Mathematische Strukturen
Teilbarkeit und Faktorisierung

Hagen Knaf

SS 2014

Einleitung

Im Ring $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ der ganzen Zahlen ist der Begriff der Teilbarkeit einer Zahl $z \in \mathbb{Z}$ durch eine Zahl $d \in \mathbb{Z}\backslash 0$ grundlegend, sowohl für die Theorie als auch in Anwendungen. Man sagt »d teilt z« oder »d ist ein Teiler von z«– in Symbolen $d|z$ – falls es ein $q \in \mathbb{Z}$ mit der Eigenschaft $z = qd$ gibt. Ganze Zahlen p ohne Teiler verschieden von $-1, 1, -p, p$ werden *Primzahlen* genannt. Als zentrales Ergebnis der elementaren Zahlentheorie gilt dann:

SATZ: *Jede ganze Zahl $z \in \mathbb{Z}$ lässt sich eindeutig als Produkt*

$$z = up_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

schreiben, wobei $u \in \{-1, 1\}$, $e_1, \ldots, e_r \in \mathbb{N}$ und $p_1, \ldots, p_r$ positive Primzahlen sind.

Ziel der folgenden Ausführungen ist es die Gründe für die Gültigkeit dieses Satzes zu analysieren, und mit Hilfe der Ergebnisse dieser Analyse eine weitgehende Verallgemeinerung zu formulieren und zu beweisen. Die Vorgehensweise beim Verfolgen dieses Zieles ist typisch für das in der Mathematik so erfolgreich angewandte »Denken in Strukturen«.

1 Teilbarkeit

Will man den Begriff der Teilbarkeit ganzer Zahlen auf Ringe verallgemeinern, so treten unmittelbar verschiedene Probleme auf:

- In einem Ring R mit nicht kommutativer Multiplikation muss man zwischen Links- und Rechts-Teilbarkeit unterscheiden: Falls für ein $r \in R$ und $d \in R \setminus 0$ eine Gleichung $r = dq$ gilt, muss eine Gleichung der Form $r = q'd$ nicht notwendig auch gelten, und umgekehrt.

  Beispiel: Für die Matrizen

  $$Q := \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix},\ D := \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$$

  gilt

  $$QD = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix},$$

  folglich ist D Rechtsteiler von $B := QD$. Aber für jede Matrix

  $$Q' := \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$$

  gilt:

  $$DQ' = \begin{pmatrix} d_1q_{11} + d_2q_{21} & d_1q_{12} + d_2q_{22} \\ 0 & 0 \end{pmatrix},$$

  womit D kein Linksteiler von B sein kann.

- In beliebigen Ringen kann man im Allgemeinen nicht »kürzen«, das heißt aus $dq = dq'$ folgt nicht notwendig $q = q'$.

  Beispiel: In $\mathbb{Z}/12$ gilt $\overline{3} \cdot \overline{2} = \overline{3} \cdot \overline{10}$.

In der durch die folgende Definition festgelegten Klasse von Ringen treten diese Probleme nicht auf:

DEFINITION 39: *Ein Ring heißt Integritätbereich, falls die Multiplikation in R kommutativ ist, und R keine Nullteiler besitzt.*

In einem Integritätsbereich kann man kürzen: Für $r, s, t \in R$, $r \neq 0$ gilt nämlich

$$rs = rt \Leftrightarrow 0 = rs - rt = r(s - t) \Leftrightarrow s - t = 0 \Leftrightarrow s = t.$$

Teilbarkeit wird nun definiert, indem man den Fall ganzer Zahlen imitiert:

DEFINITION 40: *Es sei R ein Integritätsbereich, $r \in R$ und $d \in R$, $d \neq 0$. Man sagt »d teilt r« (Notation: $d|r$), oder auch »d ist ein Teiler von r«, oder auch »r ist ein Vielfaches von d«, falls es ein Element $q \in R$ mit*

$$r = qd$$

gibt.

