Kapitel 5

Irreduzibilität

Bereits im vorigen Kapitel hatten wir gesehen, dass Faktorringe, die durch Kongruenz bzgl. eines maximalen Ideals entstehen, Körper sind. Im Ring $\mathbb{Z}$ war es einfach maximale Ideal zu erkennen: sie werden von Primzahlen erzeugt und Primzahlen fühlen sich zumindest sehr vertraut an. Im Polynomring über einem Körper allerdings haben wir noch keine einfache Möglichkeit kennengelernt, wie wir maximale Ideale bzw. irreduzible Elemente erkennen können. Bilden wir einen Polynomring in einer Veränderlichen über einem Integritätsring, der kein Körper ist, so haben wir nicht einmal mehr einen euklidischen Ring vor uns und die Situation erscheint nochmals unübersichtlicher. Es ist also höchste Zeit, sich über Irreduzibilität Gedanken zu machen.

5.1 Nullstellen und Linearfaktoren

Tragen wir zuerst ein paar Aussagen zusammen, die wir bereits früher betrachtet hatten und die für den Umgang mit Irreduzibilität von Polynomen hilfreich sein können. Vergessen wir dabei nicht, dass wir schon einige Kenntnisse über Nullstellen und Linearfaktoren besitzen.

Erinnerung 5.1.1 *Seien R, S Integritätsringe mit $R \leq S$. Dann sind $R[t]$ und $S[t]$ Integritätsringe und es gilt $R[t]^* = R^*$ sowie $S[t]^* = S^*$.*
Ein Polynom $f \in R[t]$ kann stets auch als Polynom in $S[t]$ betrachtet werden. Es kann irreduzibel in $R[t]$, aber reduzibel in $S[t]$ sein, wie etwa $t^2 + 1 \in \mathbb{R}[t]$, das in $\mathbb{C}[t]$ in die Faktoren $t - i$ und $t + i$ zerfällt.

Beobachtung 5.1.2 *Ist $R = K$ ein Körper, so ist $f \in K[t] \setminus \{0\}$ genau dann reduzibel, wenn es eine Zerlegung $f = gh$ gibt mit $g, h \in K[t]$ und $0 < \deg(g), \deg(h) < \deg(f)$. Insbesondere ist jedes $f \in K[t]$ mit $\deg(f) = 1$ irreduzibel.*
Ist andererseits R kein Körper, so kann auch ein Polynom vom Grad 1 reduzibel sein (z.B. ist $4t + 6 \in \mathbb{Z}[t]$ reduzibel mit den nicht-trivialen Faktoren 2 und $2t+3$). Ist allerdings $f = at+b \in R[t]$ mit $a \in R^*$, so ist f irreduzibel, da wegen des Grades von f höchstens ein nicht-trivialer Faktor vom Grad 1 sein kann und der andere nicht-triviale Faktor dann ein Teiler jedes Koeffizienten ist. Einheiten haben jedoch keine nicht-trivialen Teiler.

Erinnerung 5.1.3 *Seien $R \leq S$ Ringe, wobei R kommutativ ist. Dann heißt $\alpha \in S$ eine* **Nullstelle** *von $f \in R[t]$, falls α einsetzbar in Polynome über R ist und $f(\alpha) = E_\alpha(f) = 0$.*

Hier wird uns hauptsächlich die Situation eines kommutativen S interessieren, so daß jedes Element von S einsetzbar ist in Polynome über R.

Erinnerung 5.1.4 *Seien $R \leq S$ kommutative Ringe, $f \in R[t]$ und $\alpha \in S$. Dann gilt:*

$$\alpha \text{ ist Nullstelle von } f \iff (t - \alpha) \mid f.$$

Satz 5.1.5 *Seien $R \leq S$ kommutative Ringe, $f \in R[t]$ ein Polynom vom Grad $\deg(f) = n$. Dann hat f höchstens n verschiedene Nullstellen in S.*

Beweis: Seien $\alpha_1, \ldots, \alpha_s \in S$ verschiedene Nullstellen von f. Dann gilt

$$\prod_{i=1}^{s} (t - \alpha_i) \mid f,$$

weswegen der Grad des Produktes höchstens n sein kann.

