19. Polynomringe

Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Wir wollen mit Polynomen

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

mit $a_0, a_1, \ldots, a_n \in R$ und einer Unbestimmten X rechnen wie gewohnt, d.h.

$$\begin{aligned}(a_n X^n + \cdots + a_1 X + a_0) + (b_n X^n + \cdots + b_1 X + b_0) \\ = (a_n + b_n) X^n + \cdots + (a_1 + b_1) X + (a_0 + b_0)\end{aligned}$$

und

$$\begin{aligned}(a_n X^n + \cdots + a_1 X + a_0) \cdot (b_m X^m + \cdots + b_1 X + b_0) \\ = c_{m+n} X^{m+n} + \cdots + c_1 X + c_0\end{aligned}$$

wobei

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{\substack{i,j \geq 0 \\ i+j=k}} a_i b_j$$

für $0 \leq k \leq m+n$. Weiters soll gelten, dass

$$a_n X^n + \cdots + a_1 X + a_0 = b_n X^n + \cdots + b_1 X + b_0 \quad \Leftrightarrow \quad a_i = b_i \text{ für } 0 \leq i \leq n.$$

Auch wenn damit im wesentlichen alles beschrieben ist, was man zum Rechnen mit Polynomen wissen muss, handelt es sich dabei nicht um eine brauchbare Definition. Hauptgrund ist, dass man sich die Unbestimmte X nicht als Variable und die Polynome nicht als Funktionen vorstellen sollte. Eine saubere Definition erhält man folgendermaßen: Es sei S die Menge aller unendlicher Folgen $(a_0, a_1, a_2, \ldots)$ mit $a_i \in R \; \forall i \geq 0$ mit der Eigenschaft, dass nur endlich viele der $a_i \neq 0$ sind (d.h. $\exists i_0 \geq 0 \; \forall i \geq i_0 : a_i = 0$). Darauf definiert man die Addition

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

und die Multiplikation

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) := (c_0, c_1, c_2, \ldots),$$

wobei c_k für alle $k \geq 0$ definiert sei als

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{\substack{i,j \geq 0 \\ i+j=k}} a_i b_j.$$

Satz 152: Mit den eben beschriebenen Definitionen ist $(S, +, \cdot)$ ein kommutativer Ring mit Eins.

Beweis: Sind $(a_i)_{i\geq 0}, (b_i)_{i\geq 0} \in S$, so gibt es nach der Definition von S Indizes $m, n \geq 0$, derart dass $a_i = 0$ für $i \geq m$ und $b_i = 0$ für $i \geq n$. Daher ist $a_i + b_i = 0$ für $i \geq \max\{m, n\}$ und $(a_i)_{i\geq 0} + (b_i)_{i\geq 0} = (a_i + b_i)_{i\geq 0} \in S$. Ist $k \geq m + n$ und $i + j = k$ (mit $i, j \geq 0$), so muss $i \geq m$ oder $j \geq n$ gelten, woraus folgt, dass entweder $a_i = 0$ oder $b_j = 0$ gelten muss. Daraus folgt, dass $c_k = 0$ für $k \geq m + n$ und $(a_i)_{i\geq 0} \cdot (b_j)_{j\geq 0} = (c_k)_{k\geq 0} \in S$. Wegen

$$\begin{aligned}\big((a_i)_{i\geq 0} + (b_i)_{i\geq 0}\big) + (c_i)_{i\geq 0} &= \big((a_i + b_i) + c_i\big)_{i\geq 0} \\ &= \big(a_i + (b_i + c_i)\big)_{i\geq 0} = (a_i)_{i\geq 0} + \big((b_i)_{i\geq 0} + (c_i)_{i\geq 0}\big)\end{aligned}$$

ist die Addition assoziativ und wegen

$$(a_i)_{i\geq 0} + (b_i)_{i\geq 0} = (a_i + b_i)_{i\geq 0} = (b_i + a_i)_{i\geq 0} = (b_i)_{i\geq 0} + (a_i)_{i\geq 0}$$

kommutativ. Das neutrale Element der Addition ist $(0, 0, 0, \dots)$ und additives Inverses zu $(a_i)_{i\geq 0}$ ist $(-a_i)_{i\geq 0}$. Um die Assoziativität der Multiplikation zu beweisen, betrachten wir $(a_i)_{i\geq 0}, (b_j)_{j\geq 0}, (c_k)_{k\geq 0} \in S$. Es ist dann

$$\big((a_i)_{i\geq 0} \cdot (b_j)_{j\geq 0}\big) \cdot (c_k)_{k\geq 0} = \left(\sum_{\ell+k=n} \left(\sum_{i+j=\ell} a_i b_j\right) c_k\right)_{n\geq 0}$$

und

$$(a_i)_{i\geq 0} \cdot \big((b_j)_{j\geq 0} \cdot (c_k)_{k\geq 0}\big) = \left(\sum_{i+m=n} a_i \left(\sum_{j+k=m} b_j c_k\right)\right)_{n\geq 0}$$

und die Assoziativität der Multiplikation folgt aus

$$\sum_{\ell+k=n} \left(\sum_{i+j=\ell} a_i b_j\right) c_k = \sum_{i+j+k=n} a_i b_j c_k = \sum_{i+m=n} a_i \left(\sum_{j+k=m} b_j c_k\right).$$

Einselement ist $(1, 0, 0, 0, \dots)$, die Multiplikation is kommutativ wegen

$$\sum_{i+j=k} a_i b_j = \sum_{j+i=k} b_j a_i$$

und distributiv wegen

$$\sum_{i+j=k} (a_i + b_i) c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j.$$

Lemma 153: Setzt man, mit den Bezeichnungen von Satz 152, $X := (0, 1, 0, 0, 0, \dots)$, so ist $X^n = (\delta_{in})_{i\geq 0}$ für $n \geq 0$, wobei

$$\delta_{in} = \begin{cases} 1 & \text{falls } i = n \\ 0 & \text{falls } i \neq n \end{cases}$$

d.h. $X^n = (0, \dots, 0, 1, 0, 0, 0, \dots)$, wobei 1 an der Stelle mit Index n steht.

Beweis: Wir verwenden Induktion nach n. Die Behauptung ist trivial für $n \in \{0,1\}$. Weiters ist

$$X^{n+1} = X^n \cdot X = (\delta_{in})_{i\geq 0} \cdot (\delta_{j1})_{j\geq 0} = (c_k)_{k\geq 0}$$

mit

$$c_k = \sum_{i+j=k} \delta_{in}\delta_{j1} = \delta_{k,n+1},$$

denn $\delta_{in}\delta_{j1} = 0$ außer für $i = n$ und $j = 1$ (und daher $k = i + j = n + 1$).

Lemma 154: Die Abbildung $\varphi : R \to S$, $\varphi(a) = (a, 0, 0, 0, \dots)$ (wieder mit den Bezeichnungen von Satz 152) ist ein Ringmonomorphismus, der $\varphi(1_R) = 1_S$ erfüllt.

Beweis: Für $a, b \in R$ gelten

$$\varphi(a + b) = (a + b, 0, 0, 0, \dots) = (a, 0, 0, 0, \dots) + (b, 0, 0, 0, \dots) = \varphi(a) + \varphi(b)$$

und

$$\varphi(ab) = (ab, 0, 0, 0, \dots) = (a, 0, 0, 0, \dots) \cdot (b, 0, 0, 0, \dots) = \varphi(a) \cdot \varphi(b).$$

Es ist offensichtlich, dass φ injektiv ist und $\varphi(1_R) = 1_S$ erfüllt.

Konvention: Man indentifiziert R mit seinem Bild $\varphi(R) \subseteq S$, d.h. man unterscheidet nicht zwischen $a \in R$ und $\varphi(a) = (a, 0, 0, 0, \dots)$.
Jedes $(a_0, a_1, a_2, \dots) \in S$ kann nun geschrieben werden als

$$\begin{aligned}(a_0, a_1, a_2, \dots) &= (a_0, 0, 0, 0, \dots) \cdot X^0 + (a_1, 0, 0, 0, \dots) \cdot X + (a_2, 0, 0, 0, \dots) \cdot X^2 + \cdots \\ &= a_0 + a_1X + a_2X^2 + \cdots = \sum_{i\geq 0} a_iX^i,\end{aligned}$$

womit man wieder bei der für Polynome üblichen Schreibweise angelangt wäre.

Definition: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Den in Satz 152 beschriebenen Ring S bezeichnet man mit $R[X]$ und nennt ihn den Ring der Polynome mit Koeffizienten aus R in der Unbestimmten X.

Definition: Ist $R(\neq \{0\})$ ein kommutativer Ring mit Eins und

$$p(X) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$$

mit $a_n \neq 0$ (für $n \geq 0$), so sagt man, der Grad von p sei n und schreibt dafür $\operatorname{grad} p = n$. Man bezeichnet a_n als Leitkoeffizienten von p. Ist $a_n = 1$, so sagt man, p sei normiert. Zusätzlich definiert man $\operatorname{grad}(0) = -\infty$ (d.h. das Nullpolynom soll Grad $-\infty$ haben). Beim Rechnen mit den Graden von Polynomen verwendet man die Konventionen $-\infty < n$ und $-\infty + n = n + (-\infty) = -\infty$ für alle $n \in \mathbb{N} \cup \{0\}$ sowie $(-\infty) + (-\infty) = -\infty$.

Satz 155: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und $p, q \in R[X]$. Dann gelten:

(i) $\operatorname{grad}(p+q) \leq \max\{\operatorname{grad} p, \operatorname{grad} q\}$,
(ii) $\operatorname{grad}(p \cdot q) \leq \operatorname{grad} p + \operatorname{grad} q$,
(iii) Ist der Leitkoeffizient von p kein Nullteiler in R oder der Leitkoeffizient von q kein Nullteiler in R, so ist $\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$,
(iv) Ist R ein Integritätsbereich, so ist $\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q$.

Beweis: (i) Die Behauptung ist klarerweise erfüllt, wenn $p = 0$ oder $q = 0$. Es sei darum ab jetzt $p \neq 0$ und $q \neq 0$. Ist

$$p(X) = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad q(X) = \sum_{i=0}^{m} b_i X^i$$

mit $a_n \neq 0$ und $b_m \neq 0$, so ist $a_i = 0$ für $i > n$ und $b_i = 0$ für $i > m$. Daher ist $a_i + b_i = 0$ für $i > \max\{n, m\}$ und somit $\operatorname{grad}(p+q) \leq \max\{m, n\} = \max\{\operatorname{grad} p, \operatorname{grad} q\}$.
(ii) Ist $p = 0$ oder $q = 0$, so ist $pq = 0$ und daher $\operatorname{grad}(pq) = -\infty = \operatorname{grad} p + \operatorname{grad} q$. Es sei darum ab jetzt $p \neq 0$ und $q \neq 0$. Ist wieder

$$p(X) = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad q(X) = \sum_{i=0}^{m} b_i X^i$$

mit $a_n \neq 0$ und $b_m \neq 0$, so ist

$$p(X)q(X) = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0$$

und daher $\operatorname{grad}(pq) \leq n + m = \operatorname{grad} p + \operatorname{grad} q$.
(iii) Verwendet man die Bezeichnungen des Beweises von (ii) weiter, so besagt die Voraussetzung gerade, dass a_n kein Nullteiler ist oder b_m kein Nullteiler ist. Daher ist $a_n b_m \neq 0$ und $\operatorname{grad}(pq) = n + m = \operatorname{grad} p + \operatorname{grad} q$.
(iv) Folgt sofort aus (ii) und (iii).

Korollar 156: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Dann gelten:

(i) $R[X]$ ist ein Integritätsbereich $\Leftrightarrow$ R ist ein Integritätsbereich,
(ii) $R^* \subseteq R[X]^*$,
(iii) Ist R ein Integritätsbereich, so ist $R[X]^* = R^*$.

Beweis: (i) ($\Rightarrow$) Folgt daraus, dass R ein Unterring von $R[X]$ ist.
($\Leftarrow$) Sind $p, q \in R[X] \setminus \{0\}$, so ist $\operatorname{grad} p \geq 0$ und $\operatorname{grad} q \geq 0$ und (wegen Satz 155 (iv)) $\operatorname{grad}(pq) = \operatorname{grad} p + \operatorname{grad} q \geq 0$. Also ist $pq \neq 0$.

