11. Primfaktorzerlegungen

Euch ist sicher aus der Schule bekannt, dass sich jede positive ganze Zahl a als ein Produkt $a = p_1 \cdot \dots \cdot p_n$ von Primzahlen schreiben lässt, und dass diese Darstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Bei der Betrachtung von Teilern spielt diese sogenannte Primfaktorzerlegung eine große Rolle: Kennt man die Primfaktorzerlegung von a, so kann man daraus sofort alle Teiler von a ablesen, da dies genau die Zahlen sind, die sich als Produkte von einigen der Faktoren $p_1, \dots, p_n$ schreiben lassen. Der größte gemeinsame Teiler zweier Zahlen a und b (im Sinne von Notation 10.31 (a)) ist dann also genau das Produkt aller Primfaktoren (mit entsprechenden Potenzen), die in beiden Zahlen auftreten.

Wir wollen nun untersuchen, in wie weit etwas Analoges auch in beliebigen Integritätsringen existiert. Es ist klar, dass wir dafür zunächst erst einmal definieren müssen, was wir unter einem „Primelement“ in einem beliebigen Integritätsring überhaupt verstehen wollen. Denken wir hierfür noch einmal an den uns bekannten Fall des Ringes $\mathbb{Z}$: Was genau ist eigentlich eine Primzahl? Die meisten von euch würden hierauf wahrscheinlich antworten, dass eine Zahl p (positiv und größer als 1) eine Primzahl heißt, wenn sie außer 1 und p keine weiteren (positiven) Teiler besitzt. Diese Antwort ist natürlich letztlich auch richtig – allerdings ist dies *nicht* die Eigenschaft, durch die man in allgemeinen Integritätsringen Primelemente definiert. Stattdessen wird ein Element mit dieser Eigenschaft *irreduzibel* genannt und die Primeigenschaft zunächst einmal anders definiert:

Definition 11.1 (Primelemente und irreduzible Elemente)**.** Es seien R ein Integritätsring und $p \in R$ mit $p \neq 0$ und $p \notin R^*$.

(a) p heißt **irreduzibel**, wenn für alle $a, b \in R$ mit $p = a \cdot b$ gilt, dass $a \in R^*$ oder $b \in R^*$ ist.

(b) p heißt **prim**, wenn für alle $a, b \in R$ mit $p \,|\, a \cdot b$ gilt, dass $p \,|\, a$ oder $p \,|\, b$ ist.

Bemerkung 11.2.

(a) Nach Definition 11.1 (a) ist p genau dann irreduzibel, wenn jeder Teiler von p (also a in der Gleichung $p = a \cdot b$) entweder eine Einheit oder zu p assoziiert ist, d. h. wenn 1 und p bis auf Multiplikation mit Einheiten die einzigen Teiler von p sind. Dies ist also genau die Eigenschaft, über die normalerweise Primzahlen definiert werden.

(b) Denken wir wieder an die Primfaktorzerlegung in $\mathbb{Z}$, so ist es dort einleuchtend, dass auch die Eigenschaft (b) aus Definition 11.1 (für positive Zahlen) genau die Primzahlen charakterisiert: Wenn eine Primzahl p als Faktor im Produkt $a \cdot b$ enthalten ist, muss sie natürlich in der Primfaktorzerlegung von a oder b enthalten sein. Ist p hingegen keine Primzahl und kann auf nicht-triviale Art als Produkt $k \cdot l$ geschrieben werden, so könnte hingegen z. B. der Faktor k in a und l in b enthalten sein, so dass $p = k \cdot l$ zwar ein Teiler von $a \cdot b$, aber nicht von a oder b ist.

In $\mathbb{Z}$ scheinen die beiden in Definition 11.1 eingeführten Begriffe also übereinzustimmen. In der Tat werden wir dies in Bemerkung 11.6 auch noch beweisen. Gilt dies auch in allgemeinen Integritätsringen? Eine der beiden Implikationen ist einfach:

Lemma 11.3 („prim $\Rightarrow$ irreduzibel“)**.** *In einem Integritätsring ist jedes Primelement irreduzibel.*

Beweis. Es seien R ein Integritätsring und $p \in R$ prim. Ferner seien $a, b \in R$ mit $p = a \cdot b$. Dann gilt natürlich auch $p \,|\, a \cdot b$, und daher muss p als Primelement ein Teiler von a oder b sein. Nach evtl. Umbenennen der Elemente können wir $p \,|\, a$ annehmen, also $a = pc$ für ein $c \in R$. Einsetzen in $p = a \cdot b$ liefert dann $p = pcb$, nach der Kürzungsregel aus Lemma 7.8 (c) also $1 = cb$. Also ist $b \in R^*$ und p somit irreduzibel. $\square$

Leider gilt die Umkehrung dieses Lemmas jedoch nicht – wie ihr wohl schon vermuten werdet, wenn es zwei unterschiedliche Namen für diese beiden Eigenschaften gibt.

Beispiel 11.4 („irreduzibel $\not\Rightarrow$ prim“)**.** Es sei $R = \mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ wieder der Ring aus Konstruktion 7.24. Wie in Aufgabe 10.10 zeigt man schnell, dass die Zahl 2 bis auf Einheiten nur die Teiler 1 und 2 in R besitzt und damit irreduzibel in R ist. Allerdings gilt in R auch

$$(1+\sqrt{5}\,\mathrm{i})(1-\sqrt{5}\,\mathrm{i}) = 6 = 2\cdot 3 \quad \text{und damit} \quad 2\,|\,(1+\sqrt{5}\,\mathrm{i})(1-\sqrt{5}\,\mathrm{i}),$$

und da 2 wegen $\frac{1\pm\sqrt{5}\mathrm{i}}{2} \notin R$ kein Teiler von $1\pm\sqrt{5}\,\mathrm{i}$ ist, ist 2 nicht prim in R.

