G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 10

Aufgabe 40.

Die Situation soll sich laut Aufgabenstellung wie folgt darstellen.

$$\begin{tikzcd}
\mathbf{Q}[X]/(f(X)) \arrow[r, "\sim"] & \mathbf{Q}[\alpha] = \mathbf{Q}(\alpha) \\
\mathbf{Z}[X]/(f(X)) \arrow[u, hook] \arrow[r, "\sim"] & \mathbf{Z}[\alpha] \arrow[u, hook]
\end{tikzcd}$$

(1) Da $f(X)$ in $\mathbf{Z}[X]$ irreduzibel ist, und folglich prim, ist $\mathbf{Z}[X]/(f(X))$ ein Integritätsbereich. Es hat also einen Sinn, von $\operatorname{Quot}(\mathbf{Z}[X]/(f(X)))$ zu reden. Da $f(X)$ auch in $\mathbf{Q}[X]$ noch irreduzibel ist, ist $\mathbf{Q}[X]/(f(X))$ ein Körper.

Zeigen wir zunächst, daß der Ringmorphismus

$$\begin{array}{ccc}
\mathbf{Z}[X]/(f(X)) & \xrightarrow{i} & \mathbf{Q}[X]/(f(X)) \\
\bar{X} & \longmapsto & \bar{X}
\end{array}$$

injektiv ist. Wird $h(\overline{X})$ auf 0 abgebildet, so heißt dies, es ist $f(X)$ ein Teiler von $h(X)$ in $\mathbf{Q}[X]$. Da das irreduzible Polynom $f(X)$ wegen $\deg f(X) \geq 1$ primitiv zu sein hat, ist $f(X)$ auch ein Teiler von $h(X)$ in $\mathbf{Z}[X]$. Also ist $h(\bar{X}) = 0$.

Nun können wir jedes Element von $\mathbf{Q}[X]$ schreiben als $a^{-1}h(X)$ mit einem $a \in \mathbf{Z} \smallsetminus \{0\}$ und einem $h(X) \in \mathbf{Z}[X]$. Diese Eigenschaft überträgt sich auf die Quotienten modulo dem jeweils von $f(X)$ erzeugten Ideal, d.h. es ist jedes Element von $\mathbf{Q}[X]/(f(X))$ schreibbar in der Form $i(h(\bar{X}))i(a)^{-1}$, wie zu zeigen.

(2) Der $\mathbf{Q}$-Algebrenmorphismus $\mathbf{Q}[X]/(f(X)) \longrightarrow \mathbf{Q}[\alpha]$, $\bar{X} \longmapsto \alpha$ ist zunächst wohldefiniert wegen $f(\alpha) = 0$ und surjektiv wegen der Definition von $\mathbf{Q}[\alpha]$. Zeigen wir die Injektivität. Ist $g \in \mathbf{Q}[X]$ gegeben mit $g(\alpha) = 0$, so haben wir zu zeigen, daß $f(X)$ ein Teiler von $g(X)$ in $\mathbf{Q}[X]$ ist. Betrachten wir hierzu das Ideal

$$\{h(X) \in \mathbf{Q}[X] \mid h(\alpha) = 0\} \subseteq \mathbf{Q}[X]\ .$$

Sei es von $\tilde{f}(X) \in \mathbf{Q}[X]$ erzeugt. Dann ist $\tilde{f}(X)$ ein Teiler von $f(X)$. Da $(\tilde{f}(X)) \neq (1)$, ist wegen $f(X)$ irreduzibel $(\tilde{f}(X)) = (f(X))$. Insbesondere ist $g(X) \in (\tilde{f}(X)) = (f(X))$, wie zu zeigen.

Da $\mathbf{Q}[\alpha]$ demgemäß (oder nach 35 (4)) bereits ein Körper ist, ist dieser Ring auch der kleinste Teilkörper von $\mathbf{C}$, der α enthält, i.e. $\mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$.