(ii) Folgt daraus, dass R ein Unterring von $R[X]$ ist.
(iii) Es sei $p \in R[X]^*$. Dann gibt es ein $q \in R[X]$ mit der Eigenschaft $pq = 1$. Daraus folgt $0 = \operatorname{grad}(pq) = \operatorname{grad} p + \operatorname{grad} q$ wegen Satz 155 (iv). Das ist aber nur für $\operatorname{grad} p = \operatorname{grad} q = 0$ möglich. (Ist $\operatorname{grad} p = -\infty$ oder $\operatorname{grad} q = -\infty$, so ist $\operatorname{grad} p + \operatorname{grad} q = -\infty$. Also muss $\operatorname{grad} p \geq 0$ und $\operatorname{grad} q \geq 0$ gelten. Wäre nun $\operatorname{grad} p > 0$ oder $\operatorname{grad} q > 0$, so wäre $\operatorname{grad} p + \operatorname{grad} q > 0$.) Also ist $p(X) = a$ und $q(X) = b$ für gewisse $a, b \in R \setminus \{0\}$ mit der Eigenschaft $ab = 1$. Daher ist $p(X) = a \in R^*$ und $R[X]^* \subseteq R^*$.

Bemerkungen: 1) Ist R kein Integritätsbereich, kann $R^* \subsetneqq R[X]^*$ gelten. Z.B. ist $\overline{2}X + \overline{1} \in \mathbb{Z}_4[X]^* \setminus \mathbb{Z}_4^*$, da

$$\left(\overline{2}X + \overline{1}\right)^2 = \overline{2}^2 X^2 + \left(\overline{2} + \overline{2}\right)X + \overline{1}^2 = \overline{4}X^2 + \overline{4}X + \overline{1} = \overline{1}.$$

2) Ist R ein Integritätsbereich, so ist (nach Korollar 156 (i)) auch $R[X]$ ein Integritätsbereich und man kann wegen Satz 83 (ii) den Quotientenkörper $R(X) := Q(R[X])$ von $R[X]$ bilden.

Definition: Es sei R ein Integritätsbereich. Der Quotientenkörper

$$R(X) = \left\{ \frac{p(X)}{q(X)} \,\middle|\, p, q \in R[X], q \neq 0 \right\}$$

von $R[X]$ wird der Körper der rationalen Funktionen in X über R genannt.

Satz 157 (Division mit Rest): Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und $f, g \in R[X]$, wobei der Leitkoeffizient von g in R^* sein soll. Dann gibt es eindeutig bestimmte $q, r \in R[X]$ mit den Eigenschaften $f = qg + r$ und $\operatorname{grad} r < \operatorname{grad} g$.

Beweis: Existenz: Falls $\operatorname{grad} g > \operatorname{grad} f$, setze $q = 0$ und $r = f$, d.h. $f = 0 \cdot g + f$. Es sei darum nun $\operatorname{grad} g \leq \operatorname{grad} f$. Es sei

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad g(X) = \sum_{i=0}^{m} b_i X^i$$

mit $a_n \neq 0$, $b_m \neq 0$, $0 \leq m \leq n$ und $b_m \in R^*$. Wir verwenden Induktion nach n.
Falls $n = 0$ ist auch $m = 0$, d.h. $f(X) = a_0 \in R$ und $g(X) = b_0 \in R^*$. Setze $q(X) = a_0 b_0^{-1}$ und $r(X) = 0$, d.h. $a_0 = (a_0 b_0^{-1}) b_0 + 0$.
Angenommen, die Behauptung sei für $\operatorname{grad} f < n$ schon gezeigt. Dann ist

$$\operatorname{grad}\left(a_n b_m^{-1} X^{n-m} g(X)\right) = \operatorname{grad}\left(\sum_{i=0}^{m} a_n b_m^{-1} b_i X^{n-m+i}\right) = n = \operatorname{grad} f$$

und $a_n b_m^{-1} X^{n-m} g(X)$ hat Leitkoeffizienten a_n. Daher ist

$$\operatorname{grad}\big(f(X) - a_n b_m^{-1} X^{n-m} g(X)\big) < n.$$

Nach Induktionsvoraussetzung gibt es $\tilde{q}, r \in R[X]$ mit

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

und $\operatorname{grad} r < \operatorname{grad} g$. Daraus folgt

$$f(X) = \big(a_n b_m^{-1} X^{n-m} + \tilde{q}(X)\big)g(X) + r(X)$$

Setzt man nun

$$q(X) = a_n b_m^{-1} X^{n-m} + \tilde{q}(X),$$

so ist $f(X) = q(X)g(X) + r(X)$ und $\operatorname{grad} r < \operatorname{grad} g$.
Eindeutigkeit: Ist $f = q_1 g + r_1 = q_2 g + r_2$ mit $\operatorname{grad} r_1 < \operatorname{grad} g$ und $\operatorname{grad} r_2 < \operatorname{grad} g$, so gilt $(q_1 - q_2)g = r_2 - r_1$ und daher wegen Satz 155 (iii) und Satz 155 (i)

$$\operatorname{grad}(q_1 - q_2) + \operatorname{grad} g = \operatorname{grad}(r_2 - r_1) \leq \max\{\operatorname{grad} r_1, \operatorname{grad} r_2\} < \operatorname{grad} g.$$

Das ist nur möglich, wenn $\operatorname{grad}(q_1 - q_2) = -\infty$, d.h. $q_1 - q_2 = 0$, woraus $q_1 = q_2$ und auch $r_1 = r_2$ folgen.

Korollar 158: Es sei K ein Körper. Dann ist $K[X]$ ein euklidischer Ring (und daher ein Hauptidealbereich und ein faktorieller Ring).

Beweis: Da K ein Körper ist, ist $K[X]$ nach Korollar 156 (i) ein Integritätsbereich. Setzt man $\varphi : K[X] \setminus \{0\} \to \mathbb{N} \cup \{0\}$, $\varphi(p) = \operatorname{grad} p$, so wird $K[X]$ wegen Satz 157 dadurch zu einem euklidischen Ring. Aus Satz 138 folgt, dass $K[X]$ ein Hauptidealbereich ist und nach Satz 137 ist $K[X]$ ein faktorieller Ring.

Bemerkung: Wir werden später den folgenden Satz zeigen: Ist R ein faktorieller Ring, so ist $R[X]$ ein faktorieller Ring.

Lemma 159: Es sei K ein Körper. Dann gelten:

(i) $p \in K[X]^* \Leftrightarrow p \in K \setminus \{0\} \Leftrightarrow \operatorname{grad} p = 0$,
(ii) $p, q \in K[X]$ sind assoziiert $\Leftrightarrow \exists a \in K \setminus \{0\} : q(X) = ap(X)$,
(iii) Zu jedem $p \in K[X] \setminus \{0\}$ gibt es ein eindeutig bestimmtes normiertes $q \in K[X]$, das zu p assoziiert ist.

Beweis: (i) Das folgt sofort aus Korollar 156 (iii) und $K^* = K \setminus \{0\}$.
(ii) Da K ein Körper ist, ist $K[X]$ nach Korollar 156 (i) ein Integritätsbereich und die Behauptung folgt aus (i) und Satz 131 (viii).
(iii) Nach (ii) sind die zu p assoziierten Polynome genau die Polynome der Gestalt $cp(X)$ mit $c \in K \setminus \{0\}$. Ist $p(X) = a_n X^n + \cdots + a_1 X + a_0$ mit Leitkoeffizienten $a_n \neq 0$, so erhält man auf diese Weise genau für $c = a_n^{-1}$ ein normiertes Polynom.

Korollar 160: Es sei K ein Körper und $p \in K[X] \setminus K$. Dann gibt es ein $a \in K \setminus \{0\}$ und irreduzible, normierte Polynome $q_1, \dots, q_n \in K[X]$, derart dass $p(X) = aq_1(X) \cdots q_n(X)$. Diese Darstellung ist bis auf die Reihenfolge der Polynome $q_1, \dots, q_n$ eindeutig.

Beweis: Folgt aus Satz 139 und Lemma 159.

Bemerkung: Die Polynome $q_1, \dots, q_n$ in Korollar 160 sind irreduzible Elemente des Polynomrings $K[X]$. Sie können aber reduzibel sein, wenn man sie als Elemente eines Polynomrings $L[X]$ mit einem größeren Koeffizientenkörper L auffasst. So ist, wie wir in Kürze sehen werden, das Polynom X^2+1 ein irreduzibles Element des Polynomrings $\mathbb{R}[X]$. Es ist aber reduzibel, wenn man es als Element des Polynomrings $\mathbb{C}[X]$ auffasst, da $X^2 + 1 = (X + i)(X - i)$. D.h. die Faktorisierung in Korollar 160 ist zwar für einen fest gewählten Koeffizientenkörper K eindeutig, kann sich aber bei Übergang zu einem anderen Koeffizientenkörper ändern.

Lemma 161: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Dann ist $R[X]$ kein Körper.

Beweis: Wir zeigen, dass $p(X) = X \in R[X]$ kein multiplikatives Inverses besitzt. Ist $q(X) = 0$, so ist $p(X)q(X) = 0 \neq 1$. Ist $q(X) = a_nX^n + \cdots + a_1X + a_0$ mit $a_n \neq 0$ für ein $n \geq 0$, so ist $p(X)q(X) = a_nX^{n+1} + \cdots + a_1X^2 + a_0X \neq 1$.

Korollar 162: Es sei K ein Körper und $p \in K[X]$. Dann sind äquivalent:

(i) p ist ein irreduzibles Element von $K[X]$,
(ii) Der Faktorring $K[X]/\big(p(X)\big)$ ist ein Körper.

Beweis: (i) $\Rightarrow$ (ii) Da $K[X]$ (nach Korollar 158) ein Hauptidealbereich ist, folgt wegen Satz 132 (ii), dass $\big(p(X)\big)$ ein maximales Ideal von $K[X]$ ist. Nach Satz 77 ist $K[X]/\big(p(X)\big)$ ein Körper.
(ii) $\Rightarrow$ (i) Wegen Satz 77 ist $\big(p(X)\big)$ ein maximales Ideal von $K[X]$. Es ist $\big(p(X)\big) \neq (0)$. (Wäre $\big(p(X)\big) = (0)$, so wäre $p(X) = 0$ und daher

$$K[X]/\big(p(X)\big) = K[X]/(0) \cong K[X]$$

ein Körper, ein Widerspruch zu Lemma 161.) Wegen Satz 132 (ii) ist p ein irreduzibles Element von $K[X]$.

Satz 163: Es seien $R(\neq \{0\})$ und $S(\neq \{0\})$ zwei kommutative Ringe mit Eins, $\varphi : R \to S$ ein Ringhomomorphismus mit der Eigenschaft $\varphi(1_R) = 1_S$ und $c \in S$. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\varphi_c : R[X] \to S$ mit den Eigenschaften $\varphi_c \,|_R = \varphi$ (d.h. die Einschränkung von φ_c auf R ist φ bzw. φ_c setzt φ auf $R[X]$ fort) und $\varphi_c(X) = c$.

Beweis: Eindeutigkeit: Ist

$$p(X) = \sum_{i=0}^{n} a_i X^i,$$

so muss

$$\varphi_c\big(p(X)\big) = \sum_{i=0}^{n} \varphi_c(a_i)\varphi_c(X)^i = \sum_{i=0}^{n} \varphi(a_i)c^i$$

gelten.

Existenz: Setzt man

$$\varphi_c\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \varphi(a_i)c^i,$$

so sind offenbar $\varphi_c\,|_R = \varphi$ und $\varphi_c(X) = c$ erfüllt. Ist

$$p(X) = \sum_{i\geq 0} a_i X^i \quad \text{und} \quad q(X) = \sum_{i\geq 0} b_i X^i,$$

so gelten

$$\varphi_c\big(p(X) + q(X)\big) = \varphi_c\left(\sum_{i\geq 0}(a_i + b_i)X^i\right) = \sum_{i\geq 0}\varphi(a_i + b_i)c^i$$

$$= \sum_{i\geq 0}\big(\varphi(a_i) + \varphi(b_i)\big)c^i = \sum_{i\geq 0}\varphi(a_i)c^i + \sum_{i\geq 0}\varphi(b_i)c^i = \varphi_c\big(p(X)\big) + \varphi_c\big(q(X)\big)$$

und

$$\varphi_c\big(p(X)q(X)\big) = \varphi_c\left(\sum_{k\geq 0}\left(\sum_{i+j=k} a_i b_j\right)X^k\right) = \sum_{k\geq 0}\varphi\left(\sum_{i+j=k} a_i b_j\right)c^k$$

$$= \sum_{k\geq 0}\left(\sum_{i+j=k}\varphi(a_i)\varphi(b_j)\right)c^k = \left(\sum_{i\geq 0}\varphi(a_i)c^i\right)\left(\sum_{j\geq 0}\varphi(b_j)c^j\right) = \varphi_c\big(p(X)\big)\varphi_c\big(q(X)\big),$$

d.h. φ_c ist ein Homomorphismus.

