G. Nebe, M. Künzer 20.01.2005

Algebra I, WS 04/05

Lösung Probeklausur II

Aufgabe 1.

(1) Beachte, daß $\mu_{\zeta_3,\mathbf{Q}}(X) = X^2 + X + 1$, und daß insbesondere $\zeta_3^2 = -\zeta_3 - 1$.

Zunächst ist $\alpha^2/3 = -\zeta_3$ eine Einheit in $\mathbf{Z}[\zeta_3]$, und also $(\alpha)^2 = (\alpha^2) = (3)$.

Ferner wird

$$\begin{array}{rcl} R/(\alpha) & = & R/(3,\alpha) \\ & = & \mathbf{Z}[\zeta_3]/(3,\zeta_3 - 1) \\ & \simeq & \mathbf{Z}[X]/(3, X^2+X+1, X-1) \\ & \simeq & \mathbf{F}_3[X]/(X^2+X+1, X-1) \\ & = & \mathbf{F}_3[X]/(X-1) \\ & \simeq & \mathbf{F}_3\ , \end{array}$$

und somit ist α prim in R.

Zwecks späterer Probe bemerken wir noch, daß $|R/(\alpha^k)| = 3^k$ ist, wie mit Induktion aus

$$\begin{array}{rcl} R/(\alpha) & \xrightarrow{\sim} & \mathrm{Kern}(\varphi) \\ x + (\alpha) & \longmapsto & \alpha^{k-1}x + (\alpha^k) \end{array} \qquad \hookrightarrow \qquad \begin{array}{rcl} R/(\alpha^k) & \xrightarrow{\varphi} & R/(\alpha^{k-1}) \\ x + (\alpha^k) & \longmapsto & x + (\alpha^{k-1}) \end{array}$$

folgt.

(2) Wir formen zunächst z.B. wie folgt um.

$$\left(\begin{array}{ccccc} \alpha & -\alpha & 3 & 0 & 0 \\ \alpha & -\alpha & 0 & 3 & 0 \\ \alpha & \alpha & 0 & 0 & 3 \\ \hline 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccccc} \alpha & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ \hline 1 & -1 & 0 & 2\alpha+6 & \alpha+3 \\ 0 & -1 & 0 & \alpha+3 & \alpha+3 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & \alpha & 0 & 3 & 2 \end{array}\right)$$

Dies liefert zunächst

$$\mathrm{Cokern}(u) \ \simeq\ R/(\alpha) \oplus R/(\alpha) \oplus R/(3)\ .$$

Beachte, daß $\left(\begin{smallmatrix} 2\alpha+6 & \alpha+3 \\ \alpha+3 & \alpha+3 \end{smallmatrix}\right) = (\alpha+3)\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, und daß α und $\alpha + 3$ assoziiert sind.

Es wird $\left(\begin{smallmatrix} 2\alpha+6 & \alpha+3 \\ \alpha+3 & \alpha+3 \end{smallmatrix}\right)\left(\begin{smallmatrix} -\alpha & 3\alpha \\ \alpha & -6\alpha \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 9 \end{smallmatrix}\right)$.

Die Elementarteilerform von $\left(\begin{smallmatrix} 2\alpha+6 & \alpha+3 \\ \alpha+3 & \alpha+3 \end{smallmatrix}\right)$ ist $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ und somit ist

$$\mathrm{Bild}(u) \ \simeq\ R/(\alpha) \oplus R/(\alpha)\ .$$

Die Elementarteilerform von $\left(\begin{smallmatrix} -\alpha & 3\alpha \\ \alpha & -6\alpha \end{smallmatrix}\right)$ ist $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 3\alpha \end{smallmatrix}\right)$, und somit ist

$$\mathrm{Kern}(u) \ \simeq\ R/(\alpha) \oplus R/(3\alpha)\ .$$

Probe: $|\,\mathrm{Kern}(u)| = 3^4$, $|\mathrm{Bild}(u)| = 3^2$ und $|X| = 3^6$ ist in Ordnung. $|\mathrm{Bild}(u)| = 3^2$, $|\,\mathrm{Cokern}(u)| = 3^4$ und $|Y| = 3^6$ ist auch in Ordnung.