In diesem Ring R ist also nicht jedes irreduzible Element prim. Das Gegenbeispiel, das wir hier für die Umkehrung von Lemma 11.3 gefunden haben, ist damit effektiv wieder das gleiche wie das, mit dem wir in Kapitel 10 gesehen haben, dass in beliebigen Integritätsringen nicht notwendig ein größter gemeinsamer Teiler zweier Elemente existieren muss.

Wir wollen nun aber sehen, dass die Umkehrung von Lemma 11.3 zumindest in Hauptidealringen gilt.

Satz 11.5. *In einem Hauptidealring ist jedes irreduzible Element prim.*

Beweis. Es sei p ein irreduzibles Element in einem Hauptidealring R. Ferner seien $a,b \in R$ mit $p\,|\,a\cdot b$. Wir müssen zeigen, dass $p\,|\,a$ oder $p\,|\,b$ gilt.

Da R ein Hauptidealring ist, existiert nach Satz 10.13 (a) ein größter gemeinsamer Teiler von a und p. Allerdings ist p nach Voraussetzung irreduzibel und hat daher nach Bemerkung 11.2 (a) bis auf Multiplikation mit Einheiten überhaupt nur die Teiler 1 und p. Der größte gemeinsame Teiler von a und p muss also einer von diesen beiden sein:

- Ist $p \in \mathrm{ggT}(a,p)$, so gilt natürlich $p\,|\,a$ und wir sind fertig.
- Ist $1 \in \mathrm{ggT}(a,p)$, so haben wir nach Lemma 10.13 (b) eine Darstellung $1 = da + ep$ für gewisse $d,e \in R$. Multiplizieren wir diese Gleichung mit b, so erhalten wir wegen $p\,|\,ab$, also $ab \in \langle p\rangle$, auch

$$b = dab + epb \in \langle p\rangle \quad \text{und damit} \quad p\,|\,b. \qquad \square$$

Bemerkung 11.6. Für Hauptidealringe, nach Beispiel 10.23 also z. B. für $\mathbb{Z}$ oder Polynomringe über einem Körper, stimmen die Begriffe „irreduzibel“ und „prim“ nach Lemma 11.3 und Satz 11.5 also überein. Im Ring $\mathbb{Z}$ sind die positiven Elemente mit dieser Eigenschaft nach Definition genau die Primzahlen.

Aufgabe 11.7. Es seien R ein Integritätsring und $p \in R\backslash(R^* \cup \{0\})$. Ferner sei $c \in R^*$ eine Einheit. Man zeige:

(a) p ist genau dann irreduzibel, wenn $c\cdot p$ es ist.

(b) p ist genau dann prim, wenn $c\cdot p$ es ist.

Aufgabe 11.8.

(a) Zeige, dass das Polynom $t^4+t^3+t^2+t+1$ prim in $\mathbb{Z}_2[t]$ ist.

(b) Ist das Polynom $t^4-13t^3+37t^2+3t-99$ irreduzibel in $\mathbb{Z}[t]$?

Mit diesen Vorbereitungen wollen wir nun Primfaktorzerlegungen untersuchen. Da wir hierfür *beide* Eigenschaften aus Definition 11.1 benötigen werden, können wir dies nur in Hauptidealringen durchführen.

Satz 11.9 (Primfaktorzerlegung in Hauptidealringen)**.** *Es seien R ein Hauptidealring und $a \in R$ mit $a \neq 0$ und $a \notin R^*$. Dann gilt:*

(a) *Es gibt ein $n \in \mathbb{N}_{>0}$ und Primelemente $p_1,\dots,p_n \in R$, so dass $a = p_1\cdot\cdots\cdot p_n$. Man nennt eine solche Darstellung eine* ***Primfaktorzerlegung*** *von a.*

(b) *Die Darstellung aus (a) ist „bis auf die Reihenfolge und bis auf Multiplikation mit Einheiten eindeutig", d. h. sind $a = p_1 \cdot \dots \cdot p_n$ und $a = q_1 \cdot \dots \cdot q_m$ zwei Primfaktorzerlegungen wie in (a), so gilt $n = m$, und nach evtl. Umbenennen der $q_1, \dots, q_m$ ist $q_i = c_i\, p_i$ für gewisse $c_i \in R^*$ und alle $i = 1, \dots, n$.*

Beweis.

(a) Angenommen, a hätte keine solche Primfaktorzerlegung. Wir konstruieren dann wie folgt rekursiv eine Folge $a_0, a_1, a_2, \dots$ von Elementen aus $R \backslash (R^* \cup \{0\})$, die ebenfalls allesamt keine Primfaktorzerlegung besitzen: Als Startwert wählen wir $a_0 := a$. Ist nun a_n für ein $n \in \mathbb{N}$ bereits konstruiert und besitzt keine Primfaktorzerlegung, so ist a_n natürlich insbesondere nicht selbst prim, nach Satz 11.5 also auch nicht irreduzibel, und kann damit in der Form $a_n = a_{n+1} \cdot b_{n+1}$ geschrieben werden, wobei weder a_{n+1} noch b_{n+1} eine Einheit ist. Von diesen beiden Elementen kann mindestens eines keine Primfaktorzerlegung besitzen, da sonst $a_n = a_{n+1} b_{n+1}$ auch eine hätte. Nach evtl. Vertauschen von a_{n+1} mit b_{n+1} können wir also annehmen, dass a_{n+1} keine Primfaktorzerlegung besitzt, und das Verfahren so rekursiv fortsetzen.

