G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 13

Aufgabe 53.

(1) Sei $K = \mathbf{Q}$ und $E = \mathbf{Q}(\sqrt{3}+\sqrt{5})$. Es ist $|\operatorname{Gal}(E|K)| = [E:K] = 4$.

(i) Wir behalten die Notation der Lösung von 49 (2) bei, und numerieren die Nullstellen des Minimalpolynoms von $1+\sqrt{3}+\sqrt{5}$ wie folgt durch.

$$\begin{array}{lclcl} \alpha_1 & = & 1+\sqrt{3}+\sqrt{5} & & \\ \alpha_2 & = & 1-\sqrt{3}+\sqrt{5} & = & \frac{1}{2}(-\alpha_1^3+3\alpha_1^2+13\alpha_1-13) \\ \alpha_3 & = & 1+\sqrt{3}-\sqrt{5} & = & \frac{1}{2}(\alpha_1^3-3\alpha_1^2-13\alpha_1+17) \\ \alpha_4 & = & 1-\sqrt{3}-\sqrt{5} & = & -\alpha_1+2 \end{array}$$

Zweitere Gleichungen folgen mittels der in 49 (1 i) betrachteten Matrix (mit 5-ter Spalte gestrichen), hier einmal als $A \in \mathbf{Q}^{4\times 4}$ bezeichnet. So z.B. folgt die letzte Zeile, da

$$Ax = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \end{pmatrix} .$$

die Lösung $x = \begin{pmatrix} 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}$ hat.

Wir wollen die Galoisgruppe via ihrer Operation in $\mathcal{S}_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}} \simeq \mathcal{S}_4$ einbetten.
Es wird

$$\begin{array}{lclclcl} \sigma_2(\alpha_1) & = & \alpha_2 & & & & \\ \sigma_2(\alpha_2) & = & \sigma_2\left(\frac{1}{2}(-\alpha_1^3+3\alpha_1^2+13\alpha_1-13)\right) & = & \frac{1}{2}(-\alpha_2^3+3\alpha_2^2+13\alpha_2-13) & = & \alpha_1 \\ \sigma_2(\alpha_3) & = & \sigma_2\left(\frac{1}{2}(\alpha_1^3-3\alpha_1^2-13\alpha_1+17)\right) & = & \frac{1}{2}(\alpha_2^3-3\alpha_2^2-13\alpha_2+17) & = & \alpha_4 \\ \sigma_2(\alpha_4) & = & \sigma_2(-\alpha_1+2) & = & -\alpha_2+2 & = & \alpha_3 . \end{array}$$

Beachte, daß als letztes $\sigma_2(\alpha_4) = \alpha_3$ *auch ohne Rechnung* folgt, da σ_2 eine Bijektion der Nullstellen in sich liefert, und nur α_3 bislang noch nicht als Bildelement aufgetreten war. Die Rechnung durchzuführen, ist aber eine gute Probe.
Somit geht σ_2 auf $(1,2)(3,4) \in \mathcal{S}_4$. Das Erzeugnis von σ_2 hat 2 Elemente, was < 4 ist. Wir müssen also noch weitere Automorphismen als Erzeuger hinzufügen.
Etwa wird

$$\begin{array}{lclclcl} \sigma_3(\alpha_1) & = & \alpha_3 & & & & \\ \sigma_3(\alpha_2) & = & \sigma_3\left(\frac{1}{2}(-\alpha_1^3+3\alpha_1^2+13\alpha_1-13)\right) & = & \frac{1}{2}(-\alpha_3^3+3\alpha_3^2+13\alpha_3-13) & = & \alpha_4 \\ \sigma_3(\alpha_3) & = & \sigma_3\left(\frac{1}{2}(\alpha_1^3-3\alpha_1^2-13\alpha_1+17)\right) & = & \frac{1}{2}(\alpha_3^3-3\alpha_3^2-13\alpha_3+17) & = & \alpha_1 \\ \sigma_3(\alpha_4) & = & \sigma_3(-\alpha_1+2) & = & -\alpha_3+2 & = & \alpha_2 . \end{array}$$

Beachte abermals, daß als letztes $\sigma_3(\alpha_4) = \alpha_2$ *auch ohne Rechnung* folgt.
Somit geht σ_3 auf $(1,3)(2,4) \in \mathcal{S}_4$. Nun enthält $\langle \sigma_1, \sigma_2 \rangle$ alle 4 Elemente, nämlich, nach Einbettung,

$$\operatorname{Gal}(E|K) \xrightarrow{\sim} \langle (1,2)(3,4),\ (1,3)(2,4) \rangle \ = \ \{1,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\} \ \leq \ \mathcal{S}_4 .$$

Diesen Isomorphismus verwenden wir als Identifikation.

