Aufgabe 1

(a) Wir führen einen Induktionsbeweis. Sei L/K eine Körpererweiterung, sodass L Zerfällungskörper zu $f \in K[X]$ mit $\deg f = 1$ ist. Dann ist $[L\colon K] = 1 \leq 1!$. Sei die Behauptung also für alle L/K bewiesen, wobei L Zerfällungskörper zu einem $f \in K[X]$ mit $\deg f \leq n-1$ sind. Wir betrachten nun eine Körpererweiterung L/K, wobei L Zerfällungskörper zu einem $f \in K[X]$ mit $\deg f = n$ ist. Seien $\alpha_1, \dots, \alpha_n \in L$ die Nullstellen von f. Dann ist $f(\alpha_1) = 0$ mit $f \in K[X]$, also ist f ein Vielfaches des Minimalpolynoms von α_1 in K. Insbesondere ist $[K(\alpha_1)\colon K] \leq \deg f = n$. Daraus folgt

$$[L\colon K] = [K(\alpha_1, \dots, \alpha_n)\colon K(\alpha_1)] \cdot [K(\alpha_1)\colon K] \leq (n-1)! \cdot n = n!.$$

Damit ist die Aussage bereits bewiesen.

(b) Offensichtlich ist $\bigcap_{i\in I} L_i/K$ eine Teilerweiterung von L_i/K für beliebiges i und damit ebenfalls algebraisch. Sei $\alpha \in \bigcap_{i\in I} L_i$ und $f \in K[X]$ mit $f(\alpha) = 0$. Da L_i eine normale Erweiterung ist, zerfällt f in Linearfaktoren über L_i. Insbesondere liegen alle Nullstellen von f in L_i. Da dies für beliebiges i gilt, liegen alle Nullstellen von f in $\bigcap_{i\in I} L_i$. Daher zerfällt f auch über $\bigcap_{i\in I} L_i$ in Linearfaktoren. Folglich ist $\bigcap_{i\in I}$ ebenfalls algebraisch und normal.

Aufgabe 2

(a) Es gilt $N = \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Wir definieren $\sigma_{\zeta,\varepsilon} \in \mathrm{Gal}(L/\mathbb{Q})$ durch $\sigma_{\zeta,\varepsilon}(\sqrt[4]{2}) = \zeta\sqrt[4]{2}$ und $\sigma_{\zeta,\varepsilon}(i) = \varepsilon i$. Wir erhalten daher folgende Zuordnung:

$$\begin{aligned}
\sigma_{1,1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\sigma_{1,-1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ \sqrt[4]{2} & -i\sqrt[4]{2} & -\sqrt[4]{2} & i\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\
\sigma_{i,1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} & \sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\
\sigma_{i,-1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ i\sqrt[4]{2} & \sqrt[4]{2} & -i\sqrt[4]{2} & -\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
\sigma_{-1,1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ -\sqrt[4]{2} & -i\sqrt[4]{2} & \sqrt[4]{2} & i\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\
\sigma_{-1,-1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ -\sqrt[4]{2} & i\sqrt[4]{2} & \sqrt[4]{2} & -i\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\
\sigma_{-i,1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ -i\sqrt[4]{2} & \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\
\sigma_{-i,-1} &\mapsto \begin{pmatrix} \sqrt[4]{2} & i\sqrt[4]{2} & -\sqrt[4]{2} & -i\sqrt[4]{2} \\ -i\sqrt[4]{2} & -\sqrt[4]{2} & i\sqrt[4]{2} & \sqrt[4]{2} \end{pmatrix} \cong \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}
\end{aligned}$$

Dabei erhält man die Permutation, indem man $\sqrt[4]{2}$ mit 1, $i\sqrt[4]{2}$ mit 2, $-\sqrt[4]{2}$ mit 3 und $-i\sqrt[4]{2}$ mit 4 identifiziert.

(b) Wie auf Blatt 1 bewiesen, sind Elemente der D_4 eindeutig durch die Wirkung auf den Eckpunkten bestimmt. Daher können sie als Permutation der Eckpunkte $1, 2, 3, 4$ geschrieben werden. In dieser Schreibweise gilt

$$D_4 = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

Insbesondere erhalten wir einen Isomorphismus zwischen $\operatorname{Gal}(L/\mathbb{Q})$ und D_4 durch die Zuordnung von Permutationen der Nullstellen und Permutationen der Eckpunkte.

