G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 12

Aufgabe 49.

(1) (i) Wir erhalten

$$\begin{array}{rcl} a^0 & = & 1\cdot 1 + 0\cdot i \\ a^1 & = & 1\cdot 1 + 1\cdot i \\ a^2 & = & 0\cdot 1 + 2\cdot i\,, \end{array}$$

und also durch Betrachtung der Matrix $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \end{smallmatrix}\right)$ die Gleichung

$$a^2 - 2a^1 + 2a^0 \;=\; 0\,.$$

Da das Spaltentupel der um die letzte Spalte verkürzten Matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ linear unabhängig ist, ist in der Tat

$$\mu_{(1+i),\mathbf{R}}(X) \;=\; X^2 - 2X + 2$$

das Minimalpolynom von $(1+i)$ über $\mathbf{R}$.

(ii) Ein K-Algebrenmorphismus von $K(a) = K[a] \simeq K[X]/(\mu_{a,K}(X))$ (cf. Aufgabe 40 (2)) nach $K(a)$ ist gegeben durch die Angabe eines Bildes a' von a, vorausgesetzt, $\mu_{a,K}(a') = 0$. Denn dies liefert einen K-Algebrenendomorphismus, der injektiv ist, da er von einem Körper ausgeht und nicht im Nullring endet. Da $[K(a) : K]$ endlich ist, ist dieser auch surjektiv, und also ein Automorphismus.
Wir suchen also die Nullstellen von $\mu_{a,K}(X)$ in $K(a)$.
Im vorliegenden Fall erhalten wir durch Abdividieren der konstruierten Nullstelle a

$$X^2 - 2X + 2 \;=\; (X - (1+i))(X - (1-i))$$

und somit die Automorphismen

$$\begin{array}{rcl} \mathbf{R}(1+i) & \xrightarrow[\sim]{\mathrm{id}} & \mathbf{R}(1+i) \\ 1+i & \longmapsto & 1+i \\ \mathbf{R}(1+i) & \xrightarrow[\sim]{\sigma} & \mathbf{R}(1+i) \\ 1+i & \longmapsto & 1-i \end{array}$$

Beachte, daß $\mathbf{R}(1+i) = \mathbf{R}(i) = \mathbf{C}$. Es ist σ die komplexe Konjugation auf $\mathbf{C}$.
Da in $\mathbf{C}[X]$ das Polynom $\mu_{(1+i),\mathbf{R}}(X)$ bereits in Linearfaktoren zerfällt, ist $K(a) = \mathbf{C}$ ein Zerfällungskörper von $\mu_{(1+i),\mathbf{R}}(X)$.

(2) (i) Wir können in $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ rechnen. Dieser Körper hat eine Basis $(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$ über $\mathbf{Q}$, da $X^2 - 5$ auch in $\mathbf{Q}(\sqrt{3})$ noch irreduzibel ist.
Wir erhalten

$$\begin{array}{rcrcrcrcr} a^0 & = & 1\cdot 1 & + & 0\cdot\sqrt{3} & + & 0\cdot\sqrt{5} & + & 0\cdot\sqrt{15} \\ a^1 & = & 1\cdot 1 & + & 1\cdot\sqrt{3} & + & 1\cdot\sqrt{5} & + & 0\cdot\sqrt{15} \\ a^2 & = & 9\cdot 1 & + & 2\cdot\sqrt{3} & + & 2\cdot\sqrt{5} & + & 2\cdot\sqrt{15} \\ a^3 & = & 25\cdot 1 & + & 21\cdot\sqrt{3} & + & 17\cdot\sqrt{5} & + & 6\cdot\sqrt{15} \\ a^4 & = & 173\cdot 1 & + & 76\cdot\sqrt{3} & + & 60\cdot\sqrt{5} & + & 44\cdot\sqrt{15} \end{array}$$

und also durch Betrachtung der Matrix $\left(\begin{smallmatrix} 1 & 1 & 9 & 25 & 173 \\ 0 & 1 & 2 & 21 & 76 \\ 0 & 1 & 2 & 17 & 60 \\ 0 & 0 & 2 & 6 & 44 \end{smallmatrix}\right)$ die Gleichung

$$a^4 - 4a^3 - 10a^2 + 28a - 11 \;=\; 0\,.$$

Da das Spaltentupel der um die letzte Spalte verkürzten Matrix linear unabhängig ist, ist in der Tat

$$\mu_{(1+\sqrt{3}+\sqrt{5}),\mathbf{Q}}(X) \;=\; X^4 - 4X^3 - 10X^2 + 28X - 11$$

das Minimalpolynom von $1+\sqrt{3}+\sqrt{5}$ über $\mathbf{Q}$. Insbesondere folgt $\mathbf{Q}(1+\sqrt{3}+\sqrt{5}) = \mathbf{Q}(\sqrt{3},\sqrt{5})$.