(3) Der $\mathbf{Z}$-Algebrenmorphismus (i.e. Ringmorphismus) $\mathbf{Z}[X]/(f(X)) \longrightarrow \mathbf{Z}[\alpha]$, $\bar{X} \longmapsto \alpha$ ist zunächst wohldefiniert wegen $f(\alpha) = 0$ und surjektiv wegen der Definition von $\mathbf{Z}[\alpha]$. Das bislang erreichte Diagramm

$$\begin{tikzcd}
\mathbf{Q}[X]/(f(X)) \arrow[r, "\sim"] & \mathbf{Q}[\alpha] = \mathbf{Q}(\alpha) \\
\mathbf{Z}[X]/(f(X)) \arrow[u, hook] \arrow[r] & \mathbf{Z}[\alpha] \arrow[u, hook]
\end{tikzcd}$$

zeigt nun seine Injektivität (die erste Abbildung in Komposition zu einer Injektion ist injektiv).

Aufgabe 41.

(1) Wir behaupten, daß $\mathbf{Z}[i]$ ein Hauptidealbereich, und damit auch faktoriell ist. Genauer, wir wollen zeigen, daß $\mathbf{Z}[i]$ euklidsch ist.

Es ist $\mathbf{Z}[i] \simeq \mathbf{Z}[X]/(X^2+1)$ nach 41 (3), und also $\mathbf{Z}[i] = \{a + bi \mid a,\, b \in \mathbf{Z}\}$.

Sei $\delta(a + bi) := a^2 + b^2$ für $a + bi \in \mathbf{Z}[i] \smallsetminus \{0\}$. Seien $x \in \mathbf{Z}[i]$ und $y \in \mathbf{Z}[i] \smallsetminus \{0\}$ vorgegeben. Wir müssen $r,\, s \in \mathbf{Z}[i]$ so finden, daß $x = ys + r$ mit $\delta(r) < \delta(y)$ oder mit $r = 0$.

Schreibe $\frac{x}{y} = u + vi$ mit $u,\ v\ \in\ \mathbf{Q}$. Sei $m \in \mathbf{Z}$ mit $|m - u| \le \frac{1}{2}$ und $n \in \mathbf{Z}$ mit $|n - v| \le \frac{1}{2}$. Sei $s := m + ni$. Dann ist

$$\left|\frac{x}{y} - s\right| \;=\; ((m-u)^2 + (n-v)^2)^{1/2} \;\le\; \frac{\sqrt{2}}{2} \;<\; 1\;.$$

Also ist $r = x - ys = 0$ oder $\delta(r) = |x - ys|^2 < |y|^2 = \delta(y)$.

(2) Wir behaupten, daß $\mathbf{Z}[\zeta_3]$ ein Hauptidealbereich, und damit auch faktoriell ist. Genauer, wir wollen zeigen, daß $\mathbf{Z}[\zeta_3]$ euklidsch ist.

Es ist $\mathbf{Z}[\zeta_3] \simeq \mathbf{Z}[X]/(X^2 + X + 1)$ nach 41 (3), und also $\mathbf{Z}[\zeta_3] = \{a + b\zeta_3 \,|\, a,\ b\ \in\ \mathbf{Z}\}$.

Sei allgemein auf $\mathbf{Q}(\zeta_3)$ die Norm

$$\mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(u + v\zeta_3) \;:=\; (u + v\zeta_3)(u + v\zeta_3^2) \;=\; u^2 + v^2 - uv \;(\ge (u-v)^2 \ge 0)$$

für $u + v\zeta_3 \in \mathbf{Q}(\zeta_3)$ definiert. Es ist $\mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(xy) = \mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(x)\,\mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(y)$ für $x, y \in \mathbf{Q}(\zeta_3)$.

Sei $\delta(a + b\zeta_3) := \mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(a + b\zeta_3)$ für $a + b\zeta_3\ \in\ \mathbf{Z}[\zeta_3] \smallsetminus \{0\}$. Seien $x\ \in\ \mathbf{Z}[\zeta_3]$ und $y \in \mathbf{Z}[\zeta_3] \smallsetminus \{0\}$ vorgegeben. Wir müssen $r,\ s\ \in\ \mathbf{Z}[\zeta_3]$ so finden, daß $x = ys + r$ mit $\delta(r) < \delta(y)$ oder mit $r = 0$.