Anstelle des Erzeugers $1+\sqrt{3}+\sqrt{5}$ wäre es geschickter gewesen, die Erzeuger $\sqrt{3}$ und $\sqrt{5}$ zu verwenden. Hier ist das ersichtlich, im allgemeinen sieht man solche Vereinfachungen aber nicht, weswegen wir bei unserem Erzeuger geblieben sind.

(ii) Die echten Zwischenkörper ergeben sich als Fixkörper der nichttrivialen Untergruppen von $\operatorname{Gal}(E|K)$,

$$U_1 \ = \ \langle (1,2)(3,4) \rangle , \qquad U_2 \ = \ \langle (1,3)(2,4) \rangle , \qquad U_3 \ = \ \langle (1,4)(2,3) \rangle .$$

Schreibe $F_i := \mathrm{Fix}_{U_i}(E)$ für $i \in [1,3]$.

Da die Fixkörper hier jeweils Grad 2 über K haben, und 2 prim ist, genügt es, je ein Element in F_i anzugeben, welches nicht in K liegt, da echt zwischen K und F_i kein weiterer Körper mehr liegen kann. Hierfür kann man $\mathrm{S}_{E|F_i}(\xi) = \sum_{\rho \in U_i} \rho(\xi)$ für ein geeignetes $\xi \in E$ verwenden – beachte, daß $\mathrm{S}_{E|F_i} : E \longrightarrow F_i$ surjektiv ist.

So wird

$$\begin{array}{rclcl} F_1 & = & K(\alpha_1 + \sigma_2(\alpha_1)) & = & \mathbf{Q}(\sqrt{5}) \\ F_2 & = & K(\alpha_1 + \sigma_3(\alpha_1)) & = & \mathbf{Q}(\sqrt{3}) \\ F_3 & = & K(\alpha_1^2 + (\sigma_2 \circ \sigma_3)(\alpha_1^2)) & = & \mathbf{Q}(\sqrt{15})\ , \end{array}$$

da $\alpha_1^2 = 9 + 2\sqrt{3} + 2\sqrt{5} + 2\sqrt{15}$ unter $\sigma_2 \circ \sigma_3$ auf $\alpha_4^2 = 9 - 2\sqrt{3} - 2\sqrt{5} + 2\sqrt{15}$ abgebildet wird.

(iii) Da $\mathrm{Gal}(E|K)$ abelsch ist, sind alle Untergruppen normal in G, und insbesondere sind $F_1|K$, $F_2|K$ und $F_3|K$ galoisch.

Aus $E|K$ galoisch und $E|F|K$ folgt auch $E|F$ galoisch – in dieser Richtung gibt es also nichts zu entscheiden.

(2) Sei $K = \mathbf{Q}$ und $E = \mathbf{Q}(\alpha_1, \alpha_2)$, mit $\alpha_1^3 = 3$ und $\alpha_2^2 = -\alpha_1\alpha_2 - \alpha_1^2$. Es ist $|\,\mathrm{Gal}(E|K)| = [E:K] = 6$. Es war $f(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ mit $\alpha_3 := -\alpha_1 - \alpha_2$.

(i) Hier können wir *völlig ohne Rechnung* argumentieren, da wir die Operation der 6 Galoisautomorphismen auf 2 der 3 Wurzeln von $f(X)$ kennen, und damit auch auf der dritten. Aus diesen greifen wir die beiden Automorphismen

$$\begin{array}{ccc} E & \longrightarrow & E \\ (\alpha_1, \alpha_2, \alpha_3) & \overset{\sigma_1}{\longmapsto} & (\alpha_2, \alpha_1, \alpha_3) \\ (\alpha_1, \alpha_2, \alpha_3) & \overset{\sigma_2}{\longmapsto} & (\alpha_2, \alpha_3, \alpha_1) \end{array}$$