(ii) Um die Automorphismen von $\mathbf{Q}(1+\sqrt{3}+\sqrt{5})$ zu berechnen, müssen wir nun $\mu_{(1+\sqrt{3}+\sqrt{5}),\mathbf{Q}}(X)$ in $\mathbf{Q}(1+\sqrt{3}+\sqrt{5})[X] = \mathbf{Q}(\sqrt{3},\sqrt{5})[X]$ in irreduzible Faktoren zerlegen. In der Tat ist

$$X^4-4X^3-10X^2+28X-11 \;=\; (X-(1+\sqrt{3}+\sqrt{5}))(X-(1-\sqrt{3}+\sqrt{5}))(X-(1+\sqrt{3}-\sqrt{5}))(X-(1-\sqrt{3}-\sqrt{5}))\;,$$

da die obige Rechnung, die zeigte, daß $1+\sqrt{3}+\sqrt{5}$ eine Nullstelle des Polynoms $X^4-4X^3-10X^2+28X-11$ ist, ebenso für die jeweils negativen Wurzeln ihre Gültigkeit behält.

Damit erhalten wir die Automorphismen

$$\begin{array}{rcl}
\mathbf{Q}(1+\sqrt{3}+\sqrt{5}) & \xrightarrow[\sim]{\sigma_1} & \mathbf{Q}(1+\sqrt{3}+\sqrt{5}) \\
1+\sqrt{3}+\sqrt{5} & \longmapsto & 1+\sqrt{3}+\sqrt{5} \\
\mathbf{Q}(1+\sqrt{3}+\sqrt{5}) & \xrightarrow[\sim]{\sigma_2} & \mathbf{Q}(1+\sqrt{3}+\sqrt{5}) \\
1+\sqrt{3}+\sqrt{5} & \longmapsto & 1-\sqrt{3}+\sqrt{5} \\
\mathbf{Q}(1+\sqrt{3}+\sqrt{5}) & \xrightarrow[\sim]{\sigma_3} & \mathbf{Q}(1+\sqrt{3}+\sqrt{5}) \\
1+\sqrt{3}+\sqrt{5} & \longmapsto & 1+\sqrt{3}-\sqrt{5} \\
\mathbf{Q}(1+\sqrt{3}+\sqrt{5}) & \xrightarrow[\sim]{\sigma_4} & \mathbf{Q}(1+\sqrt{3}+\sqrt{5}) \\
1+\sqrt{3}+\sqrt{5} & \longmapsto & 1-\sqrt{3}-\sqrt{5}
\end{array}$$

Es ist aus Gradgründen übrigens $\mathbf{Q}(\sqrt{3},\sqrt{5}) = \mathbf{Q}(1+\sqrt{3}+\sqrt{5})$.

Da in $\mathbf{Q}(1+\sqrt{3}+\sqrt{5})[X]$ das Polynom $\mu_{(1+\sqrt{3}+\sqrt{5}),\mathbf{Q}}(X)$ bereits in Linearfaktoren zerfällt, ist $K(a) = \mathbf{Q}(1+\sqrt{3}+\sqrt{5})$ ein Zerfällungskörper von $\mu_{(1+\sqrt{3}+\sqrt{5}),\mathbf{Q}}(X)$.

(3) (i) Wir erhalten

$$\begin{array}{rcl}
a^0 & = & 1 \\
a^1 & = & T+1 \\
a^2 & = & T^2+2T+1 \\
a^3 & = & 3T^2+3T+(1+T^3)\;,
\end{array}$$

und mithin aus der Matrix $\left(\begin{smallmatrix} 1 & 1 & 1 & 1+T^3 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \end{smallmatrix}\right)$ das Minimalpolynom

$$\mu_{(1+T),\mathbf{Q}(T^3)}(X) \;=\; X^3-3X^2+3X-(1+T^3)\;.$$

(ii) Es ist nun $\mathbf{Q}(T^3)(T+1) = \mathbf{Q}(T)$. Da sich $\mu_{T+1,\mathbf{Q}(T^3)}(X)$ in $\mathbf{Q}(T)[X]$ zerlegen läßt als

$$\mu_{T+1,\mathbf{Q}(T^3)}(X) \;=\; (X-1)^3-T^3 \;=\; ((X-1)-T)((X-1)^2+(X-1)T+T^2)\;,$$

und da letzterer Faktor $(X-1)^2+(X-1)T+T^2$ mangels Nullstelle (die Diskriminante $-3T^2$ ist kein Quadrat in $\mathbf{Q}(T)$!) irreduzibel in $\mathbf{Q}(T)[X]$ ist, hat $\mu_{T+1,\mathbf{Q}(T^3)}(X)$ nur eine Nullstelle in $K(a) = \mathbf{Q}(T)$, nämlich $a = T+1$ selbst. Somit ist die identische Abbildung der einzige Automorphismus von $K(a) = \mathbf{Q}(T)$ über $K = \mathbf{Q}(T^3)$.