Nach Konstruktion gilt nun $a_n \in \langle a_{n+1} \rangle$ und damit $\langle a_n \rangle \subset \langle a_{n+1} \rangle$ für alle n. Dabei ist die Gleichheit $\langle a_n \rangle = \langle a_{n+1} \rangle$ ausgeschlossen, denn sonst wäre $a_{n+1} = a_n c_n$ für ein $c_n \in R$, woraus aber $a_n = a_{n+1} b_{n+1} = a_n c_n b_{n+1}$ und damit nach der Kürzungsregel $1 = c_n b_{n+1}$ folgen würde – was ein Widerspruch dazu wäre, dass b_{n+1} keine Einheit ist. Wir erhalten also eine unendliche aufsteigende Kette von Idealen

$$\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$$

in R, die nach Aufgabe 10.37 (b) aber in einem Hauptidealring nicht existieren kann.

(b) Es seien nun $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$ zwei Primfaktorzerlegungen von a. Wir können ohne Einschränkung $n \le m$ annehmen und zeigen nun die behauptete Gleichheit der Zerlegungen mit Induktion über n.

Da p_1 prim und ein Teiler von $q_1 \cdot \dots \cdot q_m$ ist, muss p_1 nach Definition 11.1 (b) einen der Faktoren $q_1, \dots, q_m$ teilen. Nach evtl. Umnummerieren können wir also $p_1 \,|\, q_1$ annehmen, d. h. es ist $q_1 = c_1\, p_1$ für ein $c_1 \in R$. Da aber auch q_1 prim und somit nach Lemma 11.3 auch irreduzibel ist, muss $c_1 \in R^*$ gelten. Teilen wir aus dem Ausdruck für a nun mit Hilfe der Kürzungsregel aus Lemma 7.8 (c) den Faktor p_1 heraus, so erhalten wir

$$p_2 \cdot \dots \cdot p_n = (c_1 q_2) \cdot q_3 \cdot \dots \cdot q_m. \qquad (*)$$

Wir können nun die bereits angekündigte Induktion über n durchführen:

- $n = 1$: In diesem Fall besagt $(*)$ gerade $1 = c_1 q_2 \cdot q_3 \cdot \dots \cdot q_m$, d. h. $q_2, \dots, q_m$ sind Einheiten. Da Primelemente aber nach Definition 11.1 keine Einheiten sein können, muss $m = 1$ gelten, und der Beweis ist in diesem Fall fertig.
- $n - 1 \to n$: Beachte, dass in $(*)$ nach Aufgabe 11.7 mit q_2 auch $c_1 q_2$ prim ist. Anwenden der Induktionsannahme auf $(*)$ liefert also sofort die Behauptung. □

Bemerkung 11.10. In den wichtigsten Hauptidealringen $\mathbb{Z}$ und $K[t]$ für einen Körper K können wir die Eindeutigkeit bis auf Einheiten in Satz 11.9 noch auf einfache Art durch eine „echte Eindeutigkeit" ersetzen:

(a) In $\mathbb{Z}$ sind die Einheiten genau ± 1. Beschränken wir uns hier also auf positive Zahlen und Zerlegungen in positive Primfaktoren, so besagt Satz 11.9 gerade, dass sich jedes $n \in \mathbb{N}_{>1}$ (bis auf die Reihenfolge) eindeutig als Produkt von (positiven) Primzahlen schreiben lässt. Diese Aussage, die ihr ja sicher schon aus der Schule kennt, wird oft als *Hauptsatz der elementaren Zahlentheorie* bezeichnet.

(b) Im Polynomring $K[t]$ über einem Körper K ist $K[t]^* = K^* = K \backslash \{0\}$ nach Lemma 9.9 (c) und Definition 7.6 (b), d. h. die Einheiten in $K[t]$ sind genau die konstanten Polynome ungleich Null. Es gibt also offensichtlich zu jedem Polynom $f = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ (mit

$n = \deg f \in \mathbb{N}$, also $a_n \neq 0$) genau ein *normiertes* Polynom, das sich von f nur durch Multiplikation mit einer Einheit unterscheidet, nämlich $\frac{1}{a_n} \cdot f$. Aus Satz 11.9 erhalten wir damit die Aussage, dass sich jedes normierte Polynom in $K[t]$ bis auf die Reihenfolge eindeutig als Produkt von normierten irreduziblen Polynomen schreiben lässt.

Aufgabe 11.11. Zerlege die Zahl 15 im Ring $\mathbb{Z}[\mathrm{i}]$ (der nach Aufgabe 10.24 ein Hauptidealring ist) in Primfaktoren.

13

Kennt man die Primfaktorzerlegung von Elementen, so lassen sich damit wie folgt sehr einfach größte gemeinsame Teiler (und auch kleinste gemeinsame Vielfache) bestimmen.

Folgerung 11.12 (Größte gemeinsame Teiler und kleinste gemeinsame Vielfache aus Primfaktorzerlegungen)**.** *Es seien $a, b \in R \backslash (R^* \cup \{0\})$ zwei Elemente in einem Hauptidealring R, die wir bis auf Multiplikation mit Einheiten als Primfaktorzerlegungen $a = a_0 p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ und $b = b_0 p_1^{l_1} \cdot \dots \cdot p_n^{l_n}$ schreiben, wobei $a_0, b_0 \in R^*$ und $k_1, \dots, k_n, l_1, \dots, l_n \in \mathbb{N}$ gilt und die $p_1, \dots, p_n$ paarweise nicht assoziierte Primelemente sind.*

(a) *Es gilt $b \mid a$ genau dann wenn $l_i \leq k_i$ für alle i.*

(b) *Ein größter gemeinsamer Teiler von a und b ist $p_1^{\min(k_1,l_1)} \cdot \dots \cdot p_n^{\min(k_n,l_n)}$.*

(c) *Ein kleinstes gemeinsames Vielfaches von a und b ist $p_1^{\max(k_1,l_1)} \cdot \dots \cdot p_n^{\max(k_n,l_n)}$.*

Insbesondere existiert zu a und b also immer ein kleinstes gemeinsames Vielfaches (und ist dann nach Bemerkung 10.9 bis auf Multiplikation mit Einheiten eindeutig bestimmt).

