

Aufgabe	A1	A2	A3	A4	A5	Σ
Punkte						

Aufgabe 1. (a) Es ist $f = X^5 - 3$ Minimalpolynom von $\sqrt[5]{3}$, denn $f(\sqrt[5]{3}) = 3 - 3 = 0$ und f ist primitiv und damit irreduzibel nach Eisenstein mit $p = 3$.

(b) Es ist $f = X^4 - X^2 + 1$ Minimalpolynom von $\sqrt{2} + \sqrt{3}$. Denn es ist $f(\sqrt{2} + \sqrt{3}) = 0$.

Weiter ist $2 + 2\sqrt{2}\sqrt{3} + 3 = (\sqrt{2} + \sqrt{3})^2 \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, also da $2, 3 \in \mathbb{Q}$ auch $\sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Damit folgt $(\sqrt{2} + \sqrt{3})\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und damit $2\sqrt{3} + 3\sqrt{2} - 2(\sqrt{2} + \sqrt{3}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und damit auch $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Damit folgt, da $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, dass $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Und es gilt weiter mit $g = X^2 - 2 \in \mathbb{Q}(\sqrt{3})[X]$, $g(\sqrt{2}) = 0$ und $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, dass $1 < [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \leq 2$ also damit $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$. Analog mit $h = X^2 - 3$ folgt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Insgesamt folgt mit Gradsatz $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Damit ist f bereits normiertes Polynom kleinsten Grades mit $f(\sqrt{2} + \sqrt{3}) = 0$, also f Minimalpolynom.

(c) Es ist $f = X^4 - \frac{5}{4}X^2 + \frac{5}{16}$ Minimalpolynom von $\sin(\frac{2\pi}{5})$, denn $\sin(\frac{2\pi}{5}) = \frac{1}{4}\sqrt{2(5 + \sqrt{5})}$ und damit $f(\sin(\frac{2\pi}{5})) = 0$. Außerdem ist $16f = 16X^4 - 20X^2 + 5$ primitiv, denn $5 \nmid 16$ und wegen $5 \mid 20$ irreduzibel nach Eisenstein mit $p = 5$. Also auch f irreduzibel und damit Minimalpolynom.

(d) Es ist $f = X^4 - X^2 + 1$ Minimalpolynom von $e^{\frac{i\pi}{6}} - \sqrt{3}$, denn es ist mit Euler Identität mit Euler Identität mit Euler Identität mit Euler Identität

$$\begin{aligned}
 e^{\frac{\pi i}{6}} - \sqrt{3} &= \cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right) - \sqrt{3} \\
 &= \frac{\sqrt{3}}{2} - \frac{i}{2} - \sqrt{3} \\
 &= -\frac{\sqrt{3}}{2} + \frac{i}{2} \\
 &= -\cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right) \\
 &= -\cos\left(-\frac{\pi}{6}\right) - i \sin\left(-\frac{\pi}{6}\right) \\
 &= -e^{-\frac{\pi i}{6}}.
 \end{aligned}$$

Damit folgt $f(e^{\pi i/6} - \sqrt{3}) = f(-e^{-\pi i/6}) = 0$.

Da $e^{\frac{i\pi}{6}} - \sqrt{3} = \frac{i}{2} - \frac{\sqrt{3}}{2}$, bleibt es analog zu (b) zu zeigen, dass $\sqrt{3}, i \in \mathbb{Q}(i - \sqrt{3})$. Es ist $(i - \sqrt{3})^2 = 2 - 2i\sqrt{3}$, also $i\sqrt{3} \in \mathbb{Q}(i - \sqrt{3})$. Damit folgt $\mathbb{Q}(i - \sqrt{3}) \ni i\sqrt{3}(i - \sqrt{3}) - (i - \sqrt{3}) = -4i$, also $i \in \mathbb{Q}(i - \sqrt{3})$ und damit auch $\sqrt{3} \in \mathbb{Q}(i - \sqrt{3})$, also analog zu (b): $\mathbb{Q}(i - \sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$. Mit $g = X^2 + 1$, $g(i) = 0$ und $h = X^2 - 3$, $h(\sqrt{3}) = 0$, folgt damit analog zu (b) $[\mathbb{Q}(i - \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Also ist f bereits normiertes Polynom kleinsten Grades mit $f(e^{\pi i/6} - \sqrt{3}) = 0$, also f Minimalpolynom.

Aufgabe 2. (a) Es ist $f = X^4 - 2$ Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$, denn $f(\sqrt[4]{2}) = 0$ und f normiert und irreduzibel nach Eisenstein mit $p = 2$. Damit folgt $[K : \mathbb{Q}] = \deg(f) = 4$.

