Algebra – Blatt 10 – Lösungsvorschlag

A1 (a) Falsch. Etwa $a \in R^\times$, z.B. $a = 1$. Dann ist $\mathfrak{a} = R$ für jedes Ideal $\mathfrak{a} \subseteq R$ mit $a \in \mathfrak{a}$.

(b) Wahr. Nach Bsp. 2.5.9 und Satz 2.5.10 ist $K[X]$ ein Hauptidealring. Nach Satz 2.8.2 ist damit (f) maximales Ideal gdw f irreduzibel ist. Da $f \in K[X]$ mit $\deg(f) = 1$ folgt die Beh. ($f = gh \Rightarrow \deg(g) + \deg(h) = 1 \Rightarrow g$ oder h konstant $\Rightarrow g$ oder h in $K^\times \subseteq (K[X])^\times$)

(c) Wahr. Ist $\underbrace{1+1+\ldots+1}_{p \text{ mal}} = 0$ in K, so auch in L, also $\mathrm{char}(L) \mid \underset{\overset{\shortparallel}{p}}{\mathrm{char}(K)}$, d.h. $\mathrm{char}(L) = p$.

Ist $\underbrace{1+1+\ldots+1}_{p \text{ mal}} = 0$ in L, so auch in K, also $\mathrm{char}(K) \mid \underset{\overset{\shortparallel}{p}}{\mathrm{char}(L)}$, d.h. $\mathrm{char}\, K = p$. (Satz 3.1.2)

Alternativ: Wäre $\mathrm{char}(K) = p$, $\mathrm{char}(L) = q$, p, q prim oder $= 0$, $p \neq q$, so hätten K, L nach Satz 3.1.9. verschiedene Primkörper K' und L'. Aber $K' \subseteq K \subseteq L$, also $L' \subseteq K' \subseteq K$ und damit $K' \subseteq L'$; insgesamt $K' = L'$.

(d) Wahr. Für $a \in K$ ist $a = a \cdot 1$, also
$$a + a = a \cdot 1 + a \cdot 1 = a \cdot \underbrace{(1+1)}_{=0} = a \cdot 0 \overset{\text{Nach Blatt 6 A4 (a)}}{=} 0$$

1(e) Wahr. Sind $a_1, \dots, a_n \in M$ lin. unabh. über L, so gilt (*) $\lambda_1 a_1 + \dots + \lambda_n a_n = 0 \Rightarrow \lambda_1 = \dots = \lambda_n = 0$ für alle $\lambda_1, \dots, \lambda_n \in L$. Da $K \subseteq L$ gilt (*) insbes. auch für alle $\lambda_1, \dots, \lambda_n \in K$, d.h. $a_1, \dots, a_n$ sind lin. unabh. über K.

A2) (a) Zunächst ist klar, dass $(ab) \subseteq (a) \cap (b)$ für alle Ringe R und $a, b \in R$ beliebig, – das gilt denn $x \in (ab)$ heißt, es gibt $y \in R$ mit $x = aby$, insbesondere $x \in (a)$ und $x = b(ay) \in (b)$.

Sei nun R faktoriell und a, b teilerfremd, $a, b \in R \setminus \{0\}$ (*)

(*): Für $a = 0$ ist $(a) \cap (b) = (0) = (ab)$.

Sei $x \in ((a) \cap (b)) \setminus \{0\}$ und sei $x = e \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k$ eine PFZ von x (mit $e \in R^\times$ und $p_1, \dots, p_k$ irreduzibel, wie in Blatt 9 A2(a)).

Sei $x = ay = bz$ für $y, z \in R \setminus \{0\}$ geeignet.

Nach Bl 9 A2(a) ist $a = e' \prod_{i \in I} p_i$, $y = e'' \prod_{i \in \{1, \dots, k\} \setminus I} p_i$ für geeignete $I \subseteq \{1, \dots, k\}$, $e', e'' \in R^\times$ und $b = e''' \prod_{i \in I'}$ für geeignete $I' \subseteq \{1, \dots, k\}$, $e''' \in R^\times$.

Da a, b teilerfremd sind ist $I \cap I' = \emptyset$ (wäre $i \in I \cap I'$, so wäre $p_i | a$ und $p_i | b$). Also ist $I' \subseteq \{1, \dots, k\} \setminus I$, d.h. $b | y$, also $x = ay = abw$ für ein $w \in R$, damit folgt $x \in (ab)$.

A2 (b) Wir zeigen die Beh. per Induktion über n.

<u>Ind. anfang</u> <u>$n=1$</u>. Klar. ($b = a_1$, also $R/(b) \cong R/(a_1)$).

<u>Ind. schluss</u> <u>$n \to n+1$</u>. Ang. die Beh sei wahr für n. Seien

$a_1, \dots, a_n, a_{n+1} \in R$ p.w. teilerfremd, $b = a_1 \cdots a_{n+1}$.