Beweis.

(a) „$\Rightarrow$“: Es gelte $b \mid a$, also $a = bc$ für ein $c \in R$. Schreiben wir auch c in seiner Primfaktorzerlegung $c = c_0 p_1^{m_1} \cdot \dots \cdot p_n^{m_n}$ mit $c_0 \in R^*$ (wobei wir die vorkommenden Primfaktoren bei Bedarf ergänzen und die zugehörigen Exponenten für a und b gleich 0 setzen), so bedeutet die Gleichung $a = bc$ gerade

$$a_0 p_1^{k_1} \cdot \dots \cdot p_n^{k_n} = b_0 c_0 p_1^{l_1+m_1} \cdot \dots \cdot p_n^{l_n+m_n}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt hieraus nun sofort $k_i = l_i + m_i$ (und $a_0 = b_0 c_0$), und damit $l_i \leq k_i$ für alle i.

„$\Leftarrow$“: Ist $l_i \leq k_i$ für alle i, so gilt natürlich $a = bc$ mit $c = \frac{a_0}{b_0} p_1^{k_1-l_1} \cdot \dots \cdot p_n^{k_n-l_n}$, und damit $b \mid a$.

(b) Dies ergibt sich unmittelbar daraus, dass ein Element $p_1^{m_1} \cdot \dots \cdot p_n^{m_n}$ von R nach (a) genau dann ein gemeinsamer Teiler von a und b ist, wenn $m_i \leq k_i$ und $m_i \leq l_i$, also $m_i \leq \min(k_i, l_i)$ gilt.

(c) Analog zu (b) folgt dies daraus, dass ein Element $p_1^{m_1} \cdot \dots \cdot p_n^{m_n}$ von R nach (a) genau dann ein gemeinsames Vielfaches von a und b ist, wenn $m_i \geq k_i$ und $m_i \geq l_i$ gilt, also $m_i \geq \max(k_i, l_i)$ gilt. □

Aufgabe 11.13. Es seien $m, n \in \mathbb{Z}$ mit $m, n \neq 0$. Nach Folgerung 11.12 (c) gibt es dann zu m und n ein kleinstes gemeinsames Vielfaches, das nach Bemerkung 10.9 bis auf das Vorzeichen eindeutig bestimmt ist. Analog zu Notation 10.31 (a) bezeichnen wir das eindeutig bestimmte *positive* kleinste gemeinsame Vielfache von m und n mit $\mathrm{kgv}(m, n)$.

Zeige, dass $\mathrm{ggt}(m, n) \cdot \mathrm{kgv}(m, n) = |mn|$. Lässt sich dieses Ergebnis auf andere Hauptidealringe verallgemeinern?

Bemerkung 11.14.

(a) Ein Integritätsring R, in dem jedes Element von $R \backslash (R^* \cup \{0\})$ eine bis auf Einheiten eindeutige Primfaktorzerlegung wie in Satz 11.9 besitzt, wird als ein **faktorieller Ring** oder **ZPE-Ring** (von „**Z**erlegung in **P**rimfaktoren, **e**indeutig“) bezeichnet. Satz 11.9 besagt damit also, dass jeder Hauptidealring faktoriell ist. Es gibt jedoch noch weitaus mehr faktorielle

Ringe. So kann man z. B. zeigen, dass jeder Polynomring $R[t]$ über einem faktoriellen Ring R, also z. B. $\mathbb{Z}[t]$, selbst wieder faktoriell ist – momentan wissen wir dies nur, wenn R ein Körper und $R[t]$ damit ein Hauptidealring ist.

Der Ring $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ hingegen ist nicht faktoriell, denn nach Beispiel 11.4 ist in ihm 2 nicht prim, allerdings irreduzibel und damit nicht weiter zerlegbar, und besitzt damit also insbesondere keine Primfaktorzerlegung.

(b) Der Beweis der Existenz einer Primfaktorzerlegung in Satz 11.9 ist nicht konstruktiv. In der Tat gibt es für die konkrete Berechnung einer Primfaktorzerlegung (und sogar schon für die Untersuchung, ob ein gegebenes Element prim ist) selbst im einfachsten Hauptidealring $\mathbb{Z}$ keine brauchbare Methode – also keine Methode, die wesentlich besser ist als einfach der Reihe nach von allen von der Größe her in Frage kommenden Zahlen nachzuprüfen, ob sie ein Teiler der gegebenen Zahl sind. In der Regel wird man größte gemeinsame Teiler daher nicht mit Folgerung 11.12, sondern mit dem euklidischen Algorithmus aus Satz 10.27 berechnen.

Im Polynomring über einem Körper gibt es allerdings noch ein wichtiges Hilfsmittel, das bei der Untersuchung der Irreduzibilität bzw. der Bestimmung der Primfaktorzerlegung nützlich ist:

Lemma 11.15 (Abspalten von Nullstellen in Polynomen)**.** *Es seien K ein Körper und $f \in K[t]$ ein Polynom vom Grad $n \in \mathbb{N}_{\geq 0}$. Dann gilt:*

(a) *Ist $a \in K$ eine Nullstelle von f, so gilt $t - a \mid f$.*

(b) *f hat höchstens n Nullstellen.*

Beweis.

(a) Wir können f mit Rest durch $t - a$ dividieren und erhalten $f = q(t-a) + r$ für gewisse $q, r \in K[t]$ mit $\deg r < \deg(t-a) = 1$. Insbesondere ist r also ein konstantes Polynom. Setzen wir in diese Gleichung nun den Wert a ein, so erhalten wir

$$0 = f(a) = q(a)\,(a-a) + r(a) = r(a) \qquad \in K.$$

Da r ein konstantes Polynom ist, dessen Wert an einer Stelle a gleich Null ist, muss r bereits das Nullpolynom sein. Also ist $f = q\,(t-a)$, d. h. $t - a \mid f$.

