

Lösung 12

Aufgabe 40

Sei $K(a)|K$ mit $\mu_{a,K}(X) = f(X)$. Es ist $K(a)$ Zerfällungskörper von $f(X)$; vgl. Aufgabe 36.(2). Folglich ist $|\text{Gal}(f(X))| = [K(a) : K] = 2$. Auf der anderen Seite ist $\deg f = 2$, und mithin $\text{Gal}(f(X))$ isomorph zu einer Untergruppe von $\mathcal{S}_2$. Folglich ist $\text{Gal}(f(X)) \simeq \mathcal{S}_2$.

Ist speziell $K = \mathbf{R}$ und $f(X) = X^2 + 1 \in \mathbf{R}[X]$, so folgt $\mathcal{S}_2 \simeq \text{Gal}(X^2 + 1) = \text{Gal}(\mathbf{R}(i)|\mathbf{R}) = \text{Gal}(\mathbf{C}|\mathbf{R})$.

Aufgabe 41

- (1) In der Notation von §3.4.2.1 ist der Zerfällungskörper von $X^3 + X + 1 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a, b)$ mit $a^3 + a + 1 = 0$ und $b^2 + ab + (a^2 + 1) = 0$. Insbesondere ist

$$(1, a, a^2, b, ba, ba^2)$$

eine $\mathbf{Q}$ -lineare Basis von $\mathbf{Q}(a, b)$.

Es waren $\gamma_1 = a$, $\gamma_2 = b$ und $\gamma_3 = -a - b$ die Nullstellen von $f(X)$ in $\mathbf{Q}(a, b)$.

Das Bild von $\text{Gal}(\mathbf{Q}(a, b)|\mathbf{Q})$ in $\mathcal{S}_3$ bezüglich dieser Nullstellennumerierung ist gleich $\mathcal{S}_3$.

Es ist $\langle (1, 3) \rangle = \{\text{id}, (1, 3)\}$. Die zugehörigen Automorphismen schicken

$$\begin{array}{ccc} a & \xrightarrow{\text{id}} & a & a & \xrightarrow{(1,3)} & -a - b \\ b & \longmapsto & b & b & \longmapsto & b. \end{array}$$

Da $\text{Tr}_{\langle (1,3) \rangle} : \mathbf{Q}(a, b) \longrightarrow \text{Fix}_{\langle (1,3) \rangle} \mathbf{Q}(a, b)$ eine surjektive $\mathbf{Q}$ -lineare Abbildung ist, ist das Bildtupel der $\mathbf{Q}$ -Basis $(1, a, a^2, b, ba, ba^2)$ von $\mathbf{Q}(a, b)$ ein $\mathbf{Q}$ -Erzeugendensystem von $\text{Fix}_{\langle (1,3) \rangle} \mathbf{Q}(a, b)$. Berechnen wir dieses eintragsweise, so erhalten wir

$$\begin{aligned} & (\text{Tr}_{\langle (1,3) \rangle}(1), \text{Tr}_{\langle (1,3) \rangle}(a), \text{Tr}_{\langle (1,3) \rangle}(a^2), \text{Tr}_{\langle (1,3) \rangle}(b), \text{Tr}_{\langle (1,3) \rangle}(ba), \text{Tr}_{\langle (1,3) \rangle}(ba^2)) \\ &= (1 + 1, a + (-a - b), a^2 + (-a - b)^2, b + b, ba + b(-a - b), b(a^2 + (-a - b)^2 a^2)) \\ &= (2, -b, 2a^2 + 2ab + b^2, 2b, -b^2, b(2a^2 + 2ab + b^2)) \\ &= (2, -b, 2a^2 + 2ab - ab - (a^2 + 1), 2b, ab + (a^2 + 1), b(2a^2 + 2ab - ab - (a^2 + 1))) \\ &= (2, -b, a^2 + ba - 1, 2b, a^2 + ba + 1, b(a^2 + ab - 1)) \\ &= (2, -b, a^2 + ba - 1, 2b, a^2 + ba + 1, ba^2 - a(ab + (a^2 + 1)) - 1) \\ &= (2, -b, a^2 + ba - 1, 2b, a^2 + ba + 1, ba^2 - ba^2 - a^3 - a - 1) \\ &= (2, -b, a^2 + ba - 1, 2b, a^2 + ba + 1, 0). \end{aligned}$$