Aufgabe 2.

(1) Mittels Eisensteinkriterium bezüglich des Rings $\mathbf{F}_3[T]$ und des Primelements T sehen wir, daß $f(X) = X^4 - T$ irreduzibel ist in $K[X] = \mathbf{F}_3(T)[X]$.

Da $\mathrm{ggT}(f(X), f'(X)) = \mathrm{ggT}(X^4 - T, X^3) = 1$, ist $f(X)$ separabel.

(2) Zunächst bestimmen wir den Zerfällungskörper von $f(X)$. Sei $K_0 = K$, und sei $K_1 = K_0(\alpha_1)$ mit $\alpha_1^4 = T$. Mit α_1 ist auch $-\alpha_1$ Nullstelle von $f(X)$. So wird

$$X^4 - T \;=\; (X - \alpha_1)(X + \alpha_1)(X^2 + \alpha_1^2) \;\in\; K_1[X]\,.$$

Wir behaupten, es ist $X^2 + \alpha_1^2$ irreduzibel in $K_1[X]$. Dazu genügt es zu zeigen, daß -1 kein Quadrat in K_1 ist. Nun ist $K_1 = \mathbf{F}_3(T, \alpha_1) = \mathbf{F}_3(\alpha_1) \simeq \mathbf{F}_3(S)$ mit der freien Variablen S, vermöge $\alpha_1 \longleftarrow\!\shortmid S$. Wir haben zu zeigen, daß -1 in $\mathbf{F}_3(S)$ kein Quadrat ist. Nehmen wir an, dies sei doch der Fall, und schreiben wir

$$-1 \;=\; \left(\frac{u(S)}{v(S)}\right)^2$$

mit $u(S),\, v(S) \;\in\; \mathbf{F}_3[S]$ und $\mathrm{ggT}(u(S), v(S)) \;=\; 1$. Dann ist $u(S)^2 \;=\; -v(S)^2$, woraus wegen der Teilerfremdheit $u(S),\, v(S) \in \mathbf{F}_3$ folgt, und damit, daß -1 in $\mathbf{F}_3$ ein Quadrat ist. Das ist aber nicht der Fall.

Sei $E = K_2 = K_1(\alpha_2) = K(\alpha_1, \alpha_2)$ mit $\alpha_2^2 = -\alpha_1^2$. Es wird

$$f(X) \;=\; X^4 - T \;=\; (X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2)\,.$$

Somit ist E Zerfällungskörper von $f(X)$. Halten wir fest, daß E über K die Basis $(1, \alpha_1, \alpha_1^2, \alpha_1^3, \alpha_2, \alpha_2\alpha_1, \alpha_2\alpha_1^2, \alpha_2\alpha_1^3)$ hat.

Ein Automorphismus von E über K ist durch das Tupel (β_1, β_2) der Bilder von (α_1, α_2) gegeben, vorausgesetzt, es ist β_1 eine Nullstelle von $f(X)$ und β_2 eine Nullstelle von $f(X)/((X - \beta_1)(X + \beta_1))$. Bleiben die Möglichkeiten

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

Schreibe $\alpha_3 := -\alpha_1$ und $\alpha_4 := -\alpha_2$. Da ein Automorphismus das Negative eines Elements auf das Negative des Bildes schickt, können wir etwa die beiden Automorphismen

$$\begin{array}{ccc} E & \xrightarrow{\sim} & E \\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \xmapsto{\sigma_1} & (\alpha_3, \alpha_2, \alpha_1, \alpha_4) \\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \xmapsto{\sigma_2} & (\alpha_2, \alpha_3, \alpha_4, \alpha_1) \end{array}$$

herausgreifen, 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

$$\begin{array}{rcl} \mathrm{Gal}(E|K) & \xrightarrow{\sim} & \mathcal{S}_4 \\ \sigma_1 & \longmapsto & (1,3) \\ \sigma_2 & \longmapsto & (1,2,3,4)\,. \end{array}$$

Das Bild enthält 8 Elemente, womit insbesondere $\mathrm{Gal}(E|K) = \langle \sigma_1, \sigma_2 \rangle$ folgt.