Schreibe $\frac{x}{y} = u + v\zeta_3$ mit $u,\ v\ \in\ \mathbf{R}$. Sei $m \in \mathbf{Z}$ mit $|m - u| \le \frac{1}{2}$ und $n \in \mathbf{Z}$ mit $|n - v| \le \frac{1}{2}$. Sei $s := m + n\zeta_3$. Dann ist

$$\mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}\left(\frac{x}{y} - s\right) \;=\; ((m-u)^2 + (n-v)^2 - (m-u)(n-v))^{1/2} \;\le\; \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right)^{1/2} \;=\; \frac{\sqrt{3}}{2} \;<\; 1\;.$$

Also ist $r = x - ys = 0$ oder $\delta(r) = \delta(x - ys) = \mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(x - ys) = \mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}\left(\frac{x}{y} - s\right)\mathrm{N}_{\mathbf{Q}(\zeta_3)|\mathbf{Q}}(y) < \delta(y)$.

(3) Wir behaupten, daß $\mathbf{Z}[\sqrt{-13}]$ nicht faktoriell, und damit auch kein Hauptidealbereich ist. Dazu wollen wir darin ein irreduzibles Element angeben, das nicht prim ist.

Es ist $\mathbf{Z}[\sqrt{-13}] \simeq \mathbf{Z}[X]/(X^2 + 13)$ nach 41 (3), und also $\mathbf{Z}[\sqrt{-13}] = \{a + b\sqrt{-13}\,|\, a,\ b\ \in\ \mathbf{Z}\}$.

Wir behaupten, daß 2 nicht prim ist. Es teilt 2 das Produkt $(1 + \sqrt{-13})(1 - \sqrt{-13}) = 14$, aber keinen der beiden Faktoren.

Wir behaupten, daß 2 irreduzibel ist. Sei dazu

$$2 \;=\; (a + b\sqrt{-13})(c + d\sqrt{-13}) \;=\; (ac - 13bd) + (ad + bc)\sqrt{-13}$$

angesetzt, mit $a,\ b,\ c,\ d\ \in\ \mathbf{Z}$. Ist $b = 0$, so ist a ein Teiler von 2, also $a = \pm 1$ oder $a = \pm 2$, was keine nichttriviale Zerlegung liefert. Ist $b \ne 0$, dann folgt aus $bc = -ad$ und aus $ac - 13bd = 2$, daß

$$2b \;=\; abc - 13b^2 d \;=\; -a^2 d - 13b^2 d \;=\; -d(a^2 + 13b^2)\;.$$

Insbesondere ist $d \ne 0$, und

$$4b^2 \;=\; d^2(a^2 + 13b^2)^2 \;\ge\; (a^2 + 13b^2)^2 \;\ge\; 169b^4 > 4b^2$$

wegen $b \ne 0$, was nicht geht. Dies zeigt, daß 2 irreduzibel ist.

Alternativ, definiere auf $\mathbf{Q}(\sqrt{-13})$ die Norm durch

$$\mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(u + v\sqrt{-13}) \;:=\; (u + v\sqrt{-13})(u - v\sqrt{-13}) \;=\; u^2 + 13v^2$$

für $u + v\sqrt{-13} \in \mathbf{Q}(\sqrt{-13})$. Es ist $\mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(xy) = \mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(x)\,\mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(y)$ für $x,\ y\ \in\ \mathbf{Q}(\sqrt{-13})$.

Es ist $\mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(2) = 4$. Ein Teiler von 2 in $\mathbf{Z}[\sqrt{-13}]$ hat eine Norm, die 4 teilt. Als Teiler in Frage kommen also nur ± 1 und ± 2, alle anderen Elemente von $\mathbf{Z}[\sqrt{-13}]$ haben zu große Norm. Dies zeigt erneut, daß 2 irreduzibel ist.