(c) Ist $M/\mathbb{Q}$ quadratisch, so gilt $[M\colon \mathbb{Q}] = 2$. Daher erhalten wir $8 = [L\colon \mathbb{Q}] = [L\colon M] \cdot [M\colon \mathbb{Q}] \implies 4 = [L\colon M] = \#\operatorname{Gal}(L/M)$. Wir bestimmen daher die Untergruppen $\operatorname{Gal}(L/M)$ von $\operatorname{Gal}(L/\mathbb{Q})$ mit Ordnung 4.

1. Zunächst bestimmen wir alle Untergruppen, die $\sigma_{i,1}$ enthalten. Es gilt $\sigma_{-1,1} = \sigma_{i,1}^2$, $\sigma_{-i,1} = \sigma_{i,1}^3$ und $\sigma_{1,1} = \sigma_{i,1}^4$. Daher ist $\operatorname{ord}(\sigma_{i,1}) = 4 = \operatorname{ord}\langle\sigma_{i,1}$. Folglich ist $\{\sigma_{1,1}, \sigma_{i,1}, \sigma_{-1,1}, \sigma_{-i,1}\}$ die einzige echte Untergruppe, die $\sigma_{i,1}$ enthält. Völlig analoge Argumente zeigen, dass $\sigma_{-i,1}$ dieselbe Untergruppe erzeugt und diese die einzige echte Untergruppe ist, die $\sigma_{-i,1}$ enthält.
2. Nun bestimmen wir alle restlichen Untergruppen der Ordnung 4, die $\sigma_{-1,1}$ enthalten.
   i. Angenommen, $\sigma_{\pm i,-1}$ liegt in der Untergruppe. Wegen $\sigma_{-1,1} \circ \sigma_{i,-1} = \sigma_{-i,-1}$ und $\sigma_{-1,1} \circ \sigma_{-i,-1} = \sigma_{i,-1}$ muss dann auch $\sigma_{\mp i,-1}$ in der Untergruppe liegen. Wegen $\sigma_{i,-1} \circ \sigma_{i,-1}(i) = i$ und $\sigma_{i,-1} \circ \sigma_{i,-1}(\sqrt[4]{2}) = \sigma_{i,-1}(i\sqrt[4]{2}) = -i \cdot i\sqrt[4]{2} = \sqrt[4]{2}$ ist $\sigma_{i,-1}^2 = \sigma_{1,1}$. Wegen $\sigma_{-i,-1}^2(i) = i$ und $\sigma_{-i,-1}^2(\sqrt[4]{2}) = \sigma_{-i,-1}(-i\sqrt[4]{2}) = i \cdot -i\sqrt[4]{2} = \sqrt[4]{2}$ ist $\sigma_{-i,-1}^2 = \sigma_{1,1}$. Also ist die Menge $\{\sigma_{1,1}, \sigma_{-1,1}, \sigma_{i,-1}, \sigma_{-i,-1}\}$ abgeschlossen bezüglich Multiplikation und Inversion und damit eine Untergruppe von $\operatorname{Gal}(L/\mathbb{Q})$.
   ii. Angenommen, $\sigma_{\pm 1,-1}$ liegt in der Untergruppe. Wegen $\sigma_{-1,1} \circ \sigma_{1,-1} = \sigma_{-1,-1}$ und $\sigma_{-1,1} \circ \sigma_{-1,-1} = \sigma_{1,-1}$ muss dann auch $\sigma_{\mp 1,-1}$ in der Untergruppe liegen. Es gilt $\sigma_{\pm 1,-1}^2 = \sigma_{1,1}$. Also ist die Menge $\{\sigma_{1,1}, \sigma_{-1,1}, \sigma_{1,-1}, \sigma_{-1,-1}\}$ abgeschlossen bezüglich Multiplikation und Inversion und damit eine Untergruppe von $\operatorname{Gal}(L/\mathbb{Q})$.

   Damit sind alle Elemente von $\operatorname{Gal}(L/\mathbb{Q})$ erschöpft. Wir untersuchen also im Folgenden Untergruppen, die weder $\sigma_{\pm i,1}$ noch $\sigma_{-1,1}$ enthalten.
3. Es gilt wie oben bewiesen stets $\sigma_{\zeta,-1}^2 = \sigma_{1,1}$. Sein nun $\zeta \neq \zeta'$. Dann gilt $\sigma_{\zeta,-1} \circ \sigma_{\zeta',-1} = \sigma_{\zeta'',1}$ mit $\zeta'' \neq 1$, sonst wäre das Inverse nicht eindeutig. Also gilt $\sigma_{\zeta'',1} \in \{\sigma_{\pm i,1}, \sigma_{-1,1}\}$ und damit kann keine Untergruppe der Ordnung 4 geben, die weder $\sigma_{\pm i,1}$ noch $\sigma_{-1,1}$ enthält.