□

Beobachtung 5.1.6 *Ist $R = K$ ein Körper und ist $f \in K[t]$ ein Polynom vom Grad 2 oder 3, so ist f reduzibel über K genau dann, wenn f eine Nullstelle in K besitzt. Für Grad 4 gilt das nicht mehr. Überlegen Sie warum und finden Sie ein Beispiel!*
Ist andererseits R nullteilerfreier Ring, aber kein Körper, so gilt die obige Aussage noch immer für normierte Polynome bzw. deutlich allgemeiner für Polynome mit Leitkoeffizient in R^* bzw. für Polynome, von denen sich kein nicht-trivialer konstanter Faktor abspalten läßt.

5.2 Rationale Nullstellen

Betrachten wir nun die Situation, dass R ein faktorieller Ring ist und $S = Quot(R)$, etwas genauer.

Erinnerung 5.2.1 *Die folgenden Tatsachen wurden in früheren Kapiteln implizit oder explizit bereits gezeigt:*

- *In einem faktoriellen Ring R gibt es größte gemeinsame Teiler und kleinste gemeinsame Vielfache von je zwei Ringelementen.*
- *Sind $a, b \in R$ teilerfremd und gilt $a \mid b \cdot c$ für ein $c \in R$, so gilt $a \mid c$.*
- *Seien $a, b \in R$ und $d \in R$ ein größter gemeinsamer Teiler von a und b. Dann sind $A, B \in R$ mit $a = Ad$ und $b = Bd$ teilerfremd in R.*
- *Ist $\alpha \in Quot(R)$, so existieren teilerfremde $A, B \in R$ mit $\alpha = \frac{A}{B}$.*

Satz 5.2.2 *Sei R ein faktorieller Ring mit Quotientenkörper $K = Quot(R)$. Sei ferner $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein Polynom vom Grad $n \geq 1$, d.h. insbesondere $a_n \neq 0$. Ist nun $\alpha = \frac{A}{B} \in K$ eine Nullstelle von f mit teilerfremden $A, B \in R$, $B \neq 0$, dann gilt:*

$$B \mid a_n \text{ und } A \mid a_0.$$

Beweis: Betrachte

$$0 = f(\alpha) = \sum_{i=0}^{n} a_i \left(\frac{A}{B}\right)^i.$$

Nach Multiplikation mit B^n (unschädlich, da R nullteilerfrei und $B \neq 0$) liefert das

$$0 = \sum_{i=0}^{n} a_i A^i B^{n-i} = \underbrace{a_n A^n}_{\text{Vielfaches von } A} + \underbrace{\sum_{i=1}^{n-1} a_i A^i B^{n-i}}_{\text{Vielfaches von } AB} + \underbrace{a_0 B^n}_{\text{Vielfaches von } B}.$$

Da jedes Element von R die Null teilt und damit A und B jeweils alle bis auf einen Summanden oben teilen, müssen sie jeweils auch den verbliebenen teilen. Da sie andererseits teilerfremd sind, müssen sie den jeweils verbleibenden Faktor teilen, was genau die Behauptung liefert.

□

Beispiel 5.2.3 *Ein Spezialfall des vorigen Satzes ist die bereits aus der Schule (ohne Beweis) bekannte Aussage, dass jede ganzzahlige Nullstelle eines normierten Polynoms über $\mathbb{Z}$ den konstanten Term des Polynoms teilt.*

5.3 Satz von Gauß

Seien $R \leq S$ Integritätsringe. Die Frage nach Irreduzibilität von Polynomen über R bzw. über S ist recht subtil, wie wir zu Beginn des Kapitels bereits gesehen haben: Weder impliziert Irreduzibilität über R Irreduzibilität über S, noch umgekehrt. Unser Ziel in diesem Abschnitt wird sein, die Situation für den wichtigen Spezialfall $S = Quot(R)$ konkret zu beschreiben. Im Laufe des Kapitels werden wir auch die Aussage, dass ein Polynomring über einem faktoriellen Ring wieder faktoriell ist, endlich beweisen können.

