Aufgabe 1

(a) Es genügt zu zeigen, dass

(i) alle Nullstellen von $X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$ in $L = \mathbb{Q}(\sqrt[4]{2}, i)$ liegen. Das ist allerdings aus der Produktdarstellung von $X^4 - 2$ sofort offensichtlich.

(ii) $L = \mathbb{Q}(\sqrt[4]{2}, i)$ wird von den Nullstellen von $X^4 + 2$ erzeugt. Wegen $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ ist $\mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ und wird damit von den Nullstellen von $X^4 - 2$ erzeugt.

(b) Sei σ ein $\mathbb{Q}$-Automorphismus von L. Dann gilt $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Nach Lemma 3.40 ist die Anzahl der verschiedenen $\mathbb{Q}$-Homomorphismen $\sigma\colon \mathbb{Q}(\sqrt[4]{2}) \to L$ gleich

$$|\{\alpha \in L | f^\sigma(\alpha) = f(\alpha) = 0\}| = 4,$$

wobei $f = X^4 - 2 \in \mathbb{Q}[X]$ das Minimalpolynom zu $\sqrt[4]{2}$ über $\mathbb{Q}$ bezeichne (siehe letzter Zettel) und $f^\sigma = f$ wegen $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Die einzelnen Fortsetzungen sind nach Lemma 3.40 (ii) eindeutig bestimmt durch ihren Wert auf $\alpha = \sqrt[4]{2}$. Da $g = X^2 + 1$ das Minimalpolynom zu i über $\mathbb{Q}(\sqrt[4]{2})$ darstellt, ist die Anzahl der verschiedenen Fortsetzungen auf ganz $L = \mathbb{Q}(\sqrt[4]{2})(i)$ nach Lemma 3.40 gleich

$$|\{\alpha \in L | g^\sigma(\alpha) = 0\}| = |\{\alpha \in L | \sigma(1)X^2 + \sigma(1) = 0\}| = |\{i, -i\}| = 2.$$

Die einzelnen Fortsetzungen sind nach Lemma 3.40 (ii) eindeutig bestimmt durch ihren Wert auf $\alpha = i$. Daher können wir jeden der 4 $\mathbb{Q}$-Homomorphismen auf zwei verschiedene Weisen zu einem L-Automorphismus fortsetzen, sodass wir insgesamt 8 $\mathbb{Q}$-Automorphismen erhalten, die eindeutig durch ihre Werte auf $\sqrt[4]{2}$ und i gegeben sind.

1. $\sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto i$
2. $\sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i$
3. $\sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto i$
4. $\sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto -i$
5. $\sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i$
6. $\sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto -i$
7. $\sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto i$
8. $\sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto -i$

(c) 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 2

1. Es gilt $X^4+4=(X-\sqrt{2}e^{i\frac{\pi}{4}})(X-\sqrt{2}e^{i\frac{3\pi}{4}})(X-\sqrt{2}e^{i\frac{5\pi}{4}})(X-\sqrt{7}e^{i\pi})$. Der Zerfällungskörper von X^4+4 ist daher durch $\mathbb{Q}(\sqrt{2}e^{i\frac{\pi}{4}}, \sqrt{2}e^{i\frac{3\pi}{4}}, \sqrt{2}e^{i\frac{5\pi}{4}}, \sqrt{2}e^{i\frac{7\pi}{4}})$ gegeben. Wegen $\sqrt{2}e^{i\frac{3\pi}{4}} = \frac{1}{2}\left(\sqrt{2}e^{i\frac{\pi}{4}}\right)^3$, $\sqrt{2}e^{i\frac{5\pi}{4}} = \frac{1}{4}\left(\sqrt{2}e^{i\frac{\pi}{4}}\right)^5$ und $\sqrt{2}e^{i\frac{7\pi}{4}} = \frac{1}{8}\left(\sqrt{2}e^{i\frac{\pi}{4}}\right)^7$ wird dieser Körper bereits von $\sqrt{2}e^{i\frac{\pi}{4}}$ erzeugt. Da keine der Nullstellen von X^4+4 in $\mathbb{Q}$ liegt, ist das Polynom irreduzibel und damit das Minimalpolynom zu $\sqrt{2}e^{i\frac{\pi}{4}}$. Also hat die Erweiterung $L\colon \mathbb{Q}$ Grad 4.