Dieses $\mathbf{Q}$ -Erzeugendensystem kann etwa zur $\mathbf{Q}$ -Basis

$$(1, b, a^2 + ba + 1)$$

von $\text{Fix}_{\langle (1,3) \rangle} \mathbf{Q}(a, b)$ umgeformt und ausgedünnt werden. Man erkennt auch, daß

$$\text{Fix}_{\langle (1,3) \rangle} \mathbf{Q}(a, b) = \mathbf{Q}(b),$$

da $-b^2 = ba + a^2 + 1$.

- (2) Die allgemeine Situation ist wie in (1).

Es ist $\langle (1, 2, 3) \rangle = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$. Die zugehörigen Automorphismen schicken

$$\begin{array}{ccccccc} a & \xrightarrow{\text{id}} & a & a & \xrightarrow{(1,2,3)} & b & a & \xrightarrow{(1,3,2)} & -a - b \\ b & \longmapsto & b & b & \longmapsto & -a - b & b & \longmapsto & a. \end{array}$$

Da $\text{Tr}_{\langle(1,2,3)\rangle} : \mathbf{Q}(a, b) \longrightarrow \text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b)$ eine surjektive $\mathbf{Q}$ -lineare Abbildung ist, ist das Bildtupel der $\mathbf{Q}$ -Basis $(1, a, a^2, b, ba, ba^2)$ von $\mathbf{Q}(a, b)$ ein $\mathbf{Q}$ -Erzeugendensystem von $\text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b)$. Berechnen wir dieses eintragsweise, so erhalten wir.

$$\begin{aligned} & (\text{Tr}_{\langle(1,2,3)\rangle}(1), \text{Tr}_{\langle(1,2,3)\rangle}(a), \text{Tr}_{\langle(1,2,3)\rangle}(a^2), \text{Tr}_{\langle(1,2,3)\rangle}(b), \text{Tr}_{\langle(1,2,3)\rangle}(ba), \text{Tr}_{\langle(1,2,3)\rangle}(ba^2)) \\ = & (1 + 1 + 1, a + b + (-a - b), a^2 + b^2 + (-a - b)^2, \\ & b + (-a - b) + a, ba + (-a - b)b + a(-a - b), ba^2 + (-a - b)b^2 + a(-a - b)^2) \\ = & (3, 0, 2a^2 + 2b^2 + 2ab, 0, -a^2 - b^2 - ab, -b^3 + a^3 + 3a^2b) \\ = & (3, 0, -2, 0, 1, -a + b + 3a^2b) \end{aligned}$$

Dieses $\mathbf{Q}$ -Erzeugendensystem kann etwa zur $\mathbf{Q}$ -Basis

$$(1, -a + b + 3a^2b)$$

von $\text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b)$ umgeformt und ausgedünnt werden. Man erkennt auch, daß

$$\text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b) = \mathbf{Q}(-a + b + 3a^2b) \quad (1) .$$

- (3) In der Notation der Lösung zu Aufgabe 34.(2) ist der Zerfällungskörper von $X^4 + 4X^2 + 8X + 8 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a, b)$ mit $a^4 + 4a^2 + 8a + 8 = 0$ und $b^3 + ab^2 + (a^2 + 4)b + a^3 + 4a + 8 = 0$. Insbesondere ist

$$(1, a, a^2, a^3, b, ba, ba^2, ba^3, b^2, b^2a, b^2a^2, b^2a^3)$$

eine $\mathbf{Q}$ -lineare Basis von $\mathbf{Q}(a, b)$. Wir verwenden Magma; vgl. auch Lösung zu Aufgabe 39.(1).

Seien

$$\begin{aligned} \gamma_1 &:= a \\ \gamma_2 &:= b \\ \gamma_3 &:= \frac{1}{28}(2a^3 - 3a^2 + 2a + 6)b^2 + \frac{1}{14}(-3a^3 + a^2 - 10a - 16)b + \frac{1}{14}(2a^3 - 3a^2 + 2a + 20) \\ \gamma_4 &:= \frac{1}{28}(-2a^3 + 3a^2 - 2a - 6)b^2 + \frac{1}{14}(3a^3 - a^2 + 10a + 2)b + \frac{1}{14}(-2a^3 + 3a^2 - 16a - 20) \end{aligned}$$

die Nullstellen von $X^4 + 4X^2 + 8X + 8$ in $\mathbf{Q}(a, b)$.