Die Eigenschaften der Teilbarkeitsrelation sind nun tatsächlich vergleichbar mit denen der Teilbarkeit ganzer Zahlen:

FESTSTELLUNG 41: *Die Teilbarkeitsrelation besitzt die folgenden Eigenschaften:*

1. $\forall r \in R \setminus 0 \;\; 1|r,\; r|0,\; r|r,$
2. $r|1 \Leftrightarrow r \in R^\times,$
3. $d|r \Rightarrow \forall s \in R \;\; ds|rs,$
4. $d|r_k,\; k = 1, \ldots, n \Rightarrow \forall s_1, \ldots, s_n \in R \;\; d|(r_1 s_1 + \ldots + r_n s_n),$
5. $r|s \wedge s|t \Rightarrow r|t,$
6. $r|s \wedge s|r \Rightarrow \exists u \in R^\times \;\; r = us.$

Diese Eigenschaften zu überprüfen ist eine einfache Übung. Bespielhaft wird hier der Beweis für die Eigenschaft 6 angegeben: Es gilt $s = vr$ und $r = us$, also $r = vur$. Kürzen liefert $1 = uv$ und damit wie behauptet $u \in R^\times$.

In bezug auf Teilbarkeit verhalten sich $d \in \mathbb{Z}$, $d \neq 0$ und $-d$ völlig gleich, das heißt:

$$\forall z \in \mathbb{Z}\; d|z \Leftrightarrow -d|z.$$

Man beachte dabei, dass für die Gruppe der bezüglich Multiplikation invertierbaren Elemente in $\mathbb{Z}$ gilt: $\mathbb{Z}^\times = \{-1, 1\}$.

Entsprechend gilt in einem beliebigen Integritätsbereich: Ist $d \in R$, $d \neq 0$ und gilt $r = qd$, so folgt $r = (u^{-1}q)(ud)$ für jede Einheit $u \in R^\times$. Man kann also festhalten:

$$\forall r \in R\, \forall u \in R^\times \;\; d|r \Leftrightarrow (ud)|r.$$

Dieses Verhalten motiviert die folgende

DEFINITION 42: *Die Elemente $r, s \in R$ heißen assoziiert (Notation: $r \sim s$), falls es $u \in R^\times$ mit $s = ur$ gibt.*

Das Element $d \in R \setminus 0$ heißt echter Teiler von $r \in R$, falls $r = qd$ mit $d, q \notin R^\times$ gilt.

Es ist leicht zu sehen, dass Assoziiertheit eine Äquivalenzrelation auf dem Ring R ist. Es gilt $r \sim 1$ genau dann, wenn $r \in R^\times$. Entsprechend ist d ein echter Teiler von r genau dann, wenn in $r = qd$ die Bedingungen $d \not\sim 1$ und $d \not\sim r$ gelten.

Hier drei Beispiele aus dem Ring $\mathbb{R}[X]$ der reellen Polynome in einer Variablen:

- Es gilt $(X^4 + 1) | (X^7 - 7X^5 + X^3 - 7X)$, da

  $$X^7 - 7X^5 + X^3 - 7X = (X^4 + 1)(X^3 - 7X).$$

  Hierbei ist $X^4 + 1$ ein echter Teiler, da $\mathbb{R}[X]^\times = \mathbb{R} \setminus 0$ gilt.

- Es gilt $(42X^4 + 42) | (X^4 + 1)$, aber $42X^4 + 42$ ist ein unechter Teiler, da $42 \in \mathbb{R} \setminus 0$.

- Das Polynom $X - 1$ ist kein Teiler von $X^4 + 1$, denn dann wäre 1 eine Nullstelle von $X^4 + 1$, was offenbar nicht der Fall ist.

2 Irreduzibilität und Primelemente

Nach dem Einführen der Teilbarkeit soll versucht werden den Primzahlbegriff auf Integritätsbereiche zu verallgemeinern. Hierfür scheinen zwei Eigenschaften von Primzahlen geeignet zu sein:

(I) $p = ab \Rightarrow (a \in \{-1, 1\} \vee b \in \{-1, 1\})$,

(P) $p | (ab) \Rightarrow (p | a \vee p | b)$.

Die Eigenschaft (I) besagt, dass Primzahlen keine echten Teiler besitzen. Ihre Bedeutung im Rahmen der Faktorisierung ist klar: In der Primfaktorisierung auftretende Elemente sollen nicht weiter zerlegbar sein.

Die Eigenschaft (P) ist etwas subtiler: Sind beispielsweise p_1, q_1, p_2, q_2 vier positive Primzahlen für die die Gleichung $p_1 q_1 = p_2 q_2$ gilt. Weshalb folgt dann

$p_1 = p_2$ oder $p_1 = q_2$? Könnte es nicht sein, dass p_1 zwar das Produkt $p_2 q_2$ teilt, aber keinen der Faktoren?