Proposition 5.3.1 *Sei $\varphi : R \longrightarrow S$ ein Homomorphismus kommutativer Ringe. Dann ist auch*

$$\begin{array}{rcl} \Phi : R[t] & \longrightarrow & S[t] \\ \sum_{i=0}^{n} a_i t^i & \longmapsto & \sum_{i=0}^{n} \varphi(a_i) t^i \end{array}$$

ein Ringhomomorphismus.

Beweis: Offensichtlich handelt es sich um eine wohldefinierte Abbildung von Ringen, für die wegen $\varphi(1_R) = 1_S$ auch gilt

$$\Phi(1_{R[t]}) = \Phi(1_R t^0) = \varphi(1_R) t^0 = 1_S t^0 = 1_{S[t]}.$$

Für die Verträglichkeit mit Addition und Multiplikation betrachen wir zwei

Polynome $f = \sum_{i=0}^{n} a_i t^i, g = \sum_{i=0}^{m} b_i t^i \in R[t]$ und rechnen:

$$\begin{aligned}
\Phi(f+g) &= \Phi\left(\sum_{i=0}^{\max\{m,n\}} (a_i + b_i)t^i\right) \\
&= \sum_{i=0}^{\max\{m,n\}} \varphi(a_i + b_i)t^i \\
&= \sum_{i=0}^{\max\{m,n\}} (\varphi(a_i) + \varphi(b_i))t^i \\
&= \left(\sum_{i=0}^{n} \varphi(a_i)t^i\right) + \left(\sum_{i=0}^{m} \varphi(b_i)t^i\right) \\
&= \Phi(f) + \Phi(g) \\
\Phi(f \cdot g) &= \Phi\left(\sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j t^k\right) \\
&= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} \varphi(a_i b_j)\right) t^k \\
&= \sum_{k=0}^{n+m} \sum_{i+j=k} \varphi(a_i)\varphi(b_j)t^k \\
&= \left(\sum_{i=0}^{n} \varphi(a_i)t^i\right) \cdot \left(\sum_{i=0}^{m} \varphi(b_i)t^i\right) \\
&= \Phi(f) \cdot \Phi(g)
\end{aligned}$$

Damit sind die Bedingungen an einen Ringhomomorphismus explizit nachgerechnet und die Behauptung damit bewiesen.

□

Satz 5.3.2 *Sei R ein kommutativer Ring, $I \trianglelefteq R$ ein Ideal und $J \trianglelefteq R[t]$, das von I in $R[t]$ erzeugte Ideal. Dann gilt*

a) $J \cap R = I$

b) Es gibt einen Isomorphismus

$$R[t]/J \cong (R/I)[t].$$

c) J ist genau dann Primideal, wenn I Primideal ist.

Beweis: Nach der Definition des von einer Menge erzeugten Ideals gilt

$$\begin{aligned} J &= \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, a_1, \ldots, a_n \in I, r_1, \ldots, r_n \in R[t]\} \\ &= \{\sum_{j=0}^{m} b_j t^j \mid m \in \mathbb{N}_0, b_1, \ldots, b_m \in I\} \end{aligned}$$

Damit besteht J gerade aus den Polynomen, deren Koeffizienten in I liegen und von diesen sind genau die konstanten Polynome Elemente von R, was die Aussage a) liefert.
Für die Aussage b) betrachten wir die Restklassenabbildung $\varphi : R \longrightarrow R/I$ und die davon induzierte Abbildung $\Phi : R[t] \longrightarrow (R/I)[t]$ nach Proposition 5.3.1. Offensichtlich ist Φ surjektiv und ein Polynom liegt genau dann im Kern, wenn alle Koeffizienten auf Null abgebildet werden, d.h. wenn es in J liegt. Nach dem Homomorphiesatz erhalten wir damit den gewünschten Isomorphismus.
Mittels dieses Isomorphismus ist ausserdem klar, dass $R[t]/J$ genau dann Integritätsring ist, wenn $(R/I)[t]$ Integritätsring ist, was wiederum genau dann der Fall ist, wenn R/I selbst ein Integritätsring ist. Damit ist auch Aussage c) beweisen.