Da in $\mathbf{Q}(T)[X]$ das Polynom $\mu_{(T+1),\mathbf{Q}(T^3)}(X)$ nicht in Linearfaktoren zerfällt, ist $K(a) = \mathbf{Q}(T)$ kein Zerfällungskörper von $\mu_{T+1,\mathbf{Q}(T^3)}(X)$.

(4) (i) Wir erhalten, nach Unterschlagung aller Querstriche und unter Verwendung der Bezeichnung $\mathbf{F}_{27}$ für L,

$$\begin{array}{rcl}
a^0 & = & 1 \\
a^1 & = & T^2+T+1 \\
a^2 & = & T^2-1 \\
a^3 & = & T^2-T+1\;,
\end{array}$$

und mithin aus der Matrix $\left(\begin{smallmatrix} 1 & 1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 1 \end{smallmatrix}\right)$ das Minimalpolynom

$$\mu_{1+T+T^2,\mathbf{F}_3}(X) \;=\; X^3+X^2+X-1\;.$$

(ii) Wir bemerken zunächst, daß aus Gradgründen $\mathbf{F}_{27} = \mathbf{F}_3(T^2+T+1)$.
Abdividieren der Nullstelle T^2+T+1 gibt in $\mathbf{F}_{27}[X]$ die Faktorisierung

$$\begin{array}{rcl} \mu_{1+T+T^2,\mathbf{F}_3}(X) & = & X^3+X^2+X-1 \\ & = & (X-(T^2+T+1))(X^2+X(T^2+T-1)+(-T^2+T+1)) \\ & = & (X-(T^2+T+1))(X-(T^2-T+1))(X-T^2)\,. \end{array}$$

Wir erhalten so die Automorphismen

$$\begin{array}{rclcl} \mathbf{F}_{27} & \xrightarrow[\sim]{\sigma_0} & \mathbf{F}_{27} & & \\ T^2+T+1 & \longmapsto & T^2+T+1 & = & (T^2+T+1)^1 \\ \mathbf{F}_{27} & \xrightarrow[\sim]{\sigma_1} & \mathbf{F}_{27} & & \\ T^2+T+1 & \longmapsto & T^2-T+1 & = & (T^2+T+1)^3 \\ \mathbf{F}_{27} & \xrightarrow[\sim]{\sigma_2} & \mathbf{F}_{27} & & \\ T^2+T+1 & \longmapsto & T^2 & = & (T^2+T+1)^9\,. \end{array}$$

Bezeichnen wir mit übrigens $\mathbf{F}_{27} \xrightarrow{\mathrm{F}} \mathbf{F}_{27}$, $u \longmapsto u^3$ den Frobeniusautomorphismus von $\mathbf{F}_{27}$, so erkennen wir durch Vergleich der Bilder des Erzeugers T^2+T+1, daß $\sigma_0 = \mathrm{F}^0$, $\sigma_1 = \mathrm{F}^1$ und $\sigma_2 = \mathrm{F}^2$.
Da in $\mathbf{F}_{27}[X]$ das Polynom $\mu_{1+T+T^2,\mathbf{F}_3}(X)$ bereits in Linearfaktoren zerfällt, ist $K(a) = \mathbf{F}_{27}$ ein Zerfällungskörper von $\mu_{1+T+T^2,\mathbf{F}_3}(X)$.

Aufgabe 50.

(1) (i) Sei $K_0 := K = \mathbf{Q}$. Wir bemerken zunächst, daß $X^3-3 \in \mathbf{Q}[X]$ mangels Nullstelle irreduzibel ist, wie mit Primfaktorzerlegung folgt – $\frac{m^3}{n^3} = 3$ ist mit $m,\ n \in \mathbf{Z}$ unlösbar.
Sei $K_1 = K_0(\alpha_1) = K_0[T]/(T^3-3)$, wobei α_1 die Restklasse von T bezeichne. Dann ist $\alpha_1^3 = 3$. Wir müssen das Polynom X^3-3 in $K_1[X]$ in irreduzible Faktoren zerlegen. Abdividieren der Nullstelle α_1 liefert

