G. Nebe, M. Künzer 04.02.2005

Algebra I, WS 04/05

Lösung Klausur II

Aufgabe 1.

Wir formen zunächst z.B. wie folgt um.

$$\left(\begin{array}{cccc} 2 & 2 & 4 & 0 \\ 4 & 4 & 0 & 8 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cccc} 2 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ \hline 1 & 2 & -1 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right) .$$

Dies liefert zunächst

$$\operatorname{Cokern}(u) \;\simeq\; \mathbf{Z}/(2) \oplus \mathbf{Z}/(8) .$$

Dann wird $\left(\begin{smallmatrix} -1 & 2 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 4 \\ 2 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 4 & 0 \\ 0 & 4 \end{smallmatrix}\right)$. Die Elementarteilerform von $\left(\begin{smallmatrix} -1 & 2 \\ 1 & 0 \end{smallmatrix}\right)$ ist $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, und somit ist

$$\operatorname{Bild}(u) \;\simeq\; \mathbf{Z}/(2) .$$

Die Elementarteilerform von $\left(\begin{smallmatrix} 0 & 4 \\ 2 & 2 \end{smallmatrix}\right)$ ist $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$, und somit ist

$$\operatorname{Kern}(u) \;\simeq\; \mathbf{Z}/(2) \oplus \mathbf{Z}/(4) .$$

Probe: $|\operatorname{Kern}(u)| = 2^3$, $|\operatorname{Bild}(u)| = 2$ und $|X| = 2^4$ ist in Ordnung. $|\operatorname{Bild}(u)| = 2$, $|\operatorname{Cokern}(u)| = 2^4$ und $|Y| = 2^5$ ist auch in Ordnung.

Aufgabe 2.

(1) Wir wenden das Eisensteinkriterium über $\mathbf{Z}$ bezüglich $p = 2$ an. Es sind alle Koeffizienten bis auf den Leitkoeffizienten durch 2 teilbar, und der konstante Koeffizient 2 ist nicht durch 2^2 teilbar. Also ist $X^3 + 2X^2 + 2 \in \mathbf{Q}[X]$ irreduzibel.

Jedes irreduzible Polynom über einem Körper der Charakteristik 0 wie $\mathbf{Q}$ ist separabel. Also ist $X^3 + 2X^2 + 2$ separabel.

Alternative Begründung der Separabilität. Es ist $\operatorname{ggT}(f(X), f'(X)) = \operatorname{ggT}(X^3 + 2X^2 + 2,\ 3X^2 + 4X) = 1$, wie entweder mit dem euklidschen Algorithmus folgt, oder aus der Tatsache, daß $f(0) \neq 0$ und $f(-4/3) \neq 0$

(2) Zunächst bestimmen wir den Zerfällungskörper von $f(X)$. Sei $K_0 = K$, und sei $K_1 = K_0(\alpha_1)$ mit $\alpha_1^3 = -2\alpha_1^2 - 2$. Dann wird

$$X^3 + 2X^2 + 2 \;=\; (X - \alpha_1)(X^2 + (\alpha_1 + 2)X + (\alpha_1 + 2)\alpha_1) \;\in\; K_1[X] .$$

Es ist $g(X) := X^2 + (\alpha_1 + 2)X + (\alpha_1 + 2)\alpha_1 = (X + \frac{1}{2}(\alpha_1 + 2))^2 + \frac{1}{4}(\alpha_1 + 2)(3\alpha_1 - 2)$. Da $f(-2) = 2 > 0$, hat $f(X)$ in $\mathbf{R}$ eine Nullstelle $\xi < -2$. Zunächst gibt es daher eine Einbettung $K_1 \hookrightarrow \mathbf{R}$, welche $\alpha_1 \longmapsto \xi$ schickt. Wegen $\xi < -2$ ist aber $-\frac{1}{4}(\xi + 2)(3\xi - 2) < 0$, und damit kein Quadrat in $\mathbf{R}$. Also ist auch $-\frac{1}{4}(\alpha_1 + 2)(3\alpha_1 - 2)$ kein Quadrat in K_1. Somit ist $g(X) \in K_1[X]$ irreduzibel.