Beide Eigenschaften sollen nun etwas detaillierter diskutiert werden.

Weshalb gibt es in $\mathbb{Z}$ überhaupt Zahlen mit der Eigenschaft (I)? Die Antwort wird durch ein simples Verfahren geliefert: Man wählt eine ganze Zahl $d_1 \neq 0$. Besitzt d_1 keinen echten Teiler, so hat d_1 die Eigenschaft (I). Andernfalls wählt man einen echten Teiler $d_2 | d_1$; für diesen gilt $|d_2| < |d_1|$. Besitzt d_2 keinen echten Teiler, so hat d_2 die Eigenschaft (I), andernfalls wählt man einen echten Teiler d_3 usw. Dieses Vorgehen liefert eine Folge $d_1, d_2, d_3, \ldots$ von ganzen Zahlen mit $|d_k| < |d_{k-1}|$, die Folge muss also nach endlich vielen Schritten mit einer Zahl mit der Eigenschaft (I) abbrechen.

Zahlen mit der Eigenschaft (I) gibt es also, weil es eine Betragsfunktion auf $\mathbb{Z}$ gibt.

Weshalb gibt es in $\mathbb{Z}$ Zahlen mit der Eigenschaft (P)? Zunächst beobachtet man Folgendes: Besitzt einen ganze Zahl p die Eigenschaft (P), so folgt aus $p = ab$ entweder $a = qp$ oder $b = qp$ mit $q \in \mathbb{Z}$. Im ersten Fall ergibt sich $p = qbp$ also durch Kürzen $1 = qb$, das heißt $b \in \{-1, 1\}$. Entsprechendes gilt im zweiten Fall.

Jede Zahl mit der Eigenschaft (P) besitzt also auch die Eigenschaft (I).

Gilt auch die logische Umkehrung? Es sei also p eine Zahl mit der Eigenschaft (I) und es gelte $p|(ab)$ für $a, b \in \mathbb{Z}$. Nimmt man an, dass p den Faktor a nicht teilt, so sind wegen der Eigenschaft (I) die Zahlen p und a teilerfremd. In der Vorlesung wurde der Satz von Bezout bewiesen, der im vorliegenden Fall die Existenz von Zahlen $z_1, z_2 \in \mathbb{Z}$ liefert, für die

$$z_1 a + z_2 p = 1$$

gilt. Multiplikation mit b liefert $z_1 ab + z_2 bp = b$. Da ab durch p teilbar ist, ist folglich b durch p teilbar, womit p die Eigenschaft (P) besitzt.

Jede Zahl mit der Eigenschaft (I) besitzt auch die Eigenschaft (P). Der Grund hierfür ist der Satz von Bezout, dessen Beweis darauf beruht, dass man in $\mathbb{Z}$ jede ganze Zahl $z \in \mathbb{Z}$ mit Rest durch eine ganze Zahl $d \neq 0$ teilen kann:

$$z = qd + r, \ |r| < |d|.$$

Als Schlussfolgerung kann man festhalten: Eigenschaft (I) lässt sich einfach aus Eigenschaft (P) folgern. Das Umgekehrte gilt, etwas überraschend, nicht. Man betrachtet daher die Eigenschaften (I) und (P) in Integritätsbereichen zunächst getrennt:

DEFINITION 43 (und Festellung): *Sei R ein Integritätsbereich.*

Ein Element $p \in R$ heißt irreduzibel, falls es keine Faktorzerlegung $p = ab$ mit $a, b \notin R^\times$ gibt.

Ein Element $p \in R$ heißt Primelement, falls die Eigenschaft (P) gilt.

Jedes Primelement von R ist irreduzibel.

Es gibt Integritätsbereiche, in denen es irreduzible Elemente gibt, die keine Primelemente sind.

BEWEIS DER BEHAUPTUNG ÜBER PRIMELEMENTE: Es sei p ein Primelement und $p = ab$. Dann gilt also $p|a$ oder $p|b$. Im ersten Fall ergibt sich $p = qbp$ mit einem $q \in R$ und daher durch Kürzen $qb = 1$. Folglich ist $b \in R^\times$. Der zweite Fall wird genauso behandelt.