□

Korollar 5.3.3 *Sei R Integritätsring und $p \in R \setminus \{0\}$. p ist Primelement in R, genau dann wenn das konstante Polynom p Primelement in $R[t]$ ist.*

Beweis: Die Aussage ist äquivalent dazu, dass $\langle p \rangle \trianglelefteq R$ genau dann Primideal ist, wenn $\langle p \rangle \trianglelefteq R[t]$ Primideal ist. Das ist aber gerade Satz 5.3.2, c).

□

Proposition 5.3.4 *Sei R Integritätsring und sei $a \in R$ mit einer Zerlegung als Produkt $a = \prod_{i=1}^{n} f_i$, wobei $f_1, \ldots, f_n \in R[t]$. Diese ist genau dann eine Primfaktorzerlegung von a in $R[t]$, wenn sie eine Primfaktorzerlegung von a in R ist.*

Beweis: Wegen $a \in R$ und damit $\deg(a) = 0$ gilt auch $\deg(f_i) = 0$ für jeden einzelnen der Faktoren. Damit sind alle f_i bereits Elemente von R.
Nach dem vorigen Korollar ist somit jedes f_i genau dann prim in R, wenn es prim in $R[t]$ ist, was die gewünschte Aussage liefert.

□

Korollar 5.3.5 *Sei R Integritätsring. Ist $R[t]$ faktoriell, so auch R.*

Dies ist eine unmittelbare Folge der vorstehenden Proposition. Wir werden nach ein paar Vorarbeiten sehen, dass auch die umgekehrte Implikation gilt. Dafür müssen wir aber noch ein bisschen arbeiten.

Definition 5.3.6 *Sei R ein faktorieller Ring. Ein Polynom $f \in R[t] \setminus \{0\}$ heißt* **primitiv**, *falls die Koeffizienten von f teilerfremd sind.*

Bemerkung 5.3.7 *Ganz konkret formuliert, ist $f = \sum_{i=0}^{n} a_i t^i \in R[t] \setminus \{0\}$ primitiv, falls 1 ein größter gemeinsamer Teiler von $a_0, \ldots, a_n$ ist.*

Satz 5.3.8 *Sei R faktorieller Ring und seien $f, g \in R[t] \setminus \{0\}$ primitiv. Dann ist auch $f \cdot g$ primitiv.*

Beweis: Seien $f = \sum_{i=0}^{n} a_i t^i, g = \sum_{j=0}^{m} b_j t^j \in R[t]$ zwei primitive Polynome. Dann ist 1 ein größter gemeinsamer Teiler von $a_0, \ldots, a_n$ sowie ein gemeinsamer Teiler von $b_0, \ldots, b_m$.
Zum Nachweis der Primitivität von

$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) t^k$$

nehmen wir das Gegenteil an. Sei also $p \in R \setminus R^*$ ein Primelement, das ein gemeinsamer Teiler aller Koeffizienten

$$c_k = \sum_{i+j=k} a_i b_j, \quad 0 \leq k \leq n+m$$

des Produkts ist. Wegen der Primitivität von f und g teilt p mindestens ein a_i und mindestens ein b_j nicht. Bezeichne mit i_0 den kleinsten Index mit $p \nmid a_{i_0}$ und mit j_0 den kleinsten Index mit $p \nmid b_{j_0}$ und betrachte

$$\underbrace{c_{i_0+j_0}}_{\text{teilbar durch } p} = \underbrace{\sum_{\substack{i+j=i_0+j_0 \\ i<i_0}} a_i b_j}_{\text{teilbar durch } p} + a_{i_0} b_{j_0} + \underbrace{\sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} a_i b_j}_{\text{teilbar durch } p}$$

Nach dieser Rechnung muss p auch Teiler des verbliebenen Summanden sein, was im Widerspruch steht dazu, dass p prim ist und weder Teiler von a_{i_0} noch von b_{j_0}. Damit ist $f \cdot g$ primitiv, was zu zeigen war.