Korollar 164: Es seien $R(\neq \{0\})$ und $S(\neq \{0\})$ zwei kommutative Ringe mit Eins, R ein Unterring von S, $1_R = 1_S$ und $c \in S$. Dann ist

$$\varphi_c : R[X] \to S,\ \varphi_c(a_n X^n + \cdots + a_1 X + a_0) = a_n c^n + \cdots + a_1 c + a_0$$

der durch die Bedingungen $\varphi_c(a) = a\ \forall a \in R$ und $\varphi_c(X) = c$ eindeutig bestimmte Ringhomomorphismus $R[X] \to S$.

Beweis: Folgt durch anwenden von Satz 163 auf die Einbettung $\varphi : R \to S$, $\varphi(a) = a$ für alle $a \in R$.

Definition: Der in Korollar 164 beschriebene Homomorphismus

$$\varphi_c : R[X] \to S,\ \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i c^i$$

wird Einsetzhomomorphismus genannt. Ist $p(X) = a_n X^n + \cdots + a_1 X + a_0$, so schreibt man dafür $p(c) = a_n c^n + \cdots + a_1 c + a_0$.

Bemerkungen: 1) Da der Einsetzhomomorphismus ein Ringhomomorphismus ist, darf man damit rechnen wie gewohnt, d.h.

$$(p+q)(c) = \varphi_c\big(p(X) + q(X)\big) = \varphi_c\big(p(X)\big) + \varphi_c\big(q(X)\big) = p(c) + q(c)$$

und

$$(pq)(c) = \varphi_c\big(p(X)q(X)\big) = \varphi_c\big(p(X)\big)\varphi_c\big(q(X)\big) = p(c)q(c).$$

2) Hält man nicht wie in Korollar 164 $c \in S$ fest und lässt $p \in R[X]$ variieren, sondern hält $p \in R[X]$ fest und lässt $c \in R$ variieren, so kann man jedem Polynom $p \in R[X]$ eine Polynomfunktion $S \to S$, $c \mapsto p(c)$ zuordnen. Diese Zuordnung ist im allgemeinen aber nicht injektiv. Ist z.B. $R = S = \mathbb{Z}_2$, $p(X) = \overline{0}$ und $q(X) = X^2 + X$, so ist $p \neq q$ aber $p\big(\overline{0}\big) = q\big(\overline{0}\big) = p\big(\overline{1}\big) = q\big(\overline{1}\big) = \overline{0}$.

Definition: Mit den Bezeichnungen von Korollar 164 setzt man

$$R[c] := \varphi_c\big(R[X]\big) = \big\{p(c) \mid p \in R[X]\big\} = \left\{ \sum_{i=0}^{n} a_i c^i \,\middle|\, n \geq 0 \text{ und } a_i \in R \text{ für } 0 \leq i \leq n \right\}.$$

Bemerkungen: 1) Wegen Lemma 67 (i) ist $R[c]$ ein Unterring von S. Es handelt sich dabei um den kleinsten Unterring von S, der R und c enthält.
2) In der Vorlesung sind bereits mehrere derartige Ringe aufgetaucht, nämlich:
Für $R = \mathbb{Z}$, $S = \mathbb{C}$ und $c = i$ erhält man den Ring der Gaußschen ganzen Zahlen

$$\mathbb{Z}[i] = \left\{ \sum_{k=0}^{n} a_k i^k \,\middle|\, a_0, \ldots, a_n \in \mathbb{Z} \right\} = \{a + bi \mid a, b \in \mathbb{Z}\} \text{ (da } i^2 = -1).$$

Für $R = \mathbb{Z}$, $S = \mathbb{R}$ und $c = \sqrt{2}$ erhält man

$$\mathbb{Z}\big[\sqrt{2}\big] = \left\{ \sum_{k=0}^{n} a_k \sqrt{2}^k \,\middle|\, a_0, \ldots, a_n \in \mathbb{Z} \right\} = \big\{a + b\sqrt{2} \,\big|\, a, b \in \mathbb{Z}\big\} \text{ (da } \sqrt{2}^2 = 2).$$

Ist allgemein $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, so erhält man für $R = \mathbb{Z}$, $S = \mathbb{C}$ und $c = \sqrt{d}$ den Ring

$$\mathbb{Z}\big[\sqrt{d}\big] = \left\{ \sum_{k=0}^{n} a_k \sqrt{d}^k \,\middle|\, a_0, \ldots, a_n \in \mathbb{Z} \right\} = \big\{a + b\sqrt{d} \,\big|\, a, b \in \mathbb{Z}\big\} \text{ (da } \sqrt{d}^2 = d).$$

(Für $d < 0$ setzen wir dabei $\sqrt{d} = i\sqrt{|d|}$.)

Korollar 165: Es seien $R(\neq \{0\})$ und $S(\neq \{0\})$ zwei kommutative Ringe mit Eins und $\varphi : R \to S$ ein Ringhomomorphismus mit der Eigenschaft $\varphi(1_R) = 1_S$. Bezeichnet nun $\widetilde{\varphi} : R \to S[X]$ die Zusammensetzung von φ mit der Einbettung $S \hookrightarrow S[X]$ (d.h. die Verknüpfung $R \overset{\varphi}{\to} S \hookrightarrow S[X]$), so ist

$$\varphi^* : R[X] \to S[X],\ \varphi^*\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \varphi(a_i) X^i$$

der eindeutig bestimmte Ringhomomorphismus mit den Eigenschaften $\varphi^*|_R = \widetilde{\varphi}$ und $\varphi^*(X) = X$.

Beweis: Als Verknüpfung von Ringhomomorphismen ist $\widetilde{\varphi} : R \to S[X]$ ein Ringhomomorphismus (nach Lemma 65), der $\widetilde{\varphi}(1_R) = 1_S = 1_{S[X]}$ erfüllt. Die Behauptung folgt nun aus Satz 163 (wobei man $c = X$ setzt).

Notation: Statt $\varphi^*(p)$ schreiben wir p^φ. D.h. ist

$$p(X) = \sum_{i=0}^{n} a_i X^i \in R[X],$$

so ist

$$p^\varphi(X) = \sum_{i=0}^{n} \varphi(a_i) X^i \in S[X].$$

Korollar 166: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und $I(\neq R)$ sei ein Ideal von R. Bezeichnet π den Ringepimorphismus $\pi : R \to R/I$, $\pi(a) = a + I$ und $\widetilde{\pi} : R \to (R/I)[X]$ seine Verknüpfung mit der Einbettung $R/I \hookrightarrow (R/I)[X]$, so ist

$$\pi^* : R[X] \to (R/I)[X],\ \pi^*\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \pi(a_i) X^i = \sum_{i=0}^{n} (a_i + I) X^i$$

der eindeutig bestimmte Ringhomomorphismus mit den Eigenschaften $\pi^*|_R = \widetilde{\pi}$ und $\pi^*(X) = X$.

Beweis: Es handelt sich um einen (wichtigen) Spezialfall von Korollar 165, bei dem man $S = R/I$ und $\varphi = \pi$ setzt. (Da $I \neq R$ ist dabei $R/I \neq \{0\}$ und $\pi(1_R) = 1_R + I = 1_{R/I}$.)

Bemerkung: Bei der Abbildung π^* werden die Koeffizienten des Polynoms p einzeln modulo dem Ideal I reduziert.

Korollar 167: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Dann sind äquivalent:

(i) R ist ein Körper,
(ii) $R[X]$ ist ein euklidischer Ring,
(iii) $R[X]$ ist ein Hauptidealbereich.

Beweis: (i) $\Rightarrow$ (ii) Wurde bereits in Korollar 158 bewiesen.
(ii) $\Rightarrow$ (iii) Folgt aus Satz 138.
(iii) $\Rightarrow$ (i) Wir betrachten den Einsetzhomomorphismus $\varphi_0 : R[X] \to R$, $\varphi_0(p) = p(0)$. Nach Lemma 68 (i) ist $\ker \varphi_0$ ein Ideal von $R[X]$. Dabei ist $\ker \varphi_0 \neq (0)$ (da $X \in \ker \varphi_0$) und φ_0 ist surjektiv (da $\varphi_0(a) = a \ \forall a \in R$). Nach dem Homomorphiesatz für Ringe (Korollar 70) gilt daher $R[X]/\ker \varphi_0 \cong R$. Als Hauptidealbereich ist $R[X]$ insbesondere ein Integritätsbereich. Also ist (wegen Korollar 156 (i)) auch R ein Integritätsbereich. Also ist auch $R[X]/\ker \varphi_0 (\cong R)$ ein Integritätsbereich und daher (wegen Satz 76) $\ker \varphi_0$ ein Primideal. Da $R[X]$ nach Voraussetzung ein Hauptidealbereich und $\ker \varphi_0 \neq (0)$ ist, folgt wegen Satz 132 (v), dass $\ker \varphi_0$ ein maximales Ideal ist. Daher ist $R \cong R[X]/\ker \varphi_0$ ein Körper (wegen Satz 77).

Bemerkungen: 1) Man sieht leicht, dass im Beweis von Korollar 167 $\ker \varphi_0 = (X)$ gilt. Insbesondere ist (X) ein maximales Ideal.
2) Aus Korollar 167 folgt, dass $\mathbb{Z}[X]$ kein Hauptidealbereich (und daher auch kein euklidischer Ring) ist.

Definition: Es seien $R(\neq \{0\})$ und $S(\neq \{0\})$ zwei kommutative Ringe mit Eins, R ein Unterring von S und $1_R = 1_S$. Ein $\alpha \in S$ wird Nullstelle von $p \in R[X]$ genannt, wenn $p(\alpha) = 0$ ist.

Beispiele: 1) $i \in \mathbb{C}$ ist Nullstelle von $X^2 + 1 \in \mathbb{R}[X]$.
2) $\sqrt{2} \in \mathbb{R}$ ist Nullstelle von $X^2 - 2 \in \mathbb{Z}[X]$.

Satz 168: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins, $p \in R[X] \setminus R$ und $\alpha \in R$. Dann gelten:

(i) α ist Nullstelle von $p \Leftrightarrow (X - \alpha) \mid p(X)$ (d.h. $\exists q \in R[X] : p(X) = (X - \alpha)q(X)$),
(ii) Ist R ein Integritätsbereich, so besitzt p höchstens $\operatorname{grad} p$ paarweise verschiedene Nullstellen in R.

Beweis: (i) ($\Rightarrow$) Wir dividieren $p(X)$ mit Rest durch $X - \alpha$ wie in Satz 157. (Das ist möglich, da der Leitkoeffizient von $X - \alpha$ das Einselement $1 \in R^*$ ist.) Man erhält

$$p(X) = (X - \alpha)q(X) + r(X)$$

für gewisse $q, r \in R[X]$ mit der Eigenschaft $\operatorname{grad} r < \operatorname{grad}(X-\alpha) = 1$. Daher ist $\operatorname{grad} r \leq 0$ und $\exists c \in R : r(X) = c$. Aus $0 = p(\alpha) = (\alpha-\alpha)q(\alpha)+r(\alpha) = c$ folgt $p(X) = (X-\alpha)q(X)$.
($\Leftarrow$) Wegen $p(\alpha) = (\alpha-\alpha)q(\alpha) = 0$ ist α Nullstelle von p.
(ii) Wir zeigen zu diesem Zweck mit Induktion nach k: Sind $\alpha_1, \dots, a_k \in R$ paarweise verschiedene Nullstellen von p, so ist $p(X) = (X-\alpha_1)\cdots(X-\alpha_k)q(X)$ für ein $q \in R[X]$.
Für $k = 1$ folgt $p(X) = (X-\alpha_1)q(X)$ für ein $q \in R[X]$ aus (i).
Es sei die Behauptung nun für $k-1$ bereits gezeigt, d.h.

$$p(X) = (X-\alpha_1)\cdots(X-\alpha_{k-1})\widetilde{q}(X)$$

für ein $\widetilde{q} \in R[X]$. Ist nun α_k eine weitere Nullstelle (die von $\alpha_1, \dots, \alpha_{k-1}$ verschieden ist), so ist

$$0 = p(\alpha_k) = (\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})\widetilde{q}(\alpha_k).$$

Da R ein Integritätsbereich ist und $\alpha_k - \alpha_i \neq 0$ für $1 \leq i \leq k-1$ muss $\widetilde{q}(\alpha_k) = 0$ gelten. Nach (i) ist daher $\widetilde{q}(X) = (X-\alpha_k)q(X)$ für ein $q \in R[X]$ und

$$p(X) = (X-\alpha_1)\cdots(X-\alpha_k)q(X).$$

Da R ein Integritätsbereich ist, kann man Satz 155 (iv) auf diese Gleichung anwenden und erhält $\operatorname{grad} p = k + \operatorname{grad} q$. Da $\operatorname{grad} p \geq 1$, ist $\operatorname{grad} q = -\infty$ unmöglich und daher $\operatorname{grad} q \geq 0$ und folglich $\operatorname{grad} p \geq k$.