Das folgende Beispiel zeigt, dass irreduzible Elemente im Allgemeinen keine Primelemente sein müssen: Man betrachte die Menge

$$\mathbb{Z}[\sqrt{-5}] := \{z_1 + z_2\sqrt{-5} : z_1, z_2 \in \mathbb{Z}\} \subset \mathbb{C}.$$

Es ist leicht nachzurechnen, dass $\mathbb{Z}[\sqrt{-5}]$ mit der Addition und Multiplikation komplexer Zahlen einen Integritätsbereich bildet. Die quadrierte Betragsfunktion

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0,\ N(z_1 + z_2\sqrt{-5}) = |z_1 + z_2\sqrt{-5}|^2 = z_1^2 + 5z_2^2$$

hat die Eigenschaft $N(ab) = N(a)N(b)$ für beliebige $a, b \in \mathbb{Z}[\sqrt{-5}]$.

Die Abbildung N ist sehr nützlich zur Untersuchung der Eigenschaften des Rings $\mathbb{Z}[\sqrt{-5}]$.

- $\mathbb{Z}[\sqrt{-5}]^\times = \{-1, 1\}$.

Denn: Ist $u \in \mathbb{Z}[\sqrt{-5}]^\times$, so gibt es $v \in \mathbb{Z}[\sqrt{-5}]$ mit $uv = 1$, also $1 = N(uv) = N(u)N(v)$. Da die Werte von N natürliche Zahlen sind, folgt $N(u) = 1$, woraus sich sofort $u = -1$ oder $u = 1$ ergibt. Die Tatsache, dass die Elemente -1 und 1 Einheiten sind, ist klar.

- Die Elemente $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ sind irreduzibel.

Denn: Ist a eines der drei Elemente, so gilt $N(a) = 9$. Sei nun d ein Teiler von a. Dann gilt $N(d)|9$ und damit $N(d) = 1$, $N(d) = 3$ oder $N(d) = 9$. Im ersten Fall folgt $d = 1$ oder $d = -1$. Der zweite Fall kann nicht vorkommen, da für $d \neq 0$ stets $N(d)$ eine Qudratzahl oder ≥ 5 ist. Im dritten Fall gilt $N(q) = 1$ für $a = qd$, womit $q = -1$ oder $q = 1$ folgt. Insgesamt ist d also kein echter Teiler von a.

- $3^2 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$, folglich ist 3 kein Primelement in $\mathbb{Z}[\sqrt{-5}]$.

Die Gleichung ist klar. Wäre 3 ein Primelement, so müsste $3 = (2+\sqrt{-5})b$ mit einem $b \in \mathbb{Z}[\sqrt{-5}]$ gelten. Es folgt $N(b) = 1$ und damit $b = -1$ oder $b = 1$, ein Widerspruch.

Um aus der Eigenschaft (I) die Eigenschaft (P) und damit die Existenz von Primelementen zu folgern, benötigt man in $\mathbb{Z}$ das Teilen mit Rest. Dies wird nun ebenfalls imitiert:

Definition 44: *Ein euklidischer Ring ist ein Paar (R, δ) bestehend aus einem Integritätsbereich R und einer Abbildung*

$$\delta : R \setminus 0 \to \mathbb{N}_0$$

mit folgender Eigenschaft: Zu $a, b \in R$, $a \neq 0$, gibt es ein $r \in R$ derart, dass $b = qa + r$ gilt, wobei entweder $\delta(r) < \delta(a)$ oder $r = 0$ gilt.

Eine große Klasse von Ringen sind euklidisch wie jetzt gezeigt wird.

Definition 45: *Ein kommutativer Ring K mit der Eigenschaft $K^\times = K \setminus 0$ heißt Körper.*

Da Einheiten in einem Ring keine Nullteiler sind, ist ein Körper immer ein Integritätsbereich.

Beispiele von Körpern sind: die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$, die Menge $\mathbb{Z}/p$ der Restklassen modulo einer Primzahl p.

Neben diesen aus der Vorlesung bereits gut bekannten Beispielen, sind auch die Teilmengen

$$\mathbb{Q}[\sqrt{d}] := \{q_1 + q_2\sqrt{d} : q_1, q_2 \in \mathbb{Q}\} \subset \mathbb{C}$$

für jedes $d \in \mathbb{Z}$ Körper, wenn man die Addition und Multiplikation komplexer Zahlen als Verknüpfung benutzt.