Betrachte $b' := a_1 a_2 \cdots a_n$. Dann sind b' und a_{n+1} teilerfremd, nach Lemma 2.5.11 ist also $(b', a_{n+1}) = R$. Daher können wir den chin. Restsatz auf $\mathfrak{a}_1 = (b')$ und $\mathfrak{a}_2 = (a_{n+1})$ anwenden und erhalten einen surj. Ringhom.

$$\varphi : R \longrightarrow R/(b') \times R/(a_{n+1}) \quad \text{mit}$$

$$\ker(\varphi) = (b') \cap (a_{n+1}) \underset{\underset{A2a}{\uparrow}}{=} (b' a_{n+1}) = (b)$$

Nach dem Isomorphiesatz folgt

$$R/(b) \cong \underbrace{R/(b')}_{\substack{\text{Ind. voraus.} \\ \cong \\ R/(a_1) \times \dots \times R/(a_n)}} \times R/(a_{n+1})$$

$$\cong R/(a_1) \times \dots \times R/(a_n) \times R/(a_{n+1}),$$

was zu zeigen war.

2(c) Betrachte den (Ring-) Homomorphismus $\varphi: K[X] \to K^n$ der durch $\varphi(a) = (a, a, \ldots, a)$ und

$$\varphi(X) = (a_1, a_2, \ldots, a_n)$$ induziert

wird, wobei $a_1, a_2, \ldots, a_n \in K$ genau die n verschiedenen Nullstellen von f seien.

Dann ist $\varphi((X-a_1)(X-a_2)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n))$

$$= (0, a_2-a_1, a_3-a_1, \ldots)\cdot(a_1-a_2, 0, \ldots)\cdot \ldots$$

$$= (0, \ldots, 0, \underbrace{(a_i-a_1)(a_i-a_2)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots}_{\substack{= b \\ i\text{ter Eintrag}}}, 0, \ldots, 0)$$

wobei $b \neq 0$, da $a_i \neq a_j$ für $j \neq i$.

Also $\varphi(cb^{-1}\cdot(X-a_1)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n))$

$$= (0, \ldots, 0, \underset{\uparrow\, i\text{ter Eintrag}}{c}, 0, \ldots, 0) \in K^n$$

für $c \in K$, $i \in \{1, \ldots, n\}$ beliebig, d.h. φ ist surjektiv.

Analog rechnet man nach, dass $\varphi(f) = 0$, also $(f) \subseteq \ker(\varphi)$ gilt (da $f = a(X-a_1)\cdots(X-a_n)$ für geeignetes $a \in K^\times$) und dass $\ker(\varphi) \subseteq (f)$. Mit dem Isom.satz folgt die Beh.

$$\boxed{\text{(Tatsächlich ist } \varphi(g) = (*, \ldots, *, \overset{i}{0}, *, \ldots, *) \text{ gdw } a_i \text{ NSt von } g \text{ ist, d.h. } \varphi(g) = 0 \text{ gdw } f \mid g\text{, also } \ker(\varphi) = (f).)}$$

A3 (a) Beachte zunächst $R^\times = R \setminus \mathfrak{a} \iff R^\times \cup \mathfrak{a} = R$ und $R^\times \cap \mathfrak{a} = \emptyset$

$\iff \mathfrak{a} = R \setminus R^\times$

"$\Leftarrow$" Sei nun $\mathfrak{a} = R \setminus R^\times$ ein Ideal.

Ist $\mathfrak{b} \subsetneq R$ ein Ideal, so ist $R^\times \cap \mathfrak{b} = \emptyset$ (sonst wäre $\mathfrak{b} = R$), also $\mathfrak{b} \subseteq R \setminus R^\times = \mathfrak{a}$.

D.h. jedes Ideal $\neq R$ ist in $\mathfrak{a}$ enthalten, also ist $\mathfrak{a}$ das einzige maximale Ideal; insbes. ist R lokaler Ring.

"$\Rightarrow$" Nun sei $R \setminus R^\times$ <u>kein</u> Ideal in R.

Da $R \cdot (R \setminus R^\times) \subseteq R \setminus R^\times$ ist ($r, s \in R$ mit $rs \in R^\times \Rightarrow r \in R^\times, s \in R^\times$) gibt es dann $a, b \in R \setminus R^\times$ mit $a+b \notin R \setminus R^\times$, d.h. $a+b \in R^\times$. Da a, b keine Einheiten sind ist $(a) \subsetneq R$ und $(b) \subsetneq R$; nach Satz 2.8.k gibt es maximale Ideale $\mathfrak{a}, \mathfrak{b} \subsetneq R$ mit $(a) \subseteq \mathfrak{a}$ und $(b) \subseteq \mathfrak{b}$.