Wir verwenden diese Einbettung als Identifikation.

(3) Die echten Zwischenkörper ergeben sich als Fixkörper der Untergruppen

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

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

Es wird z.B.

$$\begin{array}{rcl} L_1 &=& K(\alpha_2) \\ L_2 &=& K(\alpha_1) \\ L_3 &=& K(\alpha_1\alpha_2, \alpha_1 + \alpha_2) \\ L_4 &=& K(\alpha_1^2, \alpha_1\alpha_2) \\ L_5 &=& K(\alpha_1\alpha_2, \alpha_1 - \alpha_2) \\ L_6 &=& K(\alpha_1^3\alpha_2) \\ L_7 &=& K(\alpha_1\alpha_2) \\ L_8 &=& K(\alpha_1^2)\ . \end{array}$$

(4) Es sind nur L_4, L_6, L_7 und L_8 galoisch über K, da nur U_4, U_6, U_7 und U_8 normal in $\mathrm{Gal}(E|K)$ sind.

(5) Wir suchen ein Element $a \in E$, welches in keinem echten Zwischenkörper enthalten ist, d.h. welches unter keinem Galoisautomorphismus ungleich der Identität festgehalten wird. Dies ist z.B. für das Element $\alpha_1 + T\alpha_2$ der Fall, da $\alpha_1 + T\alpha_2 = \pm\alpha_1 \pm T\alpha_2$ nur mit zwei positiven Vorzeichen erfüllt ist, und $\alpha_1 + T\alpha_2 = \pm\alpha_2 \pm T\alpha_1$ für keine Wahl der Vorzeichen erfüllt ist.

Alternativ, das Minimalpolynom von a über K ist

$$\mu_{\alpha_1+T\alpha_2,K}(X) \;=\; X^8 + (T^5 + T)X^4 + (T^{10} + T^8 + T^4 + T^2)\ ,$$

und somit von Grad 8.

Aufgabe 3. Zur Verfügung stehen $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$ und $s_3 = X_1X_2X_3$.

Nebenrechnung. Es ist

$$\begin{array}{rcl} s_1^4 &=& (X_1^4 + \cdots) + 4(X_1^3X_2 + \cdots) + 6(X_1^2X_2^2 + \cdots) + 12(X_1^2X_2X_3 + \cdots) \\ s_1^2s_2 &=& ((X_1^2 + \cdots) + 2(X_1X_2 + \cdots))(X_1X_2 + \cdots) \\ &=& ((X_1^3X_2 + \cdots) + (X_1^2X_2X_3 + \cdots)) + (2(X_1^2X_2^2 + \cdots) + 4(X_1^2X_2X_3 + \cdots)) \\ &=& (X_1^3X_2 + \cdots) + 5(X_1^2X_2X_3 + \cdots) + 2(X_1^2X_2^2 + \cdots) \\ s_2^2 &=& (X_1^2X_2^2 + \cdots) + 2(X_1^2X_2X_3 + \cdots)\ . \end{array}$$

Es wird

$$\begin{array}{rcl} X_1^4 + X_2^4 + X_3^4 &=& s_1^4 - 4(X_1^3X_2 + \cdots) - 6(X_1^2X_2^2 + \cdots) - 12(X_1^2X_2X_3 + \cdots) \\ &=& s_1^4 - 4s_1^2s_2 + 2(X_1^2X_2^2 + \cdots) + 8(X_1^2X_2X_3 + \cdots) \\ &=& s_1^4 - 4s_1^2s_2 + 2s_2^2 + 4(X_1^2X_2X_3 + \cdots) \\ &=& s_1^4 - 4s_1^2s_2 + 2s_2^2 + 4s_1s_3\ . \end{array}$$

Aufgabe 4.

