Lösungsvorschlag zu Blatt 15

Aufgabe 1:
Es seien K ein Körper der Charakteristik $p > 0$ und L/K eine Galois-Erweiterung mit zyklischer Galois-Gruppe $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ der Ordnung p.

a) Zeige, dass die Abbildung $s : L \to L$, $\alpha \mapsto \alpha - \sigma(\alpha)$ nilpotent ist, d.h. es gibt ein $n \in \mathbb{N}$ mit $s^n = 0$.

b) Gib ein Element $\beta \in L$ an mit $\beta \notin \mathrm{Kern}(s)$ und $\beta \in \mathrm{Kern}(s^2)$.

c) Zeige, dass für ein β wie in Aufgabenteil b) gilt: $k := \sigma(\beta) - \beta$ liegt in K und $\gamma := k^{-1}\beta$ ist Nullstelle eines Polynoms $f := X^p - X - d \in K[X]$.

d) Ist f das Minimalpolynom von γ?

Lösung:

a) Wir zeigen zunächst, dass für alle $n \in \mathbb{N}$ und alle $\alpha \in L$ gilt:

$$s^n(\alpha) = \sum_{i=0}^{n} \binom{n}{i} (-1)^i \sigma^i(\alpha)$$

- $n = 0$: $s^0(\alpha) = \alpha = \sum_{i=0}^{0} \binom{0}{i}(-1)^i\sigma^i(\alpha)$
  $n = 1$: $s^1(\alpha) = \alpha - \sigma(\alpha) = \sum_{i=0}^{1} \binom{1}{i}(-1)^i\sigma^i(\alpha)$
- $n \to n+1$:
  $s^{n+1}(\alpha) = s(s^n(\alpha)) \overset{\text{(IV)}}{=} s(\sum_{i=0}^{n} \binom{n}{i}(-1)^i\sigma^i(\alpha)) = \sum_{i=0}^{n} \binom{n}{i}(-1)^i\sigma^i(\alpha)$
  $-\sigma(\sum_{i=0}^{n} \binom{n}{i}(-1)^i\sigma^i(\alpha)) = \sum_{i=0}^{n} \binom{n}{i}(-1)^i\sigma^i(\alpha) + \sum_{j=1}^{n+1} \binom{n}{j-1}(-1)^j\sigma^j(\alpha)$
  $= \alpha + \sum_{i=1}^{n} (\binom{n}{i} + \binom{n}{i-1})(-1)^i\sigma^i(\alpha) + (-1)^{n+1}\sigma^{n+1}(\alpha)$
  $= \alpha + \sum_{i=1}^{n} \binom{n+1}{i}(-1)^i\sigma^i(\alpha) + (-1)^{n+1}\sigma^{n+1}(\alpha) = \sum_{i=0}^{n+1} \binom{n+1}{i}(-1)^i\sigma^i(\alpha)$

  Insbesondere erhalten wir für alle $\alpha \in L$:
  $s^p(\alpha) = \sum_{i=0}^{p} \binom{p}{i}(-1)^i\sigma^i(\alpha) = \alpha + \sum_{i=1}^{p-1} 0 \cdot (-1)^i\sigma^i(\alpha) + (-1)^p\sigma^p(\alpha) = \alpha + (-1)^p\alpha$
  $p = 2 \Rightarrow \forall\, \alpha \in L :\ s^2(\alpha) = \alpha + \alpha = 2\alpha = 0$
  $p \neq 2 \Rightarrow p$ ungerade $\Rightarrow \forall\, \alpha \in L :\ s^p(\alpha) = \alpha - \alpha = 0$
  $\Rightarrow$ Es gilt stets $s^p = 0$.

