Übungen zur Vorlesung Algebra 1

Lösungen zu Blatt 1

Aufgabe 1

(i) *Bestimmen Sie die Punkte von* $\operatorname{Spec} \mathbb{Z}$. *Welche sind abgeschlossen und welche nicht?*

Lösung: $\mathbb{Z}$ ist ein Integritätsbereich, also ist das Nullideal (0) ein Primideal. Außerdem ist $\mathbb{Z}$ ein Hauptidealring, also sind alle weiteren Primideale in $\mathbb{Z}$ genau jene Hauptideale, die von einem primen Element in $\mathbb{Z}$ erzeugt werden. Eine ganze Zahl $z \in \mathbb{Z}$ ist prim, wenn sie von der Gestalt $z = \pm p$ für eine Primzahl $p \in \mathbb{P} = \{2, 3, 5, ...\}$ ist. Allerdings stimmen zwei Hauptideale genau dann überein, wenn ihre Erzeuger assoziiert sind (d.h., sich nur um eine Einheit unterscheiden). Somit erhalten wir

$$\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{(p) \mid p \in \mathbb{P}\}.$$

Aus der Vorlesung ist bekannt, dass die abgeschlossenen Punkte des Spektrums genau den maximalen Idealen des Rings entsprechen. Da die maximalen Ideale eines Hauptidealrings genau die Primideale ungleich (0) sind, ist also $(p) \in \operatorname{Spec} \mathbb{Z}$ abgeschlossen für jede Primzahl p, während

$$\overline{(0)} = \bigcap_{(0) \in Z(\mathfrak{I}) \subseteq \operatorname{Spec} \mathbb{Z}} Z(I) = \bigcap_{\substack{\mathfrak{I} \subseteq \mathbb{Z} \text{ Ideal}, \\ \mathfrak{I} \subseteq (0)}} Z(\mathfrak{I}) = Z((0)) = \operatorname{Spec} \mathbb{Z}.$$

(ii) *Sei k ein algebraisch abgeschlossener Körper. Bestimmen Sie die Punkte von* $\operatorname{Spec} k[x]$. *Welche sind abgeschlossen und welche nicht?*

Lösung: k ist ein Integritätsbereich, also auch $k[x]$. Somit ist das Nullideal (0) ein Primideal. Da k ein Körper ist, ist $k[x]$ außerdem ein Hauptidealring, also sind alle weiteren Primideale in $k[x]$ genau jene Hauptideale, die von einem primen (oder äquivalent, irreduziblen) Element in $k[x]$ erzeugt werden. Da k algebraisch abgeschlossen ist, besitzt jedes Polynom $f \in k[x] \setminus \{0\}$ (mit Vielfachheit gezählt) genau $\deg(f)$ Nullstellen. Deshalb hat ein primes Polynom $f \in k[x]$ notwendigerweise Grad $\deg(f) = 1$. Allerdings stimmen zwei Hauptideale genau dann überein, wenn ihre Erzeuger assoziiert sind (d.h., sich nur um eine Einheit unterscheiden). Somit beschränken wir uns auf normierte Polynome vom Grad 1 und erhalten

$$\operatorname{Spec} k[x] = \{(0)\} \cup \{(x + a) \mid a \in K\}.$$

Aus der Vorlesung ist bekannt, dass die abgeschlossenen Punkte des Spektrums genau den maximalen Idealen des Rings entsprechen. Da die maximalen Ideale eines Hauptidealrings genau die Primideale ungleich (0) sind, ist also $(x+a) \in \operatorname{Spec} k[x]$ abgeschlossen für jedes $a \in k$, während

$$\overline{(0)} = \bigcap_{(0)\in Z(\mathfrak{I})\subseteq \operatorname{Spec} k[x]} Z(I) = \bigcap_{\substack{\mathfrak{I}\subseteq k[x] \text{ Ideal},\\ \mathfrak{I}\subseteq (0)}} Z(\mathfrak{I}) = Z((0)) = \operatorname{Spec} k[x].$$

(iii) *Sei k ein algebraisch abgeschlossener Körper. Geben Sie ein Beispiel für einen nicht abgeschlossenen Punkt in* $\operatorname{Spec} k[x,y]$*, dessen Abschluss nicht der ganze Raum* $\operatorname{Spec} k[x,y]$ *ist.*