□

Proposition 5.3.9 *Sei R faktorieller Ring und $K = Quot(R)$. Für jedes $f \in K[t]$ existieren $\alpha \in K$ und $g \in R[t]$ primitiv, so dass*

$$f = \alpha g.$$

Beweis: Sei $f = \sum_{i=0}^{n} \frac{a_i}{b_i} t^i \in K[t]$ mit $a_0, \ldots, a_n \in R, b_0, \ldots, b_n \in R \setminus \{0\}$. Dann gibt es ein kleinstes gemeinsames Vielfaches $k \in R$ der Nenner $b_0, \ldots, b_n \in R$,also einen Hauptnenner der Koeffizienten von f, und es ist $k \cdot f \in R[t]$. Schreiben wir

$$k \cdot f = \sum_{i=0}^{n} c_i t^i,$$

so existiert ein größter gemeinsamer Teiler $d \in R$ der Koeffizienten $c_0, \ldots, c_n \in R$ und es gilt

$$\frac{k}{d} \cdot f = \sum_{i=0}^{n} \frac{c_i}{d} t^i,$$

wobei 1 größter gemeinsamer Teiler der $\frac{c_0}{d}, \ldots, \frac{c_n}{d} \in R$ ist. Das Polynom $g := \frac{k}{d} \cdot f \in R[t]$ ist daher primitiv und es gilt mit $\alpha := \frac{d}{k}$:

$$f = \frac{d}{k} \cdot (\frac{k}{d} f) = \alpha \cdot g.$$

□

Bemerkung 5.3.10 *Ist f in der obigen Proposition bereits aus $R[t]$, so kann der erste Schritt des Beweises entfallen, da der Hauptnenner dann 1 ist und man erhält $\alpha = d$ und $f = \alpha \cdot (\frac{1}{d} f)$. In diesem Fall nennt man α (vor allem in der Computeralgebra) auch den* **Content** *von f.*

Lemma 5.3.11 *Sei R ein faktorieller Ring, $K = Quot(R)$, seien $f, g \in R[t] \setminus \{0\}$ primitiv, so dass $f = \alpha g$ für ein $\alpha \in K$, so ist $\alpha \in R^*$.*

Beweis: f und g sind primitive Polynome mit Koeffizienten in R. Schreiben wir $\alpha = \frac{\beta}{\gamma}$, wobei $\beta, \gamma \in R$ teilerfremd gewählt sind, so gilt $\gamma f = \beta g$ und der gemeinsame Teiler γ aller Koeffizienten von γf muss jeden Koeffizienten von βg und damit wegen der Teilerfremdheit von β und γ jeden Koeffizienten von g teilen. Damit muss γ wegen der Primitivität von g eine Einheit sein. Mit der analogen Argumentation muss auch β eine Einheit sein. Damit ist $\alpha = \frac{\beta}{\gamma} \in R^*$.

□

Satz 5.3.12 *Sei R faktorieller Ring und $K = Quot(R)$. Dann gilt für jedes nicht-konstante primitive Polynom $f \in R[t] \subseteq K[t]$:*

$$f \text{ irreduzibel in } R[t] \iff f \text{ irreduzibel in } K[t]$$

Bevor wir mit dem Beweis beginnen, erinnern wir uns nochmals, dass in faktoriellen Ringen, wie z.B. $K[t]$, die Begriffe *irredzuibel* und *prim* zusammenfallen. In Integritätsringen gilt die Äquivalenz der Begriffe nicht mehr, aber *prim* impliziert noch immer *irreduzibel*, so dass diese Richtung auch in $R[t]$ nutzbar ist. Das erlaubt es uns, in einer Richtung mittels der Eigenschaft *prim* statt *irreduzibel* zu argumentieren.

Beweis: Machen Sie sich beim Nacharbeiten klar, dass/warum wir das Richtige zeigen.

"reduzibel in $K[t]$ $\implies$ reduzibel in $R[t]$"
Sei $f \in K[t]$ reduzibel mit einer (echten) Zerlegung $f = g \cdot h \in K[t]$, wobei $\deg(g) \geq 1$ und $\deg(h) \geq 1$. Dann existieren kleinste gemeinsame Vielfache $a, b \in R \setminus \{0\}$ der Nenner der Koeffizienten der Polynome g bzw. h, so dass $ag, bh \in R[t]$. Damit besitzt abf in $R[t]$ eine Zerlegung