Bemerkung: Ist R kein Integritätsbereich, so kann ein $p \in R[X]$ mehr als $\operatorname{grad} p$ Nullstellen besitzen. Z.B. besitzt $X^3 + X^2 + X + \overline{6} \in \mathbb{Z}_9[X]$ wie man leicht überprüft (genau) die vier Nullstellen $\overline{1}, \overline{3}, \overline{4}, \overline{7} \in \mathbb{Z}_9$. Zwar gilt hier z.B.

$$X^3 + X^2 + X + \overline{6} = \big(X-\overline{1}\big)\big(X-\overline{3}\big)\big(X-\overline{4}\big)$$

wie man leicht nachrechnet, allerdings ist $\big(\overline{7}-\overline{1}\big)\big(\overline{7}-\overline{3}\big)\big(\overline{7}-\overline{4}\big) = \overline{6}\cdot\overline{4}\cdot\overline{3} = \overline{0}$.

Definition: Es sei R ein Integritätsbereich, $p \in R[X] \setminus R$ und $\alpha \in R$ eine Nullstelle von p. Dann wird das (maximale) $m \in \mathbb{N} \setminus \{0\}$ mit der Eigenschaft $p(X) = (X-\alpha)^m q(X)$ für ein $q \in R[X]$ mit der Eigenschaft $(X-\alpha) \nmid q(X)$ die Vielfachheit der Nullstelle α genannt. Ist $m = 1$ (bzw. $m > 1$), so wird α eine einfache (bzw. mehrfache) Nullstelle genannt.

Bemerkung: Der Begriff der Vielfachheit ist wohldefiniert, denn angenommen

$$p(X) = (X-\alpha)^m f(X) = (X-\alpha)^n g(X)$$

mit $m, n \in \mathbb{N} \setminus \{0\}$ und $f, g \in R[X]$ mit $(X-\alpha) \nmid f(X)$ und $(X-\alpha) \nmid g(X)$. Wäre o.B.d.A. $m < n$ so würde folgen, dass $f(X) = (X-\alpha)^{n-m} g(X)$ (da $R[X]$ nach Korollar 156 (i) ein Integritätsbereich ist und man Lemma 50 anwenden kann). Dann wäre $f(\alpha) = 0$ und es würde wegen Satz 168 (i) $(X-\alpha) \mid f(X)$ folgen, ein Widerspruch.

Korollar 169: Es sei R ein Integritätsbereich, $p \in R[X] \setminus R$ und $\alpha_1, \dots, \alpha_n \in R$ paarweise verschiedene Nullstellen von p mit Vielfachheiten $m_1, \dots, m_n$. Dann ist

$$p(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_n)^{m_n} g(X)$$

für ein $g \in R[X]$, wobei $g(\alpha_i) \neq 0$ für $1 \leq i \leq n$ und $m_1 + \cdots + m_n \leq \operatorname{grad} p$.

Beweis: Wir führen den Beweis mit Induktion nach n.
Für $n = 1$ folgt die Behauptung sofort aus der Definition der Vielfachheit.
Für den Induktionschritt nehmen wir an, dass die Behauptung für $n - 1$ schon gezeigt ist und zeigen mit Induktion nach $j (\leq m_n)$, dass

$$p(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} (X - \alpha_n)^j g_j(X)$$

für ein $g_j \in R[X]$. Nach Voraussetzung ist

$$(X - \alpha_n)^{m_n} f(X) = p(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} g_0(X)$$

für $f, g_0 \in R[X]$, wobei $f(\alpha_n) \neq 0$ und $g_0(\alpha_i) \neq 0$ für $1 \leq i \leq n - 1$. Da $\alpha_n \neq \alpha_i$ für $1 \leq i \leq n-1$, muss $g_0(\alpha_n) = 0$ gelten und $g_0(X) = (X - \alpha_n) g_1(X)$ für ein $g_1 \in R[X]$, d.h.

$$p(X) = (X - \alpha_n)^{m_n} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} (X - \alpha_n) g_1(X).$$

Anwendung von Lemma 50 führt auf

$$(X - \alpha_n)^{m_n - 1} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} g_1(X)$$

Ist $m_n > 1$ kann man den Prozess fortführen. In diesem Fall ist $g_1(\alpha_n) = 0$ und man kann den Vorgang wiederholen. Ist

$$(X - \alpha_n)^{m_n - j} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} g_j(X)$$

für ein $g_j \in R[X]$ schon gezeigt und $j < m_n$ so, muss $g_j(\alpha_n) = 0$ gelten. Daraus erhält man, dass $g_j(X) = (X - \alpha_n) g_{j+1}(X)$ (für ein $g_{j+1} \in R[X]$) und

$$(X - \alpha_n)^{m_n - j} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} (X - \alpha_n) g_{j+1}(X)$$

folgt. Anwendung von Lemma 50 führt auf

$$(X - \alpha_n)^{m_n - j - 1} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} g_{j+1}(X).$$

Man führt diesen Prozess so lange fort, bis man $j = m_n$ und damit

$$f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} g_{m_n}(X)$$

erreicht hat. Setzt man nun $g := g_{m_n}$, so ist

$$p(X) = (X - \alpha_n)^{m_n} f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_{n-1})^{m_{n-1}} (X - \alpha_n)^{m_n} g(X).$$

Für $1 \leq i \leq n - 1$ ist dabei $g(\alpha_i) \neq 0$, da $g_0(X) = (X - \alpha_n)^{m_n} g(X)$ und $g_0(\alpha_i) \neq 0$. Schließlich ist $g(\alpha_n) \neq 0$, da $f(\alpha_n) \neq 0$. Wegen Satz 155 (iv) folgt

$$\operatorname{grad} p = m_1 + \cdots + m_n + \operatorname{grad} g \geq m_1 + \cdots + m_n.$$

Lemma 170: Es sei R ein faktorieller Ring und $a, b, c \in R$. Dann gelten:
(i) Sind a und b relativ prim und a und c relativ prim, so ist auch a und bc relativ prim,
(ii) Sind a und b relativ prim, so sind auch a^n und b^m relativ prim (für $n, m \in \mathbb{N} \setminus \{0\}$).

Beweis: (i) Ist $a = 0$, so ist b gemeinsamer Teiler von a und b und daher $b \mid 1$, d.h. $b \in R^*$. Analog muss $c \in R^*$ und daher $bc \in R^*$ gelten. Ist $d \in R$ ein gemeinsamer Teiler von a und bc, so muss (wegen $d \mid bc$ und $bc \mid 1$) folglich $d \mid 1$ gelten.
Ist $b = 0$, so ist a gemeinsamer Teiler von a und b und daher $a \mid 1$, d.h. $a \in R^*$. Ist $d \in R$ ein gemeinsamer Teiler von a und bc, so muss (wegen $d \mid a$ und $a \mid 1$) folglich $d \mid 1$ gelten.
Ist $c = 0$ kann man die Behauptung völlig analog beweisen.
Sind $a, b, c \in R \setminus \{0\}$, so seien

$$a = u \prod_{i \in I} \pi_i^{\alpha_i}, \ b = v \prod_{i \in I} \pi_i^{\beta_i} \quad \text{und} \quad c = w \prod_{i \in I} \pi_i^{\gamma_i}$$

die Darstellungen wie in Satz 139. Wegen Korollar 146 gilt $\min\{\alpha_i, \beta_i\} = \min\{\alpha_i, \gamma_i\} = 0$ für alle $i \in I$. Ist für ein $i \in I$ dabei $\alpha_i = 0$, so ist auch $\min\{\alpha_i, \beta_i + \gamma_i\} = 0$. Ist aber $\alpha_i > 0$, so muss $\beta_i = \gamma_i = 0$ gelten und es ist ebenfalls $\min\{\alpha_i, \beta_i + \gamma_i\} = 0$. Also sind (wieder wegen Korollar 146)

$$a = u \prod_{i \in I} \pi_i^{\alpha_i} \quad \text{und} \quad bc = vw \prod_{i \in I} \pi_i^{\beta_i + \gamma_i}$$

relativ prim.
(ii) Für $n = 1$ folgt aus (i) mit Induktion nach m, dass a und b^m relativ prim sind. (Für $m = 1$ wird die Behauptung vorausgesetzt. Ist bereits gezeigt, dass a und b^{m-1} relativ prim sind, so folgt nach (i), dass auch a und $b^{m-1} \cdot b = b^m$ relativ prim sind.) Daraus folgt nun wieder mit Induktion nach n, dass auch a^n und b^m relativ prim sind.

Lemma 171: Es sei R ein faktorieller Ring, $a_1, \ldots, a_n \in R$ und $a_i \neq 0$ für mindestens ein $i \in \{1, \ldots, n\}$. Ist g ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ und $a_j = g b_j$ mit $b_j \in R$ (für $1 \leq j \leq n$), so sind $b_1, \ldots, b_n$ relativ prim.

Beweis: Es sei zunächst $a_1, \ldots, a_n \in R \setminus \{0\}$. Ist (für $1 \leq j \leq n$)

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Darstellung von a_j wie in Satz 139, so ist (nach Satz 144)

$$g = v \prod_{i \in I} \pi_i^{\gamma_i}$$

mit $\gamma_i = \min\{\alpha_{i1}, \dots, \alpha_{in}\}$ die entsprechende Darstellung von g und daher

$$b_j = u_j v^{-1} \prod_{i \in I} \pi_i^{\alpha_{ij} - \gamma_i}$$

für $1 \leq j \leq n$. Wegen Korollar 146 und

$$\min\{\alpha_{i1} - \gamma_i, \dots, \alpha_{in} - \gamma_i\} = \min\{\alpha_{i1}, \dots, \alpha_{in}\} - \gamma_i = 0$$

für alle $i \in I$ sind $b_1, \dots, b_n$ relativ prim.
Falls $\exists j \in \{1, \dots, n\} : a_j = 0$ (aber nicht $a_1 = \cdots = a_n = 0$), folgt die Behauptung aus Lemma 142 (iv). (In diesem Fall ist $b_j = 0$ falls $a_j = 0$.)

Satz 172: Es sei R ein faktorieller Ring mit Quotientenkörper K,

$$p(X) = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus R$$

mit $a_n \neq 0$ (für ein $n \geq 1$) und $\alpha = \frac{c}{d} \in K$ eine Nullstelle von p in K (mit $c, d \in R$, $d \neq 0$ und c, d relativ prim). Dann gelten:

(i) $c \mid a_0$ und $d \mid a_n$,
(ii) Ist p normiert (d.h. $a_n = 1$), so ist $\alpha \in R$ und $\alpha \mid a_0$.

Beweis: (i) Die Voraussetzung besagt, dass

$$p(\alpha) = \sum_{i=0}^{n} a_i \frac{c^i}{d^i} = 0$$

und daher

$$\sum_{i=0}^{n} a_i c^i d^{n-i} = a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n = 0.$$

Aus der zweiten Gleichung folgen

$$-a_0 d^n = c \sum_{i=1}^{n} a_i c^{i-1} d^{n-i} \quad \text{und} \quad -a_n c^n = d \sum_{i=0}^{n-1} a_i c^i d^{n-i-1}.$$

Also gelten $c \mid a_0 d^n$ und $d \mid a_n c^n$. Nach Lemma 170 (ii) sind c^n und d relativ prim und ebenso c und d^n relativ prim. Wegen Korollar 148 folgt daher $c \mid a_0$ und $d \mid a_n$.
(ii) Wegen (i) gilt $d \mid 1$. Also ist $d \in R^*$ und daher $\alpha = \frac{c}{d} = \frac{cd^{-1}}{1} = cd^{-1} \in R$. Aus (i) folgt auch $c \mid a_0$. Wegen $cd^{-1} \mid c$ gilt daher auch $cd^{-1} \mid a_0$, d.h. $\alpha \mid a_0$.