Lösung: Betrachte das Polynom $x \in k[x,y]$. Es ist irreduzibel (oder äquivalent, prim), also ist $(x) \in \operatorname{Spec} k[x,y]$. (Alternativ kann man argumentieren, dass $k[x,y]/(x) \cong k[y]$ ein Integritätsbereich ist.) Weiters gilt

$$(x) \subsetneq (x,y) \subsetneq k[x,y],$$

also ist das Ideal (x) nicht maximal und somit $(x) \in \operatorname{Spec} k[x,y]$ nicht abgeschlossen.

Angenommen $(0) \neq \mathfrak{p} \in k[x,y]$ hat die Eigenschaft, dass $\mathfrak{p} \subseteq (x)$. Da $\mathfrak{p} \neq (0)$, existiert ein $0 \neq f \in \mathfrak{p}$. Weiters dürfen wir annehmen, dass $f \in k[x,y]$ irreduzibel ist - andernfalls schreibe f als ein Produkt irreduzibler Polynome (das ist möglich, da $k[x,y]$ faktoriell ist) und wende die definierende Eigenschaft von Primidealen an. Jedenfalls gilt dann auch $(f) \subseteq (x)$, also $x \mid f$. Aus der Irreduzibilität von f folgt nun $(f) = (x)$. Somit enthält (x) genau die Primideale (0) und (x) als Teilmengen, woraus wir

$$\overline{(x)} = \bigcap_{(x)\in Z(\mathfrak{I})\subseteq \operatorname{Spec} k[x,y]} Z(I) = \bigcap_{\substack{\mathfrak{I}\subseteq k[x,y] \text{ Ideal},\\ \mathfrak{I}\subseteq (x)}} Z(\mathfrak{I}) = Z((0)) \cap Z((x)) = Z((x))$$

erhalten. Allerdings ist $Z((x)) \subsetneq \operatorname{Spec} k[x,y]$, da beispielsweise $(y) \notin Z((x))$.

Eine allgemeinere Lösung: Sei $f \in k[x,y]$ ein irreduzibles Polynom und seien $a,b,c,d \in k$, sodass $f(a,b) = 0$ aber $f(c,d) \neq 0$ gilt. (Man überzeugt sich leicht, dass solche $a,b,c,d \in k$ für jedes irreduzible f existieren.) Wie oben ist dann $(f) \in \operatorname{Spec} k[x,y]$, aber $(f) \subsetneq (x-a, y-b) \subsetneq k[x,y]$, also (f) nicht maximal bzw. abgeschlossen. Andererseits ist $(f) \nsubseteq (x-c, y-d)$, also stimmt der Abschluss von (f) auch nicht mit dem ganzen Raum $\operatorname{Spec} k[x,y]$ überein.

Aufgabe 2

Zeigen Sie: $\operatorname{Spec} R$ *ist quasikompakt, d.h., jede offene Überdeckung besitzt eine endliche Teilüberdeckung.*

Sei Λ eine beliebige Indexmenge, und für jedes $\lambda \in \Lambda$ sei $U_\lambda \subseteq \operatorname{Spec} R$ Zariski-offen, sodass

$$\operatorname{Spec} R = \bigcup_{\lambda\in\Lambda} U_\lambda.$$

Da $U_\lambda \subseteq \operatorname{Spec} R$ Zariski-offen ist, finden wir Ideale $\mathfrak{I}_\lambda \subseteq R$, sodass $U_\lambda = Z(\mathfrak{I}_\lambda)^c$ für jedes $\lambda \in \Lambda$ ist, wobei wir wie gewohnt $Z(\mathfrak{I}_\lambda)^c = \operatorname{Spec} R \setminus Z(\mathfrak{I}_\lambda)$ schreiben.