(b) Wir zeigen die Aussage mit Induktion über n.

- $n = 0$: In diesem Fall ist die Aussage trivial, da ein konstantes Polynom $f \neq 0$ natürlich keine Nullstellen besitzt.
- $n - 1 \to n$: Hat f keine Nullstellen, so sind wir fertig. Ist andernfalls $a \in K$ eine Nullstelle von f, so können wir dieses Polynom nach (a) als $(t-a) \cdot g$ für ein $g \in K[t]$ schreiben, das nach Lemma 9.9 (a) Grad $n-1$ haben muss und nach Induktionsvoraussetzung daher höchstens $n-1$ Nullstellen besitzt. Damit hat $f = (t-a)\,g$ höchstens n Nullstellen, nämlich a und die Nullstellen von g. □

Eine wesentliche Folgerung aus diesem Lemma ist, dass der Unterschied zwischen Polynomen und Polynomfunktionen, den wir in Bemerkung 9.16 (b) gesehen hatten, nur in Körpern mit endlich vielen Elementen auftritt.

Folgerung 11.16. *Es sei K ein Körper mit unendlich vielen Elementen. Sind dann $f, g \in K[t]$ zwei Polynome mit $f(a) = g(a)$ für alle $a \in K$, so gilt bereits $f = g \in K[t]$ (d. h. „in unendlichen Körpern sind Polynome und Polynomfunktionen dasselbe“).*

Beweis. Das Polynom $f - g$ hat nach Voraussetzung unendlich viele Nullstellen – nämlich alle Elemente von K. Also muss $f - g$ nach Lemma 11.15 (b) das Nullpolynom sein, d. h. es ist $f = g$. □

Bemerkung 11.17. Für Polynome von kleinem Grad ist es nun in der Regel einfach, eine Primfaktorzerlegung zu finden bzw. zu untersuchen, ob sie irreduzibel sind. Es seien dazu K ein Körper und $f \in K[t]$.

(a) Ist $\deg f = 1$, so ist f immer irreduzibel, denn in einer möglichen Zerlegung $f = gh$ mit $g, h \in K[t]$ muss eines der Polynome g und h nach der Gradformel aus Lemma 9.9 (a) Grad 0 haben und damit konstant, also eine Einheit sein.

(b) Analog ist das Polynom f irreduzibel, wenn es keine Nullstellen hat und sein Grad gleich 2 oder 3 ist: In einer Zerlegung $f = gh$ in nicht-konstante Polynome müsste dann nämlich mindestens einer der Faktoren Grad 1 haben, so dass dieser Faktor und damit auch f eine Nullstelle haben müsste. So sind z. B. die Polynome $t^2 + 1 \in \mathbb{R}[t]$ und $t^2 + t + \overline{1} \in \mathbb{Z}_2[t]$ irreduzibel, da sie vom Grad 2 sind und in dem jeweils betrachteten Grundkörper keine Nullstellen haben.

(c) Hat umgekehrt f eine Nullstelle und ist $\deg f > 1$, so ist f sicher nicht irreduzibel, da wir die Nullstelle dann nach Lemma 11.15 abspalten können und so eine Zerlegung in Nichteinheiten erhalten.

(d) Der sogenannte *Fundamentalsatz der Algebra* besagt, dass jedes nicht-konstante Polynom über dem Körper $\mathbb{C}$ der komplexen Zahlen eine Nullstelle in $\mathbb{C}$ besitzt. Einen Beweis dieser Aussage werdet ihr erst in späteren Vorlesungen sehen (z. B. in der „Einführung in die Algebra“ oder der „Einführung in die Funktionentheorie“), da er Methoden benutzt, die deutlich über den Inhalt dieses Skripts hinaus gehen. Mit (a) und (c) können wir hier aber schon einmal festhalten, dass ein Polynom über $\mathbb{C}$ nach diesem Fundamentalsatz der Algebra genau dann irreduzibel ist, wenn es Grad 1 hat. Dementsprechend besteht die Primfaktorzerlegung eines komplexen Polynoms also ausschließlich aus linearen Faktoren.

Aufgabe 11.18 (Irreduzibilität für reelle Polynome)**.** Es sei $f \in \mathbb{R}[t]$ ein reelles Polynom. Man beweise:

(a) Ist $a \in \mathbb{C}$ eine Nullstelle von f, so ist auch die komplex konjugierte Zahl $\overline{a}$ eine Nullstelle von f.

(b) Das Polynom f ist genau dann irreduzibel in $\mathbb{R}[t]$, wenn

- $\deg f = 1$, oder
- $\deg f = 2$ und f keine reellen Nullstellen besitzt.

(Hinweis: Für Teil (b) könnt (und müsst) ihr den Fundamentalsatz der Algebra aus Bemerkung 11.17 (d) verwenden.)

Aufgabe 11.19. Es sei $f = t^{1000} + 5t^{100} + t^2 - 1 \in \mathbb{R}[t]$.

(a) Ist $t - 1$ ein Teiler von f in $\mathbb{R}[t]$?

(b) Ist $\overline{t - 1}$ invertierbar in $\mathbb{R}[t]/\langle f \rangle$?

Da wir nun in einfachen Fällen bestimmen können, ob ein gegebenes Polynom über einem Körper irreduzibel (und damit prim) ist, ist es nützlich, die Aussage aus Satz 7.10, dass $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ genau dann ein Körper ist, wenn p eine Primzahl ist, auf allgemeine Hauptidealringe zu erweitern.

Satz 11.20 (Faktorringe als Körper)**.** *Es sei p ein Element in einem Hauptidealring R. Dann sind äquivalent:*

(a) *$R/\langle p \rangle$ ist ein Körper.*

(b) *$R/\langle p \rangle$ ist ein Integritätsring.*

(c) *p ist prim.*

Beweis.