b) Wähle $\tilde{\beta} \in L \setminus K$ beliebig. Nach dem Hauptsatz der Galoistheorie gibt es ein $\tilde{\sigma} \in \mathrm{Gal}(L/K)$ mit $\tilde{\sigma}(\tilde{\beta}) \neq \tilde{\beta}$. Da σ ein Erzeuger von $\mathrm{Gal}(L/K)$ ist, gilt auch $\sigma(\tilde{\beta}) \neq \tilde{\beta}$, also $s(\tilde{\beta}) \neq 0$.
Wegen $s(\tilde{\beta}) \neq 0$ und $s^p(\tilde{\beta}) = 0$ gibt es ein maximales $i \in \{1, \ldots, p-1\}$ mit $s^i(\tilde{\beta}) \neq 0$.
Setze $\beta := s^{i-1}(\tilde{\beta})$. Es gilt:
$s(\beta) = s^i(\tilde{\beta}) \neq 0 \Rightarrow \beta \notin \mathrm{Kern}(s)$
$s^2(\beta) = s^{i+1}(\tilde{\beta}) = 0 \Rightarrow \beta \in \mathrm{Kern}(s^2)$

c)
- $\beta \in \mathrm{Kern}(s^2) \backslash \mathrm{Kern}(s) \Rightarrow \beta - 2\cdot\sigma(\beta) + \sigma^2(\beta) = 0 \Rightarrow \sigma(\sigma(\beta) - \beta) = \sigma(\beta) - \beta =: k$
  $\Rightarrow \forall\, \tilde{\sigma} \in \mathrm{Gal}(L/K) :\ \tilde{\sigma}(k) = k \Rightarrow k \in K$
- $\gamma := \frac{\beta}{\sigma(\beta)-\beta}$
  $\Rightarrow \sigma(\gamma) = \frac{\sigma(\beta)}{\sigma^2(\beta)-\sigma(\beta)} = \frac{\sigma(\beta)}{(2\cdot\sigma(\beta)-\beta)-\sigma(\beta)} = \frac{\sigma(\beta)-\beta+\beta}{\sigma(\beta)-\beta} = \frac{\beta}{\sigma(\beta)-\beta} + 1 = \gamma + 1$
  $\Rightarrow$ Für $d := \gamma^p - \gamma$ gilt:
  $\sigma(d) = \sigma(\gamma)^p - \sigma(\gamma) = (\gamma+1)^p - \gamma - 1 = \gamma^p + 1 - \gamma - 1 = \gamma^p - \gamma = d$
  $\Rightarrow \forall\, \tilde{\sigma} \in \mathrm{Gal}(L/K) :\ \tilde{\sigma}(d) = d$
  $\Rightarrow d \in K$
  Außerdem ist $\gamma^p - \gamma = d$, also $f(\gamma) = 0$.

d) Es ist $\beta \notin K$ (sonst wäre $\sigma(\beta) = \beta$ und somit $s(\beta) = 0$), also $\gamma \notin K$. Nach Blatt 13, Aufgabe 3b), liegt keine Nullstelle von f in K. Nach Blatt 13, Aufgabe 3c), ist f irreduzibel. f ist außerdem normiert, also das Minimalpolynom von γ.

Aufgabe 2:
Zeige, dass es zu jeder endlichen Gruppe G eine galoissche Körpererweiterung L/K gibt mit $\mathrm{Gal}(L/K) \cong G$.

Lösung:
Die Abbildung $\tau : G \to S_G$, $g \mapsto (x \mapsto gx)$ ist ein injektiver Gruppenhomomorphismus. Für $n := |G|$ gilt außerdem $S_G \cong S_n$, also kann o.E. $G \leq S_n$ angenommen werden.

Sei nun k ein beliebiger Körper. Setze $L := k(X_1, \ldots, X_n)$. G operiert effektiv auf L durch $\pi \cdot X_i := X_{\pi(i)}$. Es gilt also $G \leq \mathrm{Aut}(L)$. Setze $K := L^G$ wie in Blatt 14, Aufgabe 3. Dann ist (wie in Blatt 14, Aufgabe 3 gezeigt) L/K endlich und galoissch. Außerdem gilt $[L : K] = n = |G|$ und $\mathrm{Gal}(L/K) = G$.