Definition 46 (und Feststellung): *Es sei K ein Körper und $K[X]$ die Menge aller Ausdrücke der Form*

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0,$$

wobei $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in K$ sind. Diese Ausdrücke werden Polynome in der Unbestimmten X mit Koeffizienten in K genannt; die Koeffizienten sind die Körperelemente a_k.

Zwei Polynome

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

und

$$g = b_m X^m + a_{m-1} X^{m-1} + \ldots + b_0$$

sind verschieden, falls es ein $k \in \mathbb{N}$ mit $a_k \neq b_k$ gibt.

f und g werden nach der folgenden Regel addiert:

$$f+g := a_n X^n + \ldots a_{m+1} X^{m+1} + (a_m + b_m) X^m + (a_{m-1} + b_{m-1}) X^{m-1} + \ldots + (a_0 + b_0)$$

im Fall $n \geq m$. Im Fall $n < m$ gilt eine analoge Formel mit vertauschten Rollen von f und g.

f und g werden nach der folgenden Regel multipliziert:

$$fg := a_n b_m X^{n+m} + \ldots + (\sum_{i+j=k} a_i b_j) X^k + \ldots + (a_0 b_0).$$

Die Menge $K[X]$ bildet mit diesen beiden Verknüpfungen einen kommutativen Ring ohne Nullteiler.

Beweis:

- Offensichtlich sind die Summe und das Produkt von Polynomen wieder Polynome.
- Das Assoziativgesetz für die Addition gilt, weil es für das Addieren der Koeffizienten der Polynome gilt.
- Das neutrale Element der Addition ist das Nullpolynom $0 = 0 + 0X + 0X^2 + \ldots + 0X^n$.
- Das additive Inverse zu $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ ist das Polynom $-f = -a_n X^n + (-a_{n-1}) X^{n-1} + \ldots + (-a_0)$.
- Das neutrale Element der Multiplikation ist das Einspolynom $1 = 1 + 0X + 0X^2 + \ldots + 0X^n$.

- Die Gültigkeit des Assoziativgesetzes für die Multiplikation und der Distributivgesetze ergibt sich aus einer elementaren, aber länglichen Rechnung.
- Sind $f = a_n X^n + \ldots + a_0$, $a_n \neq 0$, und $g = b_m X^n + \ldots + b_0$, $b_m \neq 0$, zwei Polynome, so folgt $fg = a_n b_m X^{n+m} + \ldots + a_0 b_0 \neq 0$.

□

SATZ 47: *Der Polynomring $K[X]$ ist zusammen mit der Gradfunktion*

$$\deg : \ K[X] \to \mathbb{N}_0, \ (a_n X^n + \ldots + a_0, \ a_n \neq 0) \mapsto n$$

ein euklidischer Ring.

BEWEIS: Seien $f = a_n X^n + \ldots + a_0$, $a_n \neq 0$, und $d = b_m X^m + \ldots + b_0$, $b_m \neq 0$.

Im Fall $m > n$ kann man $f = 0 \cdot d + f$ schreiben, wobei für den Rest f die Bedingung $\deg(f) < \deg(d)$ gilt.

Der Fall $m \leq n$ wird durch voollständige Induktion nach n bewiesen.

Induktionsanfang ($n = 0$): In diesem Fall ist $f \in K \setminus 0$ und daher auch $d \in K \setminus 0$. Es gilt

$$f = f d^{-1} d,$$

womit die Behauptung in diesem Fall bewiesen ist.

Induktionsschritt ($n > 0$): Das Polynom

$$h := f - a_n b_m^{-1} X^{n-m} d$$

besitzt einen Grad kleiner als n. Daher gibt es $q, r \in K[X]$ mit

$$h = qd + r, \ r = 0 \text{ oder } \deg(r) < \deg(d).$$

Einsetzen liefert

$$f = (q + a_n b_m^{-1} X^{n-m}) d + r$$

und damit die Behauptung. □

3 Primfaktorisierung

In diesem Abschnitt wird gezeigt, dass euklidische Ringe aus der Sicht der Faktorisierung von Elementen wirklich eine interessante Klasse von Ringen darstellen. Zunächst beweist man, dass sich irreduzible Elemente und Primelemente in euklidischen Ringen genauso verhalten wie in $\mathbb{Z}$.