Daß $\mathbf{Z}[\sqrt{-13}]$ kein Hauptidealbereich ist, läßt sich am Ideal $(2, 1 + \sqrt{-13})$ auch direkt erkennen. Denn es ist $\mathbf{Z}[\sqrt{-13}]/(2, 1 + \sqrt{-13}) \simeq \mathbf{F}_2[X]/(X^2 + 13, X + 1) = \mathbf{F}_2[X]/(X + 1) \simeq \mathbf{F}_2$ von Kardinalität 2. Dagegen ist $\mathbf{Z}[\sqrt{-13}]/(x)$ von Kardinalität $\mathrm{N}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}(x)$ für $x\ \in\ \mathbf{Z}[\sqrt{-13}]$. Und es gibt in $\mathbf{Z}[\sqrt{-13}]$ kein Element von Norm 2. Also ist $(2, 1 + \sqrt{-13})$ kein Hauptideal.

Aufgabe 42.

- Sei $\mathfrak{p} \neq 0$. Wir haben zu zeigen, daß entweder (ii) oder (iii) zutreffen.

  Betrachten wir den **Fall,** daß es ein Primelement $p \in R \smallsetminus \{0\}$ gibt mit $p \in \mathfrak{p}$. Falls $(p) = \mathfrak{p}$, so trifft (ii) zu, und wir sind fertig.

  Falls $(p) \subsetneq \mathfrak{p}$, so sei $k := R/(p)$, und sei $\bar{\mathfrak{p}}$ das Bild von $\mathfrak{p}$ in $k[X]$ unter der koeffizientenweisen Restklassenabbildung $R[X] \xrightarrow{\varphi} k[X]$. Es ist $R[X]/\mathfrak{p} \xrightarrow{\sim} k[X]/\bar{\mathfrak{p}}$ ein Integritätsbereich, und also ist $\bar{\mathfrak{p}}$ prim und ungleich 0 in $k[X]$.

  Sei $h(X) \in R[X]$ normiert von Grad ≥ 1 derart gewählt, daß sein Bild $\overline{h(X)}$ in $k[X]$ das Primideal $\bar{\mathfrak{p}}$ erzeugt. Dann ist $\mathfrak{p} = \varphi^{-1}(\bar{\mathfrak{p}}) = \varphi^{-1}(\ (\overline{h(X)})\ ) = (p, h(X))$, und (iii) trifft zu.

  Betrachten wir den **Fall,** daß es kein Primelement $p \in R \smallsetminus \{0\}$ gibt mit $p \in \mathfrak{p}$. In anderen Worten, sei $\mathfrak{p} \cap R = 0$. Sei n der minimale Grad eines in $\mathfrak{p} \smallsetminus \{0\}$ auftauchenden Polynoms. Sei für $m \geq n$ das Ideal

  $$\mathfrak{a}_m \ :=\ \{a \in R \mid \text{es gibt ein Polynom in } \mathfrak{p} \smallsetminus \{0\} \text{ von Grad } m \text{ mit Leitkoeffizient } a\ \} \cup \{0\}\ \subseteq\ R$$

  definiert. Da R ein Hauptidealbereich ist, können wir $\mathfrak{a}_m = (a_m)$ mit je einem $a_m \in R$ schreiben. Wähle für jedes $m \geq n$ ein $g_m(X) \in \mathfrak{p} \smallsetminus \{0\}$ von Grad m mit Leitkoeffizient a_m. Es ist $g_m(X)$ insbesondere primitiv für alle $m \geq n$. Speziell ist also $n \geq 1$, da $\mathfrak{p} \neq R$.

  Es ist $g_n(X)$ irreduzibel in $R[X]$, da ansonsten wegen $\mathfrak{p}$ prim ein Polynom von Grad $< n$ in $\mathfrak{p} \smallsetminus \{0\}$ aufträte, oder aber ein Primelement $p \in R \smallsetminus \{0\}$ in $\mathfrak{p}$ enthalten wäre, was beides im vorliegenden Fall ausgeschlossen ist. Da $R[X]$ faktoriell ist, ist $g_n(X)$ damit auch prim.

  Wir *behaupten,* daß $\mathfrak{p} = (g_n(X))$. Sei $f(X) \in \mathfrak{p} \smallsetminus \{0\}$. Zu zeigen ist $f(X) \in (g_n(X))$. Wir führen eine Induktion über $\deg f$. Schreibe $m = \deg f$, und sei b der Leitkoeffizient von $f(X)$.