Aufgabe 3:
Berechne $\mathrm{Gal}(f)$ für $f = X^4 - 2 \in \mathbb{Q}[X]$. Ist die Gleichung $f(X) = 0$ durch Radikale auflösbar?

Lösung:
Setze $a := \sqrt[4]{2}$. f hat die Nullstellen $a, ia, -a, -ia$. Es ist $\mathrm{Gal}(f) = \mathrm{Gal}(Z(f)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(a,i)/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(a,i))$. Jedes $\sigma \in \mathrm{Gal}(f)$ bildet a auf eines der Elemente $\{a, ia, -a, -ia\}$ und i auf eines der Elemente $\{i, -i\}$ ab und ist dadurch schon eindeutig bestimmt.

Für $k = 0, \ldots, 3$ und $\varepsilon = \pm 1$ setze $\sigma_{k,\varepsilon} : \mathbb{Q}(a,i) \to \mathbb{Q}(a,i)$, $a \mapsto i^k a$ und $i \mapsto \varepsilon i$. (Beachte: $\sigma_{k,\varepsilon}$ ist a priori nicht wohldefiniert.) Da es genau $|\mathrm{Gal}(f)| = [\mathbb{Q}(a,i) : \mathbb{Q}] = 8$ verschiedene Automorphismen gibt, sind alle $\sigma_{k,\varepsilon}$ wohldefiniert, und es gilt $\mathrm{Gal}(f) = \{\sigma_{k,\varepsilon} : k \in \{0, \ldots, 3\}, \varepsilon \in \{1, -1\}\}$.

Wir wollen nun noch den Isomorphietyp von $\mathrm{Gal}(f)$ bestimmen. Wegen $\sigma_{1,1} \circ \sigma_{2,-1}(a) = -ia \neq ia = \sigma_{2,-1} \circ \sigma_{1,1}(a)$ ist $\mathrm{Gal}(f)$ nicht kommutativ und somit nach Blatt 2, Aufgabe 4 isomorph zu einer der dort angegebenen Gruppen Q oder D.

Ist $\varepsilon = -1$, so gilt $(\sigma_{k,\varepsilon})^2(a) = a$ und $(\sigma_{k,\varepsilon})^2(i) = i$, also $(\sigma_{k,\varepsilon})^2 = \mathrm{id}$.
$\Rightarrow$ In $\mathrm{Gal}(f)$ gibt es mindestens 4 Elemente der Ordnung 2.
$\Rightarrow \mathrm{Gal}(f) \cong D$

Da f ein Polynom vom Grad ≤ 4 ist, ist die Gleichung $f(X) = 0$ durch Radikale auflösbar.

Aufgabe 4:
Seien L der Zerfällungskörper des irreduziblen Polynoms $f = X^4 - 2aX^2 + c$ über $\mathbb{Q}$ und $M := \mathbb{Q}(\sqrt{a^2 - c})$. Zeige:

a) Es ist genau dann $[L : \mathbb{Q}] = 4$, wenn $\sqrt{c} \in M$ gilt.

b) Ist $\sqrt{c} \in \mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

c) Ist $\sqrt{c} \in M \setminus \mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z}$.

Lösung:
Setze $w := \sqrt{a^2 - c}$. Wäre $w \in \mathbb{Q}$, so wäre $f = (X^2 - a - w) \cdot (X^2 - a + w)$ in $\mathbb{Q}[X]$ und somit f nicht irreduzibel.
$\Rightarrow \mathbb{Q} \subsetneq M = \mathbb{Q}(w)$ und $[M : \mathbb{Q}] = 2$
Das Polynom f hat in $\mathbb{C}$ die vier Nullstellen $y_1 = \sqrt{a + w}$, $y_2 = \sqrt{a - w} = \frac{\sqrt{c}}{y_1}$, $y_3 = -y_1$, $y_4 = -y_2$. Setze $E := \mathbb{Q}(y_1) = \mathbb{Q}(\sqrt{a + w})$ und $L := \mathbb{Q}(y_1, y_2) = Z(f)$. Es ist $\mathbb{Q} \subseteq M \subseteq E \subseteq L$. Außerdem haben wir $[E : \mathbb{Q}] = 4$, $[E : M] = 2$ und $[L : E] \leq 2$.
$\Rightarrow \mathbb{Q} \overset{2}{\subsetneq} M \overset{2}{\subsetneq} E \subseteq L$