(a) $\Rightarrow$ (b): Dies ergibt sich sofort aus Lemma 7.8 (b).

(b) $\Rightarrow$ (c): Es seien $a, b \in R$ mit $p \mid ab$, also $ab \in \langle p \rangle$. Dann gilt $\overline{ab} = \overline{0}$ in $R/\langle p \rangle$. Da $R/\langle p \rangle$ ein Integritätsring ist, bedeutet dies aber gerade $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, und damit $p \mid a$ oder $p \mid b$.

(c) $\Rightarrow$ (a): Es sei p prim, und damit nach Lemma 11.3 auch irreduzibel. Bis auf Multiplikation mit Einheiten sind 1 und p also die einzigen Teiler von p. Ist nun $\overline{a} \in R/\langle p \rangle$ nicht gleich $\overline{0}$, also $p \not| a$, so ist 1 damit der einzige gemeinsame Teiler von p und a, und daher ist $\overline{a}$ nach Folgerung 10.32 eine Einheit in $R/\langle p \rangle$. Also ist $R/\langle p \rangle$ ein Körper. □

Beispiel 11.21.

(a) Für den Hauptidealring $R = \mathbb{Z}$ erhalten wir aus Satz 11.20 wieder exakt die Aussage aus Satz 7.10 zurück.

(b) Da das Polynom $t^2 + 1 \in \mathbb{R}[t]$ nach Bemerkung 11.17 (b) irreduzibel ist, ist $\mathbb{R}[t]/\langle t^2+1 \rangle$ nach Satz 11.20 ein Körper – und zwar gerade $\mathbb{C}$, wie wir in Aufgabe 10.21 (b) bereits gesehen hatten.

In der Tat ist dies algebraisch die eleganteste Art, die komplexen Zahlen als Körper zu konstruieren, indem man sie einfach als $\mathbb{C} := \mathbb{R}[t]/\langle t^2+1 \rangle$ *definiert*. Diese Definition sagt sehr anschaulich, was die Idee der komplexen Zahlen ist und wie man damit rechnen kann: Wir nehmen zu $\mathbb{R}$ ein neues Element hinzu (das hier t heißt, aber üblicherweise dann natürlich als i bezeichnet wird), das genau die eine Gleichung $t^2 + 1 = 0$ erfüllt.

(c) Auch das Polynom $f := t^2 + t + \overline{1} \in \mathbb{Z}_2[t]$ ist nach Bemerkung 11.17 (b) irreduzibel, und damit ist auch $R := \mathbb{Z}_2[t]/\langle f \rangle$ ein Körper. Da jede Klasse in R nach Aufgabe 10.21 (a) einen eindeutigen Repräsentanten der Form $a_1 t + a_0$ mit $a_0, a_1 \in \mathbb{Z}_2$ hat, ist R ein Körper mit genau 4 Elementen. Er wird in der Literatur aufgrund des englischen Worts „field“ für „Körper“ mit $\mathbb{F}_4$ bezeichnet.

Beachte, dass $\mathbb{F}_4$ natürlich nicht isomorph zu $\mathbb{Z}_4$ ist, weil $\mathbb{Z}_4$ ja kein Körper ist.

Zum Abschluss wollen wir nun als Anwendung der Primfaktorzerlegung und unserer Ergebnisse zur Teilbarkeit in Ringen noch einen häufig vorkommenden Typ von Gleichungssystemen betrachten: Angenommen, wir suchen alle ganzen Zahlen $x \in \mathbb{Z}$, die modulo bestimmter Zahlen vorgegebene Restklassen darstellen, d. h. alle Zahlen, die ein Gleichungssystem der Form

$$\begin{array}{lcl} x = a_1 \mod n_1 & & \overline{x} = \overline{a_1} \in \mathbb{Z}_{n_1} \\ \vdots & \text{bzw.} & \vdots \\ x = a_k \mod n_k & & \overline{x} = \overline{a_k} \in \mathbb{Z}_{n_k} \end{array}$$

mit gegebenen $a_1, \dots, a_k \in \mathbb{Z}$ und $n_1, \dots, n_k \in \mathbb{N}_{>0}$ erfüllen (beachte, dass wir die Notation $\overline{x}$ hierbei für die Restklassen von x in *verschiedenen* Faktorringen $\mathbb{Z}_{n_1}, \dots, \mathbb{Z}_{n_k}$ verwendet haben). Das entscheidende Hilfsmittel bei der Lösung derartiger Gleichungssysteme ist der sogenannte chinesische Restsatz (der so genannt wird, da er in China bereits im 3. Jahrhundert bekannt war). In der Tat liefert der Beweis dieses Satzes bereits einen Algorithmus zur Lösung des obigen Gleichungssystems.

Satz 11.22 (Chinesischer Restsatz). *Es seien $n_1, \dots, n_k \in \mathbb{N}_{>1}$ paarweise teilerfremde Zahlen, d. h. es gelte $\operatorname{ggt}(n_i, n_j) = 1$ für alle $i, j = 1, \dots, k$ mit $i \neq j$. Dann ist die Abbildung*

$$\begin{aligned} f \colon \mathbb{Z}_N &\to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \\ \overline{a} &\mapsto (\overline{a}, \dots, \overline{a}) \end{aligned}$$

mit $N := n_1 \cdot \dots \cdot n_k$ ein Ringisomorphismus. (Beachte, dass auch hierbei wieder die Notation $\overline{a}$ für die Restklassen von a in verschiedenen Faktorringen $\mathbb{Z}_N, \mathbb{Z}_{n_1}, \dots, \mathbb{Z}_{n_k}$ verwendet wurde.)