heraus, wobei in dieser Notation der Automorphismus eintragsweise wirke. Die Einbettung in $\mathcal{S}_{\{\alpha_1,\alpha_2,\alpha_3\}} \simeq \mathcal{S}_3$ gibt

$$\begin{array}{rcl} \mathrm{Gal}(E|K) & \hookrightarrow & \mathcal{S}_3 \\ \sigma_1 & \longmapsto & (1,2) \\ \sigma_2 & \longmapsto & (1,2,3)\ , \end{array}$$

und da das Bild bereits 6 Elemente hat, ist zum einen $\mathrm{Gal}(E|K) = \langle \sigma_1, \sigma_2 \rangle$, und zum anderen diese Einbettung ein Isomorphismus. Wir verwenden ihn als Identifikation.

(ii) Die echten Zwischenkörper ergeben sich als Fixkörper der nichttrivialen Untergruppen von $\mathrm{Gal}(E|K)$,

$$U_1 = \langle (1,2) \rangle\ , \qquad U_2 = \langle (2,3) \rangle\ , \qquad U_3 = \langle (1,3) \rangle\ , \qquad U_4 = \langle (1,2,3) \rangle\ .$$

Schreibe $F_i := \mathrm{Fix}_{U_i}(E)$ für $i \in [1,4]$.

Da die Fixkörper hier jeweils primen Grad über K haben, genügt es, je ein Element in $F_i := \mathrm{Fix}_{U_i}(E)$ anzugeben, welches nicht in K liegt. Hierfür kann man $\mathrm{S}_{E|F_i}(\xi) = \sum_{\rho \in U_i} \rho(\xi)$ für ein geeignetes $\xi \in E$ verwenden.

So wird

$$\begin{array}{rcl} F_1 & = & K(\alpha_1 + \alpha_2) \\ F_2 & = & K(\alpha_1) \\ F_3 & = & K(\alpha_2) \\ F_4 & = & K(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) \;=\; K(3\alpha_1^2\alpha_2) \;=\; K(\alpha_1^2\alpha_2)\ . \end{array}$$

Unter Verwendung der Basis $(\alpha_1^0\alpha_2^0, \ldots, \alpha_1^2\alpha_2^1)$ sieht man jeweils, daß der angegebene Erzeuger in der Tat nicht in K liegt. Das muß man beachten – so z.B. ist $K(\alpha_1 + \alpha_2 + \alpha_3)$ nicht gleich F_4, sondern gleich K wegen $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

Man auch ohne Rechnung erkennen, daß $\alpha_1 + \alpha_2 + \alpha_3$ nicht als Erzeuger taugt. Denn $\alpha_1 + \alpha_2 + \alpha_3$ ist ein symmetrisches Polynom in den Wurzeln von $f(X)$, und als solches ein Polynom in den Koeffizienten von $f(X)$, welche aber in K liegen.

Insgesamt sind hier die Elemente 1, α_1, α_2, $\alpha_1\alpha_2$, α_1^2 der gewählten K-Basis von E als ξ unbrauchbar. Man weiß aber wegen $\mathrm{S}_{E|F_4}$ surjektiv, daß nicht alle unbrauchbar sein dürfen – endliches Probieren führt zum Ziel! In der Tat *muß* nach Ausschluß der 5 anderen Basiselemente $\xi = \alpha_1^2\alpha_2$ eine geeignete Wahl sein.

(iii) Es ist nur F_4 galoisch über K, da nur U_4 normal in $\mathrm{Gal}(E|K)$ ist.

Aus $E|K$ galoisch und $E|F|K$ folgt hingegen auch $E|F$ galoisch – in dieser Richtung gibt es also nichts zu entscheiden.

(3) Sei $K = \mathbf{Q}(\sqrt{2})$, und sei $E = K(\alpha_1, \alpha_2)$, wobei $\alpha_1^4 = 2\alpha_1^2 + \sqrt{2}$ und $\alpha_2^2 = 2 - \alpha_1^2$. Ferner war $f(X) = (X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2)$.

