Aufgabe 1

- $\sqrt[5]{3}$. $f := X^5 - 3$ ist irreduzibel über $\mathbb{Q}$ nach Eisenstein. Es gilt $f(\sqrt[5]{3}) = (\sqrt[5]{3})^5 - 3 = 0$. Also ist f das Minimalpolynom zu $\sqrt[3]{5}$.
- $\sqrt{2}+\sqrt{3}$. Es gilt $f := X^4 - 10X^2 + 1$ ist primitiv. In $\mathbb{Z}/3\mathbb{Z}$ gilt $0^4 - 0^2 + 1 = 1 \neq 0$, $1^4 - 1 + 1 = 1 \neq 0$ und $2^4 - 2^2 + 1 = 16 - 4 + 1 = 13 = 1 \neq 0$. Somit ist $X^4 - X^2 + 1$ irreduzibel in $\mathbb{Z}/3\mathbb{Z}$. Nach dem Reduktionskriterium für $p = 3$ ist $X^4 - 10X^2 + 1$ daher irreduzibel über $\mathbb{Q}$. Wegen
$$\begin{aligned}(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 &= (4 + 4\cdot 2\cdot\sqrt{6} + 6\cdot 2\cdot 3 + 4\cdot 3\cdot\sqrt{6} + 9) - 10(2 + 2\sqrt{6} + 3) + 1\\ &= 49 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1\\ &= 0\end{aligned}$$
ist $f(\sqrt{2}+\sqrt{3}) = 0$. Also ist f das Minimalpolynom zu $\sqrt{2}+\sqrt{3}$.
- $\sin(2\pi/5) = \sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}$. Das Polynom $f := 16X^4 - 20X^2 + 5$ ist primitiv. In $Z/2Z$ erhalten wir $f = 1$. Nach dem Reduktionskriterium für $p = 2$ folgt also, dass f irreduzibel ist. Es gilt außerdem
$$\begin{aligned} f\left(\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}\right) &= 16\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}^4 - 20\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}^2 + 5\\ &= 16\left(\frac{5}{8}+\frac{\sqrt{5}}{8}\right)^2 - 20\left(\frac{5}{8}+\frac{\sqrt{5}}{8}\right) + 5\\ &= 16\left(\frac{25}{64}+\frac{10\sqrt{5}}{64}+\frac{5}{64}\right) - \frac{50}{4} - \frac{10\sqrt{5}}{4} + \frac{20}{4}\\ &= \frac{30}{4} + \frac{10\sqrt{5}}{4} - \frac{50}{4} - \frac{10\sqrt{5}}{4} + \frac{20}{4}\\ &= 0.\end{aligned}$$
Also ist f das Minimalpolynom von $\sin(2\pi/5)$ über $\mathbb{Q}$.
- $e^{i\pi/6} - \sqrt{3}$. $f := X^4 - X^2 + 1$ ist irreduzibel über $\mathbb{Z}/2\mathbb{Z}$, da $0^4 - 0^2 + 1 \neq 0$ und $1^4 - 1^2 + 1 \neq 0$ gilt. Nach dem Reduktionskriterium für $p = 2$ folgt, dass f irreduzibel über $\mathbb{Q}$ ist. Es gilt $e^{i\pi/6} - \sqrt{3} = \frac{\sqrt{3}}{2} + \frac{i}{2} - \sqrt{3} = \frac{1}{2}(i - \sqrt{3})$. Daher erhalten wir
$$\begin{aligned}(e^{i\pi/6} - \sqrt{3})^4 - (e^{i\pi/6} - \sqrt{3})^2 + 1 &= \frac{1}{16}(i-\sqrt{3})^4 - \frac{1}{4}(i-\sqrt{3})^2 + 1\\ &= \frac{1}{16}(-1 - 2i\sqrt{3} + 3)^2 - \frac{1}{4}(-1 - 2i\sqrt{3} + 3) + 1\\ &= \frac{1}{4}(1 - i\sqrt{3})^2 - \frac{1}{2}(1 - i\sqrt{3}) + 1\\ &= \frac{1}{4}(1 - 2i\sqrt{3} - 3) - \frac{1}{2}(1 - i\sqrt{3}) + 1\\ &= -\frac{1}{2} - \frac{i}{2}\sqrt{3} - \frac{1}{2} + \frac{i}{2}\sqrt{3} + 1\\ &= 0\end{aligned}$$

Also ist f das Minimalpolynom von $e^{i\pi/6} - \sqrt{3}$ über $\mathbb{Q}$.