Beweis. Als Erstes müssen wir die Wohldefiniertheit von f überprüfen (siehe Bemerkung 6.1): Sind $a, b \in \mathbb{Z}$ mit $\overline{a} = \overline{b} \in \mathbb{Z}_N$, also $b - a \in N\mathbb{Z}$, so ist wegen $N\mathbb{Z} \subset n_i\mathbb{Z}$ für alle $i = 1, \dots, k$ natürlich auch $b - a \in n_i\mathbb{Z}$ und damit $\overline{a} = \overline{b} \in \mathbb{Z}_{n_i}$. Also ist dann auch $(\overline{a}, \dots, \overline{a}) = (\overline{b}, \dots, \overline{b}) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$, d. h. f ist wohldefiniert.

Als Nächstes stellen wir fest, dass f in der Tat ein Ringhomomorphismus ist: Es ist $f(\overline{1}) = (\overline{1}, \dots, \overline{1})$, für alle $a, b \in \mathbb{Z}$ ist

$$f(\overline{a} + \overline{b}) = f(\overline{a+b}) = (\overline{a+b}, \dots, \overline{a+b}) = (\overline{a}, \dots, \overline{a}) + (\overline{b}, \dots, \overline{b}) = f(\overline{a}) + f(\overline{b}),$$

und eine analoge Aussage gilt natürlich genauso für die Multiplikation.

Es bleibt also nur noch die Bijektivität von f zu zeigen. Da der Start- und Zielraum von f die gleiche (endliche) Anzahl N von Elementen haben, genügt es hierfür zu zeigen, dass f surjektiv ist. Es seien dazu $a_1,\dots,a_k \in \mathbb{Z}$ beliebig. Wir müssen zeigen, dass es ein $a \in \mathbb{Z}$ gibt, das $f(\overline{a}) = (\overline{a_1},\dots,\overline{a_k})$ erfüllt und damit das oben betrachtete Gleichungssystem $\overline{x} = \overline{a_i} \in \mathbb{Z}_{n_i}$ für alle $i = 1,\dots,k$ löst. Der Beweis hierfür ist konstruktiv und ermöglicht damit auch eine explizite Lösung dieses Gleichungssystems:

(1) Für $i = 1,\dots,k$ setzen wir

$$N_i := \frac{N}{n_i} = n_1 \cdot \dots \cdot n_{i-1} \cdot n_{i+1} \cdot \dots \cdot n_k.$$

(2) Nach Voraussetzung ist $\operatorname{ggt}(n_i,n_j) = 1$ für $i \neq j$, d. h. jede Primzahl tritt in der Primfaktorzerlegung von höchstens einer der Zahlen $n_1,\dots,n_k$ auf. Damit gilt dann natürlich auch $\operatorname{ggt}(n_i,N_i) = 1$ für alle $i = 1,\dots,k$. Nach Folgerung 10.32 ist $\overline{N_i}$ also eine Einheit in $\mathbb{Z}_{n_i}$, und wir können mit dem erweiterten euklidischen Algorithmus 10.28 ihr multiplikatives Inverses $\overline{M_i}$ in $\mathbb{Z}_{n_i}$, also ein $M_i \in \mathbb{Z}$ mit

$$\overline{M_i} \cdot \overline{N_i} = \overline{1} \quad \in \mathbb{Z}_{n_i} \tag{$*$}$$

berechnen.

(3) Wir setzen nun

$$a := \sum_{i=1}^{k} a_i M_i N_i \quad \in \mathbb{Z}.$$

Dann ist a eine (und damit, wie wir schon gesehen haben, modulo N die einzige) Lösung des Gleichungssystems $\overline{x} = \overline{a_i} \in \mathbb{Z}_{n_i}$ für alle i, denn für alle i gilt in $\mathbb{Z}_{n_i}$

$$\begin{aligned}
\overline{a} &= \sum_{j=1}^{k} \overline{a_j}\,\overline{M_j}\,\overline{N_j} \\
&= \overline{a_i}\,\overline{M_i}\,\overline{N_i} \qquad (N_j \text{ enthält für } j \neq i \text{ den Faktor } n_i\text{, also ist dann } \overline{N_j} = \overline{0} \in \mathbb{Z}_{n_i}) \\
&\overset{(*)}{=} \overline{a_i}.
\end{aligned}$$

Mit anderen Worten ist die Restklasse $\overline{a} \in \mathbb{Z}_N$ ein (und damit das einzige) Urbild von $(\overline{a_1},\dots,\overline{a_k})$ unter f, d. h. f ist surjektiv. □

Beispiel 11.23. Mit Hilfe des chinesischen Restsatzes können wir nun Gleichungssysteme von Restklassen, wie wir sie oben betrachtet haben, leicht umformen. Dabei können wir den Isomorphismus aus Satz 11.22 „sowohl von links nach rechts als auch von rechts nach links lesen“:

(a) Betrachten wir für ein gegebenes $a \in \mathbb{Z}$ die Gleichung $\overline{x} = \overline{a}$ in einem Restklassenring $\mathbb{Z}_N$ und können wir dieses N als Produkt $N = n_1 \cdot \dots \cdot n_k$ von Zahlen mit $\operatorname{ggt}(n_i,n_j) = 1$ für $i \neq j$ schreiben, so lässt sich die betrachtete Gleichung durch Anwenden des Isomorphismus aus dem chinesischen Restsatz 11.22 vom Ring $\mathbb{Z}_N$ nach $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ übertragen, d. h. wir erhalten die Äquivalenz von Gleichungssystemen

$$\overline{x} = \overline{a} \in \mathbb{Z}_N \qquad \Leftrightarrow \qquad \begin{cases} \overline{x} = \overline{a} \in \mathbb{Z}_{n_1} \\ \quad\vdots \\ \overline{x} = \overline{a} \in \mathbb{Z}_{n_k}. \end{cases}$$

Konkret sind z. B. die folgenden Gleichungssysteme äquivalent:

$$x = 5 \mod 6 \qquad \Leftrightarrow \qquad \begin{array}{l} x = 5 \mod 2 \\ x = 5 \mod 3 \end{array} \qquad \Leftrightarrow \qquad \begin{array}{l} x = 1 \mod 2 \\ x = 2 \mod 3, \end{array}$$

wobei sich die zweite Äquivalenz natürlich einfach durch Reduktion der rechten Seiten modulo 2 bzw. 3 ergibt.