$$X^3-3 \;=\; (X-\alpha_1)(X^2+\alpha_1X+\alpha_1^2)\,.$$

Die Diskriminante von $X^2+\alpha_1X+\alpha_1^2$ ist $-3\alpha_1^2$. Wir behaupten, daß diese kein Quadrat in K_1 ist, so daß $X^2+\alpha_1X+\alpha_1^2$ somit irreduzibel ist.
Es genügt zu zeigen, daß -3 kein Quadrat in K_1 ist. Zum einen kann man K_1 in $\mathbf{R}$ via $\alpha_1 \longmapsto \sqrt[3]{3}$ einbetten und sich zunutze machen, daß -3 noch nicht einmal ein Quadrat in $\mathbf{R}$ ist.
Der alternative Ansatz $-3 = (u+v\alpha_1+w\alpha_1^2)^2 = (u^2+6vw)+(3w^2+2uv)\alpha_1+(v^2+2uw)\alpha_1^2$ mit $u,\ v,\ w \in \mathbf{Q}$ lieferte, wäre $w \neq 0$, $u = -\frac{v^2}{2w}$, und somit $3 = (\frac{v}{w})^3$, was, wie oben schon bemerkt, nicht möglich ist. Also ist $w = 0$ und $u^2 = -3$. Aber auch dies ist für $u \in \mathbf{Q}$ nicht möglich. Damit ist -3 kein Quadrat in K_1.
Sei $K_2 = K_1(\alpha_2) = K_1[T']/(T'^2+\alpha_1T'+\alpha_1^2)$, wobei α_2 die Restklasse von T' bezeichne. Dann ist $\alpha_2^2 = -\alpha_1\alpha_2-\alpha_1^2$.
Wir müssen das Polynom $X^2+\alpha_1X+\alpha_1^2$ in $K_2[X]$ noch in irreduzible Faktoren zerlegen. Abdividieren der Nullstelle α_2 gibt

$$X^3-3 \;=\; (X-\alpha_1)(X-\alpha_2)(X+\alpha_1+\alpha_2)\,.$$

Somit ist $E := K_2 = \mathbf{Q}(\alpha_1,\alpha_2)$ ein Zerfällungskörper von X^3-3. Es ist

$$[E:K] \;=\; [K_2:K_1][K_1:K_0] \;=\; 2\cdot 3 \;=\; 6\,.$$

(ii) Wir bemerken zunächst, daß

$$E \;\simeq\; K[T,T']/(T^3-3,T'^2+T'T+T^2)$$

als K-Algebra. Ein Automorphismus ist also gegeben durch ein Tupel (β_1,β_2) aus E mit

$$\begin{array}{rcl} \beta_1^3-3 & = & 0 \\ \beta_2^2+\beta_1\beta_2+\beta_2^2 & = & 0\,, \end{array}$$

indem die Restklasse von T, i.e. α_1, auf β_1 und die Restklasse von T', i.e. α_2, auf β_2 geschickt wird.

Wir kürzen die dritte Nullstelle von $X^3 - 3$ in E ab mit $\alpha_3 = -(\alpha_1 + \alpha_2)$, also $X^3 - 3 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$.
Wir haben zunächst

$$\beta_1 \ \in \ \{\alpha_1, \alpha_2, \alpha_3\}$$

zur Auswahl.
Wie oben erhalten wir eine Faktorisierung

$$X^2 + \beta_1 X + \beta_1^2 \ = \ (X^3 - 3)/(X - \beta_1) \ = \ (X - \beta_2)(X + (\beta_1 + \beta_2))\ ,$$

wobei β_2 eine weitere Nullstelle von $X^3 - 3$ in E ist. Damit ergeben sich die Möglichkeiten

$$(\beta_1, \beta_2) \ \in \ \{(\alpha_1, \alpha_2),\ (\alpha_1, \alpha_3),\ (\alpha_2, \alpha_1),\ (\alpha_2, \alpha_3),\ (\alpha_3, \alpha_1),\ (\alpha_3, \alpha_2)\}\ .$$

und entsprechend 6 Automorphismen von E über K vermöge $\alpha_1 \longmapsto \beta_1$, $\alpha_2 \longmapsto \beta_2$.

(iii) Setzt man z.B. $a = \alpha_1 - \alpha_2$, so wird

$$\begin{array}{rcl} a^0 & = & 1 \\ a^1 & = & \alpha_1 - \alpha_2 \\ a^2 & = & -3\alpha_1\alpha_2 \\ a^3 & = & -6\alpha_1^2\alpha_2 - 9 \\ a^4 & = & -27(\alpha_1 + \alpha_2) \\ a^5 & = & -27(2\alpha_1^2 + \alpha_1\alpha_2) \\ a^6 & = & -243\ . \end{array}$$

Die Matrix

$$\left(\begin{array}{c|ccccccc} \alpha_1^0\alpha_2^0 & 1 & 0 & 0 & -9 & 0 & 0 & -243 \\ \alpha_1^1\alpha_2^0 & 0 & 1 & 0 & 0 & -27 & 0 & 0 \\ \alpha_1^2\alpha_2^0 & 0 & 0 & 0 & 0 & 0 & -54 & 0 \\ \alpha_1^0\alpha_2^1 & 0 & -1 & 0 & 0 & -27 & 0 & 0 \\ \alpha_1^1\alpha_2^1 & 0 & 0 & -3 & 0 & 0 & -27 & 0 \\ \alpha_1^2\alpha_2^1 & 0 & 0 & 0 & -6 & 0 & 0 & 0 \end{array}\right)$$