SATZ 48: *Es sei (R, δ) ein euklidischer Ring.*

1. *Jedes $s \in R \setminus R^\times$ besitzt einen irreduziblen Teiler.*

2. *Irreduzible Elemente in R sind Primelemente.*

BEWEIS: 1. Sei $s \in R \setminus R^\times$. Beginnend mit $d_1 := s$ definiert man eine Folge $d_1, d_2, \ldots$ von Ringelementen wie folgt: Besitzt d_k einen echten Teiler, so wählt man für d_{k+1} einen echten Teiler von d_k. Kann man beweisen, dass dieses Verfahren nach endlichen vielen Schritten endet, so ist das letzte Folgenglied d_ℓ ein irreduzibler Teiler von s.

Man beweist die Endlichkeit des Verfahrens durch Widerspruch: Man nimmt also an es gibt in R eine unendlich Folge $d_1, d_2, \ldots$ von Elementen mit der Eigenschaft d_{k+1} ist echter Teiler von d_k.

Man betrachtet die Mengen $Rd_k := \{rd_k : r \in R\}$ aller Vielfachen von d_k. Nach Voraussetzung gilt $d_k = q_k d_{k+1}$ und damit $Rd_k \subseteq Rd_{k+1}$. Wäre $Rd_k = Rd_{k+1}$, so hätte man auch $d_{k+1} = s_k d_k$ und damit $d_k \sim d_{k+1}$, ein Widerspruch. Also gilt tatsächlich $Rd_k \subset Rd_{k+1}$.

Man bildet nun die Teilmenge

$$I := \bigcup_{k \in \mathbb{N}} Rd_k \subseteq R.$$

Die Menge $\delta(I \setminus 0) = \{\delta(a) : a \in I \setminus 0\} \subseteq \mathbb{N}_0$ besitzt ein Minimum $\delta(d)$, $d \in I \setminus 0$. Nach Konstruktion von I gibt es ein $\ell \in \mathbb{N}$ mit $d \in Rd_\ell$.

Sei nun $a \in I$ beliebig. Dann gilt $a = qd + r$ mit $r = 0$ oder $\delta(r) < \delta(d)$. Nach Konstruktion von I gibt es ein $k \geq \ell$ mit der Eigenschaft $a \in Rd_k$. Wegen $Rd_\ell \subset Rd_k$ ist dann auch $d \in Rd_k$. Wäre nun $r \neq 0$, so wäre $r = a - qd \in Rd_k \subseteq I$, also $r \in I$, ein Widerspruch zur Minimalität von $\delta(d)$. Folglich gilt stets $r = 0$ und damit $I \subseteq Rd_\ell$, also $I = Rd_\ell$.

Für jedes $k > \ell$ folgt hieraus $Rd_k \subseteq Rd_\ell$ und daher $Rd_k = Rd_\ell$ im Widerspruch zur früher gezeigten Ungleichheit dieser Mengen.

2. Es sei $p \in R$ irreduzibel und es gelte $p|(ab)$. Man nimmt weiter an, dass p kein Teiler von a ist. Man betrachtet die Teilmenge

$$J := \{ra + sp : r, s \in R\};$$

die Menge $\delta(J \setminus 0)$ besitzt ein minimales Element $\delta(t)$. Man kann p mit Rest durch t dividieren und erhält $p = qt + r$ mit $r = 0$ oder $\delta(r) < \delta(t)$. Ist $r \neq 0$, so gilt $r = p - qt \in J \setminus 0$ und es ergibt sich ein Widerspruch zur Minimalität von $\delta(t)$. Also ist $r = 0$ und damit $p = qt$.

Dasselbe Argument kann man mit a anstelle von p durchführen und erhält $a = q't$.