(b) Deutlich nützlicher ist die Anwendung des Isomorphismus aus Satz 11.22 „in der umgekehrten Richtung“: Indem wir die explizite Konstruktion des Umkehrisomorphismus aus dem Beweis des Satzes verwenden, können wir mehrere Gleichungen zu einer zusammenfassen. Als konkretes Beispiel hierfür wollen wir alle $x \in \mathbb{Z}$ finden, die das Gleichungssystem

$$\begin{aligned} x &= 1 \mod 2 \\ x &= 1 \mod 5 \\ x &= 2 \mod 7 \end{aligned}$$

erfüllen. Dazu gehen wir die drei Schritte aus dem Beweis des chinesischen Restsatzes durch:

(1) Es ist zunächst einmal $n_1 = 2$, $n_2 = 5$ und $n_3 = 7$, wir haben damit also $N = 2 \cdot 5 \cdot 7 = 70$ und setzen $N_1 = 5 \cdot 7 = 35$, $N_2 = 2 \cdot 7 = 14$ und $N_3 = 2 \cdot 5 = 10$.

(2) Die Inversen von N_i modulo n_i für alle i sehen wir in diesem Fall auch ohne den erweiterten euklidischen Algorithmus sofort:

- In $\mathbb{Z}_{n_1} = \mathbb{Z}_2$ ist das Inverse von $\overline{N_1} = \overline{35} = \overline{1}$ gleich $\overline{1}$, also setzen wir $M_1 = 1$.
- In $\mathbb{Z}_{n_2} = \mathbb{Z}_5$ ist das Inverse von $\overline{N_2} = \overline{14} = \overline{4}$ gleich $\overline{4}$, also setzen wir $M_2 = 4$.
- In $\mathbb{Z}_{n_3} = \mathbb{Z}_7$ ist das Inverse von $\overline{N_3} = \overline{10} = \overline{3}$ gleich $\overline{5}$, also setzen wir $M_3 = 5$.

(3) Mit den rechten Seiten $a_1 = 1$, $a_2 = 1$ und $a_3 = 2$ des Gleichungssystems bilden wir nun die Zahl

$$a = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = 1 \cdot 1 \cdot 35 + 1 \cdot 4 \cdot 14 + 2 \cdot 5 \cdot 10 = 191.$$

Die Lösung des gegebenen Gleichungssystems sind also alle $x \in \mathbb{Z}$ mit $\overline{x} = \overline{191} = \overline{51} \in \mathbb{Z}_{70}$, d. h. alle $x \in 51 + 70\mathbb{Z}$.

Eine Kontrolle dieses Ergebnisses ist natürlich sehr einfach möglich, da man ja schnell nachprüfen kann, dass die Zahl 51 wirklich das gegebene Gleichungssystem erfüllt.

Aufgabe 11.24. Bestimme alle $x \in \mathbb{Z}$, für die die folgenden Gleichungssysteme erfüllt sind:

(a) $\begin{aligned} x &= 2 \mod 4 \\ x &= 6 \mod 7 \\ x &= 3 \mod 9 \end{aligned}$ (b) $\begin{aligned} x &= 5 \mod 6 \\ 3x &= -1 \mod 14 \end{aligned}$ (c) $x = 1 \mod n$ für alle $n = 2, \dots, 10$

Aufgabe 11.25. Zeige die folgende Umkehrung des chinesischen Restsatzes: Sind $n, m \in \mathbb{N}_{>0}$ nicht teilerfremd, so ist $\mathbb{Z}_{nm}$ nicht isomorph zu $\mathbb{Z}_n \times \mathbb{Z}_m$.

Der chinesische Restsatz lässt sich schließlich noch einfach auf die Einheitengruppen übertragen:

Folgerung 11.26. *Es seien $n_1, \dots, n_k \in \mathbb{N}_{>1}$ paarweise teilerfremde Zahlen. Dann ist die Abbildung*

$$\begin{aligned} f \colon \mathbb{Z}_N^* &\to \mathbb{Z}_{n_1}^* \times \dots \times \mathbb{Z}_{n_k}^* \\ \overline{a} &\mapsto (\overline{a}, \dots, \overline{a}) \end{aligned}$$

mit $N := n_1 \cdot \dots \cdot n_k$ ein Gruppenisomorphismus.

Beweis. Die Abbildung f aus dem chinesischen Restsatz 11.22 ist ein Ringisomorphismus und bildet damit die Einheiten von $\mathbb{Z}_N$ genau auf die Einheiten von $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ ab. Letztere sind nach Aufgabe 7.15 aber genau die Elemente von $\mathbb{Z}_{n_1}^* \times \dots \times \mathbb{Z}_{n_k}^*$, woraus die Behauptung folgt. □

Aufgabe 11.27. Man beweise oder widerlege:

(a) $\mathbb{Z}_{25}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_5^*$;

(b) $\mathbb{Z}_{15}^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Aufgabe 11.28. Es sei $k \in \mathbb{N}$, so dass die drei Zahlen $6k+1$, $12k+1$ und $18k+1$ prim sind.

14 Man zeige: Für $n := (6k+1)(12k+1)(18k+1)$ und alle $a \in \mathbb{Z}$ mit $\operatorname{ggt}(a,n) = 1$ gilt $a^{n-1} = 1 \mod n$.