(in welcher in der ersten Spalte nur das zugehörige Basiselement von $\mathbf{Q}(\alpha_1, \alpha_2)$ über $\mathbf{Q}$ notiert ist), zeigt, daß $\mu_{\alpha_1 - \alpha_2, \mathbf{Q}}(X) = X^6 + 243$ (cf. Aufgabe 49).
Alternativ kann man wegen $E|K$ galoisch auch alle Automorphismen auf den zugehörigen Linearfaktor $X - a$ loslassen und erhält durch Aufmultiplizieren

$$\mu_{\alpha_1-\alpha_2,\mathbf{Q}}(X) \ = \ (X-(\alpha_1-\alpha_2))(X-(\alpha_2-\alpha_1))(X-(\alpha_1-\alpha_3))(X-(\alpha_3-\alpha_1))(X-(\alpha_2-\alpha_3))(X-(\alpha_3-\alpha_2))\ .$$

Da a nur von der Identität festgehalten wird (verifiziere mittels Basis!), und somit in keinem echten Zwischenkörper zwischen K und E liegt, zeigt dies ebenfalls, daß $K(a) = E$.

Diesen Erzeuger a muß man raten. Meist genügt eine simple Linearkombination der bislang aufgetretenen Erzeuger.

(2) (i) Sei $K_0 = K = \mathbf{Q}(\sqrt{2})$. Wir behaupten, daß $X^4 - 2X^2 - \sqrt{2} \in \mathbf{Q}(\sqrt{(2)})[X]$ irreduzibel ist.
Hätte das Polynom eine Nullstelle $\beta \in \mathbf{Q}(\sqrt{2}) \smallsetminus \{0\}$, so wäre wegen $0 = \beta^4 - 2\beta^2 - \sqrt{2} = (\beta - 1)^2 - (1 + \sqrt{2})$ das Element $1 + \sqrt{2}$ ein Quadrat in $\mathbf{Q}(\sqrt{2})$. Es folgte aus $(u + v\sqrt{2})^2 = 1 + \sqrt{2}$ mit $u,\ v \in \mathbf{Q}$, daß $u^2 + 2v^2 = 1$ und $2uv = 1$, insbesondere durch Einsetzen also $0 = u^4 - u^2 + \frac{1}{2} = (u^2 - \frac{1}{2})^2 + \frac{1}{4}$, was nicht geht.
Alternative Begründung der Nullstellenfreiheit von $X^4 - 2X^2 - \sqrt{2}$. Wir verwenden die Einbettung $\mathbf{Q}(\sqrt{2}) \xrightarrow{\varphi} \mathbf{R}$, $\sqrt{2} \longmapsto -\sqrt{2}$. Es ist $f^\varphi(X) = X^4 - 2X^2 + \sqrt{2} = (X^2 - 1)^2 + (\sqrt{2} - 1)$, so daß $f^\varphi(X)$ wegen $\sqrt{2} - 1 > 0$ keine Nullstelle in $\mathbf{R}$ hat. Folglich hat $f(X)$ keine Nullstelle in $\mathbf{Q}(\sqrt{2})$.
Bleibt die Möglichkeit zu untersuchen, daß $X^4 - 2X^2 - \sqrt{2} = (X^2 + \beta X + \gamma)(X^2 - \beta X + \gamma)$ mit $X^2 + \beta X + \gamma \in \mathbf{Q}(\sqrt{2})[X]$ irreduzibel, denn wegen $f(X) = f(-X)$ muß mit dem ersten Faktor auch der zweite auftreten. Das aber führt auf $\gamma^2 = -\sqrt{2}$, was schon wegen der Einbettung $\mathbf{Q}(\sqrt{2}) \longrightarrow \mathbf{R}$, $\sqrt{2} \longmapsto \sqrt{2}$ nicht geht. Damit ist $X^4 - 2X^2 - \sqrt{2}$ als irreduzibel nachgewiesen.
Sei $K_1 = K_0(\alpha_1) = K_0[T]/(T^4 - 2T^2 - \sqrt{2})$, wobei α_1 die Restklasse von T bezeichne. Dann ist $\alpha_1^4 = 2\alpha_1^2 + \sqrt{2}$. Wir müssen das Polynom $X^4 - 2X^2 - \sqrt{2}$ in $K_1[X]$ in irreduzible Faktoren zerlegen. Abdividieren der Nullstelle α_1 und zugleich der Nullstelle $-\alpha_1$ liefert

$$X^4 - 2X^2 - \sqrt{2} \ = \ (X - \alpha_1)(X + \alpha_1)(X^2 + (\alpha_1^2 - 2))$$