Beispiele: 1) Gesucht sind die rationalen Nullstellen von

$$p(X) = X^4 - 2X^3 - 7X^2 - \tfrac{11}{3}X - \tfrac{4}{3} \in \mathbb{Q}[X].$$

Diese stimmen mit den Nullstellen von

$$3p(X) = 3X^4 - 6X^3 - 21X^2 - 11X - 4 \in \mathbb{Z}[X]$$

überein. Ist $p(\frac{c}{d}) = 0$, muss daher (nach Satz 172(i)) $c \mid 4$ und $d \mid 3$ gelten. Also ist $c \in \{\pm 1, \pm 2, \pm 4\}$ und $d \in \{\pm 1, \pm 3\}$ und folglich

$$\tfrac{c}{d} \in \left\{\pm 1, \pm 2, \pm 4, \pm\tfrac{1}{3}, \pm\tfrac{2}{3}, \pm\tfrac{4}{3}\right\}$$

Einsetzen dieser zwölf Zahlen ergibt, dass 4 die einzige rationale Nullstelle von p ist.
2) Gesucht sind die rationalen Nullstellen von $p(X) = X^5 + X + 2 \in \mathbb{Z}[X]$. Ist $\alpha \in \mathbb{Q}$ Nullstelle von p, so folgt aus Satz 172 (ii) $\alpha \in \mathbb{Z}$ und $\alpha \mid 2$, also $\alpha \in \{\pm 1, \pm 2\}$. Einsetzen dieser vier Zahlen zeigt, dass -1 die einzige rationale Nullstelle von p ist.
3) Gesucht sind die rationalen Nullstellen von $p(X) = X^3 - X + 2 \in \mathbb{Z}[X]$. Ist $\alpha \in \mathbb{Q}$ Nullstelle von p, so folgt aus Satz 172 (ii) $\alpha \in \mathbb{Z}$ und $\alpha \mid 2$, also $\alpha \in \{\pm 1, \pm 2\}$. Einsetzen dieser vier Zahlen zeigt, dass p keine rationale Nullstelle besitzt.

Definition: Es sei R ein Integritätsbereich und

$$p(X) = \sum_{k=0}^{n} a_k X^k \in R[X].$$

Die Ableitung $p' \in R[X]$ des Polynoms p ist definiert als

$$p'(X) = \sum_{k=1}^{n} k a_k X^{k-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Satz 173: Es sei R ein Integritätsbereich, $p, q \in R[X]$ und $\alpha \in R$. Dann gelten:

(i) $(\alpha p)' = \alpha p'$,
(ii) $(p + q)' = p' + q'$,
(iii) $(pq)' = p'q + pq'$,
(iv) $(p^n)' = np^{n-1}p'$ $\forall n \in \mathbb{N} \setminus \{0\}$.

Beweis: Es seien

$$p(X) = \sum_{k=0}^{n} a_k X^k \quad \text{und} \quad q(X) = \sum_{\ell=0}^{m} b_\ell X^\ell.$$

(i) Aus

$$(\alpha p)(X) = \sum_{k=0}^{n} (\alpha a_k) X^k$$

folgt

$$(\alpha p)'(X) = \sum_{k=1}^{n} k(\alpha a_k) X^{k-1} \overset{\text{Lemma 48 (v)}}{=} \alpha \sum_{k=1}^{n} k a_k X^{k-1} = \alpha p'(X).$$

(ii) Aus

$$(p+q)(X) = \sum_{k\geq 0} (a_k + b_k) X^k$$

folgt

$$(p+q)'(X) = \sum_{k\geq 1} k(a_k+b_k)X^{k-1} = \sum_{k\geq 1} k a_k X^{k-1} + \sum_{k\geq 1} k b_k X^{k-1} = p'(X) + q'(X).$$

(iii) Aus

$$(pq)(X) = a_0 b_0 + \sum_{\substack{0\leq k\leq n\\ 0\leq \ell\leq m\\ k+\ell\geq 1}} a_k b_\ell X^{k+\ell}$$

folgt

$$\begin{aligned}
(pq)'(X) &\overset{\text{(ii)}}{=} \sum_{\substack{0\leq k\leq n\\ 0\leq \ell\leq m\\ k+\ell\geq 1}} (k+\ell) a_k b_\ell X^{k+\ell-1} = \sum_{\substack{0\leq k\leq n\\ 0\leq \ell\leq m\\ k+\ell\geq 1}} k a_k b_\ell X^{k+\ell-1} + \sum_{\substack{0\leq k\leq n\\ 0\leq \ell\leq m\\ k+\ell\geq 1}} \ell a_k b_\ell X^{k+\ell-1} \\
&= \sum_{\substack{1\leq k\leq n\\ 0\leq \ell\leq m}} k a_k b_\ell X^{k+\ell-1} + \sum_{\substack{0\leq k\leq n\\ 1\leq \ell\leq m}} \ell a_k b_\ell X^{k+\ell-1} \\
&= \left(\sum_{k=1}^{n} k a_k X^{k-1}\right)\left(\sum_{\ell=0}^{m} b_\ell X^\ell\right) + \left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{\ell=1}^{m} \ell b_\ell X^{\ell-1}\right) \\
&= p'(X)q(X) + p(X)q'(X)
\end{aligned}$$

(iv) Wir verwenden Induktion nach n. Der Fall $n = 1$ ist trivial und

$$\begin{aligned}
\left(p^{n+1}\right)' &= (p^n \cdot p)' \overset{\text{(iii)}}{=} (p^n)' \cdot p + p^n \cdot p' \overset{\text{IV}}{=} (n p^{n-1} p') \cdot p + p^n \cdot p' \\
&= n p^n p' + p^n p' = (n+1) p^n p'.
\end{aligned}$$

Bemerkung: Satz 173 (i) folgt auch aus (iii), wurde wegen seiner Wichtigkeit aber trotzdem extra bewiesen.

Lemma 174: Es sei R ein Integritätsbereich und $p \in R[X]$ mit $\operatorname{grad} p \geq 1$. Dann gelten:

(i) $\operatorname{grad} p' \leq \operatorname{grad} p - 1$,

(ii) Ist $\operatorname{char} R = 0$, so ist $\operatorname{grad} p' = \operatorname{grad} p - 1$.

Beweis: (i) Folgt sofort aus der Definition.
(ii) Ist $p(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ mit $\operatorname{grad} p = n \geq 1$, so ist

$$n \cdot a_n = n \cdot (1_R \cdot a_n) \overset{\text{Lemma 48 (v)}}{=} (n \cdot 1_R) \cdot a_n \neq 0$$

und daher $\operatorname{grad} p' = n - 1$, denn $n \cdot 1_R \neq 0$ wegen Satz 88 und $a_n \neq 0$ da $\operatorname{grad} p = n$.

Bemerkung: Ist $\operatorname{char} R > 0$, so ist $\operatorname{grad} p' < \operatorname{grad} p - 1$ möglich. Für $p(X) = X^3 \in \mathbb{Z}_3[X]$ ist z.B. $p' = 0 \in \mathbb{Z}_3[X]$, denn $X^3 = \overline{1} \cdot X^3$ und $p'(X) = 3 \cdot \overline{1} \cdot X^2$, wobei $3 \cdot \overline{1} = \overline{1} + \overline{1} + \overline{1} = \overline{0}$.

Satz 175: Es seien R und S Integritätsbereiche, R ein Unterring von S, $p \in R[X] \setminus R$ und $\alpha \in S$. Dann sind äquivalent:

(i) α ist mehrfache Nullstelle von p,
(ii) $p(\alpha) = p'(\alpha) = 0$.

Beweis: (i) $\Rightarrow$ (ii) Nach Voraussetzung gibt es $m \in \mathbb{N}$, $m \geq 2$ und $q \in S[X]$, derart dass $p(X) = (X - \alpha)^m q(X)$. Aus Satz 173 (iii) und (iv) folgt

$$p'(X) = m(X - \alpha)^{m-1} q(X) + (X - \alpha)^m q'(X)$$

und daher $p(\alpha) = p'(\alpha) = 0$.
(ii) $\Rightarrow$ (i) Da $p(\alpha) = 0$, gibt es $m \in \mathbb{N} \setminus \{0\}$ und $q \in S[X]$, derart dass $p(X) = (X - \alpha)^m q(X)$ und $q(\alpha) \neq 0$. Wäre $m = 1$, so wäre

$$p'(X) = q(X) + (X - \alpha) q'(X)$$

und daher $p'(\alpha) = q(\alpha) \neq 0$. Also ist $m \geq 2$ und α daher eine mehrfache Nullstelle von p.

Korollar 176: (i) Es sei K ein Körper, R ein Integritätsbereich, K ein Unterring von R und $p \in K[X] \setminus K$.

(i) Sind p und p' relativ prim (als Elemente von $K[X]$), so besitzt p keine mehrfachen Nullstellen in R.
(ii) Ist p irreduzibel (als Element von $K[X]$) und R enthält eine Nullstelle von p, so gilt:
R enthält keine mehrfachen Nullstellen von $p \Leftrightarrow p' \neq 0$ (Nullpolynom).

Beweis: (i) Nach Korollar 158 ist $K[X]$ ein Hauptidealbereich. Wegen Korollar 147 gibt es $f, g \in K[X]$ mit der Eigenschaft $f \cdot p + g \cdot p' = 1$. Wäre $\alpha \in R$ eine mehrfache Nullstelle von p, so würde wegen Satz 175

$$0 = f(\alpha) p(\alpha) + g(\alpha) p'(\alpha) = 1$$

gelten, ein Widerspruch.
(ii) ($\Rightarrow$) Ist $p' = 0$ und $\alpha \in R$ Nullstelle von p, so ist α nach Satz 175 mehrfache Nullstelle von p.
($\Leftarrow$) Ist $q \in K[X]$ und $q \mid p$ (Teilbarkeit in $K[X]$), so folgt wegen der Irreduzibilität von

p aus Satz 132 (viii), dass entweder $q \in K[X]^* = K \setminus \{0\}$ oder dass q zu p assoziiert ist (in $K[X]$). Sind q und p zueinander assoziiert, so ist $\operatorname{grad} q = \operatorname{grad} p$. Dann muss aber $q \nmid p'$ gelten, da $\operatorname{grad} p' < \operatorname{grad} p$ und $p' \neq 0$. (Wäre $p' = qf$ für ein $f \in K[X]$, so wäre $\operatorname{grad} p > \operatorname{grad} p' = \operatorname{grad} q + \operatorname{grad} f \geq \operatorname{grad} q = \operatorname{grad} p$, ein Widerspruch.) Die gemeinsamen Teiler von p und p' sind daher genau die Elemente von $K \setminus \{0\} = K[X]^*$. Daher sind p und p' relativ prim (wegen Korollar 146) und aus (i) folgt, dass p keine mehrfachen Nullstellen in R besitzt.

Lemma 177: Es sei R ein Integritätsbereich.
(i) Ist $\alpha \in R$ irreduzibel (in R), so ist α auch irreduzibel als Element von $R[X]$.
(ii) Ist $p(X) = uX + \alpha \in R[X]$ mit $u \in R^*$, so ist p irreduzibel in $R[X]$.
(iii) Ist R ein Körper und $p \in R[X]$ mit $\operatorname{grad} p = 1$, so ist p irreduzibel in $R[X]$.

Beweis: (i) Ist $\alpha = p(X)q(X)$ für $p, q \in R[X]$, so folgt $0 = \operatorname{grad} p + \operatorname{grad} q$, woraus sofort $\operatorname{grad} p = \operatorname{grad} q = 0$ folgt und daher $p, q \in R$. Da α in R irreduzibel ist, muss entweder $p \in R^* = R[X]^*$ oder $q \in R^* = R[X]^*$ gelten.
(ii) Ist $p = f \cdot g$ mit $f, g \in R[X]$, so ist $1 = \operatorname{grad} f + \operatorname{grad} g$. Daraus folgt o.B.d.A. $\operatorname{grad} f = 0$ und $\operatorname{grad} g = 1$, d.h. $f(X) = a \in R \setminus \{0\}$ und $g(X) = bX + c$ mit $b, c \in R$ und $b \neq 0$. Daher ist $uX + \alpha = a(bX + c) = abX + ac$ und folglich $ab = u$, woraus man sofort $abu^{-1} = 1$ erhält. Das zeigt aber $f(X) = a \in R^* = R[X]^*$.
(iii) Folgt sofort aus (ii).

Beispiele: 1) Das Polynom $2X + 2$ ist (nach Lemma 177 (iii)) irreduzibel als Element von $\mathbb{Q}[X]$, es ist aber reduzibel als Element von $\mathbb{Z}[X]$, da $2X + 2 = 2(X + 1)$ mit den Faktoren $2, X + 1 \notin \{-1, 1\} = \mathbb{Z}^* = \mathbb{Z}[X]^*$.
2) Das Polynom $X^2 + 1$ ist irreduzibel als Element von $\mathbb{R}[X]$. (Wäre $X^2 + 1$ reduzibel, so gäbe es $p, q \in \mathbb{R}[X]$ mit der Eigenschaft $X^2 + 1 = p(X)q(X)$ und $\operatorname{grad} p = \operatorname{grad} q = 1$. Dann würde $X^2 + 1$ aber eine reelle Nullstelle besitzen, Widerspruch.) Das Polynom ist aber reduzibel als Element von $\mathbb{C}[X]$, da $X^2 + 1 = (X - i)(X + i)$ mit den Faktoren $X - i, X + i \notin \mathbb{C} \setminus \{0\} = \mathbb{C}^* = \mathbb{C}[X]^*$.