$$(ab)f = (ag) \cdot (bh).$$

Ist $(ab) \in R^*$, so ist bereits eine Zerlegung von f in $R[t]$ gefunden. Im anderen Fall muss jeder Primfaktor von $ab \in R$ das Produkt $(ag) \cdot (bh)$ und damit einen der beiden Faktoren teilen. In diesem Fall können wir die Gleichung durch den Primfaktor teilen, ohne $R[t]$ zu verlassen. Iterieren wir dieses Argument, indem wir nacheinander alle (Assoziiertheitsklassen von) Primfaktoren

der (wegen Faktorialität von R eindeutigen) Primfaktorzerlegung von ab abarbeiten, so wurde die Gleichung am Ende durch alle Primfaktoren von ab geteilt und wir haben eine Zerlegung

$$f = g_{neu} h_{neu} \in R[t]$$

erhalten mit $\deg(g_{neu}) = \deg(g)$ und $\deg(h_{neu}) = \deg(h)$. Es handelt sich daher um eine nicht-triviale Zerlegung von f in $R[t]$ und somit ist f reduzibel in $R[t]$.

"prim in $K[t]$ $\implies$ prim in $R[t]$"
Sei $f \in R[t]$ derart, dass es aufgefaßt als Element von $K[t]$ prim ist. Seien $g, h \in R[t]$, so dass das Produkt $g \cdot h \in R[t]$ von f geteilt wird.
Dann ist f offensichtlich auch Teiler dieses Produktes, aufgefaßt in $K[t]$. Da f prim in $K[t]$ ist, teilt f einen der beiden Faktoren, sagen wir g, d.h. es existiert ein $f_1 \in K[t]$ mit $f \cdot f_1 = g$. Dann existieren gemäß Lemma 5.3.9 $c, k \in K$ und $f_2, g_1 \in R[t]$, so dass f_2 und g_1 primitiv sind und $f_1 = k \cdot f_2$ sowie $g = c \cdot g_1$ gilt. Dabei ist insbesondere $c \in R$ nach 5.3.10, da $g \in R[t]$. Dann gilt

$$f \cdot f_2 \cdot \frac{k}{c} = g_1,$$

wobei $f \cdot f_2$ als Produkt zweier primitiver Polynome nach 5.3.8 wieder primitiv ist und damit $\frac{k}{c}$ nach 5.3.11 ein Element von R^*, Daher ist f in $R[t]$ Teiler von g_1 und dann (wegen $c \in R$) auch von $g = c \cdot g_1$.

□

Bemerkung 5.3.13 *Im vorangehenden Beweis haben wir für die Richtung "$\Longrightarrow$" nur die Voraussetzung benutzt, dass f nicht konstant ist, nicht aber die Primitivität. Für die andere Richtung "$\Longleftarrow$" haben wir dann die Primitivität verwendet, aber nicht die Voraussetzung, dass das Polynom nicht konstant ist. Die einzelnen Richtungen gelten also auch unter jeweils passend abgeschwächten Bedingungen.*

Satz 5.3.14 *(Lemma von Gauß) Ist R faktorieller Ring, so ist auch $R[t]$ faktoriell.*

An dieser Stelle erinnern wir uns noch kurz, dass Polynomringe in einer Variable über Körpern stets euklidische Ringe sind und als solche auch faktorielle Ringe. Dies nutzen wir im Beweis aus.

Beweis: Sei $g \in R[t] \setminus (\{0\} \cup R^*)$ und bezeichne K den Quotientenkörper $Quot(R)$. Zerlege nun mittels Bemerkung 5.3.10 g in ein Produkt

$$g = \alpha \cdot f$$

mit $\alpha \in R$ und $f \in R[t]$ primitiv. Dann besitzt f als Element des faktoriellen Ringes $K[t]$ eine Zerlegung in Primelemente

$$f = \prod_{i=1}^{s} q_i,$$

wobei $s \in \mathbb{N}$ und $q_1, \ldots, q_s \in K[t]$ prim. Für jeden Index i, $1 \leq i \leq s$, können wir nun nach Lemma 5.3.9 ein $c_i \in K$ und ein primitives Polynom $p_i \in R[t]$ mit $q_i = c_i \cdot p_i$ finden. Dabei sind q_i und p_i in $K[t]$ assoziiert, so dass auch p_i ein Primelement in $K[t]$ ist. Nach Satz 5.3.12 sind die p_i damit auch Primelemente in $R[t]$. Da die einzelnen p_i primitiv sind, ist es nach Lemma 5.3.8 auch ihr Produkt. In der Gleichung