In Magma kann man $\text{Tr}_{\langle(1,2,3)\rangle}$ (nach Eingabe der benötigten Daten wie in Lösung zu Aufgabe 39.(1)) z.B. wie folgt eingeben.

```
RBIG<A,B> := PolynomialRing(KKK,2);
Tr := func< u | Evaluate(u,[ga1,ga2]) + Evaluate(u,[ga2,ga3]) + Evaluate(u,[ga3,ga1])>;
```

Will man damit die Spur von, sagen wir, a^2b wissen, muß $\text{Tr}(A^2*B)$; eingegeben werden.

Das Resultat notieren wir als Matrix. In den Zeilen stehen die Koeffizienten der Bilder der obigen

¹Cf. `MinimalPolynomial(b*a^2 + (-a-b)*b^2 + a*(-a-b)^2,Q)`; vorausgesetzt, $\mathbf{Q}(a, b)$ ist in Magma wie in §3.4.2.1 eingegeben.

Basiselemente von $\mathbf{Q}(a, b)$, ausgedrückt in ebendieser Basis.

	a^0b^0	a^1b^0	a^2b^0	a^3b^0	a^0b^1	a^1b^1	a^2b^1	a^3b^1	a^0b^2	a^1b^2	a^2b^2	a^3b^2
$\text{Tr}_{\langle(1,2,3)\rangle}(a^0b^0)$	84	0	0	0	0	0	0	0	0	0	0	0
$\text{Tr}_{\langle(1,2,3)\rangle}(a^1b^0)$	40	32	-6	4	-4	-20	2	-6	6	2	-3	2
$\text{Tr}_{\langle(1,2,3)\rangle}(a^2b^0)$	-48	40	-4	12	-40	-32	-8	-4	32	20	-2	6
$\text{Tr}_{\langle(1,2,3)\rangle}(a^3b^0)$	-560	-112	0	0	0	56	-28	28	0	0	14	0
$\text{Tr}_{\langle(1,2,3)\rangle}(a^0b^1)$	40	32	-6	4	-4	-20	2	-6	6	2	-3	2
$\text{Tr}_{\langle(1,2,3)\rangle}(a^1b^1)$	-64	-40	4	-12	40	32	8	4	-32	-20	2	-6
$\text{Tr}_{\langle(1,2,3)\rangle}(a^2b^1)$	-48	-16	-32	-16	128	24	20	-4	-80	-64	-2	-8
$\text{Tr}_{\langle(1,2,3)\rangle}(a^3b^1)$	96	-192	-48	32	-32	64	-96	64	48	16	32	16
$\text{Tr}_{\langle(1,2,3)\rangle}(a^0b^2)$	-48	40	-4	12	-40	-32	-8	-4	32	20	-2	6
$\text{Tr}_{\langle(1,2,3)\rangle}(a^1b^2)$	176	-16	80	-16	-96	24	20	-4	32	48	-2	-8
$\text{Tr}_{\langle(1,2,3)\rangle}(a^2b^2)$	288	96	-32	-16	128	-32	48	-32	-80	-64	-16	-8
$\text{Tr}_{\langle(1,2,3)\rangle}(a^3b^2)$	512	320	-368	96	352	-256	-64	-32	-80	-176	-16	48

In Magma kann man Matrizen mit Einträgen in $\mathbf{Q}$ wie folgt eingeben. Der Quelltext

```
Q := Rationals();
M := RMatrixSpace(Q,2,3)!Matrix([[1,2,3],[4,5,6]]);
```

z.B. liefert die 2×3 -Matrix $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \mathbf{Q}^{2 \times 3}$.