Lemma 178: Es sei R ein faktorieller Ring und $a_1, \ldots, a_n \in R$.
(i) Ist R ein Körper, so gilt

$$a_1, \ldots, a_n \text{ sind nicht relativ prim} \Leftrightarrow a_1 = \cdots = a_n = 0,$$

(ii) Ist R kein Körper, so gilt

$$a_1, \ldots, a_n \text{ sind nicht relativ prim} \Leftrightarrow \exists \pi \in R,\ \pi \text{ irreduzibel } \forall j \in \{1, \ldots, n\} : \pi \mid a_j.$$

Beweis: (i) Ist $a_1 = \cdots = a_n = 0$, so sind $a_1, \ldots, a_n$ nicht relativ prim, denn in diesem Fall ist (nach Lemma 142 (v)) 0 der einzige größte gemeinsame Teiler von $a_1, \ldots, a_n$. Gibt

es ein $j \in \{1, \dots, n\}$, derart dass $a_j \neq 0$, so gilt $a_j \mid 1$. Ist nun $d \in R$ ein gemeinsamer Teiler von $a_1, \dots, a_n$, so gilt auch $d \mid a_j$ und daher $d \mid 1$.
(ii) ($\Rightarrow$) Es sei zunächst $a_1 = \cdots = a_n = 0$. Da R kein Körper ist, gibt es ein irreduzibles $\pi \in R$ und $\pi \mid a_j$ für $1 \leq j \leq n$.
Es sei nun o.B.d.A. $a_1, \dots, a_k \in R \setminus \{0\}$ und $a_{k+1} = \cdots = a_n = 0$ (für ein $k \in \{1, \dots, n\}$) und

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Produktdarstellung von a_j wie in Satz 139 (für $1 \leq j \leq k$). Da $a_1, \dots, a_n$ nicht relativ prim sind, sind wegen Lemma 142 (iv) auch $a_1, \dots, a_k$ nicht relativ prim und wegen Korollar 146 gibt es ein $i \in I$ mit der Eigenschaft $\min\{\alpha_{i1}, \dots, \alpha_{ik}\} > 0$. Daher gilt $\pi_i \mid a_j$ für $1 \leq j \leq n$.
($\Leftarrow$) Wären $a_1, \dots, a_n$ relativ prim, würde $\pi \mid 1$ und daher $\pi \in R^*$ gelten, ein Widerspruch.

Definition: Es sei R ein faktorieller Ring und

$$p(X) = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus \{0\}.$$

Als Inhalt $C(p)$ von p bezeichnet man die größten gemeinsamen Teiler der Koeffizienten $a_0, a_1, \dots, a_n$. Das Polynom p wird primitiv genannt, wenn die Koeffizienten relativ prim sind.

Bemerkungen: 1) Der Inhalt wird in der Literatur oft als ein ausgewählter größter gemeinsamer Teiler der Koeffizienten des Polynoms definiert. Das macht manche Rechnungen einfacher, allerdings ist der Inhalt dann nur bis auf Einheiten definiert. Wir werden unter dem Inhalt im folgenden die Menge der größten gemeinsamen Teiler der Koeffizienten verstehen.
2) Ist $p \in R[X] \setminus \{0\}$ ein primitives Polynom, so ist sein Inhalt nach Definition $C(p) = R^*$.
3) Ist R ein Körper, so ist nach Lemma 178 (i) jedes Polynom $p \in R[X] \setminus \{0\}$ primitiv.

Lemma 179: Es sei R ein faktorieller Ring und $p \in R[X] \setminus \{0\}$.

(i) Ist $b \in R \setminus \{0\}$, so ist $C(bp) = bC(p)$,
(ii) Ist $p = cq$ mit $c \in C(p)$ und $q \in R[X]$, so ist q primitiv.

Beweis: (i) Es sei

$$p(X) = \sum_{j=0}^{n} a_j X^j$$

und für $0 \leq j \leq n$ sei

$$a_j = u_j \prod_{i \in I} \pi_i^{\alpha_{ij}}$$

die Produktdarstellung von $a_j \neq 0$ wie in Satz 139 und ebenso

$$b = v \prod_{i \in I} \pi_i^{\beta_i}$$

die Produktdarstellung von b wie in Satz 139. Dann ist

$$bp(X) = \sum_{j=0}^{n} b a_j X^j$$

mit

$$ba_j = v u_j \prod_{i \in I} \pi_i^{\alpha_{ij}+\beta_i}$$

für $0 \leq j \leq n$ mit $a_j \neq 0$. Aus Satz 144 und Lemma 142 (iv) ergibt sich

$$\begin{aligned}
C(bp) &= \left\{ u \prod_{i \in I} \pi_i^{\min\{\alpha_{ij}+\beta_i \mid 0 \leq j \leq n, a_j \neq 0\}} \,\middle|\, u \in R^* \right\} \\
&= \left\{ u \prod_{i \in I} \pi_i^{\beta_i + \min\{\alpha_{ij} \mid 0 \leq j \leq n, a_j \neq 0\}} \,\middle|\, u \in R^* \right\} \\
&= \left\{ v \prod_{i \in I} \pi_i^{\beta_i} \cdot u \prod_{i \in I} \pi_i^{\min\{\alpha_{ij} \mid 0 \leq j \leq n, a_j \neq 0\}} \,\middle|\, u \in R^* \right\} \\
&= v \prod_{i \in I} \pi_i^{\beta_i} \cdot \left\{ u \prod_{i \in I} \pi_i^{\min\{\alpha_{ij} \mid 0 \leq j \leq n, a_j \neq 0\}} \,\middle|\, u \in R^* \right\} \\
&= bC(p).
\end{aligned}$$

(ii) Ist p wie in (i) und

$$q(X) = \sum_{j=0}^{n} b_j X^j,$$

so ist $a_j = cb_j$ für $0 \leq j \leq n$ und $b_0, \ldots, b_n$ sind relativ prim nach Lemma 171.

Satz 180: Es sei R ein faktorieller Ring und $p, q \in R[X] \setminus \{0\}$. Dann gelten:

(i) Sind p und q primitiv, so ist auch pq primitiv,
(ii) $C(pq) = C(p)C(q)$.

Beweis: (i) Ist R ein Körper, so ist jedes Polynom in $R[X]\setminus\{0\}$ primitiv und die Behauptung ist trivialerweise erfüllt. Es sei darum jetzt R kein Körper und

$$p(X)=\sum_{i=0}^{n} a_iX^i \quad \text{und} \quad q(X)=\sum_{j=0}^{m} b_jX^j.$$

Dann ist

$$(p\cdot q)(X)=\sum_{k=0}^{m+n} c_kX^k \quad \text{mit} \quad c_k=\sum_{i+j=k} a_ib_j.$$

Wäre pq nicht primitiv, so würde es nach Lemma 178 (ii) ein irreduzibles $\pi\in R$ mit der Eigenschaft $\pi \mid c_k$ (für $0\le k\le m+n$) geben. Da p primitiv ist, ist $\pi \mid a_i$ für $0\le i\le n$ unmöglich. Daher gibt es ein (minimales) $s\in\{0,1,\dots,n\}$ mit der Eigenschaft

$$\pi \mid a_0,\ \pi \mid a_1,\ \dots,\ \pi \mid a_{s-1},\ \pi \nmid a_s.$$

Analog gibt es ein (minimales) $t\in\{0,1,\dots,m\}$ mit der Eigenschaft

$$\pi \mid b_0,\ \pi \mid b_1,\ \dots,\ \pi \mid b_{t-1},\ \pi \nmid b_t.$$

Nun ist

$$c_{s+t}=a_0b_{s+t}+\dots+a_{s-1}b_{t+1}+a_sb_t+a_{s+1}b_{t-1}+\dots+a_{s+t}b_0$$

und aus $\pi \mid c_{s+t}$ und $\pi \mid a_ib_{s+t-i}$ für $0\le i\le s-1$ und $s+1\le i\le s+t$ folgt $\pi \mid a_sb_t$. Da π nach Satz 134 auch prim ist, müsste $\pi \mid a_s$ oder $\pi \mid b_t$ gelten, ein Widerspruch.
(ii) Es sei $p=c_p\cdot\overline{p}$ und $q=c_q\cdot\overline{q}$ mit $c_p\in C(p)$, $c_q\in C(q)$ und $\overline{p},\overline{q}\in R[X]$. Dabei sind $\overline{p}$ und $\overline{q}$ primitiv (nach Lemma 179 (ii)) und aus (i) folgt, dass auch $\overline{p}\cdot\overline{q}$ primitiv ist. Daraus ergibt sich $C(\overline{p}\cdot\overline{q})=R^*=R^*\cdot R^*=C(\overline{p})C(\overline{q})$ und daher (wegen Lemma 179 (i))

$$\begin{aligned} C(pq)&=C(c_p\overline{p}\cdot c_q\overline{q})=C(c_pc_q\cdot\overline{p}\cdot\overline{q})=c_pc_qC(\overline{p}\cdot\overline{q})\\ &=c_pc_qC(\overline{p})C(\overline{q})=C(c_p\overline{p})C(c_q\overline{q})=C(p)C(q).\end{aligned}$$

Lemma 181: Es sei R ein faktorieller Ring mit Quotientenkörper K und $p,q\in R[X]\setminus\{0\}$ primitiv. Dann sind äquivalent:

(i) p und q sind assoziiert als Elemente von $R[X]$,
(ii) p und q sind assoziiert als Elemente von $K[X]$.

Beweis: (i) $\Rightarrow$ (ii) Wegen Korollar 156 (i) ist $R[X]$ ein Integritätsbereich. Nach Voraussetzung gibt es ein $u\in R[X]^*=R^*$ mit der Eigenschaft $p(X)=uq(X)$. Wegen $R^*\subseteq K^*=K[X]^*$ sind p und q auch in $K[X]$ assoziiert.
(ii) $\Rightarrow$ (i) Nach Voraussetzung gibt es ein $u\in K[X]^*=K^*=K\setminus\{0\}$ mit der Eigenschaft $p(X)=uq(X)$. Da K Quotientenkörper von R ist, ist $u=\frac{a}{b}$ für gewisse $a,b\in R\setminus\{0\}$. Daher ist $bp(X)=aq(X)$, woraus man mit Hilfe von Lemma 179 (i)

$$bC(p) = C(bp) = C(aq) = aC(q)$$

erhält. Da p und q primitiv sind, ist $C(p) = C(q) = R^*$ und es muss ein $v \in R^*$ mit der Eigenschaft $a = bv$ geben. Durch einsetzen erhält man $bp(X) = aq(X) = bvq(X)$ und daraus mittels Lemma 50 $p(X) = vq(X)$. Also sind p und q auch in $R[X]$ assoziiert.

Satz 182: Es sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R[X] \setminus R$ primitiv. Dann sind äquivalent:

(i) p ist irreduzibel als Elemente von $R[X]$,
(ii) p ist irreduzibel als Elemente von $K[X]$.

Beweis: Ist R ein Körper, so ist die Behauptung trivial, da in diesem Fall $K = R$ gilt. Wir können darum ab jetzt voraussetzen, dass R kein Körper ist.
(i) $\Rightarrow$ (ii) Ist p reduzibel in $K[X]$, so gibt es $\overline{f}, \overline{g} \in K[X] \setminus K$ mit der Eigenschaft $p = \overline{f} \cdot \overline{g}$. Wähle nun $a, b \in R \setminus \{0\}$, derart dass

$$\widetilde{f}(X) := a\overline{f}(X) \in R[X] \text{ und } \widetilde{g}(X) := b\overline{g}(X) \in R[X].$$

Schließlich seien $f, g \in R[X]$ durch $\widetilde{f}(X) = c_f \cdot f(X)$ und $\widetilde{g}(X) = c_g \cdot g(X)$ definiert, wobei $c_f \in C(\widetilde{f})$ und $c_g \in C(\widetilde{g})$ gelten soll. Wegen Lemma 179 (ii) sind f und g dabei primitive Polynome in $R[X]$. Nach Satz 180 (i) ist auch fg ein primitives Polynom. Durch einsetzen erhält man

$$abp(X) = \big(a\overline{f}(X)\big) \cdot \big(b\overline{g}(X)\big) = \widetilde{f}(X) \cdot \widetilde{g}(X) = c_f c_g f(X) g(X)$$

und daraus $abC(p) = c_f c_g C(fg)$ wegen Lemma 179 (i). Da p und fg primitiv sind, ist $C(p) = C(fg) = R^*$. Daher gibt es ein $u \in R^*$ mit der Eigenschaft $c_f c_g = uab$. Durch einsetzen und kürzen erhält man $p(X) = uf(X)g(X)$, d.h. p ist auch als Element von $R[X]$ reduzibel.
(ii) $\Rightarrow$ (i) Ist p reduzibel in $R[X]$, so gibt es $f, g \in R[X] \setminus R^*$ mit der Eigenschaft $p = f \cdot g$. Da p primitiv ist, muss dabei $\operatorname{grad} f \geq 1$ und $\operatorname{grad} g \geq 1$ gelten. (Wäre etwa $f(X) = a \in R \setminus R^*$ mit $a \neq 0$, so würde es ein irreduzibles $\pi \in R$ mit der Eigenschaft $\pi \mid a$ geben. Dann wäre π aber gemeinsamer Teiler der Koeffizienten von p und p daher nicht primitiv, ein Widerspruch.) Daher sind $f, g \notin K \setminus \{0\} = K[X]^*$ und p ist auch als Element von $K[X]$ reduzibel.