Damit erhalten wir drei Untergruppen der Ordnung 4:

1. $H_1 \coloneqq \{\sigma_{1,1}, \sigma_{i,1}, \sigma_{-1,1}, \sigma_{-i,1}\}$
2. $H_2 \coloneqq \{\sigma_{1,1}, \sigma_{-1,1}, \sigma_{i,-1}, \sigma_{-i,-1}\}$
3. $H_3 \coloneqq \{\sigma_{1,1}, \sigma_{-1,1}, \sigma_{1,-1}, \sigma_{-1,-1}\}$

Diese Untergruppen korrespondieren zu drei Zwischenkörpern $M_1 \coloneqq L^{H_1}$, $M_2 \coloneqq L^{H_2}$ und $M_3 \coloneqq L^{H_3}$. Es gilt

1. $M_1 = \{a \in L \coloneqq \sigma(a) = a \forall \sigma \in H_1\}$. Offensichtlich ist $\sigma(a) = a \forall a \in K$. Darüberhinaus sieht man leicht, dass $\sigma(i) = i \forall \sigma \in H_1$ und damit $K(i) \subset M_1$. Wegen $[K(i)\colon K] = 2$ folgt $M_1 = K(i)$.
2. $M_2 = \{a \in L \coloneqq \sigma(a) = a \forall \sigma \in H_2\}$. Offensichtlich ist $\sigma(a) = a \forall a \in K$. Wir betrachten nun $i\sqrt{2} \in L$. Es gilt offensichtlich $\sigma_{1,1}(i\sqrt{2}) = i\sqrt{2}$.

$$\begin{aligned}\sigma_{-1,1}(i\sqrt{2}) &= \sigma_{-1,1}(i) \cdot \sigma_{-1,1}(\sqrt[4]{2})^2 = i \cdot (-\sqrt[4]{2})^2 = i\sqrt{2}\\ \sigma_{i,-1}(i\sqrt{2}) &= \sigma_{i,-1}(i) \cdot \sigma_{i,-1}(\sqrt[4]{2})^2 = -i \cdot (i\sqrt[4]{2})^2 = i\sqrt{2}\\ \sigma_{-i,-1}(i\sqrt{2}) &= \sigma_{-i,-1}(i) \cdot \sigma_{-i,-1}(\sqrt[4]{2})^2 = -i \cdot (-i\sqrt[4]{2})^2 = i\sqrt{2}\end{aligned}$$

   Daher ist $K(i\sqrt{2}) \subset M_2$. Das Minimalpolynom von $i\sqrt{2}$ über K ist $x^2 + 2$, also ist $K(i\sqrt{2})$ bereits eine quadratische Erweiterung und damit $M_2 = K(i\sqrt{2})$.
3. $M_3 = \{a \in L \coloneqq \sigma(a) = a \forall \sigma \in H_3\}$. Offensichtlich ist $\sigma(a) = a \forall a \in K$. Wir betrachten nun $\sqrt{2} \in L$. Es gilt offensichtlich $\sigma_{1,1}(\sqrt{2}) = \sqrt{2}$.

$$\begin{aligned}\sigma_{-1,1}(\sqrt{2}) &= \sigma_{-1,1}(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt{2}\\ \sigma_{1,-1}(\sqrt{2}) &= \sigma_{1,-1}(\sqrt[4]{2})^2 = (\sqrt[4]{2})^2 = \sqrt{2}\\ \sigma_{-1,-1}(\sqrt{2}) &= \sigma_{-1,-1}(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt{2}\end{aligned}$$

   Daher ist $K(\sqrt{2}) \subset M_3$. Das Minimalpolynom von $\sqrt{2}$ über K ist $x^2 - 2$, also ist $K(\sqrt{2})$ bereits eine quadratische Erweiterung und damit $M_3 = K(\sqrt{2})$.