Wir bestimmen dieses Polynom als Minimalpolynom eines Erzeugers von $\mathbf{F}_{2^6}$ über $\mathbf{F}_2$.

Zunächst sei $\mathbf{F}_8 = \mathbf{F}_2(\alpha_1)$ mittels $X^3 + X + 1 \in \mathbf{F}_2[X]$ konstruiert, i.e. es sei $\alpha_1^3 = \alpha_1 + 1$. Dieses Polynom ist mangels Nullstelle irreduzibel.

Dann sei $\mathbf{F}_{64} = \mathbf{F}_8(\alpha_2)$ mittels $X^2 + X + \alpha_1 + 1$ konstruiert, i.e. es sei $\alpha_2^2 = \alpha_2 + \alpha_1 + 1$. Probieren aller 8 Elemente von $\mathbf{F}_8$ zeigt, daß dieses Polynom mangels Nullstelle in $\mathbf{F}_8$ irreduzibel ist.

Es ist $\mu_{\alpha_2,\mathbf{F}_8}(X)$ ein echter Teiler von $\mu_{\alpha_2,\mathbf{F}_2}(X)$. Also ist $\mathbf{F}_2(\alpha_2)$ als Teilkörper von $\mathbf{F}_{64}$ von Grad 3 oder von Grad 6 über $\mathbf{F}_2$. Wäre $\mu_{\alpha_2,\mathbf{F}_2}(X)$ von Grad 3, so gäbe es ein $\xi \in \mathbf{F}_8$ mit $(X - \xi)\mu_{\alpha_2,\mathbf{F}_8}(X) = \mu_{\alpha_2,\mathbf{F}_2}(X)$. Dies führt zu $\xi(\alpha_1 + 1) = 1$, was wiederum dazu führt, daß der Koeffizient $1 + \xi$ bei X^2 von $(X - \xi)\mu_{\alpha_2,\mathbf{F}_8}(X)$ nicht in $\mathbf{F}_2$ liegen kann.

Somit ist $[\mathbf{F}_2(\alpha_2) : \mathbf{F}_2] = 6$, und folglich $\mu_{\alpha_2,\mathbf{F}_2}(X)$ ein irreduzibles Polynom von Grad 6.

Altenativ kann man auch nachrechnen, daß α_2 in keinem echten Teilkörper von $\mathbf{F}_{64}$ liegt, und dazu nachweisen, daß es unter keinem nichtidentischen Galoisautomorphismus fest bleibt. Es ist $\mathrm{Gal}(\mathbf{F}_{64}|\mathbf{F}_2) = \langle \mathrm{F} \rangle$, wobei $\mathrm{F} : \xi \longmapsto \xi^2$. Es wird

$$\begin{array}{lclcl}
\mathrm{F}(\alpha_2) & = & \alpha_2^2 & = & 1 + \alpha_1 + \alpha_2 \\
\mathrm{F}^2(\alpha_2) & = & \alpha_2^4 & = & \alpha_1 + \alpha_1^2 + \alpha_2 \\
\mathrm{F}^3(\alpha_2) & = & \alpha_2^8 & = & 1 + \alpha_2 \\
\mathrm{F}^4(\alpha_2) & = & \alpha_2^{16} & = & \alpha_1 + \alpha_2 \\
\mathrm{F}^5(\alpha_2) & = & \alpha_2^{32} & = & 1 + \alpha_1 + \alpha_1^2 + \alpha_2 \; ,
\end{array}$$

und in dieser Liste taucht α_2 selbst nicht auf.