Satz 183: Es sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R[X]$. Dann sind äquivalent:

(i) p ist irreduzibel als Elemente von $R[X]$,
(ii) $p \in R$ und p ist ein irreduzibles Element von R oder
$p \in R[X] \setminus R$, p ist primitiv und irreduzible in $K[X]$.

Beweis: (ii) $\Rightarrow$ (i) Ist $p \in R$ irreduzibel (als Element von R), so ist es nach Lemma 177 (i) auch irreduzibel als Element von $R[X]$. Ist $p \in R[X] \setminus R$ primitiv und irreduzibel als Element von $K[X]$, so ist es nach Satz 182 irreduzibel als Element von $R[X]$.
(i) $\Rightarrow$ (ii) Ist $p \in R \setminus R^*$, $p \neq 0$ reduzibel als Element von R, so ist $p \notin R[X]^*$ und es gibt $a, b \in R \setminus R^*$ mit der Eigenschaft $p = ab$. Da dann auch $a, b \notin R[X]^*$, ist p auch reduzibel als Element von $R[X]$. Ist $p \in R[X]$ mit $\operatorname{grad} p \geq 1$ nicht primitiv, so gibt es ein $a \in R \setminus R^*$ und ein $q \in R[X]$ mit $\operatorname{grad} q \geq 1$, derart dass $p(X) = aq(X)$, d.h. $a, q(X) \notin R[X]^*$ und p ist auch reduzibel als Element von $R[X]$. Ist $p \in R[X] \setminus R$ mit $\operatorname{grad} p \geq 1$ primitiv aber reduzibel als Element von $K[X]$, so ist p auch reduzibel als Element von $R[X]$ nach Satz 182.

Satz 184: Es sei R ein faktorieller Ring. Dann ist $R[X]$ ebenfalls ein faktorieller Ring.

Beweis: Es sei K der Quotientenkörper von R.
Wir zeigen zunächst, dass sich jedes $p \in R[X] \setminus R^*$, $p \neq 0$ als Produkt irreduzibler Elemente von $R[X]$ (wie sie in Satz 183 beschrieben wurden) geschrieben werden kann.
Ist $\operatorname{grad} p = 0$, so ist $p \in R$ und lässt sich nach Voraussetzung als Produkt irreduzibler Elemente von R schreiben. Ist $\operatorname{grad} p \geq 1$, so fassen wir p als Element von $K[X]$ auf. Nach Korollar 158 ist $K[X]$ ein faktorieller Ring, d.h. es gibt $\overline{q}_1, \ldots, \overline{q}_n \in K[X]$, die irreduzible Elemente von $K[X]$ sind, derart dass $p = \overline{q}_1 \cdots \overline{q}_n$. Für $1 \leq i \leq n$ sei nun $b_i \in R \setminus \{0\}$ derart dass $b_i \overline{q}_i \in R[X]$, $a_i \in R \setminus \{0\}$ sei ein größter gemeinsamer Teiler der Koeffizienten von $b_i \overline{q}_i(X)$ und $q_i(X) \in R[X]$ sei durch die Relation $b_i \overline{q}_i(X) = a_i q_i(X)$ definiert. D.h.

$$\overline{q}_i(X) = \frac{a_i}{b_i} q_i(X)$$

und q_i ist primitiv nach Lemma 179 (ii). Setzt man $a := a_1 \cdots a_n$ und $b := b_1 \cdots b_n$, so ist

$$bp = b_1 \cdots b_n \overline{q}_1 \cdots \overline{q}_n = a_1 \cdots a_n q_1 \cdots q_n = a q_1 \cdots q_n$$

und daher (wegen Lemma 179 (i) und Satz 180 (ii))

$$bC(p) = C(bp) = C(aq_1 \cdots q_n) = aC(q_1) \cdots C(q_n).$$

Ist $c \in C(p)$, so folgt, da $C(q_1) = \cdots = C(q_n) = R^*$, dass bc und a assoziiert sind (als Elemente von R), d.h. es gibt ein $u \in R^*$ mit der Eigenschaft $a = ubc$ und daher

$$p(X) = \frac{a}{b} q_1(X) \cdots q_n(X) = ucq_1(X) \cdots q_n(X).$$

Ist dabei $c \notin R^*$, kann c als Produkt irreduzibler $c_1, \ldots, c_m \in R$ geschrieben werden. (Falls $c \in R^*$, fassen wir $c_1 \cdots c_m$ als leeres Produkt mit Wert 1 auf.) D.h. es ist nun

$$p(X) = c_1 \cdots c_m \big(u q_1(X)\big) q_2(X) \cdots q_n(X).$$

Dabei ist q_i, aufgefasst als Element von $K[X]$, zu $\overline{q}_i(X)$ assoziiert (für $2 \leq i \leq n$) und uq_1 ist zu $\overline{q}_1$ assoziiert (wieder in $K[X]$). D.h. $uq_1, q_2, \ldots, q_n$ sind primitiv und irreduzibel, wenn man sie als Elemente von $K[X]$ auffasst. Wegen Satz 183 sind $uq_1, q_2, \ldots, q_n$ auch irreduzible Elemente von $R[X]$.
Wir zeigen nun die Eindeutigkeit der Darstellung: Angenommen, es ist

$$a_1 \cdots a_k p_1 \cdots p_\ell = b_1 \cdots b_m q_1 \cdots q_n$$

mit

$$a_1, \ldots, a_k, b_1, \ldots, b_m \in R$$

irreduzibel (als Elemente von R) und

$$p_1, \ldots, p_\ell, q_1, \ldots, q_n \in R[X] \setminus R$$

primitiv und irreduzible (als Elemente von $K[X]$). Dann ist

$$\begin{aligned} a_1 \cdots a_k C(p_1) \cdots C(p_\ell) &= C(a_1 \cdots a_k p_1 \cdots p_\ell) \\ =C(b_1 \cdots b_m q_1 \cdots q_n) &= b_1 \cdots b_m C(q_1) \cdots C(q_n). \end{aligned}$$

Da $p_1, \ldots, p_\ell, q_1, \ldots, q_n$ primitiv sind, sind $a_1 \cdots a_k$ und $b_1 \cdots b_m$ assoziiert (als Elemente von R) und es gibt folglich ein $u \in R^*$, derart dass $a_1 \cdots a_k = ub_1 \cdots b_m$. Da R faktoriell ist, muss $k = m$ gelten und es gibt ein $\sigma \in S_k$, derart dass a_i zu $b_{\sigma(i)}$ assoziiert ist (als Elemente von R und daher auch als Elemente von $R[X]$) für $1 \leq i \leq k$. Durch Kürzen erhält man, dass $p_1 \cdots p_\ell$ zu $q_1 \cdots q_n$ assoziiert ist, d.h. es gibt ein $v \in R^*$, derart dass $p_1 \cdots p_\ell = vq_1 \cdots q_n$. Da $K[X]$ faktoriell ist, gilt $\ell = n$ und es gibt ein $\tau \in S_\ell$, derart dass p_i und $q_{\tau(i)}$ in $K[X]$ assoziiert sind (für $1 \leq i \leq \ell$). Wegen Lemma 181 sind p_i und $q_{\tau(i)}$ dann auch als Elemente von $R[X]$ assoziiert.

Beispiele: 1) $\mathbb{Z}[X]$ ist ein faktorieller Ring, aber kein Hauptidealbereich nach Korollar 167.
2) $\mathbb{Z}[i][X]$ ist ein faktorieller Ring (da $\mathbb{Z}[i]$ ein euklidischer Ring und daher faktoriell ist).
3) $\mathbb{Z}\big[\sqrt{2}\big][X]$ ist ein faktorieller Ring (da $\mathbb{Z}\big[\sqrt{2}\big]$ ein euklidischer Ring und faktoriell ist).
4) $\big(\mathbb{Z}[X]\big)[Y]$ ist ein faktorieller Ring, da $\mathbb{Z}[X]$ ein faktorieller Ring ist.

Satz 185 (Eisensteinsches Irreduzibilitätskriterium): Es sei R ein faktorieller Ring mit Quotientenkörper K,

$$p(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$$

mit $\operatorname{grad} p = n \geq 1$ und $\pi \in R$ irreduzibel. Gelten

$$\pi \mid a_i \text{ für } 0 \leq i \leq n-1,\ \pi \nmid a_n \text{ und } \pi^2 \nmid a_0,$$

so ist p irreduzibel in $K[X]$. Ist p primitiv, so ist es auch in $R[X]$ irreduzibel.

Beweis: Es sei $p(X) = cq(X)$ mit $c \in C(p)$ und $q \in R[X]$ primitiv. Ist

$$q(X) = \sum_{i=0}^{n} b_i X^i,$$

so ist $a_i = cb_i$ (für $0 \leq i \leq n$). Dabei gilt $\pi \nmid c$ (da sonst $\pi \mid a_n$ folgen würde). Da π auch prim ist, folgt $\pi \mid b_i$ für $0 \leq i \leq n-1$ (denn $\pi \mid a_i \Rightarrow \pi \mid cb_i \Rightarrow \pi \mid c \vee \pi \mid b_i \Rightarrow \pi \mid b_i$), $\pi \nmid b_n$ (da $\pi \mid b_n \Rightarrow \pi \mid a_n$) und $\pi^2 \nmid b_0$ (da $\pi^2 \mid b_0 \Rightarrow \pi^2 \mid a_0$).
Angenommen, $q(X) = f(X)g(X)$ mit $f, g \in R[X]$, $\operatorname{grad} f = k$, $\operatorname{grad} g = \ell$,

$$f(X) = \sum_{i=0}^{k} \alpha_i X^i \quad \text{und} \quad g(X) = \sum_{i=0}^{\ell} \beta_i X^i.$$

Dann ist $b_0 = \alpha_0\beta_0$. Aus $\pi \mid b_0$ folgt $\pi \mid \alpha_0$ oder $\pi \mid \beta_0$. Gilt o.B.d.A. $\pi \mid \alpha_0$, so muss $\pi \nmid \beta_0$ gelten (da sonst $\pi^2 \mid b_0$ folgen würde). Andererseits muss $\pi \nmid \alpha_k$ gelten (da wegen $b_n = \alpha_k\beta_\ell$ sonst $\pi \mid b_n$ folgen würde). Also gibt es ein (minimales) $i \in \{1, \ldots, k\}$ mit der Eigenschaft $\pi \mid \alpha_0$, $\pi \mid \alpha_1$, …, $\pi \mid \alpha_{i-1}$, $\pi \nmid \alpha_i$. Nun ist $b_i = \alpha_0\beta_i + \cdots + \alpha_{i-1}\beta_1 + \alpha_i\beta_0$ und $\pi \mid (\alpha_0\beta_i + \cdots + \alpha_{i-1}\beta_1)$. Aus $\pi \mid b_i$ würde daher $\pi \mid \alpha_i\beta_0$ folgen und daher auch $\pi \mid \alpha_i$ oder $\pi \mid \beta_0$, ein Widerspruch. Also ist $\pi \nmid b_i$ und daher $i = n$. Das ist nur möglich für $k = n$ und $\ell = 0$, d.h. $g \in R$. Da q primitiv ist, folgt $g \in R^* = R[X]^*$. Also ist q irreduzibel in $R[X]$ und (wegen Satz 182) auch irreduzibel in $K[X]$. Da p und q in $K[X]$ assoziiert sind, ist (wegen Satz 132 (vi)) auch p irreduzibel in $K[X]$. Ist p primitiv, so ist es (wegen Satz 182) auch irreduzibel in $R[X]$.