Aufgabe 2

(a) Sei $f = X^4 - 2$. Dann gilt $f(\sqrt[4]{2}) = 0$. Außerdem ist f nach Eisenstein irreduzibel über $\mathbb{Q}$ und damit Minimalpolynom von $\sqrt[4]{2}$. Es gilt daher $[K\colon \mathbb{Q}] = \deg f = 4$.

(b) Sei $f = X^2 + 1$. Dann gilt $f(i) = 0$. In L gilt $f = (X - i)(X + i)$. Wäre f reduzibel über K, so gäbe es in K eine Darstellung $f = a \cdot b$ mit $\deg a = \deg b = 1$. Wegen $K \subset L$ wäre dies auch eine Darstellung in L. Aufgrund der Eindeutigkeit der Primfaktorzerlegung müsste dann aber o.B.d.A. $a = X - i$ sein. Wegen $i \notin K$ ist dies ein Widerspruch. Also ist f das Minimalpolynom von i über K und $[L : K] = \deg f = 2$. Nach dem Gradsatz gilt außerdem $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 2 \cdot 4 = 8$.

(c) Es gilt $\sqrt{2} = (\sqrt[4]{2})^2 \in L$. Sei $f = X^2 - 2$. Dann gilt $f(\sqrt{2}) = 0$. Nach Eisenstein ist f aber bereits irreduzibel über $\mathbb{Q}$, also ist f das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ und es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg f = 2$. Nun ist $X^2 + 1$ aus völlig analogen Gründen wie in Teilaufgabe b das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$ und es gilt $[\mathbb{Q}(\sqrt{2}, i)\colon \mathbb{Q}(\sqrt{2})] = \deg X^2 + 1 = 2$. Insgesamt ergibt sich $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i)\colon \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

(d) Sei $f = X^2 - 2\sqrt{2}X + 3 \in \mathbb{Q}(\sqrt{2})$. Dann gilt $f(\sqrt{2} + i) = 1 + 2\sqrt{2}i - 4 - 2\sqrt{2}i + 3 = 0$. Wäre f reduzibel, so gäbe es eine Zerlegung in zwei Linearfaktoren über $\mathbb{Q}(\sqrt{2})$. Dann müsste mindestens einer der beiden Linearfaktoren $X - (\sqrt{2} + i)$ sein. Dann wäre aber $\sqrt{2} + i \in \mathbb{Q}(\sqrt{2})$. Das ist aber nicht der Fall, also muss f irreduzibel und damit das Minimalpolynom von $\sqrt{2} + i$ sein. Daher ist aber $[\mathbb{Q}(\sqrt{2}, \sqrt{2} + i) : \mathbb{Q}(\sqrt{2})] = 2$ und nach dem Gradsatz $\mathbb{Q}(\sqrt{2}, \sqrt{2} + i)\colon \mathbb{Q}] = 4$. Wegen $\sqrt{2} = \frac{1}{6}(5(\sqrt{2} + i) - (\sqrt{2} + i)^3)$ ist aber $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$ bereits enthalten. Also ist $\mathbb{Q}(\sqrt{2}+i, \sqrt{2}) = \mathbb{Q}(\sqrt{2}+i)$. Offensichtlich ist $\sqrt{2}+i \in \mathbb{Q}(\sqrt{2}, i)$ und damit $\mathbb{Q}(\sqrt{2}+i) \subset \mathbb{Q}(\sqrt{2}, i)$. Wegen $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + i) = \dim_Q \mathbb{Q}(\sqrt{2} + i, \sqrt{2}) = 4 = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, i)$ folgern wir mit LA1, dass dann $\mathbb{Q}(\sqrt{2} + i) = \mathbb{Q}(\sqrt{2}, i)$ gelten muss.