Aus der Vorlesung ist bekannt, dass $Z(\sum_{\lambda\in\Lambda}\mathfrak{I}_\lambda) = \bigcap_{\lambda\in\Lambda} Z(\mathfrak{I}_\lambda)$, woraus wir

$$\operatorname{Spec} R = \bigcup_{\lambda\in\Lambda} Z(\mathfrak{I}_\lambda)^c = \Big(\bigcap_{\lambda\in\Lambda} Z(\mathfrak{I}_\lambda)\Big)^c = Z(\sum_{\lambda\in\Lambda}\mathfrak{I}_\lambda)^c,$$

also $\emptyset = (\operatorname{Spec} R)^c = Z(\sum_{\lambda\in\Lambda}\mathfrak{I}_\lambda)$ erhalten. Für ein beliebiges Ideal $\mathfrak{I} \subseteq R$ gilt nun aber $Z(\mathfrak{I}) = \emptyset$ genau dann, wenn $\mathfrak{I} = R$ ist. Insbesondere ist also $1 \in \sum_{\lambda\in\Lambda}\mathfrak{I}_\lambda$. Gemäß der Definition der Summe von Idealen (endliche Summen!) finden wir also $\lambda_1, ..., \lambda_n \in \Lambda$ und $r_1 \in \mathfrak{I}_{\lambda_1}, ..., r_n \in \mathfrak{I}_{\lambda_n}$, sodass $1 = r_1 + ..., r_n$. Doch dann ist bereits $\sum_{i=1}^n \mathfrak{I}_{\lambda_i} = R$, also gehen wir nun unser obiges Argument "rückwärts" und folgern so, dass

$$\operatorname{Spec} R = Z(R)^c = Z(\sum_{i=1}^n \mathfrak{I}_{\lambda_i})^c = \Big(\bigcap_{i=1}^n Z(\mathfrak{I}_{\lambda_i})\Big)^c = \bigcup_{i=1}^n Z(\mathfrak{I}_{\lambda_i})^c = \bigcup_{i=1}^n U_{\lambda_i}.$$

Das ist eine endliche Teilüberdeckung.

Aufgabe 3

Sei R ein Ring. Ein Element $e \in R$ heißt idempotent, wenn $e^2 = e$. Zeigen Sie:

(i) *Ein Ring R ist zerlegbar, d.h., $R \cong R_1 \oplus R_2$ für zwei Ringe R_1, R_2, genau dann, wenn R ein idempotentes Element $e \neq 0, 1$ enthält.*

Lösung: Falls $R \cong R_1 \oplus R_2$, dann sind $e = (1_{R_1}, 0)$ oder $e = (0, 1_{R_2})$ Beispiele für idempotente Elemente $e \notin \{(0,0), (1_{R_1}, 1_{R_2})\}$ in $R_1 \oplus R_2$.
Also nehmen wir an, dass $e \neq 0, 1$ ein idempotentes Element in R ist. Da

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e,$$

ist dann auch $1 - e \neq 0, 1$ idempotent. Betrachte nun die beiden Hauptideale $(0) \subsetneq (e), (1-e) \subsetneq R$ (wobei wir '$\subsetneq$' schreiben, da $e \neq 0, 1$ und da Nullteiler niemals Einheiten sind).

Lösungsvariante 1: Das Einzige, was ein Ideal davon abhalten kann selbst ein Ring zu sein, ist die (fehlende) Existenz eines neutralen Elements bezüglich der Multiplikation. Ist aber $r \in (e)$, d.h., $r = es$ für ein $s \in R$, dann gilt $er = e(es) = e^2 s = es = r$ und wegen der Kommutativität natürlich auch $re = r$. Analog zeigt man, dass $(1-e)r = r(1-e) = r$ für alle $r \in (1-e)$ erfüllt ist. Somit können wir $R_1 = (e)$ und $R_2 = (1-e)$ als Ringe (mit $1_{R_1} = e$ und $1_{R_2} = 1 - e$) auffassen und die Ringhomomorphismen

$$\phi_1 \colon R \to R_1 \oplus R_2,$$

$$\phi_2 \colon R_1 \oplus R_2 \to R,$$

definiert durch $\phi_1(r) = (er, (1-e)r)$ und $\phi_2((x,y)) = x + y$ betrachten.
Nicht ganz klar mag auf den ersten Blick sein, dass ϕ_1 und ϕ_2 tatsächlich multiplikativ sind. Doch tatsächlich ist