$$f = \left(\prod_{i=1}^{s} c_i \right) \cdot \left(\prod_{i=1}^{s} p_i \right)$$

sind somit beiden Polynome primitiv, weswegen der Faktor $c := \prod_{i=1}^{s} c_i \in K$ nach Lemma 5.3.11 bereits in $R^* \subseteq R$ liegen muss. Damit besitzt c und dann auch $c \cdot \alpha$ ein Zerlegung als Produkt von Primfaktoren nach der Faktorialität von R, wobei jeder dieser Faktoren nach Korollar 5.3.3 auch prim als Element von $R[t]$ ist. Somit haben wir durch die beiden Primfaktorzerlegungen bereits eine Zerlegung von $g = \alpha \cdot f$ in Primfaktoren erhalten. $R[t]$ ist folglich ein faktorieller Ring.

□

Mit dieser Aussage ist die Bringschuld aus Bemerkung 3.2.12 nun abgetragen und wir haben endlich beweisen, dass z.B. $\mathbb{Z}[t]$ und $\mathbb{Q}[x_1, \ldots, x_n]$ faktorielle Ringe sind.

5.4 Irreduzibilitätskriterien

Auch wenn wir bereits wichtige Aussagen über Irreduzibilität und über Faktorialität in diesem Kapitel beweisen konnten, haben wir immer noch keine praxistaugliche Möglichkeit, die Irreduzibilität eines Polynoms zu überprüfen. Natürlich kann man in kleinen Graden einfach einen Ansatz (bzw. mehrere je nach möglichen Ausspaltungen des Grades des Polynoms) machen und dann durch Koeffizientenvergleich versuchen zu Ergebnissen zu kommen. Dieses Vorgehen 'mit der Brechstange' ist aber sehr umständlich und oft nicht zielführend. Daher betrachten wir nun Kriterien, die uns Irreduzibilität entscheiden lassen.

Sei in diesem Abschnitt stets R ein faktorieller Ring mit Quotientenkörper $K = Quot(R)$. Sei $p \in R$ ein Primelement und bezeichne $\pi_p : R \longrightarrow R/\langle p\rangle$ die kanonische Restklassenabbildung und 'by abuse of notation' auch die kanonische Restklassenabbildung $\pi_p : R[t] \longrightarrow (R/\langle p\rangle)[t]$. Beachten Sie dabei die Isomorphie aus 5.3.2,b). Vor diesem Hintergrund ist die doppelte Nutzung derselben Bezeichnung ungefährlich.

Satz 5.4.1 *(Reduktionskriterium) Seien R, K und p wie gerade beschrieben und sei $f \in R[t]$ ein primitives Polynom vom Grad $n \geq 1$ mit $p \nmid LC(f)$. Dann gilt:*

$$\pi_p(f) \text{ irreduzibel in } (R/\langle p\rangle)[t] \Longrightarrow f \text{ irreduzibel in } R[t].$$

Beweis: Ist $f \in R[t]$ reduzibel, so gibt es $g, h \in R[t]$ mit $f = g \cdot h$. Da f primitiv ist, kann weder g noch h vom Grad Null sein, so dass gilt $1 \leq \deg(g), \deg(h) < n$. Da p kein Teiler von $LC(f)$ ist und es sich bei π_p um einen Ringhomomorphismus handelt, gilt ausserdem

$$\deg(\pi_p(g)) + \deg(\pi_p(h)) = \deg(\pi_p(f)) = \deg(f) = \deg(g) + \deg(h),$$

so dass es sich bei $\pi_p(g)$ und $\pi_p(h)$ um echte Teiler von $\pi_p(f)$ vom gleichen Grad wie g bzw. h handeln muss. Daher ist auch $\pi_p(f)$ reduzibel, was die Behauptung beweist.