Da p keine echten Teiler besitzt und p kein Teiler von a ist, muss $t \in R^\times$ gelten. Man erhält also

$$1 = t^{-1}(r_1 a + s_1 p)$$

mit gewissen $r_1, s_1 \in R$. Multiplikation dieser Gleichung mit b liefert

$$b = t^{-1}(r_1 ab + s_1 bp);$$

da nach Voraussetzung $p|(ab)$ gilt, folgt $p|b$ und man hat gezeigt, dass p tatsächlich ein Primelement ist. □

Der zuletzt bewiesene Satz enthält alle Zutaten für das Hauptergebnis dieses Abschnitts. Um dieses analog zum Fall der ganzen Zahlen formulieren zu können, wählt man eine bestimmte Menge von Primelementen aus:

Definition 49: *Sei R ein euklidischer Ring. Eine Teilmenge $P \subset R$ von Primelementen heißt repräsentativ, falls sie die folgenden beiden Eigenschaften besitzt:*

- *Zu jedem Primelement $q \in R$ gibt es ein Primelement $p \in P$ mit $p \sim q$.*
- *Für je zwei verschiedene $p_1, p_2 \in P$ gilt $p_1 \not\sim p_2$.*

Die Menge aller positiven Primzahlen $\{2, 3, 5, 7, \ldots\}$, aber auch die Menge aller negativen Primzahlen $\{-2, -3, -5, -7, \ldots\}$ sind eine repräsentative Menge von Primelementen von $\mathbb{Z}$.

Satz 50: *Es sei (R, δ) ein euklidischer Ring und $P \subset R$ eine repräsentative Menge von Primelementen. Dann kann man jedes $r \in R \setminus 0$ in der Form*

$$r = u \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

schreiben, wobei $u \in R^\times$, $p_1, \ldots p_r \in P$ und $e_1, \ldots, e_r \in \mathbb{N}$ gilt. Alle diese Elemente sind durch r eindeutig bestimmt.

BEWEIS: Nach Satz 48 Punkt 1 kann man jedes $r \in R \setminus 0$ in der Form

$$r = q_1 \cdot \ldots \cdot q_m$$

schreiben, wobei die q_k sämtlich irreduzibel sind. Denn r ist entweder selbst irreduzibel oder besitzt einen irreduziblen Teiler q_1, das heißt es gilt $r = q_1 r_1$. Nun ist r_1 irreduzibel oder besitzt einen irreduziblen Teiler. Im zweiten Fall folgt $r = q_1 q_2 r_2$ und man argumentiert mit r_2 weiter. Das Verfahren endet, weil r_1 Teiler von r, r_2 Teiler von r_1 und so weiter ist. Im Beweis von Satz 48 wurde gezeigt, dass eine solche Folge von echten Teilern endlich ist.

Nach Satz 48 Punkt 2 ist jedes q_k ein Primelement. Da die Menge P repräsentativ ist, gibt es also jeweils ein $u_k \in R^\times$ mit $q_k = u_k p_k$ mit einem $p_k \in P$. Fasst man alle Einheiten in einem Produkt zusammen, so ergibt sich die behauptete Darstellung von r.

Es seien nun $u \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ und $v \cdot q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}$ zwei Darstellungen des gleichen Elements $r \in R$. Dann gilt

$$p_1 | (q_1^{f_1} \cdot \ldots \cdot q_s^{f_s})$$

und folglich, da p_1 ein Primelement ist, $p_1 | q_j$ für ein $j \in \{1, \ldots, s\}$. Da q_j als Primelement irreduzibel ist, folgt $p_1 \sim q_j$. Da P repräsentativ ist, ist dies nur für $p_1 = q_j$ möglich.

Kürzen liefert dann

$$u \cdot p_1^{e_1 - 1} \cdot \ldots \cdot p_r^{e_r} = v \cdot q_1^{f_1} \cdot \ldots \cdot q_j^{f_j - 1} \cdot \ldots \cdot q_s^{f_s}.$$

Die Wiederholung dieses Verfahrens liefert schließlich zwei Faktorisierungen des gleichen Elements, wobei in der einen das Primelement p_1 nicht mehr vorkommt. Da man annehmen kann, dass sowohl die Primelemente p_i als auch die Primelemente q_i paarweise verschieden sind, und da die Menge P repräsentativ ist, kann dann p_1 auch in der zweiten Faktorisierung nicht mehr vorkommen. Man hat also auch $e_1 = f_j$ gezeigt.

Nun wiederholt man das Verfahren mit dem Primelement p_2, dann mit p_3 und so weiter. Schließlich erhält man $u = v$ und die Eindeutigkeit ist bewiesen. □

Die Bedeutung der Sätze 48 und 50 soll nun am Beispiel des Polynomrings $K[X]$ mit Koeffizienten in einem Körper K erläutert werden.