Unsere 12×12 -Matrix kann unter Zuhilfenahme von Magma via `EchelonForm(M)`; zeilenweise umgeformt werden zu

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & -4 & 2 & -2 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 4 & -4 & 2 & 0 & -4 & -2 & 0 & 2 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Wir erhalten als $\mathbf{Q}$ -Basis von $\text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b)$

$$(1, 8a - 4ab + 2a^2b - 2a^3b - a^2b^2, a^2 - 2b + b^2 + ab^2, 4a - 4a^2 + 2a^3 - 4ab - 2a^2b + 2b^2 + a^3b^2).$$

Da `MinimalPolynomial(a^2 - 2b + b^2 + a b^2, Q)`; das Minimalpolynom des dritten Basiselements über $\mathbf{Q}$ zu $X^4 + 8X^3 + 80X^2 - 192 * X + 128 \ni \mathbf{Q}[X]$ liefert, ist in der Tat

$$\text{Fix}_{\langle(1,2,3)\rangle} \mathbf{Q}(a, b) = \mathbf{Q}(a^2 - 2b + b^2 + ab^2).$$

- (4) Sei $\mathbf{F}_{16} = \mathbf{F}_4(\delta)$ mit $\delta^4 + \delta + 1 = 0$; vgl. Lösung zu Aufgabe 24.(4). Es ist $\mathbf{F}_{16}$ der Zerfällungskörper von $X^{16} - X$; vgl. §2.5.4. Es ist $\text{o}(\text{Frob}_{\mathbf{F}_{16}}) = 4$, also $\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle = \{\text{Frob}_{\mathbf{F}_{16}}^0, \text{Frob}_{\mathbf{F}_{16}}^2\}$.

Die $\mathbf{F}_2$ -Basis $(1, \delta, \delta^2, \delta^3)$ von $\mathbf{F}_{16}$ wird also abgebildet auf

$$\begin{aligned} & (\text{Tr}_{\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle}(1), \text{Tr}_{\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle}(\delta), \text{Tr}_{\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle}(\delta^2), \text{Tr}_{\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle}(\delta^3)) \\ &= (1 + 1, \delta + \delta^4, \delta^2 + \delta^8, \delta^3 + \delta^{12}) \\ &= (0, 1, 1, \delta^2 + \delta + 1). \end{aligned}$$

Vgl. Lösung zu Aufgabe 27.(6). Dies kann zur Basis

$$(1, \delta^2 + \delta)$$

von $\text{Fix}_{\langle \text{Frob}_{\mathbf{F}_{16}}^2 \rangle} \mathbf{F}_4$ umgeformt werden. Vgl. auch das Ergebnis von Aufgabe 24.(4).

Es fällt auf, daß in allen betrachteten Beispielen $[L : \text{Fix}_U L] = |U|$ ist. Wir werden dies noch allgemein bestätigen; cf. Satz 8.(1).

Aufgabe 42

- (1) Für die Wohldefiniertheit der Multiplikation ist zu zeigen, daß im Falle $gN = g'N$ und $\tilde{g}N = \tilde{g}'N$ auch $(g \cdot \tilde{g})N = (g' \cdot \tilde{g}')N$ ist, wobei $g, g', \tilde{g}, \tilde{g}' \in G$.

In der Tat ist dann $g' = gn$ und $\tilde{g}' = \tilde{g}\tilde{n}$ für gewisse $n, \tilde{n} \in N$, und es wird

$$g'\tilde{g}' = gn\tilde{g}\tilde{n} = g\tilde{g}\underbrace{\tilde{g}^{-1}n\tilde{g}}_{\substack{\in N \\ \in N}}\tilde{n},$$

mithin $g'\tilde{g}'N = g\tilde{g}N$.

Die Gruppeneigenschaften wie Assoziativität, Einselement $1_G N$ und Inverses $g^{-1}N$ zu $gN \in G/N$ vererben sich nun alle aus denen für G .

- (2) Für die Wohldefiniertheit ist zu zeigen, daß aus $g \text{ Kern } f = g' \text{ Kern } f$ auch $f(g) = f(g')$ folgt, wobei $g, g' \in G$. In der Tat haben wir diesenfalls $g' = gn$ für ein $n \in \text{Kern } f$. Es wird $f(g') = f(gn) = f(g)f(n) = f(g) \cdot 1_H = f(g)$.