  Es ist $f(X) - \frac{b}{a_m} g_m(X)$ gleich 0 oder von Grad $< m$. Ist es gleich 0, so ist $f(X) \in (g_m(X))$. Ist es von Grad $< m$, so ist nach Induktion $f(X) - \frac{b}{a_m} g_m(X) \in (g_n(X))$ und also $f(X) \in (g_m(X), g_n(X))$. Es bleibt somit $g_m(X) \in (g_n(X))$ zu zeigen.

  Wegen $X^{m-n} g_n(X) \in \mathfrak{p} \smallsetminus \{0\}$ von Grad m mit Leitkoeffizient a_n ist a_m ein Teiler von a_n. Mit Induktion ist $X^{m-n} g_n(X) - \frac{a_n}{a_m} g_m(X) \in (g_n(X))$, also $\frac{a_n}{a_m} g_m(X) \in (g_n(X))$. Da $g_n(X)$ prim ist, und da $n \geq 1$, ist $g_n(X)$ ein Teiler von $g_m(X)$. Dies zeigt die Behauptung, es trifft also (ii) zu.

- Enthalte nun R unendlich viele Primideale. Wann liegt ein maximales Ideal vor?

  Im Fall (i) ist $\mathfrak{p} = 0$ kein maximales Ideal, da $R[X]/\mathfrak{p} \simeq R[X]$ kein Körper ist – z.B. ist $X \in R[X] \smallsetminus (R[X]^* \cup \{0\})$.

  Im Fall (ii) *behaupten* wir, daß $\mathfrak{p} = (g(X))$ kein maximales Ideal ist.

  Ist $\deg g(X) = 0$, so ist $g(X) =: q$ ein Primelement in $R \smallsetminus 0$, und $R[X]/(q) \simeq (R/(q))[X]$ als Polynomring über einem Körper selbst kein Körper.

  Sei nun $\deg g(X) \geq 1$. Sei a der Leitkoeffizient von $g(X)$. Es liegt (a) in endlich vielen Primidealen, nämlich in genau denen, die von Primteilern von a erzeugt werden. Da R nach Voraussetzung unendlich viele Primideale enthält, können wir einen Erzeuger p eines Primideals ungleich 0 wählen, welches nicht (a) enthält. Wäre p invertierbar in $R[X]/\mathfrak{p}$, so wäre $1 - pf(X) \in (g(X))$ für ein $f(X) \in R[X]$, also $1 - pf(X) = g(X)w(X)$ für ein $w(X) \in R[X]$, und also $1 = \overline{g(X)}\,\overline{w(X)}$ in $(R/(p))[X]$. Nun hat das Bild $\overline{g(X)}$ von $g(X)$ in $(R/(p))[X]$ ebenfalls Grad $n \geq 1$, da $a \not\equiv_p 0$, und damit ist $0 = \deg 1 = \deg \overline{g(X)} + \deg \overline{w(X)} \geq 1$, Widerspruch. Also ist p weder invertierbar noch gleich 0 in $R[X]/\mathfrak{p}$, und dieser Quotient mithin kein Körper. Dies zeigt die Behauptung.

  Im Fall (iii) ist $\mathfrak{p} = (p, h(X))$ ein maximales Ideal, da $R[X]/\mathfrak{p} \simeq (R/(p))[X]/(\overline{h(X)})$ ein Körper ist.

Aufgabe 43.

(1) Ist ein Primideal. In der Tat ist $X^{12} + 55X^7 + 125X^3 - 505X + 5$ nach dem Eisensteinkriterium irreduzibel.

(2) Ist kein Primideal. In der Tat ist $X^2 + 30X + 125 = (X + 5)(X + 25)$ reduzibel. (Eisenstein hilft nicht!)