Bemerkung: Ein wichtiger Spezialfall des Eisensteinschen Irreduzibilitätskriteriums ist der Fall $R = \mathbb{Z}$ (und damit $K = \mathbb{Q}$). Ist

$$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$$

mit $\operatorname{grad} f = n \geq 1$ und p eine Primzahl mit der Eigenschaft

$$p \mid a_0,\ p \mid a_1,\ \ldots,\ p \mid a_{n-1},\ p \nmid a_n \text{ und } p^2 \nmid a_0,$$

so ist f irreduzibel in $\mathbb{Q}[X]$. Ist $\operatorname{ggT}(a_0, a_1, \ldots, a_n) = 1$, so ist f irreduzibel in $\mathbb{Z}[X]$.

Beispiele: 1) Es sei $f(X) = 3X^5 + 2X^3 - 4X^2 + 2 \in \mathbb{Z}[X]$. Da

$$2 \mid 2,\ 2 \mid 0,\ 2 \mid (-4),\ 2 \mid 2,\ 2 \mid 0,\ 2 \nmid 3 \text{ und } 4 \nmid 2,$$

ist f irreduzibel in $\mathbb{Q}[X]$. Da $\operatorname{ggT}(2, 0, -4, 2, 0, 3) = 1$, ist f irreduzibel in $\mathbb{Z}[X]$.

2) Es sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann ist $f_n(X) = X^n - p$ irreduzibel in $\mathbb{Q}[X]$, da $p \mid (-p)$, $p \mid 0$, $p \nmid 1$ und $p^2 \nmid p$. Da $\operatorname{ggT}(1, 0, -p) = 1$, ist f_n auch irreduzibel in $\mathbb{Z}[X]$. Für $n \geq 2$ folgt, dass $\sqrt[n]{p} \notin \mathbb{Q}$. (Wäre $\sqrt[n]{p} \in \mathbb{Q}$, so würde wegen Satz 168 (i) folgen, dass $\big(X - \sqrt[n]{p}\big) \mid (X^n - p)$ und $X^n - p$ wäre nicht irreduzibel in $\mathbb{Q}[X]$, ein Widerspruch.)

Lemma 186: Es sei R ein Integritätsbereich, $\alpha \in R^*$ und $\beta \in R$.

(i) Die Abbildung $R[X] \to R[X]$, $p(X) \mapsto p(\alpha X + \beta)$ ist ein Isomorphismus,

(ii) Für $p \in R[X]$ gilt: $p(X)$ ist irreduzibel (in $R[X]$)
$\Leftrightarrow p(\alpha X + \beta)$ ist irreduzibel (in $R[X]$).

Beweis: (i) Die Abbildung $\Phi : R[X] \to R[X]$, $p(X) \mapsto p(\alpha X+\beta)$ ist ein Homomorphismus, da es sich um einen Einsetzhomomorphismus handelt (mit $S = R[X]$ und $c = \alpha X + \beta$ mit den Bezeichnungen von Korollar 164). Aus dem selben Grund ist die Abbildung $R[X] \to R[X]$, $p(X) \mapsto p\big(\alpha^{-1}(X - \beta)\big) = p(\alpha^{-1}X - \alpha^{-1}\beta)$ ein Homomorphismus, der zu Φ invers ist (da $\alpha^{-1}\big((\alpha X + \beta) - \beta\big) = \alpha\big(\alpha^{-1}(X - \beta)\big) + \beta = X$). Daher ist Φ bijektiv und ein Isomorphismus.
(ii) Ist $p \in R$, so ist $p(X) = p(\alpha X + \beta)$ und Behauptung ist erfüllt. Es sei darum nun $p \in R[X] \setminus R$. Ist $p(X)$ reduzibel, so gibt es $q_1, q_2 \in R[X] \setminus R^*$, sodass $p(X) = q_1(X)q_2(X)$ und daher $p(\alpha X + \beta) = q_1(\alpha X + \beta)q_2(\alpha X + \beta)$ und $p(\alpha X + \beta)$ ist ebenfalls reduzibel. Ist $p(\alpha X + \beta)$ reduzibel, so gibt es $q_1, q_2 \in R[X] \setminus R^*$, sodass $p(\alpha X + \beta) = q_1(X)q_2(X)$ und daher $p(X) = q_1\big(\alpha^{-1}(X - \beta)\big)q_2\big(\alpha^{-1}(X - \beta)\big)$, d.h. $p(X)$ ist ebenfalls reduzibel.

Beispiel: Auf $p(X) = X^2 + X + 2 \in \mathbb{Z}[X]$ kann man das Eisensteinkriterium nicht direkt anwenden, aber auf $p(X+3) = (X+3)^2+(X+3)+2 = X^2+7X+14$ kann man es anwenden (da $7 \mid 14$, $7 \mid 7$, $7 \nmid 1$ und $49 \nmid 14$). Nach Satz 185 ist $p(X + 3) = X^2 + 7X + 14$ irreduzibel in $\mathbb{Z}[X]$. Lemma 186 impliziert, dass auch $p(X) = X^2 + X + 2$ in $\mathbb{Z}[X]$ irreduzibel ist.

Satz 187 (Reduktionskriterium): Es sei R ein faktorieller Ring, P ein Primideal von R und $p \in R[X]$ primitiv, wobei

$$p(X) = \sum_{i=0}^{n} a_i X^i$$

mit $\operatorname{grad} p = n \geq 1$ und $a_n \notin P$ gelten soll. Weiters bezeichne π den Epimorphismus $\pi : R \to R/P$, $\pi(a) = a + P$ und $\pi^* : R[X] \to R/P[X]$ seine Fortsetzung (wie in Korollar 166). Dann gilt: Ist

$$\pi^*(p)(X) = \sum_{i=0}^{n} \pi(a_i) X^i$$

irreduzibel in $R/P[X]$, so ist p irreduzibel in $R[X]$.

Beweis: Wir nehmen an, p sei reduzibel in $R[X]$. Dann gibt es $f, g \in R[X] \setminus R^*$ mit der Eigenschaft $p = fg$. Da p primitiv ist, muss $\operatorname{grad} f \geq 1$ und $\operatorname{grad} g \geq 1$ gelten. Dann ist $\pi^*(p) = \pi^*(f)\pi^*(g)$. Da $a_n \notin P$, ist $\pi(a_n) \neq 0$ und daher $\operatorname{grad} \pi^*(p) = \operatorname{grad} p$. Wegen

$$\operatorname{grad} f + \operatorname{grad} g = \operatorname{grad} p = \operatorname{grad} \pi^*(p) = \operatorname{grad} \pi^*(f) + \operatorname{grad} \pi^*(g)$$

und $\operatorname{grad} \pi^*(f) \leq \operatorname{grad} f$ und $\operatorname{grad} \pi^*(g) \leq \operatorname{grad} g$ muss auch $\operatorname{grad} \pi^*(f) = \operatorname{grad} f$ und $\operatorname{grad} \pi^*(g) = \operatorname{grad} g$ gelten. Also ist auch $\pi^*(p)$ reduzibel in $R/P[X]$.

Bemerkung: Ein wichtiger Spezialfall von Satz 187 ist $R = \mathbb{Z}$ und die Reduktion modulo einer Primzahl p (d.h. $P = (p) = p\mathbb{Z}$). In diesem Fall ist $R/P = \mathbb{Z}/(p) = \mathbb{Z}_p$ ein endlicher Körper. Daher gibt es nur endlich viele Polynome, die $\pi^*(p)$ in $R/P[X] = \mathbb{Z}_p[X]$ teilen könnten.

Beispiel: Es sei wieder $p(X) = X^2 + X + 2 \in \mathbb{Z}[X]$ (d.h. $R = \mathbb{Z}$) und $P = (3) = 3\mathbb{Z}$. Dann ist $\pi : \mathbb{Z} \to \mathbb{Z}_3$, $\pi(a) = \overline{a}$ und $\pi^* : \mathbb{Z}[X] \to \mathbb{Z}_3[X]$. Wäre $\pi^*(p) = X^2 + X + \overline{2}$, reduzibel, so wäre es Produkt zweier linearer Polynome und würde daher eine Nullstelle in $\mathbb{Z}_3$ besitzen. Das ist wegen $0^2 + 0 + 2 \equiv 2 \pmod 3$, $1^2 + 1 + 2 \equiv 1 \pmod 3$ und $2^2 + 2 + 2 \equiv 2 \pmod 3$ aber nicht der Fall. Also ist $\pi^*(p)$ irreduzibel in $\mathbb{Z}_3[X]$ und daher p irreduzibel in $\mathbb{Z}[X]$.

Anhang: Polynomringe in mehreren Unbestimmten

Völlig analog zu Polynomringen in einer Unbestimmten kann man Polynomringe in mehreren Unbestimmten folgendermaßen einführen: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und $n \in \mathbb{N} \setminus \{0\}$. Wir setzen

$$I = \{0, 1, 2, 3, \dots\}^n = \{(k_1, \dots, k_n) \in \mathbb{Z}^n \mid k_1, \dots, k_n \geq 0\}.$$

und bezeichnen mit $R^{(I)}$ die Menge aller Abbildungen $I \to R$ mit der Eigenschaft, dass $f(k_1, \dots, k_n) = 0$ für alle bis auf endlich viele $(k_1, \dots, k_n) \in I$. Versieht man $R^{(I)}$ mit der Addition $(f + g)(k) = f(k) + g(k)$ für alle $k \in I$ und der Multiplikation

$$(f \cdot g)(k) = \sum_{\substack{\ell, m \in I \\ \ell + m = k}} f(\ell) g(m) \quad \text{für alle } k \in I,$$

so wird $R^{(I)}$ dadurch zu einem kommutativen Ring mit Eins. Man bettet nun R durch die folgende Abbildung in $R^{(I)}$ ein: $\varphi : R \to R^{(I)}$, $a \mapsto f_a$, wobei

$$f_a(k_1, \dots, k_n) = \begin{cases} a & \text{falls } (k_1, \dots, k_n) = (0, \dots, 0) \\ 0 & \text{sonst} \end{cases}$$

und identifiziert a mit f_a. Dadurch kann man R als Unterring von $R^{(I)}$ auffassen. Setzt man (für $1 \leq i \leq n$)

$$X_i(k_1, \dots, k_n) = \begin{cases} 1 & \text{falls } k_i = 1 \text{ und } k_1 = \cdots = k_{i-1} = k_{i+1} = \cdots = k_n = 0 \\ 0 & \text{sonst} \end{cases}$$

so besitzt jedes $f \in R^{(I)}$ eine eindeutige Darstellung

$$f = \sum_{k_1,\dots,k_n \geq 0} a_{k_1,\dots,k_n} X_1^{k_1} \cdots X_n^{k_n},$$

wobei $a_{k_1,\dots,k_n} \in R$ und $a_{k_1,\dots,k_n} \neq 0$ nur für endlich viele $(k_1,\dots,k_n) \in I$. Man verwendet statt $R^{(I)}$ die Bezeichnung $R[X_1,\dots,X_n]$ und spricht vom Polynomring in den Unbestimmten $X_1,\dots,X_n$ mit Koeffizienten in R. Es gilt ein Analogon zu Satz 163, insbesondere gibt es wieder einen Einsetzhomomorphismus. Der Polynomring besitzt die Eigenschaft

$$R[X_1,\dots,X_n,X_{n+1}] \cong R[X_1,\dots,X_n][X_{n+1}],$$

die man auch für seine Definition verwenden kann. Mit Induktion nach n kann man nun folgendes beweisen:

Satz: Ist R ein Integritätsbereich, so ist $R[X_1,\dots,X_n]$ ein Integritätsbereich.

Das verallgemeinert Korollar 156 (i), das Induktionsanfang und Induktionsschritt liefert. Insbesondere sind $K[X_1,\dots,X_n]$ (mit K ein Körper), $\mathbb{Z}[X_1,\dots,X_n]$, $\mathbb{Z}[i][X_1,\dots,X_n]$ und $\mathbb{Z}\big[\sqrt{2}\big]\,[X_1,\dots,X_n]$ Integritätsbereiche.

Ist R ein Integritätsbereich, so bezeichnet man den Quotientenkörper von $R[X_1,\dots,X_n]$ mit $R(X_1,\dots,X_n)$ und spricht vom Körper der rationalen Funktionen.

Satz: Ist R ein faktorieller Ring, so ist $R[X_1,\dots,X_n]$ ein faktorieller Ring.

Das verallgemeinert Satz 184, der Induktionsanfang und Induktionsschritt liefert. Insbesondere sind $K[X_1,\dots,X_n]$ (wenn K ein Körper ist), $\mathbb{Z}[X_1,\dots,X_n]$, $\mathbb{Z}[i][X_1,\dots,X_n]$ und $\mathbb{Z}\big[\sqrt{2}\big]\,[X_1,\dots,X_n]$ faktorielle Ringe.