$$\phi_1(r \cdot s) = (ers, (1-e)rs) = ((er)\cdot(es), (1-e)r \cdot (1-e)s)$$

$$= (er, (1-e)r) \cdot (es, (1-e)s) = \phi_1(r) \cdot \phi_1(s)$$

für alle $r, s \in R$, und schreibt man $x_1 = er_1, x_2 = er_2, y_1 = (1-e)s_1, y_2 = (1-e)s_2$, dann

$$\phi_2((x_1, y_1)) \cdot \phi_2((x_2, y_2)) = (x_1+y_1) \cdot (x_2+y_2) = x_1x_2 + y_1y_2 + e(1-e)(r_1s_2 + r_2s_1)$$

$$= x_1x_2 + y_1y_2 + 0 \cdot (r_1s_2 + r_2s_1) = x_1x_2 + y_2y_1 = \phi_2((x_1x_2, y_1y_2)) = \phi_2((x_1, x_2) \cdot (y_1, y_2)).$$

Nun prüft man aber leicht nach, dass $\phi_1 \circ \phi_2 = \mathrm{Id}_{R_1 \oplus R_2}$ und $\phi_2 \circ \phi_1 = \mathrm{Id}_R$ gilt. Somit haben wir $R \cong R_1 \oplus R_2$ bewiesen.

Lösungsvariante 2: Wir betrachten den Ringhomomorphismus

$$\phi \colon R \to R/(e) \oplus R/(1-e) \text{ definiert durch } r \mapsto \big(r + (e), r + (1-e)\big).$$

Zunächst ist $R/(e), R/(1-e) \neq \{0\}$, da ja $(0) \subsetneq (e), (1-e) \subsetneq R$. Weiters ist

$$\phi(e) = \big(e + (e), e + (1-e)\big) = \big(0 + (e), 1 + (1-e)\big) = (0_{R/(e)}, 1_{R/(1-e)})$$

und

$$\phi(1-e) = \big(1-e+(e), 1-e+(1-e)\big) = \big(1+(e), 0+(1-e)\big) = (1_{R/(e)}, 0_{R/(1-e)}),$$

was die Surjektivität von ϕ beweist. Hat schließlich $r \in R$ die Eigenschaft, dass $\phi(r) = (0_{R/(e)}, 0_{R/(1-e)})$, dann muss $r \in (e) \cap (1-e)$, also $r = es_1 = (1-e)s_2$ für $s_1, s_2 \in R$ sein. Doch dann ist

$$r = es_1 = e \cdot (es_1) = e(1-e)s_2 = 0s_2 = 0,$$

womit unser Beweis der Bijektivität von ϕ vollendet ist.

(ii) $\operatorname{Spec} R$ *mit der Zariskitopologie ist unzusammenhängend, d.h.,* $\operatorname{Spec} R$ *ist disjunkte Vereinigung zweier nichttrivialer, abgeschlossener Teilmengen, genau dann, wenn* R *ein idempotentes Element* $e \neq 0, 1$ *enthält.*

Lösung: Angenommen R enthält ein idempotentes Element $e \neq 0, 1$, dann betrachte die Ideale $(0) \subsetneq (e), (1-e) \subsetneq R$. Da Nullteiler niemals Einheiten sind, ist $\emptyset \subsetneq Z((e)), Z((1-e)) \subsetneq \operatorname{Spec} R$ abgeschlossen, und wegen $e + (1-e) = 1, e(1-e) = 0$ haben wir

$$(e) + (1-e) = R, (e) \cdot (1-e) = (0).$$

Daraus folgt nun die Behauptung, da

$$Z((e)) \cap Z((1-e)) = Z((e) + (1-e)) = Z(R) = \emptyset,$$

$$Z((e)) \cup Z((1-e)) = Z((e) \cdot (1-e)) = Z((0)) = \operatorname{Spec} R.$$

Nehmen wir nun andererseits an, dass es Ideale $(0) \subsetneq \mathfrak{I}, \mathfrak{J} \subsetneq R$ gibt mit