Einsetzen von $\sqrt{2}$ in $X^4 - 2X^2 - \sqrt{2}$ liefert den negativen Wert $-\sqrt{2}$. Also gibt es eine Nullstelle α_1' dieses Polynoms in $\mathbf{R}$ mit $\alpha_1' > \sqrt{2}$. Wir erhalten eine Einbettung $K_1 \longrightarrow \mathbf{R}$, $\alpha_1 \longmapsto \alpha_1'$. Im Bild dieser Einbettung ist $-({\alpha_1'}^2 - 2) < 0$ kein Quadrat. Also ist auch $-({\alpha_1'}^2 - 2)$ kein Quadrat und $X^2 + (\alpha_1^2 - 2)$ somit irreduzibel.
Sei $K_2 = K_1(\alpha_2) = K_1[T]/(T^2 + (\alpha_1^2 - 2))$, wobei α_2 die Restklasse von T bezeichne. Dann ist $\alpha_2^2 = 2 - \alpha_1^2$. Es zerfällt insgesamt

$$X^4 - 2X^2 - \sqrt{-2} \;=\; (X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2)\;.$$

Somit ist $E := K_2 = \mathbf{Q}(\alpha_1, \alpha_2)$ ein Zerfällungskörper von $X^4 - 2X^2 - \sqrt{2}$. Es ist

$$[E : K] \;=\; [K_2 : K_1][K_1 : K_0] \;=\; 2 \cdot 4 \;=\; 8\;.$$

(ii) Wir bemerken zunächst, daß

$$E \;\simeq\; K[T, T']/(T^4 - 2T^2 - \sqrt{2}, T'^2 + T^2 - 2)$$

als K-Algebra. Ein Automorphismus ist also gegeben durch ein Tupel (β_1, β_2) aus E mit

$$\begin{array}{rcl} \beta_1^4 - 2\beta_1^2 - \sqrt{2} & = & 0 \\ \beta_2^2 + \beta_1^2 - 2 & = & 0\;, \end{array}$$

indem die Restklasse von T, i.e. α_1, auf β_1 und die Restklasse von T', i.e. α_2, auf β_2 geschickt wird.
Wir haben zunächst

$$\beta_1 \;\in\; \{\alpha_1, -\alpha_1, \alpha_2, -\alpha_2\}$$

zur Auswahl.
Wie oben erhalten wir eine Faktorisierung

$$X^2 + \beta_1^2 - 2 \;=\; (X^4 - 2X^2 - \sqrt{2})/(X^2 - \beta_1^2) \;=\; (X - \beta_2)(X + \beta_2)\;,$$

wobei β_2 aus den Nullstelle von $X^4 - 2X^2 - \sqrt{2}$, welche nicht schon in $\{-\beta_1, +\beta_1\}$ liegen, zu wählen ist. Damit ergeben sich die Möglichkeiten

$$(\beta_1, \beta_2) \;\in\; \{(\alpha_1, \alpha_2),\; (\alpha_1, -\alpha_2),\; (-\alpha_1, \alpha_2),\; (-\alpha_1, -\alpha_2),\; (\alpha_2, \alpha_1),\; (\alpha_2, -\alpha_1),\; (-\alpha_2, \alpha_1),\; (-\alpha_2, -\alpha_1)\}\;,$$

und entsprechend 8 Automorphismen von E über K vermöge $\alpha_1 \longmapsto \beta_1$, $\alpha_2 \longmapsto \beta_2$.

(iii) Setzt man z.B. $a = \alpha_1 + 2\alpha_2$, so beobachten wir unter Verwendung von (ii) zunächst, daß wegen des Automorphismus $\alpha_1 \longmapsto -\alpha_1$, $\alpha_2 \longmapsto -\alpha_2$ das Minimalpolynom von a über K auch $-a$ annullieren muß. In anderen Worten, $\mu_{a,K}(-X)$ annulliert a ebenfalls. Es folgt $\mu_{a,K}(-X) = \mu_{a,K}(X)$. Somit können wir uns zur Bestimmung von $\mu_a(X)$ auf die Betrachtung der geraden Potenzen von a beschränken, das spart etwas Arbeit. Wir erhalten, nach zugegebenermaßen längerer Rechnung,

$$\begin{array}{rcrrrr} a^0 & = & 1 & & & \\ a^2 & = & 8 & -3\alpha_1^2 & +4\alpha_1\alpha_2 & \\ a^4 & = & (64 - 7\sqrt{2}) & -30\alpha_1^2 & +64\alpha_1\alpha_2 & -24\alpha_1^3\alpha_2 \\ a^6 & = & (512 - 222\sqrt{2}) & +(-252 + 117\sqrt{2})\alpha_1^2 & +(768 + 44\sqrt{2})\alpha_1\alpha_2 & -360\alpha_1^3\alpha_2 \\ a^8 & = & (3042 - 4092\sqrt{2}) & +(-2040 + 2340\sqrt{2})\alpha_1^2 & +(8192 + 554\sqrt{2})\alpha_1\alpha_2 & +(-4032 + 336\sqrt{2})\alpha_1^3\alpha_2 \end{array}$$

und daraus

$$\mu_{\alpha_1 + 2\alpha_2, \mathbf{Q}(\sqrt{2})}(X) \;=\; X^8 - 20X^6 + (132 + 14\sqrt{2})X^4 + (-320 - 140\sqrt{2})X^2 + (1506 + 800\sqrt{2})\;.$$