Zunächst führt man dazu den Begriff des *normierten Polynoms* ein: Ein Polynom $f \in K[X]$ heißt normiert, wenn es die Form

$$f = X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

besitzt. Wegen $K[X]^\times = K \setminus 0$ gilt:

- Jedes Polynom ist zu einem normierten Polynom assoziiert und zwei verschiedene normierte Polynome sind nicht assoziiert.

Nach Satz 47 ist $K[X]$ zusammen mit der Gradfunktion ein euklidischer Ring. Irreduzible Polynome sind nach Satz 48 also Primelemente. Man erhält:

- Die Menge P der normierten irreduziblen Polynome ist eine repräsentative Menge von Primelementen von $K[X]$.

Die Anwendung von Satz 50 liefert nun direkt:

SATZ 51: *Im Polynomring $K[X]$ kann jedes Polynom $f \neq 0$ in der Form*

$$f = c \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

geschrieben werden, wobei $c \in K \setminus 0$, $p_1, \ldots, p_r$ normierte irreduzible Polynome und $e_1, \ldots, e_r \in \mathbb{N}$ sind. Die Darstellung ist eindeutig.

Der Satz 51 nimmt für verschiedenen Körper verschiedene Formen an:

Komplexe Koeffizienten: Nach dem Fundamentalsatz der Algebra besitzt jedes Polynom $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, $n \geq 1$, mit komplexen Koeffizienten $a_k \in \mathbb{C}$ eine Nullstelle in $\mathbb{C}$. Folglich kann man es in der Form $f = (X-a)g$, $a \in \mathbb{C}$, schreiben. Hieraus ergeben sich unmittelbar die folgenden beiden Fakten:

- Die Menge der linearen Polynome $\{X - a : a \in \mathbb{C}\}$ bildet eine repräsentative Menge von Primelementen von $\mathbb{C}[X]$.
- Jedes $f \in \mathbb{C}[X] \setminus 0$ kann eindeutig in der Form

  $$f = c \cdot (X - a_1)^{e_1} \cdot \ldots \cdot (X - a_r)^{e_r}$$

  geschrieben werden.

Reelle Koeffizienten: Ist $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, $n \geq 1$, ein Polynom ungeraden Grades mit reellen Koeffizienten $a_k \in \mathbb{R}$, so besitzt es nach dem Zwischenwertsatz der Analysis eine Nullstelle in $\mathbb{R}$.

Ist $z = a + bi \in \mathbb{C}$ eine Nullstelle von f, so auch die komplex-konjugierte Zahl $a - bi$ und es gilt

$$(X - (a + bi))(X - (a - bi)) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$$

ist ein irreduzibles Polynom, sofern $b \neq 0$ gilt. Hieraus ergeben sich unmittelbar die folgenden beiden Fakten:

- Die Menge $L \cup Q$ der Polynome

$$L := \{X - a : a \in \mathbb{R}\}, \;\; Q := \{X^2 + aX + b : \frac{a^2}{4} - b < 0\}$$

  bildet eine repräsentative Menge von Primelementen von $\mathbb{R}[X]$.

- Jedes $f \in \mathbb{R}[X] \setminus 0$ kann eindeutig in der Form

$$f = c \cdot (X - a_1)^{e_1} \cdot \ldots \cdot (X - a_r)^{e_r} \cdot q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}, \; q_k \in Q,$$

  geschrieben werden.

Rationale Koeffizienten: Es existieren irreduzible Polynome $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ mit rationalen Koeffizienten $a_k \in \mathbb{Q}$ von beliebig großem Grad n. Es ist hier nicht möglich eine repräsentative Menge von Primelementen in einfacher Form anzugeben.

Koeffizienten in $\mathbb{Z}/p$: Es existieren auch in diesem Fall irreduzible Polynome $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ von beliebig großem Grad n. Allerdings gibt es genau p^{n+1} Polynome vom Grad n. Daher kann man alle (normierten) irreduziblen Polynome $f \in \mathbb{Z}/p[X]$ vpm Grad n mit endlich vielen Rechenoperationen bestimmen, und damit auch die Primfaktorisierung jedes Polynoms.