(i) Auch hier können wir ohne Rechnung vorgehen, da ein Automorphismus ein Negatives einer Nullstelle auf das entsprechende Negative des Bildes schickt. Numerieren wir vollends durch mittels $\alpha_3 := -\alpha_1$ und $\alpha_4 := -\alpha_2$, so können wir aus den in 50 (2 ii) gefundenen Automorphismen folgende beiden auswählen.

$$\begin{array}{rcl} E & \longrightarrow & E \\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \overset{\sigma_1}{\longmapsto} & (\alpha_3, \alpha_2, \alpha_1, \alpha_4) \\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \overset{\sigma_2}{\longmapsto} & (\alpha_2, \alpha_3, \alpha_4, \alpha_1) \end{array}$$

heraus, wobei in dieser Notation der Automorphismus eintragsweise wirke. Die Einbettung in $\mathcal{S}_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}} \simeq \mathcal{S}_4$ gibt

$$\begin{array}{rcl} \mathrm{Gal}(E|K) & \hookrightarrow & \mathcal{S}_3 \\ \sigma_1 & \longmapsto & (1,3) \\ \sigma_2 & \longmapsto & (1,2,3,4)\ , \end{array}$$

und deren das Bild bereits 8 Elemente hat, ist $\mathrm{Gal}(E|K) = \langle \sigma_1, \sigma_2 \rangle$ erreicht. Wir verwenden diese Einbettung als Identifikation.

Es folgt somit auch, daß $\mathrm{Gal}(E|K) \simeq D_8$. Das war zwar nicht direkt gefragt, ist aber nützlich zu wissen, da man ja die Untergruppen und Normalteiler dieser Galoisgruppe braucht.

(ii) Die echten Zwischenkörper ergeben sich als Fixkörper der nichttrivialen Untergruppen von $\mathrm{Gal}(E|K)$,

$$\begin{array}{llll} U_1 = \langle (1,3) \rangle\ , & U_2 = \langle (2,4) \rangle\ , & U_3 = \langle (1,2)(3,4) \rangle\ , & U_4 = \langle (1,3)(2,4) \rangle\ , \\ U_5 = \langle (1,4)(2,3) \rangle\ , & U_6 = \langle (1,2,3,4) \rangle\ , & U_7 = \langle (1,2)(3,4), (1,3)(2,4) \rangle\ , & \\ U_8 = \langle (1,3), (1,3)(2,4) \rangle\ . & & & \end{array}$$

Schreibe $F_i := \mathrm{Fix}_{U_i}(E)$ für $i \in [1,8]$.

Für die Fixkörper mit Grad 2 über K genügt es, je ein Element in $F_i := \mathrm{Fix}_{U_i}(E)$ anzugeben, welches nicht in K liegt. Hierfür kann man $\mathrm{S}_{E|F_i}(\xi) = \sum_{\rho \in U_i} \rho(\xi)$ für ein geeignetes $\xi \in E$ verwenden.

Das Minimalpolynom $T^4 - 2T^2 - \sqrt{2}$ von α_1 und von α_2 über K hat Grad 4 (siehe 50 (2 i)). Somit ist $K(\alpha_2)$ bereits gleich F_2 wegen $[F_2 : K] = 4 = [K(\alpha_2) : K]$.

Es liegen F_7 und F_8 in F_4, und da echt zwischen F_4 und F_8 kein weiterer Körper mehr liegt, erzeugen die Erzeuger von F_7 und F_8 zusammen F_4.

Bleiben F_3 und F_5, welche beide F_7 enthalten. Eine Basis von F_7 über K ist gegeben durch $(1, \alpha_1\alpha_2)$. Für F_3 brauchen wir noch ein weiteres Element, welches fix unter $(1,2)(3,4)$ bleibt, aber nicht in F_7 liegt. Zum Beispiel $\alpha_1 + \alpha_2$. Nun geht U_5 aus U_3 durch Konjugation mit $(1,3)$ von links hervor. Also geht F_5 aus F_3 durch Anwenden von $(1,3)$ hervor, und dieser Automorphismus schickt $\alpha_1\alpha_2$ auf $-\alpha_1\alpha_2$ sowie $\alpha_1 + \alpha_2$ auf $-\alpha_1 + \alpha_2$.