$$Z(\mathfrak{I}) \cup Z(\mathfrak{J}) = \operatorname{Spec} R = Z((0)),$$

$$Z(\mathfrak{I}) \cap Z(\mathfrak{J}) = \emptyset = Z(R).$$

Aus der Vorlesung ist bekannt, dass dann

$$\mathfrak{I} \cdot \mathfrak{J} \subseteq \sqrt{\mathfrak{I} \cdot \mathfrak{J}} = \sqrt{(0)} \text{ und } \sqrt{\mathfrak{I} + \mathfrak{J}} = \sqrt{R} = R \Longrightarrow \mathfrak{I} + \mathfrak{J} = R$$

erfüllt ist. Letzteres impliziert, dass es $r \in \mathfrak{I}, s \in \mathfrak{J}$ mit $r + s = 1$ gibt, und aus Ersterem können wir folgern, dass $(rs)^n = 0$ für hinreichend großes $n \geq 1$ gilt. Weil somit $(r) + (s) = R$ ist, folgern wir aus den Eigenschaften der Radikale, dass

$$\sqrt{(r^n) + (s^n)} = \sqrt{\sqrt{(r^n)} + \sqrt{(s^n)}} = \sqrt{\sqrt{(r)} + \sqrt{(s)}} = \sqrt{(r) + (s)} = R$$

und somit auch $(r^n) + (s^n) = R$ gilt. Das bedeutet aber, dass es $u, v \in R$ gibt mit $ur^n + vs^n = 1$. Setze nun $e := ur^n \in (r) \subseteq \mathfrak{I} \neq R$. Dann ist $1 - e = vs^n \in (s) \subseteq \mathfrak{J} \neq R$, also $e \neq 0, 1$. Außerdem ist

$$e^2 = ur^n \cdot ur^n = ur^n \cdot (1 - vs^n) = ur^n - uv(rs)^n = ur^n = e,$$

also ist e idempotent und die Behauptung folgt.

Alternative: Sind r, s wie oben gegeben, dann kann man einen Kandidaten für e auch direkt konstruieren: Der binomische Lehrsatz gilt in jedem kommutativen Ring und besagt in unserer Situation, dass

$$1 = (r + s)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} r^i s^{2n-i}$$

ist, wobei wir (wie üblich) $z \in \mathbb{Z}$ mit seinem Bild $\phi(z) \in R$ unter dem eindeutigen Ringhomomorphismus $\phi \colon \mathbb{Z} \to R$ idenzifizieren. Gemäß der Wahl von n verschwindet $\binom{2n}{n} r^n s^n$, der n-te Term in der obigen Summe, was uns erlaubt, $1 = e + (1 - e)$ zu schreiben für

$$e = \sum_{i=0}^{n-1} \binom{2n}{i} r^i s^{2n-i},$$

$$1 - e = \sum_{i=n+1}^{2n} \binom{2n}{i} r^i s^{2n-i}.$$

Daraus folgt dann bereits $e - e^2 = (1 - e)e = 0$, da für alle $0 \leq i < n < j \leq 2n$ sowohl $i + j$ als auch $(2n - i) + (2n - j)$ größer als n ist. Abschließend bemerken wir, dass $e \neq 1$, da wegen $e \in (s) \subseteq \mathfrak{J}$ sonst $\mathfrak{J} = R$ wäre, und dass $e \neq 0$, da wegen $1 - e \in (r) \subseteq \mathfrak{I}$ sonst $\mathfrak{I} = R$ wäre, was wir beides ausgeschlossen haben.

Aufgabe 4

Sei R ein Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Zeigen Sie:

(i) *f ist nilpotent genau dann, wenn alle a_i nilpotent sind.*

Lösung 1: Nehmen wir zuerst an, dass R ein Integritätsbereich ist. Dann ist auch $R[x]$ ein Integritätsbereich, also ist f nilpotent genau dann, wenn $f = 0$