<u>Beh.</u> $\mathfrak{a} \neq \mathfrak{b}$; insbes. ist R kein lokaler Ring.

<u>Bew.</u> Es ist $a+b \in \underbrace{(\mathfrak{a} \cup \mathfrak{b})}_{\text{das von } \mathfrak{a} \text{ und } \mathfrak{b} \text{ erzeugte Ideal}} \cap R^\times$, aber $\mathfrak{a} \cap R^\times = \emptyset$

also $(\mathfrak{a} \cup \mathfrak{b}) \supsetneq \mathfrak{a}$, d.h. $\mathfrak{a} \not\supseteq \mathfrak{b}$, insbes. $\mathfrak{a} \neq \mathfrak{b}$.

3b) Betrachte $R = \left\{ \frac{a}{b} \;\middle|\; \begin{array}{l} a,b \text{ teilerfremd} \\ b \text{ ungerade} \end{array} \right\} \subseteq \mathbb{Q}$

(Das ist genau der Ring R' aus B8A3 für $R = \mathbb{Z}$ und $S = \mathbb{Z} \setminus 2\mathbb{Z}$

Beh: $R \setminus R^\times = (2)$, insbesondere ist $R \setminus R^\times$ ein Ideal (und R damit ein lokaler Ring nach (a).)

Bew: Sei zunächst $x \in (2) \subseteq R$. Dann gibt es $a, b \in \mathbb{Z}$ teilerfremd, b ungerade mit $x = 2 \cdot \frac{a}{b} = \frac{2a}{b}$. Angenommen $x \in R^\times$, d.h. es gibt $c, d \in \mathbb{Z}$ teilerfremd mit d ungerade und $\frac{2a}{b} \cdot \frac{c}{d} = 1$, d.h. $2ac = \underset{\text{ung.}}{b}\underset{\text{ung.}}{d}$ ungerade $\lightning$. Also muss $x \in R \setminus R^\times$ gelten, das zeigt "$\supseteq$". Für "$\subseteq$" sei nun $x \notin (2)$. Wir zeigen $x \in R^\times$. Schreibe $x = \frac{a}{b}$, a, b teilerfremd, b ungerade. Da $x \notin (2)$ ist a ungerade (für $a = 2a'$ wäre $x = 2 \cdot \underset{\in R}{\frac{a'}{b}}$), also ist $\frac{b}{a} \in R$ mit $\frac{a}{b} \cdot \frac{b}{a} = 1$, d.h. $\frac{a}{b} \in R^\times$.

Dies zeigt "$\subseteq$", also ist die Beh. bewiesen.

Nach Teil (a) folgt, dass R ein lokaler Ring ist.

A4 (a) Nach Satz 2.8.3. und 2.8.2 ist $K = \mathbb{Q}[X]/(f)$ ein Körper gdw $f \in \mathbb{Q}[X]$ irreduzibel ist (beachte, dass $\mathbb{Q}[X]$ nach Bsp 2.5.9 und Satz 2.5.10 ein Hauptidealring ist).

Das ist nach Bsp. 2.7.8. der Fall, da 5 prim ist.

($f(X) = 1 + X + \dots + X^4 \in \mathbb{Q}[X]$ irreduzibel)

(b) Ja, da $\bar{X}^4 = -1 - \bar{X} - \bar{X}^2 - \bar{X}^3 \iff \bar{X}^4 + \bar{X}^3 + \bar{X}^2 + \bar{X} + \bar{1} = \bar{0}$

$$\iff \underbrace{\overline{X^4 + X^3 + X^2 + X + 1}}_{= \bar{f} = (f) = 0 \text{ in } \mathbb{Q}[X]/(f)} = \bar{0}$$

(c) Es ist $\bar{X}^5 = \overline{X \cdot X^4} = \bar{X} \cdot \bar{X}^4$, also nach (b):

$$\bar{X}^5 = -\bar{X} - \bar{X}^2 - \bar{X}^3 - \bar{X}^4 = -\bar{X} - \bar{X}^2 - \bar{X}^3 - (-1 - \bar{X} - \bar{X}^2 - \bar{X}^3) = 1,$$

also $\bar{X}^6 = \bar{X} \cdot \bar{X}^5 = \bar{X}$. $\leadsto g_2(X) = X$ funktioniert.

(d) Nach Bsp. 2.2.8 lässt sich jedes Element von K eindeutig in der Form

$$a_0 + a_1 X + a_2 X^2 + a_3 X^3 + (f)$$

schreiben (mit $a_0, a_1, a_2, a_3 \in \mathbb{Q}$). Folglich ist $\{1, X, X^2, X^3\}$ eine Basis von K als $\mathbb{Q}$-VR, d.h. $[K : \mathbb{Q}] = \dim_{\mathbb{Q}}(K) = 4$.