Aufgabe 3

(a) Angenommen, es gäbe kein solches α. Da L/K endlich ist, wäre dann $L = K(\alpha_1, \dots, \alpha_n)$. Insbesondere gäbe es einen Körper $K \subsetneq K(\alpha_1) \subsetneq L$. Da $[L\colon K]$ eine Primzahl ist, kann es nach Korollar 3.14 eine solche Inklusionskette von Körpern nicht geben.

(b) Wir nehmen an, dass f keine Nullstelle in K besitzt. Dann ist f über K irreduzibel. Ist nun $\alpha \in L$ eine Nullstelle von f, so ist f das Minimalpolynom von α in K. Somit erhalten wir

$$2^k = [L\colon K] = [L\colon K(\alpha)] \cdot [K(\alpha)\colon K] = [L\colon K(\alpha)] \cdot 3,$$

das kann aber für $k \in \mathbb{N}$ nicht sein. Also muss f eine Nullstelle in K besitzen.

(c) Sei $f \in K[X]$ das Minimalpolynom von α. Dann gilt $\deg f = 2n + 1$. Jedes Polynom lässt sich in der Form $f(X) = X \cdot g(X^2) + h(X^2)$ schreiben. Wegen $\deg f = 2n + 1$, muss $g \neq 0$ sein, sonst wäre $f(X) = h(X^2)$ und der Grad von f wäre gerade. Insbesondere erhalten wir also

$$0 = f(\alpha) = \alpha \cdot g(\alpha^2) + h(\alpha^2) \implies \alpha = -\frac{h(\alpha^2)}{g(\alpha^2)}.$$

Daher gilt $\alpha \in K(\alpha^2)$ und damit $K(\alpha) \subset K(\alpha^2)$. Die Inklusion $K(\alpha^2) \subset K(\alpha)$ ist trivial. Daher gilt $K(\alpha) = K(\alpha^2)$.

Aufgabe 4

(a) Sei $N := |\overline{K}|$. Da $\overline{K}$ ein algebraischer Abschluss ist, besitzt jedes $f \in \overline{K}[X]$ eine Nullstelle in $\overline{K}$. Wir betrachten die normierten Polynome vom Grad 2. Die Anzahl dieser Polynome ist gerade N^2, da es sowohl für den ersten als auch für den zweiten N mögliche Wahlen gibt. Da f in Linearfaktoren zerfällt, besitzt jedes f auch eine Darstellung der Form $f(x) = (x-a)(x-b)$. Da die Reihenfolge der beiden Faktoren egal ist, gibt es nur $N^2/2$ Möglichkeiten für eine Darstellung in Produktform. Zu jedem $f = x^2+ax+b$ gibt es aber eine eindeutige Darstellung in Produktform. Das ist ein Widerspruch. Also muss $|\overline{K}|$ unendlich sein.

(b) Wir gehen an der Konstruktion im Skript entlang. Ist K abzählbar, so ist auch $K[X]$ abzählbar. Damit ist auch $I = \{f \in K[x],\ \deg f \geq 1\}$ und $\mathbb{N}_0^{(I)}$ abzählbar. Dann muss aber $K[\mathfrak{X}]$ und somit auch L_1 abzählbar sein. Führt man diese Konstruktion fort, so ist L_i abzählbar $\forall i \in \mathbb{N}$. Dann ist aber auch die abzählbare Vereinigung $\bigcup_{i=1}^{\infty} L_i$ abzählbar.