(3) Ist ein Primideal. Substitution $X \longmapsto X - 1$ (i.e. das Bild unter diesem Ringautomorphismus von $\mathbf{Z}[X]$) gibt

$$(X-1)^5 - (X-1)^4 + (X-1)^3 + (X-1)^2 + 2(X-1) + 1 \ = \ X^5 - 6X^4 + 15X^3 - 18X^2 + 12X - 3\ ,$$

welches mit Eisenstein irreduzibel ist.

(4) Wir haben die $\mathbf{Q}$-Algebrenmorphismen

$$\begin{array}{rcl} \mathbf{Q}[X,Y]/(X^2-Y, X-Y^2) & \xrightarrow{\sim} & \mathbf{Q}[Y]/(Y^4-Y) \\ \bar{X} & \longmapsto & \bar{Y}^2 \\ \bar{Y} & \longmapsto & \bar{Y} \\ \bar{Y} & \longleftarrow\!\shortmid & \bar{Y}\,, \end{array}$$

die beide wohldefiniert sind und sich gegenseitig invertieren.

Nun ist $\mathbf{Q}[Y]/(Y^4-Y)$ kein Körper, da $Y^4-Y = (Y^2+Y+1)(Y-1)Y$ nicht irreduzibel ist.

Alternativ, nehmen wir einmal an, $\mathfrak{a} := (X^2-Y, X-Y^2)$ sei prim. Dann ist wegen $\mathfrak{a} \ni (X^2-Y) - X(X-Y^2) = Y(XY-1)$ das Polynom Y oder das Polynom $XY-1$ in $\mathfrak{a}$. Nun ist $\mathbf{Q}[X,Y]/\mathfrak{a} \longrightarrow \mathbf{Q}$, $X \longmapsto 1$, $Y \longmapsto 1$ wohldefiniert. Ist $Y \in \mathfrak{a}$, so muß es auf 0 abgebildet werden, was nicht der Fall ist. Also ist $XY-1 \in \mathfrak{a}$. Nun hat aber kein Element in $\mathfrak{a}$ einen konstanten Term ungleich 0, und wir sind an einem Widerspruch angelangt.

Das erste Argument hilft immer dann, wenn eine Variable in einem Idealerzeuger isoliert werden kann, wie hier X. Dann kann man in den Idealerzeugern einsetzen und diese Variable unterschlagen, wie hier geschehen.

Die zweite Art von Argument lautet: gewisse Idealelemente in verdächtig aussehende Faktoren zerlegen. Auch das geht nur in Einzelfällen.

Ein methodisches Vorgehen haben wir keines kennengelernt.

(5) Wir behaupten, daß das Ideal $\mathfrak{a} = (X^2-Y, X-Y^2-1)$ prim ist.

Wir haben $\mathbf{Q}$-Algebrenmorphismen

$$\begin{array}{rcl} \mathbf{Q}[X,Y]/(X^2-Y, X-Y^2-1) & \xrightarrow{\sim} & \mathbf{Q}[Y]/((Y^2+1)^2-Y) \\ \bar{X} & \longmapsto & \bar{Y}^2+1 \\ \bar{Y} & \longmapsto & \bar{Y} \\ \bar{Y} & \longleftarrow\!\shortmid & \bar{Y}\,, \end{array}$$

die beide wohldefiniert sind und sich gegenseitig invertieren.

Bleibt zu zeigen, daß $((Y^2+1)^2-Y) = Y^4+2Y^2-Y+1$ irreduzibel ist. Dazu genügt es zu zeigen, daß das Bild Y^4+Y+1 in $\mathbf{F}_2[Y]$ irreduzibel ist (vgl. 44 (2)). Linearfaktor gibt es mangels Nullstelle keinen. Als irreduzibler Faktor von Grad 2 kommt nur Y^2+Y+1 in Frage, welcher aber kein Teiler ist, da $Y^4+Y+1 = (Y^2+Y+1)(Y^2+Y)+1$.

Um diese Aufgabe mit Aufgabe 40 in Deckung zu bringen, bemerken wir, daß bei Verwendung von $R = \mathbf{Q}[Y]$ sich $(X^2-Y, X-Y^2-1) = (\underbrace{Y^4+2Y^2-Y+1}_{=p}, \underbrace{X-Y^2-1}_{=h(X)})$ ergibt, oder aber, bei Verwendung von $R = \mathbf{Q}[X]$, daß $(X^2-Y, X-Y^2-1) = (\underbrace{X^4-X+1}_{=p}, \underbrace{Y-X^2}_{=h(Y)})$.