Berechnen wir das Minimalpolynom $\mu_{\alpha_2,\mathbf{F}_2}(X)$. Bezüglich der Basis $(1, \alpha_1, \alpha_1^2, \alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2)$ erhalten wir die Matrix

$$\begin{pmatrix} 1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&1 \\ 0&0&0&0&1&0&0 \\ 0&1&1&0&1&1&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&0&1&1 \end{pmatrix} ,$$

wobei die Spalten die Potenzen von α_2 durchlaufen. Man kann auch diese Rechnung direkt – als dritte Alternative – dazu anführen, daß in der Tat $\mathbf{F}_2(\alpha_2) = \mathbf{F}_{64}$, wobei hierbei nun die lineare Unabhängigkeit der Spalten zu α_2^0 bis α_2^5 nachzuprüfen ist. (Dazu genügt im vorliegenden Fall die lineare Unabhängigkeit der Spalten zu α_2^0 bis α_2^3 - warum?)

Jedenfalls ergibt dies das irreduzible Polynom

$$\mu_2(X) \;=\; X^6 + X^5 + X^3 + X^2 + 1 \;\in\; \mathbf{F}_2[X]$$

von Grad 6.

Aufgabe 5.

Sei p prim, und sei $m \geq 1$. Wir führen eine Induktion über m.

Falls $m \not\equiv_p 0$, so wird

$$\begin{array}{rcl}
\Phi_m(X^p) & = & \dfrac{X^{pm} - 1}{\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_d(X^p)} \qquad = \quad \dfrac{X^{pm} - 1}{\left(\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_{pd}(X)\right)\left(\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_d(X)\right)} \\[2em]
& = & \dfrac{X^{pm} - 1}{\left(\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_{pd}(X)\right)\left(\prod\limits_{d \mid m} \Phi_d(X)\right)} \cdot \Phi_m(X) \;\; = \;\; \dfrac{X^{pm} - 1}{\left(\prod\limits_{\substack{d \mid pm \\ d \neq pm \\ d \equiv_p 0}} \Phi_d(X)\right)\left(\prod\limits_{\substack{d \mid pm \\ d \neq pm \\ d \not\equiv_p 0}} \Phi_d(X)\right)} \cdot \Phi_m(X) \\[2em]
& = & \Phi_{pm}(X) \cdot \Phi_m(X) \; .
\end{array}$$

Falls $m \equiv_p 0$, so wird

$$\begin{aligned}
\Phi_m(X^p) &= \frac{X^{pm}-1}{\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_d(X^p)} && = \frac{X^{pm}-1}{\Big(\prod\limits_{\substack{d \mid m \\ d \neq m \\ d \equiv_p 0}} \Phi_d(X^p)\Big)\Big(\prod\limits_{\substack{d \mid m \\ d \neq m \\ d \not\equiv_p 0}} \Phi_d(X^p)\Big)} \\
&= \frac{X^{pm}-1}{\Big(\prod\limits_{\substack{d \mid m \\ d \neq m \\ d \equiv_p 0}} \Phi_{pd}(X)\Big)\Big(\prod\limits_{\substack{d \mid m \\ d \neq m \\ d \not\equiv_p 0}} \Phi_{pd}(X)\Phi_d(X)\Big)} && = \frac{X^{pm}-1}{\Big(\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_{pd}(X)\Big)\Big(\prod\limits_{\substack{d \mid m \\ d \neq m \\ d \not\equiv_p 0}} \Phi_d(X)\Big)} \\
&= \frac{X^{pm}-1}{\Big(\prod\limits_{\substack{d \mid m \\ d \neq m}} \Phi_{pd}(X)\Big)\Big(\prod\limits_{\substack{d \mid m \\ d \not\equiv_p 0}} \Phi_d(X)\Big)} && = \frac{X^{pm}-1}{\Big(\prod\limits_{\substack{d \mid pm \\ d \neq pm \\ d \equiv_p 0}} \Phi_d(X)\Big)\Big(\prod\limits_{\substack{d \mid pm \\ d \not\equiv_p 0}} \Phi_d(X)\Big)} \\
&= \Phi_{pm}(X)\,.
\end{aligned}$$

Aufgabe 6. Schreibe $G := \mathrm{Gal}(E|K)$. Bezeichne $A = (\sigma(x_i))_{\sigma\in G,\, i\in[1,n]}$ und $d := \det A \in E$.