(c) Da $\overline{Q}$ abzählbar ist, ist auch $\overline{Q}[X]$ und daher $\overline{Q}[\pi] \cong \overline{Q}(\pi)$ abzählbar. Dann ist auch $\overline{\overline{Q}(\pi)}$ abzählbar. Gäbe es keine transzendenten Zahlen über $\overline{Q}(\pi)$, so wäre $\mathbb{C} \subset \overline{Q}(\pi)$ und daher insbesondere abzählbar. $\mathbb{C}$ ist aber nicht abzählbar. Also muss es komplexe Zahlen geben, die transzendent über $\overline{Q}(\pi)$ sind.

(d) **fehlt**

Aufgabe 5

(a) $(K^\times)^2$ ist eine Untergruppe von $K^\times$. Es gilt nämlich $1 = 1^2 \in (K^\times)^2$, $a^2, b^2 \in (K^\times)^2 \implies a^2b^2 = (ab)^2 \in (K^\times)^2$ und $a^2 \in (K^\times)^2 \implies (a^{-1})^2 \in (K^\times)^2$ mit $a^2 \cdot (a^{-1})^2 = 1$. Es gilt $\overline{1} = \{a^2\colon\ a \in K^\times\}$. Es gilt $\ker\varphi = \{a \in K^\times\colon\ a^2 = 1\}$. Wegen $(p-1)^2 = p^2 - 2p + 1 = 1 \mod p$ ist $(p-1) \in \ker\varphi$. Da K ein Körper ist, hat das Polynom $x^2 - a$ höchstens zwei Nullstellen. Daher ist $\ker\varphi = \{1, p-1\}$. Also liefert uns der Homomorphiesatz $K^\times/\ker\varphi \cong \operatorname{im}\varphi = (K^\times)^2$. Eine Äquivalenzklasse in $K^\times/\ker\varphi$ hat dabei stets die Form $\{a, -a\}$ für ein $a \in K^\times$ und damit genau 2 Elemente. Da K^x in die disjunkte Vereinigung der Äquivalenzklassen zerfällt gilt $|K^\times| = |K^\times/\{-1,1\}| \cdot |\{1,-1\}| = |(K^\times)^2| \cdot 2$, also hat $(K^\times)^2$ den Index 2.

(b) Angenommen, keine der drei Zahlen ist ein Quadrat. Dann liegen alle drei in $K^\times \setminus (K^\times)^2$. Da es sich hierbei um eine Äquivalenzklasse in $K^\times/(K^\times)^2$ handelt, muss $-2 = 2 \cdot -1 = 2 \cdot (-1)^{-1} \in (K^\times)^2$ gelten. Damit haben wir bereits einen Widerspruch konstruiert.

(c) Ist $-1 = a^2$ für ein $a \in K^\times$, so schreiben wir $X^4+1 = X^4-(-1) = (X^2-a)(X^2+a)$. Ist $2 = a^2$ für ein $a \in K^\times$, so schreiben wir $X^4+1 = (X^2+1)^2-2X^2 = (X^2+1+aX)(X^2+1-aX)$. Ist $-2 = a^2$ für ein $a \in K^\times$, so schreiben wir $X^4+1 = (X^2-1)^2 - (-2)X^2 = (X^2-1+aX)(X^2-1-aX)$.

(d) Angenommen, X^4+1 ist reduzibel. Dann existiert eine Zerlegung in Polynome vom Grad ≥ 1 mit Koeffizienten in $\mathbb{Q}$. Per Inklusion können wir diese Faktoren als Polynome in $\mathbb{C}$ auffassen. Wegen $(\frac{\sqrt{2}}{2} + i \cdot \frac{\sqrt{2}}{2})^4 + 1 = 0$, muss aufgrund der Eindeutigkeit der Primfaktorzerlegung einer der Faktoren aus $\mathbb{Q}[X]$ assoziert sein zu $(X - (\frac{\sqrt{2}}{2} + i \cdot \frac{\sqrt{2}}{2}))$. Da aber $i \notin \mathbb{Q}$, erhalten wir sofort einen Widerspruch. Also muss $X^4 + 1$ irreduzibel sein.