(b) Es ist $f = X^2 + 1$ Minimalpolynom von i über K , denn $f(i) = 0$ und f irreduzibel über $\mathbb{R}$, also insbesondere über $K \subseteq \mathbb{R}$. Damit ist $[L : K] = \deg(f) = 2$ und damit mit Gradsatz $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] \stackrel{(a)}{=} 2 \cdot 4 = 8$.

(c) Es ist $\sqrt[4]{2} \in L$, also auch $L \ni \sqrt[4]{2}^2 = \sqrt{2}$.

Weiter gilt $f = X^2 - 2$ normiert und irreduzibel nach Eisenstein mit $p = 2$, also Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$, denn $f(\sqrt{2}) = 0$. Damit folgt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(f) = 2$.

Außerdem ist $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $f = X^2 + 1$ normiert und irreduzibel über $\mathbb{R}$, also insbesondere über $\mathbb{Q}(\sqrt{2})$. Also ist f , wegen $f(i) = 0$, Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$. Damit folgt $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$.

Insgesamt folgt damit mit Gradsatz: $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4$.

- (d) Es ist $f = X^2 - 2\sqrt{2}X + 3$ Minimalpolynom von $\sqrt{2} + i$ über $\mathbb{Q}(\sqrt{2})$, denn $\sqrt{2} + i \notin \mathbb{Q}(\sqrt{2})$, also insbesondere $\mathbb{Q}(\sqrt{2} + i) \neq \mathbb{Q}(\sqrt{2})$. Damit ist f bereits normiertes Polynom kleinsten Grades, also Minimalpolynom von $\sqrt{2} + i$ über $\mathbb{Q}(\sqrt{2})$.

Es ist $i \in \mathbb{Q}(\sqrt{2} + i)$, denn mit $(\sqrt{2} + i)^2 = 1 + 2i\sqrt{2}$ folgt $i\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$, also auch $\mathbb{Q}(\sqrt{2} + i) \ni \sqrt{2}i(\sqrt{2} + i) + (\sqrt{2} + i) = 2i - \sqrt{2} + \sqrt{2} + i = 3i$. Damit folgt auch $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$. Da $\sqrt{2} + i \in \mathbb{Q}(\sqrt{2}, i)$ folgt insgesamt $\mathbb{Q}(\sqrt{2} + i) = \mathbb{Q}(\sqrt{2}, i)$.

Aufgabe 3. (a) Beh.: Ist $[L : K] = p$ eine Primzahl, dann ex. ein $\alpha \in L$ mit $L = K(\alpha)$.

Beweis. Es ist $[L : K] = p < \infty$. Das heißt $\exists \alpha_1, \dots, \alpha_n \in L$ mit $\alpha_1, \dots, \alpha_n$ algebraisch mit $L = K(\alpha_1, \dots, \alpha_n)$. Dann folgt

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \dots \subseteq K(\alpha_1, \dots, \alpha_n) = L.$$

Mit Gradsatz folgt damit

$$p = [L : K] = [K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})] \cdot \dots \cdot [K(\alpha_1) : K].$$

Da p Primzahl sind alle Faktoren 1 bis auf einer. oE.: $[K(\alpha_1) : K] = p$. Damit sind $K(\alpha_1) = K(\alpha_1, \alpha_2) = \dots = K(\alpha_1, \dots, \alpha_n) = L$. $\square$

- (b) Beh.: Ist $[L : K] = 2^k$ und $f \in K[X]$ Polynom vom Grad 3 mit Nullstelle in L , dann hat f auch Nullstelle in K .

Beweis. Sei $[L : K] = 2^k$ und $f \in K[X]$ mit $\alpha \in L$ und $f(\alpha) = 0$. Ang.: $\alpha \notin K$. Dann ist f bereits irreduzibel vom Grad 3 über K , da f keine Nullstelle hat über Körper K . Damit $\exists g \in K[X]$ mit $g \stackrel{\wedge}{=} f$ und g normiert mit $\deg(g) = \deg(f) = 3$. Dann ist g Minimalpolynom von α über K . Also folgt $[K(\alpha) : K] = 3$ und damit nach Gradsatz

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = 3n$$

für ein $n \in \mathbb{N}$. Also $2^k = 3n$ $\nmid$, denn einziger Primfaktor von 2^k ist 2. $\square$

- (c) Beh.: Ist $[L : K]$ ungerade und $L = K(\alpha)$ für ein $\alpha \in L$, so gilt $L = K(\alpha^2)$.