So wird

$$\begin{array}{rcl} F_1 & = & K(\alpha_2) \\ F_2 & = & K(\alpha_1) \\ F_3 & = & K(\alpha_1\alpha_2, \alpha_1 + \alpha_2) \\ F_4 & = & K(\alpha_1^2, \alpha_1\alpha_2) \\ F_5 & = & K(\alpha_1\alpha_2, \alpha_1 - \alpha_2) \\ F_6 & = & K(\mathrm{S}_{E|F_6}(\alpha_1^3\alpha_2)) \ = \ K((\alpha_1^2 - 1)\alpha_1\alpha_2) \\ F_7 & = & K(\alpha_1\alpha_2) \\ F_8 & = & K(\alpha_1^2)\ . \end{array}$$

Man kommt unter Verwendung von $\mathrm{S}_{E|F_i}$ und mit Berechnung von Minimalpolynomen auch ohne die angeführten Abkürzungen aus, muß dafür aber mehr Aufwand betreiben.

(iii) Es sind nur F_4, F_6, F_7 und F_8 galoisch über K, da nur U_4, U_6, U_7 und U_8 normal in $\mathrm{Gal}(E|K)$ sind. Aus $E|K$ galoisch und $E|F|K$ folgt hingegen auch $E|F$ galoisch – in dieser Richtung gibt es also nichts zu entscheiden.

Aufgabe 54.

(1) Da $L_i = L_{i+1}(X_{i+1})$, genügt es für $[L_i : L_{i+1}] \leq i+1$ zu zeigen, daß es ein Polynom von Grad $\leq i+1$ in $L_{i+1}[T] \smallsetminus \{0\}$ gibt, welches X_{i+1} annulliert. Dies wird von

$$f_{i+1}(T) \;=\; (T - X_1)\cdots(T - X_{i+1})$$

geleistet, da $f_{i+1}(T)$ Koeffizienten in L_{i+1} hat, wie mit absteigender Induktion folgt, mit dem Induktionsanfang $f_n(T) = f(T) \in L_n[T] = \tilde{K}[T]$.

Es ist

$$[E : \tilde{K}] \;=\; [L_0 : L_n] \;=\; [L_0 : L_1][L_1 : L_2]\cdots[L_{n-1} : L_n] \;\leq\; n!\,.$$

Nun ist aber $[E : K] = [E : \mathrm{Fix}_{\mathcal{S}_n}(E)] = |\mathcal{S}_n| = n!$, so daß aus $n! \geq [E : \tilde{K}] = [E : K][K : \tilde{K}] = n![K : \tilde{K}]$ folgt, daß $K = \tilde{K}$.

(2) Da aus (1) insbesondere $[E : \tilde{K}] = [L_0 : L_1][L_1 : L_2]\cdots[L_{n-1} : L_n] = n!$ folgt, ist auch $[L_i : L_{i+1}] = i+1$. Insbesondere ist $(X_{i+1}^0, \dots, X_{i+1}^i)$ eine Basis von L_i über L_{i+1}, und folglich ist

$$\underline{b} \;:=\; (X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \mid a_i \in [0, i-1])$$

eine Basis von $E = L_0$ über $K = L_n$.

Sei $R = \mathbf{Z}[s_1, \dots, s_n]$. Es ist $f_n(T) = f(T) \in R[T]$. Polynomdivision zeigt, daß für $i \in [0, n-1]$ das Polynom $\mu_{X_{i+1}, L_i}(T) = f_{i+1}(T) \in R[X_{i+2}, \dots, X_n][T]$ liegt. Daher ist jede Potenz von X_{i+1} eine Linearkombination in $(X_{i+1}^0, \dots, X_{i+1}^i)$ mit Koeffizienten in $R[X_{i+2}, \dots, X_n]$. Diese Reduktion iteriert durchgeführt, angefangen mit den Potenzen von X_1, zeigt, daß jedes Element von $R[X_1, \dots, X_n]$ sich mit Koeffizienten in R als Linearkombination in $\underline{b}$ schreiben läßt. Und diese Koeffizienten liegen für ein solches gegebenes Element eindeutig fest.

Ist nun ein Element in $\mathbf{Z}[X_1, \dots, X_n] \smallsetminus \{0\}$ fix unter $\mathcal{S}_n$, so liegt es in K und hat bezüglich der Basis $\underline{b}$ nur einen nichtverschwindenden Koeffizienten, nämlich den bei 1 für $a_1 = \cdots = a_n = 0$. Mit dem eben Gesagten ist dieser Koeffizient in R, in anderen Worten, das fragliche Element liegt bereits in R.