Nach Konstruktion liegt nun ein surjektiver Gruppenmorphismus $G/N \longrightarrow \text{Im } f$, $g \text{ Kern } f \longmapsto f(g)$ vor.

Für die Injektivität ist zu zeigen, daß sein Kern gleich $\{1_G\}$ ist. Sei $g \in G$ so, daß $g \text{ Kern } f \longmapsto f(g) = 1_H$. Dann ist $g \in \text{Kern } f$, i.e. $g \text{ Kern } f = 1_G \text{ Kern } f$.

- (3) Nach Aufgaben 38.(1.c), 37.(2) ist $|\text{Im } f|$ ein Teiler von $|H|$. Nach Aufgabe 37.(5) ist insbesondere $N \leq G$. Die Lösung zur Aufgaben 38.(1.c) zeigt nun, daß $|G| = |N||G/N|$ – in der Tat kann G in $|G/N|$ Teilmengen der Kardinalität $|N|$ disjunkt zerlegt werden. Mit (2) ist also $|\text{Im } f| = |G/N|$ ein Teiler von $|G|$.

Aufgabe 43

- (1) Sei $\sigma \in \mathcal{S}_n$. Wir behaupten, daß es genau einen Automorphismus $\hat{\sigma}$ von $K(T_1, \dots, T_n)$ mit $\hat{\sigma}(T_i) = T_{\sigma(i)}$ für $i \in [1, n]$ und $\hat{\sigma}|_K = \text{id}_K$ gibt, sowie, daß für $\sigma, \rho \in \mathcal{S}_n$ gilt, daß $\widehat{\rho \circ \sigma} = \hat{\rho} \circ \hat{\sigma}$.

Nach der Gebrauchsanweisung für Polynomringe gibt es genau einen Ringmorphismus

$$\tilde{\sigma} : K[T_1, \dots, T_n] \longrightarrow K[T_1, \dots, T_n]$$

mit $\sigma(T_i) = T_{\sigma(i)}$ für $i \in [1, n]$ und $\tilde{\sigma}|_K$ gleich der Einbettung $K \xrightarrow{c} K[T_1, \dots, T_n]$, i.e. $\tilde{\sigma}|_K = \text{id}_K$; vgl. §1.6.2.

Nach der Gebrauchsanweisung für Quotientenkörper, angewandt auf das Kompositum

$$K[T_1, \dots, T_n] \xrightarrow{\tilde{\sigma}} K[T_1, \dots, T_n] \xrightarrow{\lambda} K(T_1, \dots, T_n),$$

gibt es genau einen Ringmorphismus – dann auch Körpermorphismus –

$$\hat{\sigma} : K(T_1, \dots, T_n) \xrightarrow{\hat{\sigma}} K(T_1, \dots, T_n)$$

mit $\hat{\sigma} \circ \lambda = \lambda \circ \tilde{\sigma}$.

$$\begin{array}{ccc} K[T_1, \dots, T_n] & \xrightarrow{\tilde{\sigma}} & K[T_1, \dots, T_n] \\ \lambda \downarrow & & \downarrow \lambda \\ K(T_1, \dots, T_n) & \xrightarrow{\hat{\sigma}} & K(T_1, \dots, T_n) \end{array}.$$

Insgesamt gibt es genau einen Körpermorphismus $K(T_1, \dots, T_n) \xrightarrow{\hat{\sigma}} K(T_1, \dots, T_n)$ mit $\hat{\sigma}(T_i) = T_{\sigma(i)}$ für $i \in [1, n]$.

Seien nun $\sigma, \rho \in \mathcal{S}_n$ gegeben. Es ist $\widehat{\rho \circ \sigma}$ der einzige Körpermorphismus von $K(T_1, \dots, T_n)$ in sich mit

$$\widehat{\rho \circ \sigma}(T_i) = T_{\widehat{\rho \circ \sigma}(i)} = T_{(\rho \circ \sigma)(i)}$$

für $i \in [1, n]$. Nun ist aber auch für den Körpermorphismus $\hat{\rho} \circ \hat{\sigma}$ von $K(T_1, \dots, T_n)$ in sich

$$(\hat{\rho} \circ \hat{\sigma})(T_i) = \hat{\rho}(\hat{\sigma}(T_i)) = \hat{\rho}(T_{\sigma(i)}) = T_{\rho(\sigma(i))}$$

für $i \in [1, n]$. Also ist $\widehat{\rho \circ \sigma} = \hat{\rho} \circ \hat{\sigma}$.