□

Satz 5.4.2 *(Transformationskriterium) Seien R und K wie zuvor, sei $f \in R[t]$ ein nicht-konstantes Polynom und sei $a \in R$. Dann gilt:*

$$f \text{ irreduzibel} \Longleftrightarrow f(t+a) \text{ irreduzibel}\,.$$

Beweis: Offensichtlich ist

$$\begin{array}{rcl} \Phi_a : R[t] & \longrightarrow & R[t] \\ f(t) & \longmapsto & f(t+a) \end{array}$$

ein Ringisomorphismus mit Inverser Φ_{-a}. Daher bleibt Irreduzibilität unter der Abbildung sowie ihrer Inversen erhalten.

□

Satz 5.4.3 *(Kriterium von Eisenstein) Seien R und K wie zuvor und sei $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ primitiv vom Grad $n \in \mathbb{N}$. Existiert ein Primelement $p \in R$ mit*

(i) $p \nmid a_n$

(ii) $p \mid a_i \ \ \forall 0 \leq i < n$

(iii) $p^2 \nmid a_0$,

dann ist f irreduzibel in $R[t]$.

Beweis: Beginnen wir den Beweis mit einer Erinnerung: In einem Produkt zweier Polynome in einem nullteilerfreien Ring ist der von Null verschiedene Term kleinsten Grades das Produkt der von Null verschiedenen Terme kleinsten Grades der Faktoren.
Nun beginnen wir mit dem Beweis: Angenommen ein primitives $f \in R[t]$ erfüllt die Bedingungen (i),(ii) und (iii), ist aber reduzibel mit der nichttrivialen Zerlegung $f = g \cdot h$, wobei wegen der Primitivität von f $1 \leq \deg(g), \deg(h) < n$.
Betrachten wir nun $[LC(f)]_p t^n \overset{(i),(ii)}{=} \pi_p(f) = \pi_p(g) \cdot \pi_p(h)$. Wegen der Nullteilerfreiheit von $R/\langle p \rangle$, wegen der Gestalt von $\pi_p(f)$ und wegen der Erinnerung zu Beginn des Beweises sind die Bilder von g und h unter der Restklassenabbildung von der Gestalt $\pi_p(g) = [LC(g)]_p t^m \neq [0]_p$ und $\pi_p(h) = [LC(h)]_p t^s \neq [0]_p$ für geeignete $m, s \in \{1, \ldots, n-1\}$ mit $n = m + s$. Insbesondere sind damit die konstanten Terme von g und h beide durch p teilbar, weswegen p^2 Teiler von a_0 ist im Widerspruch zu (iii). Die Annahme war also falsch und das Kriterium ist damit bewiesen.

□

Bemerkung 5.4.4 *Ist ein $f \in R[t]$ von positivem Grad irreduzibel, so ist es auch irreduzibel als Element in $K[t]$ nach Bemerkung 5.3.13. In diesem Sinne können die obigen Kriterien auch (durch einen Umweg über $R[t]$) als Kriterien für Irreduzibilität in $K[t]$ eingesetzt werden.*

Anwendung 5.4.5 *Für jede Primzahl $p \in \mathbb{N}$ ist das p-te* **zyklotomische Polynom** *(oder p-te* **Kreisteilungspolynom***)*

$$F_p = \frac{t^p - 1}{t - 1} = \sum_{i=0}^{p-1} t^i$$

in $\mathbb{Z}[t]$ irreduzibel und damit auch in $\mathbb{Q}[t]$.

Beweis: $R = \mathbb{Z}$ hat als Quotientenkörper $K = \mathbb{Q}$, so dass wir uns in der allgemeinen Situation dieses Abschnitts befinden.
Nun wissen wir nach dem Transformationskriterium, dass $F_p(t)$ genau dann irreduzibel in $\mathbb{Z}[t]$ ist, wenn auch $F_p(t+1)$ dies ist. Wir rechnen

$$F_p(t+1) = \frac{(t+1)^p - 1}{(t+1) - 1} = t^{p-1} + \sum_{i=1}^{p-2} a_i t^i + p,$$

wobei nach dem Binomischen Lehrsatz alle Koeffizienten außer $LC(F_p)$ durch p teilbar sind, aber der konstante Term nicht durch p^2 teilbar ist. Damit ist $F_p(t+1)$ irreduzibel in $\mathbb{Z}[t]$, was dann die Irreduzibilität von $F_p(t)$ in $\mathbb{Z}[t]$ und damit auch in $\mathbb{Q}[t]$ beweist.

□