(und damit jedes $a_i = 0$) ist.
Im allgemeinen Fall nehmen wir zuerst an, dass f nilpotent ist. Sei $\mathfrak{p} \subseteq R$ ein Primideal und bezeichne mit $\pi_\mathfrak{p}\colon R[x] \to (R/\mathfrak{p})[x]$ die Erweiterung der kanonischen Projektion $R \to R/\mathfrak{p}$ (definiert durch $\pi_\mathfrak{p}(x) = x$). Ist $f^m = 0$, dann gilt auch $\pi_\mathfrak{p}(f)^m = \pi_\mathfrak{p}(f^m) = 0$, d.h., $\pi_\mathfrak{p}(f) \in (R/\mathfrak{p})[x]$ ist nilpotent. Da $\mathfrak{p} \subseteq R$ prim ist, ist $R/\mathfrak{p}$ jedoch ein Integritätsbereich und folglich $\pi_\mathfrak{p}(f) = 0$. Sei nun $0 \leq i \leq n$ beliebig, dann bedeutet das gerade, dass $\pi_\mathfrak{p}(a_i) = 0$, also dass $a_i \in \mathfrak{p}$ für jedes $\mathfrak{p} \subseteq R$ prim ist. Daraus folgt nun insbesondere

$$a_0, ..., a_n \in \bigcap_{\mathfrak{p} \subseteq R \text{ prim}} \mathfrak{p} = \{r \in R \mid r \text{ nilpotent}\}.$$

Gehen wir nun davon aus, dass $a_0, ..., a_n \in R$ nilpotent sind. Dann ist für jedes $1 \leq i \leq n$ auch $a_i x^i \in R[x]$ nilpotent, da aus $a_i^{m_i} = 0$ für hinreichend großes $m_i \geq 0$ bereits $(a_i x^i)^{m_i} = a_i^{m_i} x^{m_i \cdot i} = 0 x^{m_i \cdot i} = 0$ folgt. Da $f = \sum_{i=0}^n a_i x^i$ und da die Menge aller nilpotenter Elemente in $R[x]$ ein Ideal (das Nilradikal von $R[x]$) bildet, muss somit auch f nilpotent sein.

Lösung 2: Angenommen $f \in R[x] \setminus \{0\}$ ist nilpotent. Wir zeigen durch Induktion nach $\deg(f) = n$, dass dann alle a_i nilpotent sein müssen. Im Falle $n = 0$ erhält man unmittelbar, dass a_0 nilpotent sein muss.
Sei die Behauptung nun für alle Polynome vom Grad $< n$ war. Da f nilpotent ist, gibt es ein hinreichend großes $k \geq 0$, sodass

$$0 = f^k = a_n^k x^{nk} + ...$$

Koeffizientenvergleich liefert nun $a_n^k = 0$, also ist a_n nilpotent. Da die nilpotenten Elemente in $R[x]$ ein Ideal (das Nilradikal) bilden, können wir folgern, dass sowohl $a_n x^n$ als auch $f - a_n x^n = \sum_{i=0}^{n-1} a_i x^i$ nilpotent sind. Daraus folgt nun die Behauptung, weil $\deg(f - a_n x^n) < n$ ist.
Nehmen wir hingegen an, dass $a_0, ..., a_n \in R$ nilpotent sind, dann kann man wie in *Lösung 1* vorgehen.

(ii) *f ist eine Einheit genau dann, wenn a_0 eine Einheit ist und a_1,...,a_n nilpotent sind.*

Lösung: Nehmen wir zuerst an, dass R ein Integritätsbereich ist. Dann gilt die Formel $\deg(gh) = \deg g + \deg h$ für alle $g, h \in R[x]$, also insbesondere $R[x]^\times = R^\times$. Somit ist $f \in R[x]^\times$ genau dann, wenn $f \in R^\times$, also wenn a_0 eine Einheit und $a_1 = ... = a_n = 0$ ist.
Im allgemeinen Fall nehmen wir zuerst an, dass f eine Einheit ist, d.h., dass $g \in R[x]$ existiert mit $f \cdot g = g \cdot f = 1$. Sei nun $\mathfrak{p} \subseteq R$ ein Primideal und bezeichne wieder mit $\pi_\mathfrak{p}\colon R[x] \to (R/\mathfrak{p})[x]$ die Erweiterung der kanonischen Projektion $R \to R/\mathfrak{p}$ (definiert durch $\pi_\mathfrak{p}(x) = x$). Dann folgt

$$1 = \pi_\mathfrak{p}(1) = \pi_\mathfrak{p}(fg) = \pi_\mathfrak{p}(f) \cdot \pi_\mathfrak{p}(g),$$