Beweis. Sei $\alpha \in L$ mit $L = K(\alpha)$ und $K(\alpha) \neq K(\alpha^2)$. Da $\alpha^2 \in K(\alpha)$ ist $K \subseteq K(\alpha^2) \subseteq K(\alpha)$. Da aber $K(\alpha) \neq K(\alpha^2)$ ist $[K(\alpha) : K(\alpha^2)] \geq 2$. Da außerdem mit $f = X^2 - \alpha^2 \in K(\alpha^2)[X]$ gilt, dass $f(\alpha) = 0$, folgt $[K(\alpha) : K(\alpha^2)] \leq 2$, also insgesamt $[K(\alpha) : K(\alpha^2)] = 2$. Damit folgt mit Gradsatz

$$[L : K] = [K(\alpha) : K(\alpha^2)] \cdot [K(\alpha^2) : K] = 2n$$

für ein $n \in \mathbb{N}$, also insbesondere $[L : K]$ gerade. $\square$

Aufgabe 4. (a) Beh.: $\overline{K}$ ist unendlich.

Beweis. Sei $\overline{K}$ endlich. Dann sei $\overline{K} = \{a_1, \dots, a_n\}$ mit $n \in \mathbb{N}$. Betrachte $f = (X - a_1)(X - a_2) \dots (X - a_n) + 1$. Dann ist $\deg(f) \geq 1$, denn $\overline{K}$ Körper, insbesondere $0, 1 \in \overline{K}$, also $n \geq 2$.

Aber f hat keine Nullstelle in $\overline{K}$, denn $\forall a \in \overline{K} : (a - a_1)(a - a_2) \dots (a - a_n) = 0$, also $f(a) = 1$. Also $\overline{K}$ nicht algebraisch abgeschlossen. $\square$

- (b) Beh.: K abzählbar $\implies \overline{K}$ abzählbar.

Beweis. Sei K abzählbar. Dann existieren abzählbar viele Polynome über K , insbesondere abzählbar viele normierte, irreduzible Polynome, also insbesondere abzählbar viele algebraische Elemente $\alpha \in \overline{K}$ über K . Also $\overline{K}$ abzählbar. $\square$

- (c) Beh.: Es existieren Zahlen $z \in \mathbb{C}$, die transzendent über $\overline{\mathbb{Q}}(\pi)$ sind.

Beweis. Ang. alle Elemente $z \in \mathbb{C}$ sind algebraisch über $\overline{\mathbb{Q}}(\pi)$. Da $\mathbb{C}$ algebraisch abgeschlossen folgt damit, dass $\mathbb{C}$ ein algebraischer Abschluss von $\overline{\mathbb{Q}}(\pi)$ ist. Allerdings ist $\mathbb{Q}$ abzählbar, nach (b) insbesondere $\overline{\mathbb{Q}}$ abzählbar und $\overline{\mathbb{Q}}(\pi) \cong \overline{\mathbb{Q}}^2$ abzählbar. Damit ist erneut nach (b) $\mathbb{C}$ abzählbar $\nless$. $\square$

(d) Beh.: $\overline{K}(X)$ ist nicht algebraisch abgeschlossen.

Beweis. Betrachte $f = T^2 - X \in \overline{K}(X)[T]$. Ang. f hat Nullstelle $g \in \overline{K}(X)$. Also $g = \frac{p}{q}$ für $p, q \in \overline{K}[X]$ mit $p, q \neq 0$ da $f \neq 0$, also $\deg(p), \deg(q) \geq 0$. Aus $f(g) = 0$ folgt $\left(\frac{p}{q}\right)^2 = X$, also $p^2 = Xq^2$. Damit

$$\deg(p^2) = \deg(X) + \deg(q^2) = 1 + \deg(q^2).$$

Nach Gradsatz ist $\deg(p^2) = 2\deg(p)$ und $\deg(q^2) = 2\deg(q)$, also folgt

$$\underbrace{2\deg(p)}_{\in 2\mathbb{Z}} = 1 + \underbrace{2\deg(q)}_{\notin 2\mathbb{Z}} \quad \nless.$$

$\square$

Aufgabe 5. (a) Beh.: $(K^\times)^2 = \text{Bild}(\varphi)$ Untergruppe vom Index 2 in $K^\times$.

Beweis. Sei K endlich und $\text{char}(K) \neq 2$.

Es ist zunächst für $a, b \in K^\times$: $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$. Also φ Grp.hom und damit im φ Untergruppe in $K^\times$.