2. Es gilt $X^8-1=(X-e^{i\frac{\pi}{4}})(X-e^{i\frac{\pi}{2}})(X-e^{i\frac{3\pi}{4}})(X-e^{i\pi})(X-e^{i\frac{5\pi}{4}})(X-e^{i\frac{3\pi}{2}})(X-e^{i\frac{7\pi}{4}})(X-e^{i2\pi})$. Analog zum Polynom X^4+4 lässt sich hier jede Nullstelle als Potenz von $e^{i\frac{\pi}{4}}$ schreiben. Daher ist der Zerfällungskörper von X^8-1 einfach $\mathbb{Q}(e^{i\frac{\pi}{4}})$. Wegen $\left(e^{i\frac{\pi}{4}}\right)^4+1=0$ ist X^4+1 das Minimalpolynom zu $e^{i\frac{\pi}{4}}$ (Irreduzibilität folgt aus der Bonusaufgabe auf dem letzten Zettel). Insbesondere hat also $\mathbb{Q}(e^{i\frac{\pi}{4}})/\mathbb{Q}$ Grad 4.

3. Es gilt
$$\begin{aligned} X^4+2X^2-2 &= (X^2+1+\sqrt{3})(X^2+1-\sqrt{3}) \\ &= (X+\sqrt{1+\sqrt{3}})(X-\sqrt{1+\sqrt{3}})(X+\sqrt{1-\sqrt{3}})(X+\sqrt{1-\sqrt{3}}) \end{aligned}$$
Der Zerfällungskörper von X^4+2X^2-2 ist daher $\mathbb{Q}(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}})$. Die Erweiterung $\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$ hat Grad 4, da X^4+2X^2-2 nach Eisenstein irreduzibel ist und damit Minimalpolynom zu $\sqrt{1+\sqrt{3}}$. Da $\sqrt{1-\sqrt{3}}$ einen nicht verschwindenden Imaginärteil hat, kann es nicht in $\mathbb{Q}(\sqrt{1+\sqrt{3}}) \subset \mathbb{R}$ enthalten sein. Da das Polynom $X^2+\sqrt{1+\sqrt{3}}^2-2$ die beiden Nullstellen $\pm\sqrt{1-\sqrt{3}}$ besitzt, ist es folglich irreduzibel über $\mathbb{Q}(\sqrt{1+\sqrt{3}})$. Also hat die Erweiterung $\mathbb{Q}(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}})/\mathbb{Q}(\sqrt{1+\sqrt{3}})$ Grad 2. Insgesamt hat die Erweiterung daher Grad $8=4\cdot 2$.

Aufgabe 3

(a) Sei $f \in K[X]$ das Minimalpolynom zu α. Sei
$$M \coloneqq \{x \in L\colon f(x)=0\}.$$
die Menge der Nullstellen von f, wobei die Koeffizienten von f gemäß der Körpererweiterung L/K als Elemente von L auffassen. Da σ ein K-Automorphismus ist, gilt $0=f^{\sigma_i}(\sigma_i(x)) = f(\sigma_i(x))\forall x \in M$. Also ist $\sigma_i(\alpha) \in M$. M enthält also die n verschiedenen Elemente $\sigma_i(\alpha)\forall 1 \le i \le n$. Damit hat f mindestens Grad n. Allerdings hat f auch höchstens Grad n, da $[L\colon K]=n$ ist. Daher ist $\deg f = n$. Damit ist $[K(\alpha)\colon K]=n$. Insbesondere ist also $\dim_K K(\alpha) = \dim_K L$, $K(\alpha) \subset L$ und nach LA1 also $K(\alpha)=L$.

(b) Da Körperhomomorphismen stets injektiv sind, genügt es zu zeigen, dass jedes $\alpha \in L$ ein Urbild $a \in L$ unter $\sigma\colon L \to L$ besitzt, wobei es sich bei σ um einen K-Homomorphismus handelt, d.h.
$$\begin{aligned} \sigma_K\colon K &\to L \\ k &\mapsto k. \end{aligned}$$

Sei also $\alpha \in L$. Da die Erweiterung algebraisch ist, existiert ein Minimalpolynom $f \in K[X]$ mit $f(\alpha) = 0$, wobei wir hier und in der nächsten Definition die Koeffizienten von f gemäß der Körpererweiterung L/K als Elemente von L auffassen. Sei also

$$M \coloneqq \{x \in L \colon f(x) = 0\}.$$

die Menge der Nullstellen von f. Nach Lemma 3.40 ist dann auch $0 = f^\sigma(\sigma(x)) = f(\sigma(x)) \forall x \in M$, wobei die letzte Gleichheit gilt, weil $\sigma_K = \mathrm{id}_K$ ist. Daraus folgt $\sigma(M) \subset M$. Da M eine endliche Menge und f injektiv ist, muss aber bereits $f^\sigma(M) = M$ gelten und wegen $\alpha \in M$ existiert ein Urbild $a \in M$ mit $\sigma(a) = \alpha$. Ist die Körpererweiterung nicht algebraisch, so gilt die Aussage nicht. Für die Körpererweiterung $K(t)/K$ ist

$$\begin{aligned} \sigma \colon K(t) \to K(t)k && \mapsto k \forall k \in K \\ t \mapsto t^2 && \end{aligned}$$

ein K-Homomorphismus, der nicht surjektiv ist, weil t kein Urbild besitzt.