(3) Es stehen die symmetrischen Polynome $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$ und $s_3 = X_1X_2X_3$ zur Verfügung. Zunächst wird ausmultipliziert und lexikographisch sortiert, und dann schrittweise reduziert. Dabei wird jeweils das erste Monom durch ein geeignetes Polynom in s_1, s_2 und s_3 entfernt. Ist das erste Polynom etwa $X_1^4X_2^2$, so kann man dazu $s_1^2 s_2^2$ nehmen. Ist es $-4X_1^4X_2X_3$, so kann man $-4s_1^3s_3$ nehmen. Usf. So wird

$$\begin{array}{rl}
& (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2 \\
= & X_1^4X_2^2 - 2X_1^4X_2X_3 + X_1^4X_3^2 - 2X_1^3X_2^3 + 2X_1^3X_2^2X_3 + 2X_1^3X_2X_3^2 - 2X_1^3X_3^3 + X_1^2X_2^4 + 2X_1^2X_2^3X_3 \\
& - 6X_1^2X_2^2X_3^2 + 2X_1^2X_2X_3^3 + X_1^2X_3^4 - 2X_1X_2^4X_3 + 2X_1X_2^3X_3^2 + 2X_1X_2^2X_3^3 - 2X_1X_2X_3^4 + X_2^4X_3^2 - 2X_2^3X_3^3 \\
& + X_2^2X_3^4 \\
= & s_1^2s_2^2 - 4X_1^4X_2X_3 - 4X_1^3X_2^3 - 6X_1^3X_2^2X_3 - 6X_1^3X_2X_3^2 - 4X_1^3X_3^3 - 6X_1^2X_2^3X_3 - 21X_1^2X_2^2X_3^2 - 6X_1^2X_2X_3^3 \\
& - 4X_1X_2^4X_3 - 6X_1X_2^3X_3^2 - 6X_1X_2^2X_3^3 - 4X_1X_2X_3^4 - 4X_2^3X_3^3 \\
= & s_1^2s_2^2 - 4s_1^3s_3 - 4X_1^3X_2^3 + 6X_1^3X_2^2X_3 + 6X_1^3X_2X_3^2 - 4X_1^3X_3^3 + 6X_1^2X_2^3X_3 + 3X_1^2X_2^2X_3^2 + 6X_1^2X_2X_3^3 \\
& + 6X_1X_2^3X_3^2 + 6X_1X_2^2X_3^3 - 4X_2^3X_3^3 \\
= & s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18X_1^3X_2^2X_3 + 18X_1^3X_2X_3^2 + 18X_1^2X_2^3X_3 + 27X_1^2X_2^2X_3^2 + 18X_1^2X_2X_3^3 + 18X_1X_2^3X_3^2 \\
& + 18X_1X_2^2X_3^3 \\
= & s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27X_1^2X_2^2X_3^2 \\
= & s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2\,.
\end{array}$$

(4) Sei E Zerfällungskörper von f, und sei $T^3 + uT + v = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \in E[X]$. Dann verschwindet zunächst $s_1(\alpha_1, \alpha_2, \alpha_3)$ als das Negative des Koeffizienten von T^2. Ferner ist $s_2(\alpha_1, \alpha_2, \alpha_3) = u$ und $s_3(\alpha_1, \alpha_2, \alpha_3) = -v$. Es hat f genau dann keine mehrfachen Nullstellen in E, wenn

$$0 \neq (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4s_2^3 - 27s_3^2 = -(4u^3 + 27v^2)\,,$$

wie behauptet.

Aufgabe 55.

(1) Sei $\tilde{E}$ Zerfällungskörper von $X^m - 1$. Beachte, daß die Nullstellen von $X^m - 1$ in $\tilde{E}$ wegen $\mathrm{ggT}(X^m - 1, mX^{m-1}) = 1$ paarweise verschieden sind.