Alternativ kann man wegen $E|K$ galoisch auch alle Automorphismen auf den zugehörigen Linearfaktor $X - a$ loslassen und erhält durch Aufmultiplizieren

$$\begin{array}{rcl} \mu_{\alpha_1 + 2\alpha_2, \mathbf{Q}}(X) & = & (X - (\alpha_1 + 2\alpha_2))(X - (\alpha_1 - 2\alpha_2))(X - (-\alpha_1 + 2\alpha_2))(X - (-\alpha_1 - 2\alpha_2)) \cdot \\ & & \cdot (X - (\alpha_2 + 2\alpha_1))(X - (\alpha_2 - 2\alpha_1))(X - (-\alpha_2 + 2\alpha_1))(X - (-\alpha_2 - 2\alpha_1))\;. \end{array}$$

Da a nur von der Identität festgehalten wird (verifiziere mittels Basis!), und somit in keinem echten Zwischenkörper zwischen K und E liegt, zeigt dies ebenfalls, daß $K(a) = E$.

(3) (i) Es ist $(X^3 - S^3)$ ein irreduzibler Faktor von $f(X)$, da $(X^3 - S^3) = (X - S)^3$ in $\mathbf{F}_3(S,T)[X]$ zerfällt, da die dortige Nullstelle S nicht in $\mathbf{F}_3(S^3, T^3)$ liegt, und da daher $X^3 - S^3$ keine Nullstelle in $\mathbf{F}_3(S^3, T^3)$ hat.

Sei $K_0 := \mathbf{F}_3(S^3, T^3)$ und sei $K_1 := \mathbf{F}_3(S^3, T^3)(S) = \mathbf{F}_3(S, T^3)$ aus Adjunktion einer Nullstelle dieses irreduziblen Faktors zu K_0 innerhalb $\mathbf{F}_3(S,T)$ gebildet. In $\mathbf{F}_3(S, T^3)[X]$ ist nun $f(X) = (X - S)^3(X^3 - T^3)$, mit einem irreduziblen Faktor $X^3 - T^3$. Dessen Nullstelle T können wir ebenfalls innerhalb $\mathbf{F}_3(S,T)$ adjungieren, und wir erhalten $K_2 := \mathbf{F}_3(S, T^3)(T) = \mathbf{F}_3(S,T)$. Nun ist in $\mathbf{F}_3(S,T)[X]$ das Polynom $f(X) = (X - S)^3(X - T)^3$ in Linearfaktoren zerlegt. Also ist $E := K_2$ Zerfällungskörper und

$$[E : K] \;=\; [K_2 : K_1][K_1 : K_0] \;=\; 3 \cdot 3 \;=\; 9\,.$$

(ii) Wir behaupten, daß die Identität der einzige Automorphismus von E über K ist. Sei dazu σ ein solcher Automorphismus. Sei $\xi \in E$. Es ist

$$(\sigma(\xi))^3 \;=\; \sigma(\xi^3) \;=\; \xi^3\,,$$

da $\xi^3 \in K$, und da σ alle Elemente von K festhält, i.e. $\sigma|_K = \mathrm{id}_K$. Nun ist aber der Frobeniusendomorphismus auf E, der η auf η^3 schickt, injektiv, und es folgt $\sigma(\xi) = \xi$.

(iii) Wir behaupten, daß es kein $a \in E = \mathbf{F}_3(S,T)$ mit $K(a) = \mathbf{F}_3(S^3, T^3, a) = \mathbf{F}_3(S,T) = E$ gibt. In der Tat ist $a^3 \in \mathbf{F}_3(S^3, T^3) = K$, so daß das Polynom $X^3 - a^3 \in K[X]$, welches a annulliert, zeigt, daß

$$[K(a) : K] \;=\; \deg \mu_{a,K}(X) \;\le\; \deg(X^3 - a^3) \;=\; 3\,,$$

im Gegensatz zu $[E : K] = 9$.

Aufgabe 51.

(1) Der Endomorphismenring ergibt sich zu

$$\operatorname{End} M \simeq \begin{pmatrix} \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ (3) & \mathbf{Z} & \mathbf{Z} \\ (9) & (3) & \mathbf{Z} \end{pmatrix} \Big/ \begin{pmatrix} (3) & (3) & (3) \\ (9) & (9) & (9) \\ (27) & (27) & (27) \end{pmatrix}\,,$$

und wir erhalten $3^{(1+1+1)+(1+2+2)+(1+2+3)} = 3^{14}$ Endomorphismen.