a) Es gilt $[L : \mathbb{Q}] = 4 \Leftrightarrow L = E \Leftrightarrow y_2 \in E$.

"$\Rightarrow$": $[L : \mathbb{Q}] = 4 \Rightarrow y_2 \in E \Rightarrow \exists\, \alpha_0, \ldots, \alpha_3 \in \mathbb{Q} :\ y_2 = \alpha_0 + \alpha_1 y_1 + \alpha_2 y_1^2 + \alpha_3 y_1^3$
$\Rightarrow 2 \cdot (\alpha_1 + \alpha_3(a+w)) \cdot \sqrt{c} = (a - w) + (a+w)(\alpha_1 + \alpha_3(a+w))^2 - (\alpha_0 + \alpha_2(a+w))^2$
$=: \beta \in M$

Annahme: $\alpha_1 + \alpha_3(a + w) = 0$

- $\alpha_3 \neq 0 \Rightarrow w = \frac{-\alpha_1 - \alpha_3 a}{\alpha_3} \in \mathbb{Q}$, ein Widerspruch.
- $\alpha_3 = 0 \Rightarrow \alpha_1 = 0 \Rightarrow y_2 = \alpha_0 + \alpha_2(a + w) = (\alpha_0 + \alpha_2 a) + \alpha_2\sqrt{a^2 - c}$
  Das ist ein Widerspruch, da $(\alpha_0 + \alpha_2 a) + \alpha_2\sqrt{a^2 - c}$ Grad 2 über $\mathbb{Q}$ hat, aber y_2 hat Grad 4.

$\Rightarrow \alpha_1 + \alpha_3(a + w) \neq 0 \Rightarrow \sqrt{c} = \frac{\beta}{2 \cdot (\alpha_1 + \alpha_3(a+w))} \in M$

"$\Leftarrow$": $\sqrt{c} \in M \Rightarrow y_2 = \frac{\sqrt{c}}{y_1} \in E \Rightarrow [L : \mathbb{Q}] = 4$

b) Sei $\sqrt{c} \in \mathbb{Q}$. Sei $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.
$\Rightarrow \sigma(y_2) = \sigma(\frac{\sqrt{c}}{y_1}) = \frac{\sqrt{c}}{\sigma(y_1)}$, $\sigma(y_3) = \sigma(-y_1) = -\sigma(y_1)$ und $\sigma(y_4) = \sigma(-y_2) = -\frac{\sqrt{c}}{\sigma(y_1)}$
$\Rightarrow \sigma$ ist durch die Angabe von $\sigma(y_1)$ eindeutig bestimmt.
$\Rightarrow \mathrm{Gal}(f) = \{\sigma_1, \ldots, \sigma_4\}$, wobei σ_i gegeben ist durch $\sigma_i(y_1) = y_i$.
Es gilt:

$\sigma_1(y_1) = y_1$
$\sigma_2(y_2) = \frac{\sqrt{c}}{\sigma_2(y_1)} = \frac{\sqrt{c}}{y_2} = y_1$
$\sigma_3(y_3) = -\sigma_3(y_1) = -y_3 = y_1$
$\sigma_4(y_4) = -\frac{\sqrt{c}}{\sigma_4(y_1)} = -\frac{\sqrt{c}}{y_4} = y_1$
$\Rightarrow \forall\, i = 1, \ldots, 4 :\ \sigma_i^2(y_1) = \sigma_i(y_i) = y_1 \Rightarrow \sigma_i^2 = \mathrm{id}$
$\Rightarrow \mathrm{Gal}(f) \cong (\mathbb{Z}/2\mathbb{Z})^2$

c) Sei $\sqrt{c} \in M \setminus \mathbb{Q}$. Nach dem Hauptsatz der Galoistheorie gibt es ein $\sigma \in \mathrm{Gal}(f)$ mit $\sigma(\sqrt{c}) \neq \sqrt{c}$, also $\sigma(\sqrt{c}) = -\sqrt{c}$.
Beachte: In beiden Gruppen $G = \mathbb{Z}/4\mathbb{Z}$ und $G = (\mathbb{Z}/2\mathbb{Z})^2$ gilt die folgende Aussage:
$\forall\, x \in G\ \exists\, y, z \in G \setminus \{x\} :\ y + z = x$
Damit gibt es noch einen zweiten Automorphismus σ', der $\sqrt{c}$ auf $-\sqrt{c}$ abbildet, denn sonst ließe sich σ schreiben als $\sigma = \sigma_1 \circ \sigma_2$ mit $\sigma_1(\sqrt{c}) = \sqrt{c} = \sigma_2(\sqrt{c})$, also $\sigma(\sqrt{c}) = \sqrt{c}$.
Wegen $\sigma(\sqrt{c}) = \sigma'(\sqrt{c}) \neq \sqrt{c}$ gilt selbstverständlich $\sigma, \sigma' \neq \mathrm{id}$.
Annahme: $\mathrm{Gal}(f) \cong (\mathbb{Z}/2\mathbb{Z})^2$
Setze $\sigma'' := \sigma \circ \sigma'$. Es gilt dann $\mathrm{Gal}(f) = \{\mathrm{id}, \sigma, \sigma', \sigma''\}$.

1.Fall: $\sigma(y_1) = \pm y_1$ und $\sigma'(y_1) = \pm y_1$
$\Rightarrow \sigma''(y_1) = \sigma \circ \sigma'(y_1) = \pm y_1$
$\Rightarrow \forall\, \tau \in \mathrm{Gal}(f) :\ a + \tau(w) = \tau(a + w) = \tau(y_1^2) = (\pm y_1)^2 = y_1^2 = a + w$
$\Rightarrow \tau(w) = w$
Nach dem Hauptsatz der Galoistheorie gilt somit $w \in \mathbb{Q}$, ein Widerspruch.

2.Fall: $\sigma(y_1) = \pm y_2$ oder $\sigma'(y_1) = \pm y_2$, o.E. $\sigma(y_1) = \pm y_2$
$\Rightarrow \sigma^2(y_1) = \sigma(\pm y_2) = \pm\sigma(y_2) = \pm\sigma(\frac{\sqrt{c}}{y_1}) = \pm\frac{-\sqrt{c}}{\pm y_2} = -\frac{\sqrt{c}}{y_2} = -y_1 \neq y_1$
$\Rightarrow \sigma^2 \neq \mathrm{id}$, ein Widerspruch zu $\mathrm{Gal}(f) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

$\Rightarrow$ Die Annahme ist falsch, und es gilt $\mathrm{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z}$.

Aufgabe 5:
$\mathbb{R}$ hat keine echte Körpererweiterung von ungeradem Grad.
$\mathbb{C}$ hat keine Körpererweiterung vom Grad 2.
$\mathbb{C}$ ist algebraisch abgeschlossen.