1. Lösung. Wir wollen zeigen, daß $\rho(d) = d$ für alle $\rho \in G$. Es ist $\rho \det A = \det((\rho(\sigma(x_i)))_{\sigma\in G,\, i\in[1,n]})$, und diese Matrix geht aus A durch Zeilenvertauschung hervor. Die Permutation dieser Zeilenvertauschung ist gegeben durch das Element

$$\begin{array}{ccc} G & \xrightarrow[\sim]{\hat\rho} & G \\ \sigma & \longmapsto & \rho\circ\sigma \end{array}$$

in $\mathcal{S}_G$. Wir haben zu zeigen, daß das Vorzeichen von $\hat\rho$ gleich $+1$ ist.

Nun ist dieses Element von ungerader Ordnung, da $|G| = [E:K] \equiv_2 1$. Und ein Element ungerader Ordnung in einer symmetrischen Gruppe hat nur Zykel ungerader Länge, und also positives Vorzeichen.

Alternatves Argument hierfür. Sei m die Ordnung von $\hat\rho$. Es ist $m \equiv_2 1$. Also ist $\mathrm{sgn}(\hat\rho) = \mathrm{sgn}(\hat\rho)^m = \mathrm{sgn}(\hat\rho^m) = \mathrm{sgn}(\mathrm{id}) = 1$.

2. Lösung. Es wird $A^{\mathrm t}A = (\sum_{\sigma\in G}\sigma(x_ix_j))_{i,j\,\in[1,n]} = (\mathrm{S}_{E|K}(x_ix_j))_{i,j\,\in[1,n]}$. Folglich ist $d^2 = \det(A^{\mathrm t}A)$ in K. Damit ist $[K(d):K] \in \{1,2\}$. Nun kann aber wegen $[E:K] \equiv_2 1$ der Grad der Zwischenerweiterung nicht 2 sein, da er den Grad $[E:K]$ der gesamten Erweiterung teilt. Also ist $[K(d):K] = 1$ und $d \in K$.

Aufgabe 7.

(1) Die Aussage ist richtig. Sei $R \xrightarrow{\varphi} R_{\mathfrak p}$, $x \longmapsto \frac{x}{1}$.

1. Lösung.

Sei $\mathfrak a \subseteq R_{\mathfrak p}$ ein Ideal, und sei $\mathfrak b := \varphi^{-1}(\mathfrak a)$. Da $\mathfrak b$ ein Ideal in R ist, ist es endlich erzeugt. Sei etwa $\mathfrak b = (b_1,\dots,b_n)$. Wir behaupten, daß $\mathfrak a = (\frac{b_1}{1},\dots,\frac{b_n}{1})$. Per Konstruktion gilt die Inklusion $\supseteq$.

Zeigen wir die Inklusion $\subseteq$. Sei dazu ein Element $\frac{x}{s} \in \mathfrak a$ vorgegeben, mit $x \in R$ und $s \in R \smallsetminus \mathfrak p$. Dann ist $x = \sum_{i\in[1,n]} r_ib_i$ für gewisse $r_i \in R$, da aus $\frac{x}{s} \in \mathfrak a$ zunächst $\frac{x}{1} = \frac{s}{1}\frac{x}{s} \in \mathfrak a$, und somit $x \in \mathfrak b$ folgt. Somit ist

$$\frac{x}{s} = \sum_{i\in[1,n]} \frac{r_i}{s}\frac{b_i}{1} \in (\frac{b_1}{1},\dots,\frac{b_n}{1})\,.$$