Es ist $\boldsymbol{\mu}_m := \{z \in \tilde{E}^* \mid z^m = 1\} \subseteq \tilde{E}^*$ eine endliche Untergruppe von $\tilde{E}^*$, da sie genauer gesagt gerade m Elemente enthält. Also ist sie zyklisch. Es gibt mithin ein $\zeta_m \in \tilde{E}^*$ mit

$$X^m - 1 = \prod_{i\in[0,m-1]} (X - \zeta_m^i)\,.$$

Wir behaupten, daß $\Phi_m(X) = \prod_{i\in[0,m-1],\ \mathrm{ggT}(i,m)=1}(X - \zeta_m^i)$ ist. In anderen Worten, wir behaupten, daß der Linearfaktor $X - \zeta_m^i$ für $i \in [0, m-1]$ genau dann in $\Phi_m(X)$ auftaucht, wenn ζ_m^i Ordnung m in $\tilde{E}^*$ hat. Wir führen dazu eine Induktion über m.

Sei $d \mid m$, $d \neq m$. Nach Induktionsvoraussetzung ist das Produkt aller Linearfaktoren der Form $X - \zeta_m^i$ mit $i \in [0, m-1]$ und ζ_m^i von Ordnung d gerade gleich $\Phi_d(X)$. Da ζ_m^i als Ordnung stets einen Teiler von m hat, bleibt von $X^m - 1$ nach Division durch $\prod_{\substack{d \mid m\\ d\neq m}} \Phi_d(X)$ gerade das Produkt der Linearfaktoren $X - \zeta_m^i$ übrig mit $i \in [0, m-1]$ und ζ_m^i von Ordnung m, und das ist nach Definition gleich $\Phi_m(X)$.

Dies zeigt nun zunächst nur $\Phi_m(X) \in \mathbf{Z}[\zeta_m][X]$, und $\Phi_m(X)$ normiert.

Wir behaupten, daß die Koeffizienten von $\Phi_m(X)$ in $\mathbf{Z}$ liegen. Abermals führen wir eine Induktion über m. Nach Induktionsvoraussetzung ist $\prod_{\substack{d \mid m\\ d\neq m}} \Phi_d(X) \in \mathbf{Z}[X]$, und ferner ist es normiert. Polynomdivision zeigt nun, daß auch Division von $X^m - 1$ durch dieses Polynom ein Ergebnis in $\mathbf{Z}[X]$ liefert.

(2) Da $\Phi_m(X)$ ein Teiler von $X^m - 1$ ist, können wir seinen Zerfällungskörper als Teilkörper von $\tilde{E}$ aus der Lösung von (1) bilden. Eine Nullstelle von $\Phi_m(X)$ ist darin ein Gruppenerzeuger von $\boldsymbol{\mu}_m$. Da wir in (1) ζ_m als einen solchen Gruppenerzeuger gewählt haben, können wir dort die Wahl so treffen, daß die Bedeutungen von ζ_m in (2) (vorgegebene Nullstelle von $\Phi_m(X)$) und in (1) (Gruppenerzeuger von $\boldsymbol{\mu}_m$) übereinstimmen.

In (1) haben wir nun schon gesehen, daß $\mathbf{Q}(\zeta_m)$ bereits gleich dem Zerfällungskörper E von $\Phi_m(X)$ (und ebenfalls gleich dem Zerfällungskörper $\tilde{E}$ von $X^m - 1$) ist.

Auch haben wir gesehen, daß ζ_m von multiplikativer Ordnung m ist. Ist d ein echter Teiler von m, so ist mithin $\zeta_m^d \neq 1$.

(3[1]) Schreibe $f(X) := X^m - 1$ und $g(X) := f(X)/\Psi(X)$. Beachte noch, daß mit dem Lemma von Gauß $\Psi(X)$ und $g(X)$ in $\mathbf{Z}[X]$ liegen.

Sei $\mathbf{Z} \xrightarrow{\nu} \mathbf{Z}/(p) = \mathbf{F}_p$, $x \longmapsto x + (p)$ die Restklassenabbildung.

Es ist $(f^\nu)'(X) = mX^{m-1}$, was insbesondere wegen $m \not\equiv_p 0$ nicht verschwindet, also X als einzigen Primteiler hat, und mithin zu $f^\nu(X) = X^m - 1$ teilerfremd ist. Also hat $f^\nu(X)$ in seinem Zerfällungskörper nur einfache Nullstellen. Wegen $f^\nu(X) = g^\nu(X)\Psi^\nu(X)$ sind mithin $g^\nu(X)$ und $\Psi^\nu(X)$ teilerfremd – wären sie es nicht, hätten sie über Zerfällungskörper von $f^\nu(X)$ über $\mathbf{F}_p$ einen gemeinsamen Linearfaktor, und $f^\nu(X)$ hätte darin eine mehrfache Nullstelle.

