist $\eta^4 \notin \mathbb{Z}[\sqrt{d}]$, andernfalls wäre $\eta = \eta^4\eta^{-3} \in \mathbb{Z}[\sqrt{d}]$, was ein Widerspruch ist. Es ist $\eta^6 = (\eta^3)^2 \in \mathbb{Z}[\sqrt{d}]$ und $\mathrm{N}(\eta^6) = (-1)^6 = 1$. Dies impliziert $n = 6$. □