Aufgabe 3

(a) Bei $\mathbb{F}_9^\times$ handelt es sich um eine zyklische Gruppe der Ordnung 8. Es existiert also ein $a \in \mathbb{F}_9^\times$ mit $\mathbb{F}_9^\times = \langle a \rangle$. Sei a eine Nullstelle des Polynoms $X^4 + 1$. Dann gilt $a^4 \neq 1$. Angenommen, a wäre kein Erzeuger der Einheitengruppe. Dann gäbe es ein kleinstes $k < 8$ mit $a^k = 1$. Für $\nu \in \mathbb{N}$ ist dann auch $a^{\nu k} = 1$. Nun ist aber $a^4 \neq 1$. Angenommen, $k > 4$. Dann ist $1 = a^8 = a^k \cdot a^{8-k} = a^{8-k}$. Dann hätte man aber statt k auch $8 - k < k$ wählen können, Widerspruch. Also muss $k < 4$ sein. k kann auch nicht 1 oder 2 sein, da dann $a^4 = 1$ wäre. Also muss $k = 3$ sein. Daraus folgt aber $a = a^9 = (a^3)^3 = 1$. Aus diesem Widerspruch folgt, dass a ein Erzeuger der Einheitengruppe sein muss. Wegen $X^9 - X = X(X^4+1)(X^4-1)$ und weil $\mathbb{F}_9$ gerade aus den 9 Nullstellen von $X^9 - 9$ besteht, muss es vier Elemente a geben, die die Bedingung $a^4 + 1 = 0$ erfüllen. Eines dieser a ist dann das gesuchte primitive Element.

Es gilt $[\mathbb{F}_9 \colon \mathbb{F}_3] = 2$. Daher handelt es sich um eine normale Erweiterung. Außerdem sind endliche Körper vollkommen, sodass die Erweiterung auch separabel und damit galoissch ist. Wie in Beispiel 4.2 erläutert ist $\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3)$ zyklisch von der Ordnung 2 und wird erzeugt vom Frobenius-Automorphismus $\sigma\colon \mathbb{F}_9 \to \mathbb{F}_9,\ a \mapsto a^3$. Es gilt $\sigma^2 = (a \mapsto a^9 = a) = \mathrm{id}_{\mathbb{F}_9}$. Daher ist $\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \{\sigma, \mathrm{id}_{\mathbb{F}_9}\}$.

(b) Es gilt $(\sqrt{3} + \sqrt{5})^3 = 18\sqrt{3} + 14\sqrt{5}$. Daher gilt

$$\sqrt{3} = \frac{(\sqrt{3} + \sqrt{5})^3 - 14(\sqrt{3} + \sqrt{5})}{4} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}).$$

Insbesondere ist auch
$$\sqrt{5} = \sqrt{3} + \sqrt{5} - \sqrt{3} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}).$$
Daraus folgt die Inklusion $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Die andere Inklusion ist trivial, also ist $\sqrt{3}+\sqrt{5}$ ein primitives Element. Wegen $\operatorname{char} \mathbb{Q} = 0$ ist $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ separabel. Die Familie $(X^2 - 3, X^2 - 5)$ von Polynomen aus $\mathbb{Q}[X]$ zerfällt in Linearfaktoren über $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Die Nullstellen der Polynome in der Familie sind gerade $\pm\sqrt{3}, \pm\sqrt{5}$. Also ist $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ der Zerfällungskörper dieser Familie. Insbesondere ist die Erweiterung $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ normal und aufgrund der Separabilität bereits galoissch. Das Minimalpolynom $f \in \mathbb{Q}[X]$ von $\sqrt{3} + \sqrt{5}$ ist gegeben durch $X^4 - 16X^2 + 4$ (Reduktionskriterium für $p = 3$). Es gilt
$$X^4 - 16X^2 + 4 = (X - (\sqrt{3} + \sqrt{5}))(X + (\sqrt{3} + \sqrt{5}))(X - (\sqrt{3} - \sqrt{5}))(X + (\sqrt{3} - \sqrt{5}))$$
Die Menge aller Nullstellen ist daher
$$N = \{\sqrt{3} + \sqrt{5}, -\sqrt{3} - \sqrt{5}, \sqrt{3} - \sqrt{5}, -\sqrt{3} + \sqrt{5}\}.$$
Wegen Lemma 3.40 ist ein $\mathbb{Q}$-Automorphismus $\sigma\colon \mathbb{Q}(\sqrt{3}+\sqrt{5}) \to \mathbb{Q}(\sqrt{3}+\sqrt{5})$ eindeutig bestimmt durch $\sigma(\sqrt{3+5}) \in N$. Die Galoisgruppe ist daher gegeben durch
$$\operatorname{Gal}(\mathbb{Q}(\sqrt{3} + \sqrt{5})/\mathbb{Q}) = \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5})) = \{\sigma_\zeta \colon \zeta \in N\},$$
wobei $\sigma_\zeta \in \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5}))$ eindeutig bestimmt ist durch $\sigma_\zeta(\sqrt{3} + \sqrt{5}) = \zeta$.

