

Algebra
Übungsblatt 10
Lösungsvorschlag

Aufgabe 1.

- a) Der Polynom $x^2 - p$ ist irreduzibel in $\mathbb{Q}[x]$ bei der Eisenstein Kriterium: es gilt $p \nmid a_2 = 1$, $p|a_1 = 0$, und $p|a_0 = p$ aber $p^2 \nmid a_0$. Da $x^2 - p$ irreduzibel ist, hat er insbesondere keine Nullstelle in $\mathbb{Q}$, also $\sqrt{p} \notin \mathbb{Q}$.
- b) Seien $a, b \in \mathbb{Q}$ mit $a + b\sqrt{p} = 0$. Wenn $a \neq 0$ ist, gilt $\sqrt{p} = -\frac{b}{a} \in \mathbb{Q}$, ein Widerspruch. Also ist $a = 0$, und es gilt $b\sqrt{p} = 0$. Da $\sqrt{p} \neq 0$ ist, haben wir $b = 0$; das heißt, 1 und $\sqrt{p}$ sind $\mathbb{Q}$ -linear unabhängig.

Aufgabe 2.

- a) Falsch: seien z.B. $K = \mathbb{Q}$ und $L = M = \mathbb{R}$. Dann sind 1 und $\sqrt{p}$ $\mathbb{Q}$ -linear unabhängig aber $\mathbb{R}$ -linear abhängig.
- b) Wahr: seien $a_1, \dots, a_n \in M$ L -linear unabhängig, und seien $\lambda_1, \dots, \lambda_n \in K$ mit $\lambda_1 a_1 + \dots + \lambda_n a_n = 0$. Da $K \subseteq L$ ist, sind alle $\lambda_i \in L$. Da $a_1, \dots, a_n$ L -linear unabhängig sind, gilt $\lambda_i = 0$ für alle i , also $a_1, \dots, a_n$ sind K -linear unabhängig.
- c) Wahr: sei $x \in \langle a_1, \dots, a_n \rangle_K$, dann existieren $\lambda_1, \dots, \lambda_n \in K$ mit $x = \lambda_1 a_1 + \dots + \lambda_n a_n$. Da $K \subseteq L$ ist, gilt $\lambda_i \in L$ für alle i . Also $x \in \langle a_1, \dots, a_n \rangle_L$.
- d) Falsch: wir nehmen $K \neq L$, z.B. $K = \mathbb{Q}$ und $L = M = \mathbb{R}$. Dann gilt $\langle 1 \rangle_K = K$, $\langle 1 \rangle_L = L$, und $L \not\subseteq K$.

Aufgabe 3.

- a) Wir sehen f als ein Element von $\mathbb{Z}[x]$. f ist primitiv, also gibt es kein $n \in \mathbb{Z}$ mit $|n| > 1$ und $n|f$. Seien nun $g, h \in \mathbb{Z}[x]$ mit $f = gh$ und mit $\deg(g) = 1$, dann existieren $a, b \in \mathbb{Z}$ mit $g = ax + b$. Dann teilt a der zu x^3 Koeffizient von f , also $a|1$ und $a = \pm 1$. Dann ist $f = gh = \pm(x \pm b)h$, also $\pm b$ ist eine Nullstelle von f , die in $\mathbb{Z}$ liegt.

Wir zeigen nun, dass f keine Nullstelle in $\mathbb{Z}$ hat: es gilt $f'(x) = 3x^2 + 4$, also $f'(x) > 0$ für alle $x \in \mathbb{R}$ und f ist monoton steigend auf $\mathbb{R}$. Es gilt $f(0) = -1$ und $f(1) = 4$, also f hat genau eine Nullstelle in $\mathbb{R}$, und sie liegt zwischen 0 und 1. Insbesondere hat f keine Nullstelle in $\mathbb{Z}$.

Schließlich gilt, dass f irreduzibel in $\mathbb{Z}[x]$ ist. Da f primitiv ist, folgt aus Satz 2.6.7, dass f irreduzibel in $\mathbb{Q}[x]$ ist.