Aufgabe 44.

(1) Die Aussage ist falsch. Sei e.g. $R = \mathbf{Z}[X]$, $x = X$ und $y = 2$. Dann ist $\mathrm{ggT}(X,2) = 1$, aber $(X,2) \subsetneq (1)$, da $\mathbf{Z}[X]/(2,X) \simeq \mathbf{F}_2[X]/(X) \simeq \mathbf{F}_2 \neq 0$.

Ist hingegen R ein Hauptidealbereich, so trifft die Aussage zu.

(2) Die Aussage ist richtig. Denn hätte man eine Zerlegung $f(X) = g(X)h(X)$ in Nichteinheiten $g(X)$ und $h(X)$ aus $\mathbf{Z}[X]$, so wären beide normiert und daher von Grad ≥ 1. Dies lieferte eine nichttriviale Zerlegung $f(X) = \overline{g(X)}\,\overline{h(X)}$ in $\mathbf{F}_p[X]$.

(3) Die beiden Aussagen sind richtig. Es ist $nX-m$ primitiv, und wie auch $X-\frac{m}{n}$ ein Teiler von $f(X)$ in $\mathbf{Q}(X)$. Also gibt es ein primitives Polynom $h(X)$ und ein $r \in \mathbf{Q}$ mit $(nX-m)(rh(X)) = f(X)$. Da nach Gauß' Lemma $(nX-m)h(X)$ primitiv ist, ist $r \in \mathbf{Z}$. Also ist n ein Teiler von a und m ein Teiler von b.

(4) Die Aussage ist falsch. Sei e.g. $p \in \mathbf{Z}_{>0}$ prim, sei $R = \mathbf{Z}_{(p)}$, und sei $\mathfrak{p} = (pX-1)$. Es ist $pX-1$ irreduzibel, da linear und primitiv. Da $\mathbf{Z}_{(p)}[X]$ faktoriell ist, ist $(pX-1)$ in der Tat ein Primideal. Betrachte den Ringmorphismus

$$\begin{array}{rcl} \mathbf{Z}_{(p)}[X]/(pX-1) & \longrightarrow & \mathbf{Q} \\ X & \longmapsto & \frac{1}{p}\,. \end{array}$$

Dieser ist surjektiv, da sich jedes Element von $\mathbf{Q}$ schreiben läßt als $p^{-n}x$ mit $n \geq 0$ und $x \in \mathbf{Z}_{(p)}$. Wir *behaupten,* daß er injektiv ist. Ein Polynom $f(X) \in \mathbf{Z}_{(p)}[X]$, für welches $f(\frac{1}{p}) = 0$ gilt, ist in $\mathbf{Q}[X]$ durch $X - \frac{1}{p}$ und also dort auch durch $pX - 1$ teilbar ist. Da $pX - 1$ primitiv ist, ist $f(X)$ auch in $\mathbf{Z}[X]$ durch $pX - 1$ teilbar.

(5) Die Aussage ist falsch. Sei z.B. $f(X) = 2$. Es ist $\mathbf{Z}[X]/(2) \simeq \mathbf{F}_2[X]$, wohingegen $\mathbf{Q}[X]/(2) \simeq 0$. Die angegebene Abbildung kann also nicht injektiv sein.

(6) Die Aussage ist richtig. Denn es ist $\mathbf{F}_p^* \simeq C_{p-1}$. Sei $a \in \mathbf{F}_p$ ein Erzeuger dieser Gruppe. Dann hat a die Ordnung $p-1$, und also hat $a^{(p-1)/2}$ die Ordnung 2. Ein Element von Ordnung 2 in $\mathbf{F}_p^*$ ist Nullstelle von $X^2 - 1 = (X-1)(X+1)$ und ungleich 1, also gleich -1. Insgesamt ist also $a^{(p-1)/2} = -1$ in $\mathbf{F}_p$.