also ist auch $\pi_\mathfrak{p}(f) \in (R/\mathfrak{p})[x]^\times$. Da $\mathfrak{p}$ prim ist, ist $R/\mathfrak{p}$ ein Integritätsbereich und folglich $\pi_\mathfrak{p}(a_0) \in (R/\mathfrak{p})^\times$ sowie $\pi_\mathfrak{p}(a_1) = ... = \pi_\mathfrak{p}(a_n) = 0$. Wie in (i) argumentiert man nun, dass $a_i \in \mathfrak{p}$ für jedes $1 \leq i \leq n$ und $\mathfrak{p} \subseteq R$ prim ist, also insbesondere

$$a_1, ..., a_n \in \bigcap_{\mathfrak{p} \subseteq R \text{ prim}} \mathfrak{p} = \{r \in R \mid r \text{ nilpotent}\}$$

gilt. Ist hingegen $\mathfrak{p} = \mathfrak{m} \subseteq R$ maximal, dann ist $\pi_{\mathfrak{p}}(a_0) \in (R/\mathfrak{p})^\times$ äquivalent zu $a_0 \notin \mathfrak{m}$ (da $R/\mathfrak{p} = R/\mathfrak{m}$ ein Körper ist), also erhalten wir hier, dass

$$a_0 \in R \setminus \Big(\bigcup_{\mathfrak{m} \subseteq R \text{ maximal}} \mathfrak{m} \Big) = R^\times.$$

Gehen wir nun davon aus, dass $a_0 \in R$ eine Einheit ist und $a_1, ..., a_n \in R$ nilpotent sind. Nach Teilaufgabe (i) ist dann $g := f - a_0 \in R[x]$ nilpotent, also gibt es $m \geq 0$ hinreichend groß und ungerade (!), sodass $g^m = 0$ ist. Da $f = g + a_0$, folgt aus der Identität

$$(g + a_0) \cdot (g^{m-1} - g^{m-2}a_0 + g^{m-3}a_0^2 - ... + a_0^{m-1}) = g^m + a_0^m = a_0^m \in R^\times$$

nun unmittelbar, dass $f \in R[x]^\times$ ist.

(iii) f *ist Nullteiler genau dann, wenn ein* $a \in R \setminus \{0\}$ *mit* $a \cdot f = 0$ *existiert.*

Lösung: Falls ein $a \in R \setminus \{0\}$ mit $a \cdot f = 0$ existiert, so ist f nach Definition ein Nullteiler.
Nehmen wir also an, dass f ein Nullteiler ist, d.h., dass ein $g = \sum_{j=0}^m b_j x^j \in R[x], b_m \neq 0$, minimalen Grades (!) mit $fg = 0$ gibt. Um einen Widerspruch herzuleiten, wollen wir annehmen, dass $m \geq 1$ ist. Insbesondere ist dann $b_m f \neq 0$, somit existiert ein maximales $k \in \{0, ..., n\}$ mit $a_k g \neq 0$. Daraus erhalten wir nun

$$f \cdot g = \Big(\sum_{i=0}^k a_i x^i \Big) \Big(\sum_{j=0}^m b_j x^j \Big) = 0,$$

also $a_k b_m = 0$. Doch das bedeutet dann $\deg(a_k g) < m = \deg(g)$, aber $f \cdot (a_k g) = a_k \cdot (fg) = 0$, im Widerspruch zur Minimalität von $m = \deg(g)$.

Eine unvollendete Lösung: Ist f Nullteiler, dann könnten wir wie in (i) folgern, dass $\pi_{\mathfrak{p}}(f) = 0$ ist für jedes Primideal $\mathfrak{p} \subseteq R$, also dass die Koeffizienten $a_0, ..., a_n \in R$ nilpotent sind. Sind nun $m_i \geq 0$ hinreichend groß gewählt, sodass $a_i^{m_i} = 0$ ist, dann hat das Element

$$a := \prod_{i=0}^n a_i^{m_i - 1} \in R$$

die Eigenschaft, dass $a \cdot f = 0$ ist. Doch selbst wenn wir stets $a_i^{m_i-1} \neq 0$ voraussetzen (und Koeffizienten, die bereits gleich 0 sind, weglassen), haben wir nun Schwierigkeiten zu zeigen, dass $a \neq 0$ ist.