- b) Da f irreduzibel ist und $\mathbb{Q}$ ein Körper ist, folgt dass (f) ein maximal Ideal ist, und daraus folgt dass $\mathbb{Q}[x]/(f)$ ein Körper bildet.
- c) Aus Bsp. 2.2.14 folgt, dass L ein $\mathbb{Q}$ -Vektorraum ist, mit Basis $1, \bar{x}, \bar{x}^2$; also $[L : \mathbb{Q}] = \dim_{\mathbb{Q}}(L) = 3$.
- d) In L gilt $\bar{f} = 0$, also $\bar{x}^3 + 4\bar{x} - 1 = 0$, und $\bar{x}^3 = 1 - 4\bar{x}$.
- e) Es gilt $\bar{x} \cdot \bar{g} = a_0\bar{x} + a_1\bar{x}^2 + a_2\bar{x}^3 = a_0\bar{x} + a_1\bar{x}^2 + a_2(1 - 4\bar{x}) = a_2 \cdot 1 + (a_0 - 4a_2) \cdot \bar{x} + a_1 \cdot \bar{x}^2$.
- f) Da $1, \bar{x}, \bar{x}^2$ eine Basis von L bildet, es gilt dass $L \rightarrow \mathbb{Q}^3, a_0 + a_1\bar{x} + a_2\bar{x}^2 \mapsto \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$ ein Isomorphismus (von $\mathbb{Q}$ -Vektorräume) ist. Es gilt $\alpha(a_0 + a_1\bar{x} + a_2\bar{x}^2) = a_2 \cdot 1 + (a_0 - 4a_2) \cdot \bar{x} + a_1 \cdot \bar{x}^2$, also wenn $A \in \mathbb{Q}^{3 \times 3}$ existiert, sodass $A \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_2 \\ a_0 - 4a_2 \\ a_1 \end{pmatrix}$ für alle $a_0, a_1, a_2 \in \mathbb{Q}$, dann ist α linear und ist A die zu α assoziierte Matrix. Die Matrix $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{pmatrix}$ ist eine solche Matrix.
- g) Sei $\bar{g} \in L$, es gilt $\beta(\bar{g}) = \bar{g} \cdot \bar{h} = \bar{g} \cdot (b_0 + b_1\bar{x} + b_2\bar{x}^2) = b_0\bar{g} + b_1\bar{g} \cdot \bar{x} + b_2\bar{g} \cdot \bar{x}^2 = b_0 \text{id}(\bar{g}) + b_1\alpha(\bar{g}) + b_2\alpha^2(\bar{g}) = (b_0 \text{id} + b_1\alpha + b_2\alpha^2)(\bar{g})$, also die Matrix B gleich $b_0I_3 + b_1A + b_2A^2$ ist.
- h) Sei $\bar{g} \in L$ sodass $\overline{gx} = 1$, das heißt, $\alpha(\bar{g}) = 1$. Seien $a_0, a_1, a_2 \in \mathbb{Q}$ mit $\bar{g} = a_0 + a_1\bar{x} + a_2\bar{x}^2$. Dann gilt $A \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, das heißt, $\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.
- Da $A^{-1} = \begin{pmatrix} 4 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, wir haben $\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \\ 1 \end{pmatrix}$ und $\bar{g} = 4 + \bar{x}^2$.

Aufgabe 4. Wir betrachten der Ringisomorphismus $\varphi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[y], g(x) \mapsto g(y+1)$. Sei $f(x) = 1 + x^p + x^{2p} + \dots + x^{(p-1)p}$. Dann ist $\varphi(f) = f(y+1) = 1 + (y+1)^p + \dots + (y+1)^{(p-1)p}$. Seien $a_0, \dots, a_{(p-1)p} \in \mathbb{Z}$ mit $f(y+1) = \sum_{i=0}^{(p-1)p} a_i y^i$. Es gilt $a_0 = \varphi(f)(0) = f(1) = p$.

Es gilt auch $(x^p - 1)f(x) = x^p + x^{2p} + \dots + x^{p^2} - 1 - x^p - x^{2p} - \dots - x^{(p-1)p} = x^{p^2} - 1$.

Wir arbeiten nun modulo p : sei $\bar{f}(y+1) = \sum_{i=0}^{(p-1)p} \bar{a}_i y^i \in (\mathbb{Z}/p\mathbb{Z})[y]$. Es gilt $(x^p - 1)\bar{f}(x) = x^{p^2} - 1$, also $((y+1)^p - 1)f(y+1) = (y+1)^{p^2} - 1$. Da $(y+1)^p \equiv y^p + 1 \pmod{p}$, es gilt $(y+1)^p - 1 \equiv y^p$, und $(y+1)^{p^2} - 1 \equiv (y^p + 1)^p - 1 \equiv y^{p^2} + 1 - 1 \equiv y^{p^2}$. Das heißt, $y^p \bar{f}(y+1) \equiv y^{p^2} \pmod{p}$, aus wer folgt $y^p(\bar{f}(y+1) - y^{p-1}p) \equiv 0 \pmod{p}$, also $\bar{f}(y+1) - y^{p-1}p \equiv 0 \pmod{p}$. Das heißt, $\bar{f}(y+1) \equiv \sum_{i=0}^{(p-1)p} \bar{a}_i y^i \equiv y^{(p-1)p} \pmod{p}$, also, $a_i \equiv 0 \pmod{p}$ für alle $i < (p-1)p$, und $a_{(p-1)p} \equiv 1 \pmod{p}$.

Wir haben dann, dass $p|a_i$ für alle $i < (p-1)p$, $p \nmid a_{(p-1)p}$, und $p^2 \nmid a_0$. Bei der Einsenstein Kriterium, folgt dass $f(y+1)$ irreduzibel in $\mathbb{Q}[y]$ ist. Da φ ein Isomorphismus ist, ist auch $f(x) = \varphi^{-1}(f)$ irreduzibel.