Aufgabe 4

(a) Sei $0 \neq \alpha \in R$. Da R ein Ring ist, gilt $K[\alpha] \subset R$. Dann gilt nach Satz 3.20 $K[\alpha] = K(\alpha)$. Insbesondere ist also auch $\alpha^{-1} \in R$. Daher ist $R^\times = R \setminus \{0\}$ und folglich ist R ein Körper.

(b) Es gilt $K \subset E, F \subset L$, wobei K und L Körper sind. Daher genügt es zu zeigen, dass $M = \{\sum_{i=1}^n a_i b_i | n \in \mathbb{N}, a_i \in E, b_i \in F\}$ bezüglich Addition und Multiplikation abgeschlossen ist. Es gilt

$$\sum_{i=1}^n a_i b_i + \sum_{i=1}^m a'_i b'_i \overset{\text{Umnummerierung}}{=} \sum_{i=1}^{n+m} a_i b_i \in M.$$

Außerdem gilt

$$\left(\sum_{i=1}^n a_i b_i\right)\left(\sum_{j=1}^m a'_j b'_j\right) = \sum_{(i,j) \in \{1,\dots,n\} \times \{1,\dots,m\}} \underbrace{a_i a'_j}_{\alpha_k} \underbrace{b_i b'_j}_{\beta_k} = \sum_{k=1}^{n \cdot m} \alpha_k \beta_k \in M.$$

Nach Aufgabe (a) muss M also ein Körper sein. Offensichtlich muss jedes Element von M in EF enthalten sein. Daher ist M gerade der kleinste Teilkörper, der E und F enthält.

(c) Sind $[E : K]$ und $[F : K]$ endlich, so gilt $E = K(\alpha_1, \dots, \alpha_n)$ und $F = K(\beta_1, \dots, \beta_m)$. Dann ist $EF \subset K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$, da $K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ die beiden Körper E und F enthält. Jeder Körper, der E und F enthält, enthält auch sofort $\alpha_1, \dots, \alpha_n$ und $\beta_1, \dots, \beta_m$. Also ist auch $K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \subset EF$.

$$\dim_K EF = \dim_K K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m).$$

Sei f_i das Minimalpolynom von α_i über $K(\alpha_1, \dots, \alpha_{i-1})$ und analog g_i das Minimalpolynom von β_i über $K(\beta_1, \dots, \beta_{i-1})$.

$$[E : K] = \prod_{i=1}^n \deg f_i \qquad [F : K] = \prod_{i=1}^m \deg g_i$$

Sei außerdem h_i das Minimalpolynom von β_i über $K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{i-1})$. Dann gilt $\deg h_i \leq \deg g_i$ und

$$[K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \colon K(\alpha_1, \dots, \alpha_n)] = \prod_{i=1}^{n} \deg h_i$$

$$\begin{aligned}
[EF \colon K] &= [K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \colon K] \\
&= [K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \colon K(\alpha_1, \dots, \alpha_n)] \cdot [K(\alpha_1, \dots, \alpha_n) : K] \\
&= \prod_{i=1}^{n} \deg h_i \cdot \prod_{i=1}^{n} \deg f_i \\
&\leq \prod_{i=1}^{n} \deg g_i \cdot \prod_{i=1}^{n} \deg f_i \\
&= [F : K] \cdot [E : K]
\end{aligned}$$

(d) Sind $[F : K]$ und $[E : K]$ teilerfremd, so gibt es keine Darstellung $E = K(\alpha_1, \dots, \alpha_n)$ und $F = K(\beta_1, \dots, \beta_m)$, sodass es α_i, β_j und zugehörige Minimalpolynome f_i, g_j gibt mit $\deg f_i = \deg g_j$. Also kann es kein Element a in $F \setminus K$ geben, dass auch in $E \setminus K$ liegt. Sonst könnte man o.B.d.A. $\alpha_1 = a$ und $\beta_1 = a$ wählen und erhielte zwei identische Minimalpolynome mit insbesondere gleichem Grad. Daher ist $[E(\beta_1, \dots, \beta_i) : E(\beta_1, \dots, \beta_{i-1})] = [K(\beta_1, \dots, \beta_i) : K(\beta_1, \dots, \beta_{i-1})]$. Insbesondere ist also stets $\deg h_i = \deg g_i$. Damit wird die Abschätzung in Aufgabe (c) zu einer Gleichheit.