(2) Reduktion aller Einträge modulo 3 gibt einen Ringmorphismus von $\operatorname{End} M$ in die oberen Dreiecksmatrizen

$$\begin{pmatrix} \mathbf{F}_3 & \mathbf{F}_3 & \mathbf{F}_3 \\ 0 & \mathbf{F}_3 & \mathbf{F}_3 \\ 0 & 0 & \mathbf{F}_3 \end{pmatrix}\,.$$

Dieser induziert einen Gruppenmorphismus auf den Gruppen der invertierbaren Elemente, d.h. von den Automorphismen in die invertierbaren oberen Dreiecksmatrizen.

Dieser Gruppenmorphismus ist surjektiv, wie man durch die Wahl einer oberen Dreiecksmatrix als Urbild sieht (ein solches Urbild mit invertierbaren Diagonalelementen liefert einen injektiven und damit bijektiven Endomorphismus). Es gibt $(3-1)^3 \cdot 3^3$ invertierbare obere Dreiecksmatrizen.

Der Kern dieses Morphismus besteht aus den Restklassen der Matrizen, die zur Einheitsmatrix eine Differenz in $\begin{pmatrix} (3) & (3) & (3) \\ (3) & (3) & (3) \\ (9) & (3) & (3) \end{pmatrix}$ aufweisen. Solche Matrizen haben eine zu 3 teilerfremde Determinante, sind also unter Verwendung eines Inversen zur Determinante in $\mathbf{Z}/27\mathbf{Z}$ mithilfe der Cramerschen Regel in E invertierbar, wie man sich insbesondere an den Positionen $(2,1)$, $(3,1)$ und $(3,2)$ überzeugt. Damit besteht dieser Kern aus $3^{(0+0+0)+(1+1+1)+(1+2+2)} = 3^8$ Elementen.

Insgesamt wird

$$|\operatorname{Aut} M| \;=\; (3-1)^3 \cdot 3^3 \cdot 3^8 = 2^3 \cdot 3^{11}\,.$$

Aufgabe 52.

(1) Die Aussage ist richtig. Wählen wir eine $K(a)$-lineare Basis $(x_1, \ldots, x_n)$ von L, und eine K-lineare Basis $(y_1, \ldots, y_m)$ von $K(a)$, so wird $(x_1y_1, x_1y_2, \ldots, x_ny_m)$ eine K-lineare Basis von L bezüglich welcher sich die Abbildung $L \longrightarrow L$, $t \longrightarrow at$ als Blockmatrix mit $[L : K(a)]$ Blöcken schreibt, welche alle gleich der Matrix sind, die die Abbildung $K(a) \longrightarrow K(a)$, $t \longmapsto at$ bezüglich der Basis $(y_1, \ldots, y_m)$ beschreibt. Es bleibt also zu zeigen, daß das charakteristische Polynom der letztgenannten Matrix gleich ihrem Minimalpolynom ist. Nun hat das Minimalpolynom dieser Matrix, i.e. $\mu_{a,K}(X)$, den Grad $m = [K(a) : K]$. Da es das charakteristische Polynom teilt, und da das charakteristische Polynom der vorliegenden $m \times m$-Matrix ebenfalls Grad m hat, ist in der Tat $\mu_{a,K}(X)$ auch deren charakteristisches Polynom.

(2) Die Aussage ist falsch. Seien z.B. $K = \mathbf{R}$, $f(X) = X^2 + 1$ und $g(X) = X^2 - 2X + 2$. Beide Wurzelkörper sind isomorph zu $\mathbf{C}$ (cf. 49 (1 i)).

(3) Die Aussage ist richtig. Denn es teilt $\mu_{a,K}(X)$ das Polynom $f(X)$, so daß sich aus der Tatsache, daß $f(X)$ irreduzibel und normiert ist, in der Tat $f(X) = \mu_{a,K}(X)$ ergibt.

(4) Die Aussage ist richtig. Denn wir haben eine injektive Abbildung $K[X]/(\mu_{a,K}(X)) \longrightarrow L$, $\bar{X} \longmapsto a$, deren Bild $K[a]$ wegen $K[a]$ endlichdimensionaler Integritätsbereich wieder ein Körper ist, i.e. $K[a] = K(a)$. Damit ist $(\mu_{a,K}(X)) \subseteq K[X]$ ein maximales Ideal, i.e. es ist $\mu_{a,K}(X)$ irreduzibel.

(5) Die Aussage ist richtig.

Sind u und v algebraisch über E, so ist die Erweiterung $K(u, v)$ endlich und mithin algebraisch über K. Damit sind insbesondere deren Elemente $u + v$ und uv algebraisch über K.

Umgekehrt, sind $u+v$ und uv algebraisch über K, so sind u und v als Nullstellen des Polynoms $X^2-(u+v)X+uv$ algebraisch über $K(uv, u+v)$. Es ist mithin die Erweiterung $K(u, v)|K(uv, u+v)$ algebraisch, genauso wie nach Voraussetzung auch die Erweiterung $K(uv, u + v)|K$. Damit ist auch $K(u, v)|K$ algebraisch, und insbesondere sind u und v algebraisch über K.