Aufgabe 4

(a) Sei $\mathscr{M}$ die Menge aller Zwischenkörper von K und L. Sei nun $f_M \in M[X]$ gegeben. Definiere dann
$$A := \bigcap_{\substack{M' \in \mathscr{M} \\ f_M \in M'}} M'.$$
Daher ist $f_M \in A[X]$ und daher $M \subset A$. Allerdings ist auch $f_M \in M[X]$ und daher $A = \bigcap_{\substack{M' \in \mathscr{M} \\ f_M \in M'}} M' \subset M$. Daraus folgt bereits die Gleichheit und wir haben M eindeutig bestimmt. Wir können f_K als Element von $M[X]$ auffassen. Auch dann gilt noch $f_K(\alpha) = 0$. Per Definition des Minimalpolynoms ist dann f_M ein Teiler von f_K in $M[X]$ und daher insbesondere auch in $L[X]$.

Aufgrund der Eindeutigkeit der Primfaktorzerlegung, weil es nur endlich viele Primfaktoren gibt und jeder Teiler von f_K sich als Produkt einer Teilmenge der Primfaktoren schreiben lässt, kann es nur endlich viele Teiler von f_K geben.

Gäbe es unendlich viele verschiedene Zwischenkörper M, so gäbe es auch unendlich viele verschiedene dazugehörige Minimalpolynome f_M und damit auch unendlich viele verschiedene Teiler von f_K in L, Widerspruch. Also gibt es nur endlich viele Zwischenkörper.

(b) Wir zeigen zunächst den Fall $L = K(\alpha, \beta)$. Angenommen, es gäbe keine $c \neq c' \in K$ mit $K(\alpha + c\beta) = K(\alpha + c'\beta)$. Dann gäbe es zu zwei verschiedenen Elementen $c, c' \in K$ stets verschiedene Körpererweiterungen $K(\alpha + c\beta)$ und $K(\alpha + c'\beta)$. Wegen $\#K = \infty$ gäbe es also unendlich viele verschiedene Körpererweiterungen der Form $K(\alpha + c\beta)$. Es gilt aber $K \subset K(\alpha + c\beta) \subset$

$K(\alpha, \beta) \forall c \in K$. Insbesondere gäbe es also unendlich viele Zwischenkörper zu der Erweiterung L/K. Das steht aber im Widerspruch zur Voraussetzung.

Es existieren also $c, c' \in K$ mit $c \neq c'$ und $M := K(\alpha + c\beta) = K(\alpha + c'\beta)$. Insbesondere ist

$$\beta = \frac{\alpha + c\beta - (\alpha + c'\beta)}{c - c'} \in M$$

und damit auch

$$\alpha = \alpha + c\beta - c \cdot \beta \in K.$$

Also ist $K(\alpha, \beta) = K(\alpha + c\beta)$.

Nun betrachten wir den allgemeinen Fall $L = K(\alpha_1, \ldots, \alpha_n)$. Wir zeigen die Aussage per Induktion. Für $n = 1$ ist sie offensichtlich wahr. Sei die Aussage für $n = k - 1$ bewiesen. Dann gilt $K(a_1, \ldots, a_k) = (K(a_1, \ldots, a_{k-1}))(a_k) = K(\beta)(a_k) = K(\alpha)$. Also gilt die Aussage auch für $n = k$. Per Induktion folgt die Behauptung.

Aufgabe 5

Zu jedem Zwischenkörper M von L/K existiert nach dem Hauptsatz der Galoistheorie eine Untergruppe H von $\mathrm{Gal}(L/K)$ mit $M = L^H$. Da L/K abelsch ist, muss H als Untergruppe einer abelschen Gruppe ein Normalteiler sein, M/K ist also normal. Insbesondere ist M also Zerfällungskörper eines Polynoms in $K[X]$. Wählt man ein beliebiges irreduzibles Polynom $f \in K[X]$ mit einer Nullstelle in L, so erhält man durch den Zerfällungskörper dieses Polynoms einen Zwischenkörper M. Gibt man nun eine beliebige Nullstelle $\alpha \in L$ dieses Polynoms an, so erhält man durch Adjunktion den Körper $K(\alpha)$. Offenbar gilt $K(\alpha) \subset M$, da f über M in Linearfaktoren zerfällt. Da $K(\alpha)/K$ aber ebenfalls normal ist, liegen alle anderen Nullstellen von f auch in $K(\alpha)$. Damit ist $K(\alpha)$ bereits Zerfällungskörper von f. Da zwei Zerfällungskörper stets isomorph sind und $K(\alpha) \subset M$ folgt $K(\alpha) = M$. Der Weihnachtsmann wurde also nicht betrogen.