Beachte noch, daß $\hat{\text{id}} = \text{id}$, da die Identität die verlangte Eigenschaft $\text{id}(T_i) = T_i = T_{\text{id}(i)}$ hat.

Insbesondere zeigt $\widehat{\sigma^{-1} \circ \sigma} = \widehat{\sigma^{-1}} \circ \widehat{\sigma} = \hat{\text{id}} = \text{id}$, daß $\hat{\sigma}$ auch surjektiv und damit ein Automorphismus von $K(T_1, \dots, T_n)$ ist.

Dies zeigt die *Behauptung*.

Damit haben wir einen Gruppenmorphismus $\mathcal{S}_n \longrightarrow \text{Aut}(K(T_1, \dots, T_n)|K)$, $\sigma \longmapsto \hat{\sigma}$, definiert. Dieser ist injektiv, da $\hat{\sigma} = \text{id}$ insbesondere zu $T_{\sigma(i)} = \hat{\sigma}(T_i) = T_i$ für $i \in [1, n]$ führt, und somit zu $\sigma = \text{id}$.

Die angesprochene Identifikation bedeutet in der Praxis, daß wir fürderhin einfach wieder σ statt $\hat{\sigma}$ schreiben.

(2) Wir setzen

$$u(X) := +s_n X^n - s_{n-1} X^{n-1} + \dots \pm s_1 X \mp s_0 := (X - T_1)(X - T_2) \cdots (X - T_n) \in E[X].$$

In anderen Worten, es ist s_i die Summe aus allen Produkten aus $n - i$ verschiedenen Faktoren aus $\{T_1, \dots, T_n\}$, wobei $i \in [0, n]$.

Z.B. wird für $n = 3$

$$\begin{aligned} s_0 &= T_1 T_2 T_3 \\ s_1 &= T_1 T_2 + T_1 T_3 + T_2 T_3 \\ s_2 &= T_1 + T_2 + T_3 \\ s_3 &= 1. \end{aligned}$$

(3) Ist $\sigma \in \mathcal{S}_n$, so wird, in der Notation der Lösung zu (2),

$$\begin{aligned} u^\sigma(X) &\stackrel{1}{=} ((X - T_1)(X - T_2) \cdots (X - T_n))^\sigma \\ &= (X - T_1)^\sigma (X - T_2)^\sigma \cdots (X - T_n)^\sigma \\ &= (X - \sigma(T_1))(X - \sigma(T_2)) \cdots (X - \sigma(T_n)) \\ &= (X - T_{\sigma(1)})(X - T_{\sigma(2)}) \cdots (X - T_{\sigma(n)}) \\ &= (X - T_1)(X - T_2) \cdots (X - T_n) \\ &= u(X) \\ &= +s_n X^n - s_{n-1} X^{n-1} + \dots \pm s_1 X \mp s_0 \\ &\stackrel{2}{=} (+s_n X^n - s_{n-1} X^{n-1} + \dots \pm s_1 X \mp s_0)^\sigma \\ &= +\sigma(s_n) X^n - \sigma(s_{n-1}) X^{n-1} + \dots \pm \sigma(s_1) X \mp \sigma(s_0). \end{aligned}$$

Koeffizientenvergleich gibt $\sigma(s_i) = s_i$ für $i \in [0, n]$. Ist

Beachte, daß L ein Teilkörper von E ist, da L das Element 1_E enthält, und da Differenz und Quotient zweier Elemente von L wieder in L liegen, wobei bei der Quotientenbildung der Nenner ungleich 0 sei.

Ist $\frac{f(s_0, \dots, s_{n-1})}{g(s_0, \dots, s_{n-1})}$ wie in der Aufgabenstellung ein beliebig gewähltes Element aus L , und ist $\sigma \in \mathcal{S}_n$, so wird

$$\sigma\left(\frac{f(s_0, \dots, s_{n-1})}{g(s_0, \dots, s_{n-1})}\right) = \frac{\sigma(f(s_0, \dots, s_{n-1}))}{\sigma(g(s_0, \dots, s_{n-1}))} = \frac{f(\sigma(s_0), \dots, \sigma(s_{n-1}))}{g(\sigma(s_0), \dots, \sigma(s_{n-1}))} = \frac{f(s_0, \dots, s_{n-1})}{g(s_0, \dots, s_{n-1})}.$$

Also ist $\sigma|_L^L = \text{id}_L$.