2. Lösung.

Sei $\mathfrak{a} \subseteq R_\mathfrak{p}$. Wir behaupten zunächst, daß $R_\mathfrak{p}\varphi(\varphi^{-1}(\mathfrak{a})) = \mathfrak{a}$. Die Inklusion $\subseteq$ gilt per Konstruktion. Zeigen wir die Inklusion $\supseteq$. Sei $\frac{x}{s} \in \mathfrak{a}$. Dann ist auch $\frac{x}{1} \in \mathfrak{a}$, also $x \in \varphi^{-1}(\mathfrak{a})$, also $\frac{x}{1} \in \varphi(\varphi^{-1}(\mathfrak{a}))$, und schließlich $\frac{x}{s} = \frac{1}{s}\frac{x}{1} \in R_\mathfrak{p}\varphi(\varphi^{-1}(\mathfrak{a}))$.

Sind also Ideale $\mathfrak{a} \subsetneq \mathfrak{a}'$ in $R_\mathfrak{p}$ gegeben, so ist auch $\varphi^{-1}(\mathfrak{a}) \subsetneq \varphi^{-1}(\mathfrak{a}')$, da aus Gleichheit wiederum $\mathfrak{a} = R_\mathfrak{p}\varphi(\varphi^{-1}(\mathfrak{a})) = R_\mathfrak{p}\varphi(\varphi^{-1}(\mathfrak{a}')) = \mathfrak{a}'$ folgte. Gäbe es nun eine unendliche echt aufsteigende Kette von Idealen in $R_\mathfrak{p}$, so wäre die Kette der Urbilder unter φ eine echt aufsteigende Kette von Idealen von R. Eine solche gibt es aber wegen R noethersch nicht.

(2) Die Aussage ist falsch. Zwar ist $\alpha+\beta \in \mathbf{Q}(\alpha,\beta)$, und $\mathbf{Q}(\alpha,\beta)$ ist algebraisch über $\mathbf{Q}$, doch die Aussage über den Grad des Minimalpolynoms trifft im allgemeinen nicht zu.

Sei z.B. $\alpha = \sqrt{2}$, also $\mu_{\alpha,\mathbf{Q}}(X) = X^2 - 2$, und $\beta = i$, also $\mu_{\beta,\mathbf{Q}}(X) = X^2 + 1$. Da -1 kein Quadrat in $\mathbf{Q}(\sqrt{2}) \hookrightarrow \mathbf{R}$ ist, ist $X^2 + 1$ auch in $\mathbf{Q}(\sqrt{2})[X]$ noch irreduzibel, und wir erhalten eine Basis $(1, \sqrt{2}, i, i\sqrt{2})$ von $\mathbf{Q}(\sqrt{2}, i)$ über $\mathbf{Q}$.

Das Minimalpolynom von $i + \sqrt{2}$ berechnet sich nun über die Matrix bezüglich der angeführten Basis

$$\begin{pmatrix} 1 & 0 & 1 & 0 & -7 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 5 & 0 \\ 0 & 0 & 2 & 0 & 4 \end{pmatrix},$$

die in den Spalten die Potenzen von $i + \sqrt{2}$ aufführt, zu

$$\mu_{i+\sqrt{2},\mathbf{Q}}(X) \;=\; X^4 - 2X^2 + 9\,.$$

(3) Die Aussage ist richtig. Ist $G := \mathrm{Gal}(E|K)$, ist $f(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n) \in E[X]$ mit $n := \deg(f)$, und schreiben wir $A := \{\alpha_1, \ldots, \alpha_n\}$, so ist $\sigma \longmapsto \sigma|_A$ ein injektiver Gruppenmorphismus von G nach $\mathcal{S}_A \simeq \mathcal{S}_n$. Somit ist $|G|$ ein Teiler von $|\mathcal{S}_n| = n!$.