Lösung:

a) Sei L eine Körpererweiterung von $\mathbb{R}$ von ungeradem Grad $d := [L : \mathbb{R}]$. Seien $\alpha \in L$ ein primitives Element, also $L = \mathbb{R}(\alpha)$, und $m \in \mathbb{R}[X]$ das Minimalpolynom von α.
$\Rightarrow \mathrm{grad}(m) = [\mathbb{R}(\alpha) : \mathbb{R}] = [L : \mathbb{R}] = d$
Als Polynom ist m auch eine stetige Funktion $m : \mathbb{R} \to \mathbb{R}$. Da m ungeraden Grad hat, hat m eine Nullstelle in $\mathbb{R}$. (Das sagt der Zwischenwertsatz aus der Analysis.)
Da m außerdem irreduzibel ist, gilt $\mathrm{grad}(m) = 1$.
$\Rightarrow [L : \mathbb{R}] = 1 \Rightarrow L = \mathbb{R}$

b) Sei L eine Körpererweiterung von $\mathbb{C}$ vom Grad 2. Seien $\alpha \in L \setminus \mathbb{C}$ ein primitives Element, also $L = \mathbb{C}(\alpha)$, und $m \in \mathbb{C}[X]$ das Minimalpolynom von α. α hat Grad 2, d.h. es gibt $a, b \in \mathbb{C}$ mit $m = X^2 + aX + b$.
$\Rightarrow m$ hat die Nullstellen $\frac{-a+\sqrt{a^2-4b}}{2}$ und $\frac{-a-\sqrt{a^2-4b}}{2}$.
$\Rightarrow m$ ist nicht irreduzibel, ein Widerspruch.
$\Rightarrow$ Es kann kein solches L geben.

c) Sei $\mathbb{R} \subsetneq \mathbb{C} \subseteq L \subseteq \overline{\mathbb{C}}$. Dabei ist L ein Erweiterungskörper von $\mathbb{C}$ und $\overline{\mathbb{C}}$ ein geeigneter algebraischer Abschluss von $\mathbb{C}$, der L enthält. Ohne Einschränkung sei L normal (gehe sonst zur normalen Hülle von L über).
Sei $G := \mathrm{Gal}(L/\mathbb{R})$. $|G| = [L : \mathbb{R}]$ ist endlich, schreibe also $|G| = 2^r \cdot m$ mit $r, m \in \mathbb{N}$, $r \geq 1$ und m ungerade. Nach den Sylowsätzen gibt es eine Untergruppe

$U \leq G$ mit $|U| = 2^r$. Nach dem Hauptsatz der Galoistheorie entspricht diesem U ein Zwischenkörper $\mathbb{R} \subseteq E \subseteq L$ mit $\mathrm{Gal}(L/E) = U$.
$2^r \cdot m = |G| = [L : \mathbb{R}] = [L : E] \cdot [E : \mathbb{R}] = |U| \cdot [E : \mathbb{R}] = 2^r \cdot [E : \mathbb{R}]$
$\Rightarrow [E : \mathbb{R}] = m$ ist ungerade $\overset{a)}{\Rightarrow} m = 1$ und $E = \mathbb{R} \Rightarrow U = \mathrm{Gal}(L/\mathbb{R}) = G$
$\Rightarrow 2^r = [L : \mathbb{R}] = [L : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2 \cdot [L : \mathbb{C}] \Rightarrow [L : \mathbb{C}] = 2^{r-1}$

Annahme: $r \geq 2$
$\Rightarrow |\mathrm{Gal}(L/\mathbb{C})| = 2^{r-1} \geq 2$
$\Rightarrow$ Es gibt[1] eine Untergruppe U' von $\mathrm{Gal}(L/\mathbb{C})$ der Ordnung 2^{r-2}.
Zu U' gehört ein Zwischenkörper $\mathbb{C} \subseteq E' \subseteq L$ mit $\mathrm{Gal}(L/E') = U'$
$\Rightarrow 2^{r-1} = [L : \mathbb{C}] = [L : E'] \cdot [E' : \mathbb{C}] = |U'| \cdot [E' : \mathbb{C}] = 2^{r-2} \cdot [E' : \mathbb{C}]$
$\Rightarrow [E' : \mathbb{C}] = 2$ im Widerspruch zu b).
$\Rightarrow r = 1$ und somit $L = \mathbb{C}$.