Wir müssen zeigen, daß $g(\zeta_m^{ip}) \neq 0$. Wäre $g(\zeta_m^{ip}) = 0$, so wäre ζ_m^i eine Nullstelle von $g(X^p)$ und also $\Psi(X)$ ein Teiler von $g(X^p)$, sagen wir, $g(X^p) = \Psi(X)k(X)$ mit $k(X) \in \mathbf{Z}[X]$. Dann wäre aber auch $g^\nu(X)^p = g^\nu(X^p) = \Psi^\nu(X)k^\nu(X)$. Somit können $g^\nu(X)$ und $\Psi^\nu(X)$ nicht teilerfremd sein, und wir haben einen Widerspruch.

(4) Sei $\Psi(X)$ der normierte irreduzible Faktor von $\Phi_m(X)$ mit Nullstelle ζ_m. Sei $i \in [0, m-1]$ teilerfremd zu m. Wir behaupten, daß $\Psi(\zeta_m^i) = 0$. Zerlegt man i in Primfaktoren, so ist jeder Faktor teilerfremd zu m. Die Behauptung folgt nun mit iterierter Anwendung von (3) bezüglich dieser Primfaktoren. Beachte, daß sich das in (3) benötigte Polynom $\Psi(X)$ während dieses Prozesses nicht ändert.

Da Ψ mit (3) daher jedes Element von $\boldsymbol{\mu}_m$ von Ordnung m zur Nullstelle hat, folgt aus der Lösung zu (1), daß $\Psi(X) = \Phi_m(X)$, womit $\Phi_m(X)$ als irreduzibel nachgewiesen ist.

Insbesondere ist $\Phi_m(X)$ wegen $\Phi_m(\zeta_m) = 0$ das Minimalpolynom des (abstrakt konstruierten) Elements ζ_m (vgl. 52 (3)).

[1] Mit Dank an Frau stud. math. Piesniak für eine Vereinfachung der Lösung.

Um zu zeigen, daß $\Phi_m(X)$ auch das Minimalpolynom von $\tilde{\zeta}_m := \exp(2\pi i/m)$ ist, genügt es zu zeigen, daß $\Phi_m(\tilde{\zeta}_m) = 0$. Es hat $\tilde{\zeta}_m$ die Ordnung m in $\mathbf{C}^*$. Für einen echten Teiler d von m hat das Polynom $\Phi_d(X)$ in seinem Zerfällungskörper keine Nullstelle von multiplikativer Ordnung m. Da wir diesen Zerfällungskörper in $\mathbf{C}$ einbetten können, hat $\Phi_d(X)$ auch in $\mathbf{C}$ keine Nullstelle von multiplikativer Ordnung m, und insbesondere ist $\Phi_d(\tilde{\zeta}_m) \neq 0$. Da aber $X^m - 1$ die Nullstelle $\tilde{\zeta}_m$ hat, muß $\tilde{\zeta}_m$ Nullstelle des verbleibenden Faktors $\Phi_m(X)$ sein.

Insbesondere ist $\mathbf{Q}(\tilde{\zeta}_m) \subseteq \mathbf{C}$ ebenfalls Zerfällungskörper von $\Phi_m(X)$, isomorph zu $\mathbf{Q}(\zeta_m)$ via $\zeta_m \longmapsto \tilde{\zeta}_m$.

(5) Anwenden der Definition liefert mit Polynomdivision

$$
\begin{array}{rcl}
\Phi_1(X) & = & X - 1 \\
\Phi_2(X) & = & X + 1 \\
\Phi_3(X) & = & X^2 + X + 1 \\
\Phi_4(X) & = & X^2 + 1 \\
\Phi_5(X) & = & X^4 + X^3 + X^2 + X + 1 \\
\Phi_6(X) & = & X^2 - X + 1 \\
\Phi_7(X) & = & X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_8(X) & = & X^4 + 1 \\
\Phi_9(X) & = & X^6 + X^3 + 1 \\
\Phi_{10}(X) & = & X^4 - X^3 + X^2 - X + 1\,.
\end{array}
$$