Da dies für alle $\sigma \in \mathcal{S}_n$ gilt, ist $L \subseteq \text{Fix}_{\mathcal{S}_n} E$.

Mit der Folgerung zu Satz 7 (Dedekinds Lemma) ist also $[E : L] \geq [E : \text{Fix}_{\mathcal{S}_n} E] \geq |\mathcal{S}_n| = n!$.

(4) Sei $i \in [1, n]$. Betrachte

$$g_i(X) := (X - T_i) \cdots (X - T_n) = \frac{u(X)}{(X - T_1) \cdots (X - T_{i-1})} \in E(X).$$

Ersterer Ausdruck zeigt, daß $g_i(X) \in E[X]$ liegt. Insbesondere geht die Polynomdivision von $u(X)$ durch $(X - T_1) \cdots (X - T_{i-1})$ auf. Nun liegen aber $u(X) \in L[X] \subseteq L(T_1, \dots, T_{i-1})[X]$ und $(X - T_1) \cdots (X - T_{i-1}) \in L(T_1, \dots, T_{i-1})[X]$. Der Polynomdivisionsalgorithmus zeigt nun, daß auch der Quotient $g_i(X)$ in $L(T_1, \dots, T_{i-1})[X]$ liegt.

Es ist also $g_i(X)$ ein normiertes Polynom mit Nullstelle T_i . Insbesondere ist T_i algebraisch über $L(T_1, \dots, T_{i-1})$. Ferner ist $\mu_{T_i, L(T_1, \dots, T_{i-1})}(X)$ ein Teiler von $g_i(X)$; vgl. Satz 2.(2), §2.3.2. Mit loc. cit. ist auch

$$[L(T_1, \dots, T_{i-1}, T_i) : L(T_1, \dots, T_{i-1})] = \deg \mu_{T_i, L(T_1, \dots, T_{i-1})} \leq \deg g_i = n - i + 1.$$

Beachte schließlich, daß $L(T_1, \dots, T_n) = E$. In der Tat ist jedes Polynom in $T_1, \dots, T_n$ mit Koeffizienten in K in der linken Seite enthalten. Ist ein solches Polynom ungleich null, so ist, da $L(T_1, \dots, T_n)$ ein Teilkörper von E ist, also auch sein Inverses in $L(T_1, \dots, T_n)$. Damit ist auch jedes beliebige Element von E , das sich ja als Bruch zweier solcher Polynome mit Nenner ungleich null schreiben läßt, in $L(T_1, \dots, T_n)$.

In der Produktzerlegung

$$[E : L] = [L(T_1) : L] \cdots [L(T_1, T_2) : L(T_1)] \cdots [L(T_1, \dots, T_n) : L(T_1, \dots, T_{n-1})]$$

ist der i -te Faktor $\leq n - i + 1$, wohingegen das Produkt $\geq n! = \prod_{i \in [1, n]} (n - i + 1)$ ist. Mithin ist der i -te Faktor

$$[L(T_1, \dots, T_{i-1}, T_i) : L(T_1, \dots, T_{i-1})] = n - i + 1$$

für $i \in [1, n]$. Somit ist $\mu_{T_i, L(T_1, \dots, T_{i-1})}(X) = g_i(X) = (X - T_i) \cdots (X - T_n)$ für $i \in [1, n]$; vgl. Satz 2.(2).

Eine L -lineare Basis von E ist also etwa gegeben durch

$$(T_1^{\alpha_1} \cdots T_n^{\alpha_n} : \alpha_i \in [0, n - i] \text{ für } i \in [1, n]).$$

In der Tat folgt aus Gradgründen auch $L(T_1, \dots, T_{n-1}) = E$. Dies sieht man auch direkt ein, denn $T_n = s_{n-1} - (T_1 + \cdots + T_{n-1})$.