Aufgabe 6:
Sei L/K eine endliche Körpererweiterung. Für ein primitives[2] Element $\alpha \in L$ sei $\Phi : L \to L$ gegeben durch $\Phi(x) := \alpha x$.

a) Φ ist K-linear.

b) Das Minimalpolynom von Φ ist das Minimalpolynom von α.

c) Berechne $\mathrm{Spur}(\Phi)$, $\det(\Phi)$, eine Basis von L sowie eine Abbildungsmatrix von Φ.

d) Wie verhalten sich charakteristisches Polynom und Minimalpolynom von Φ zueinander?

Lösung:

a) $\forall\, \lambda, \mu \in K\ \forall\, x, y \in L$:
$\Phi(\lambda x + \mu y) = \alpha \cdot (\lambda x + \mu y) = \lambda \alpha x + \mu \alpha y = \lambda \cdot \Phi(x) + \mu \cdot \Phi(y)$

c) Sei $d := [L : K]$. Dann ist eine Basis von L gegeben durch $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.
Sei $m = X^d + c_{d-1}X^{d-1} + \ldots + c_1 X + c_0 \in K[X]$ das Minimalpolynom von α.
$\Phi(1) = \alpha, \Phi(\alpha) = \alpha^2, \ldots, \Phi(\alpha^{d-2}) = \alpha^{d-1}$
$\Phi(\alpha^{d-1}) = \alpha^d = -c_{d-1}\alpha^{d-1} - \ldots - c_1\alpha - c_0$
$\Rightarrow$ Die Abbildungsmatrix von Φ bzgl. B ist $A = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -c_0 \\ 1 & \ddots & & \vdots & -c_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -c_{d-2} \\ 0 & \ldots & 0 & 1 & -c_{d-1} \end{pmatrix}$.
$\Rightarrow \mathrm{Spur}(\Phi) = \mathrm{Spur}(A) = -c_{d-1}$

[1] Das wurde in der Vorlesung/Übung nicht gezeigt, ist aber nicht schwer. (Benutze dazu, dass das Zentrum einer p-Gruppe stets nichttrivial ist.)
[2] Auf dem Übungsblatt stand diese Voraussetzung noch nicht drauf.

d) Das charakteristische Polynom p_Φ berechnet sich folgendermaßen:

$$p_\Phi(X) = \det(A - X\mathcal{E}) = \begin{vmatrix} -X & & & 0 & -c_0 \\ 1 & \ddots & & & -c_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & -X & -c_{d-2} \\ 0 & \dots & 0 & 1 & -c_{d-1} - X \end{vmatrix}$$

$$= \sum_{i=0}^{d-2} (-c_i)(-1)^{d+i+1}(-X)^i + (-c_{d-1} - X)(-X)^{d-1}$$

$$= \sum_{i=0}^{d-2} c_i(-1)^{1+d+i+1+i} X^i + c_{d-1}(-1)^d X^{d-1} + (-1)^d X^d$$

$$= \sum_{i=0}^{d-2} c_i(-1)^d X^i + c_{d-1}(-1)^d X^{d-1} + (-1)^d X^d$$

$$= (-1)^d \cdot (\sum_{i=0}^{d-1} c_i X^i + X^d) = (-1)^d \cdot m$$

c) $\det(\Phi) = \det(A) = p_\Phi(0) = (-1)^d \cdot m(0) = (-1)^d \cdot c_0$

b) Sei m_Φ das Minimalpolynom von Φ. Nach dem Satz von Cayley-Hamilton gilt $p_\Phi(\Phi) = 0$, also $m(\Phi) = 0$ und somit $m_\Phi \mid m$. Da m und m_Φ beide normiert, m irreduzibel und $\text{grad}(m_\Phi) \geq 1$ ist, gilt daher $m = m_\Phi$.