Dann sei $a \in K^\times$ mit $\varphi(a) = 1$. Dann folgt, da K Körper, insbesondere nullteilerfrei

$$a^2 = 1 \implies a^2 - 1 = 0 \implies (a+1)(a-1) = 0 \implies a = 1 \vee a = -1.$$

Es folgt also $\ker \varphi = \{1, -1\}$. Ang.: $1 = -1$, dann ist $0 = 1 + (-1) = 1 + 1$, also $\text{char}(K) = 2$ $\nless$. Also folgt $\text{ord}(\ker \varphi) = 2$ (*).

Dann ist nach Homomorphiesatz $K^\times / \ker \varphi \cong \text{im } \varphi$, insbesondere

$$K^\times : \ker \varphi = \text{ord}(K^\times / \ker \varphi) = \text{ord}(\text{im } \varphi) \quad (**).$$

Außerdem gilt nach Satz von Lagrange

$$K^\times : \text{im } \varphi \stackrel{\text{Lagrange}}{=} \frac{\text{ord}(K^\times)}{\text{ord}(\ker \varphi)} \stackrel{(**)}{=} \frac{\text{ord}(K^\times)}{K^\times : \ker \varphi} \stackrel{\text{Lagrange}}{=} \text{ord}(\ker \varphi) \stackrel{(*)}{=} 2.$$

$\square$

(b) Beh.: Eine der Zahlen $-1, -2, 2$ ist ein Quadrat.

Beweis. Sei K endlich. Falls $\text{char}(K) = 2$ folgt $-1 = 1$, denn $1 + 1 = 0$. Also ist $-1 = 1 = 1^2$ ein Quadrat.

Sei nun $\text{char}(K) \neq 2$. Ang.: -2 und 2 sind keine Quadrate. Betrachte φ aus (a). Dann ist $2, -2 \notin \text{im } \varphi$. Nach (a) gibt es jedoch nur zwei Nebenklassen bezüglich $\text{im } \varphi$ in $K^\times$. Also folgt $2 = -2$, also $(-2)^{-1}2 \in \text{im } \varphi$. Da $(-1)(-1) = 1$ folgt $(-1)^{-1} = -1$, also damit

$$-1 = (-1)^{-1} = (-1)^{-1} \cdot 1 = (-1)^{-1}2^{-1}2 = (-2)^{-1}2 \in \text{im } \varphi.$$

Also $\exists a \in K^\times$ mit $a^2 = -1$. Damit folgt da K nullteilerfrei

$$0 = -1 + 1 = -1 - (-1) = -1 - a^2 \implies (-1 - a)(-1 + a) = 0 \implies a = -1 \vee a = 1.$$

Also folgt

$$-1 = a^2 = (-1)^2 = 1 \vee -1 = a^2 = 1^2 = 1.$$

Also $-1 = 1$ und damit $0 = 1 + (-1) = 1 + 1$, also $\text{char } K = 2$ $\nless$. $\square$

(c) Beh.: $X^4 + 1 \in \mathbb{F}_p[X]$ für p Primzahl lässt sich als Produkt zweier quadratischer Polynome schreiben.

Beweis. Sei p Primzahl. Dann ist $\mathbb{F}_p[X]$ endlicher Körper, also nach (b) mindestens eine der Zahlen $-1, -2, 2$ ein Quadrat. Falls

- $\exists a \in \mathbb{F}_p^\times$ mit $a^2 = -1$: Dann ist

$$X^4 + 1 = X^4 - (-1) = X^4 - a^2 = (X^2 - a)(X^2 + a).$$

- $\exists a \in \mathbb{F}_p^\times$ mit $a^2 = 2$: Dann ist

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1)^2 - a^2X^2 = (X^2 + 1 - aX)(X^2 + 1 + aX).$$

- $\exists a \in \mathbb{F}_p^\times$ mit $a^2 = -2$: Dann ist

$$X^4 + 1 = (X^2 - 1)^2 - (-2)X^2 = (X^2 - 1)^2 - a^2X^2 = (X^2 - 1 - aX)(X^2 - 1 + aX).$$

Das zeigt die Behauptung. $\square$

(d) Beh.: $X^4 + 1$ ist irreduzibel in $\mathbb{Q}[X]$.

Beweis. Betrachte

$$f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

Dann ist $f(X + 1)$ irreduzibel nach Eisenstein mit $p = 2$ in $\mathbb{Q}[X]$, also auch f irreduzibel in $\mathbb{Q}[X]$. $\square$