Sei $E = K_2 = K_1(\alpha_2) = K(\alpha_1, \alpha_2)$ mit $\alpha_2^2 = -(\alpha_1 + 2)(\alpha_1 + \alpha_2)$. Dann wird mit $\alpha_3 := -\alpha_1 - \alpha_2 - 2$

$$f(X) \;=\; (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) .$$

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

Ein Automorphismus von E ist gegeben durch das Tupel der Bilder (β_1, β_2) von (α_1, α_2), vorausgesetzt, es ist β_1 eine Nullstelle von $f(X)$ und β_2 eine Nullstelle von $f(X)/(X - \beta_1)$. Wegen $f(X)$ separabel bleiben die 6 Möglichkeiten

$$\{(\alpha_1, \alpha_2),\ (\alpha_1, \alpha_3),\ (\alpha_2, \alpha_1),\ (\alpha_2, \alpha_3),\ (\alpha_3, \alpha_1),\ (\alpha_3, \alpha_2)\}$$

für die Bilder von (α_1, α_2). Dabei wird α_3 jeweils auf die dritte verbleibende Nullstelle von $f(X)$ abgebildet.

Aus diesen greifen wir die beiden Automorphismen

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

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

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

Wir verwenden diesen Isomorphismus als Identifikation.

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

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

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

Es wird z.B.

$$\begin{array}{rcl} L_1 & = & K(\alpha_1+\alpha_2) \\ L_2 & = & K(\alpha_1) \\ L_3 & = & K(\alpha_2) \\ L_4 & = & K(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) \;=\; K(\alpha_1(3\alpha_1\alpha_2 + 4\alpha_2 + 2\alpha_1 + 4))\ . \end{array}$$

(4) Es ist nur L_4 galoisch über K, da nur U_4 normal in $\mathrm{Gal}(E|K)$ ist.

(5) Da die Elemente von $\mathrm{Gal}(L_4|K)$ durch die Identität und die Einschränkung von σ_1 gegeben sind, suchen wir ein Element $\xi \in L_4$ mit $(\xi, \sigma_1(\xi))$ eine K-Basis von L_4. Mit $\xi := \alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1$ wird $\sigma_1(\xi) = \alpha_2^2\alpha_1+\alpha_1^2\alpha_3+\alpha_3^2\alpha_2$. Nun ist

$$\begin{array}{rcl} \xi + \sigma_1(\xi) & = & \alpha_1\alpha_2(\alpha_1+\alpha_2) + \alpha_2\alpha_3(\alpha_2+\alpha_3) + \alpha_3\alpha_1(\alpha_3+\alpha_1) \\ & = & \alpha_1\alpha_2(-2-\alpha_3) + \alpha_2\alpha_3(-2-\alpha_1) + \alpha_3\alpha_1(-2-\alpha_2) \\ & = & -2s_2(\alpha_1,\alpha_2,\alpha_3) - 3s_3(\alpha_1,\alpha_2,\alpha_3) \\ & = & -2\cdot 0 - 3\cdot(-2) \\ & = & 6\ , \end{array}$$

wie man den Koeffizienten von $f(X)$ entnimmt. Damit liegen 1 und ξ im K-linearen Erzeugnis von $(\xi, \sigma_1(\xi))$, und es ist nach Konstruktion (ξ^0, ξ^1) eine K-lineare Basis von L_4. Somit ist auch $(\xi, \sigma_1(\xi))$ eine K-lineare Basis von L_4.

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 $s_3 = X_1X_2X_3$. Es wird

$$\begin{array}{rcl} X_1^3 + X_2^3 + X_3^3 & = & s_1^3 - 3(X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2) - 6X_1X_2X_3 \\ & = & s_1^3 - 3s_1s_2 + 9X_1X_2X_3 - 6X_1X_2X_3 \\ & = & s_1^3 - 3s_1s_2 + 3s_3\ . \end{array}$$

Aufgabe 4.

Sei $\mathbf{F}_4 = \mathbf{F}_2(\alpha)$ mit $\alpha^2 + \alpha + 1 = 0$.

Ein Polynom von Grad ≥ 2 kann nicht irreduzibel sein, wenn sein konstanter Term verschwindet.

Ein Polynom 2ten Grades kann in $\mathbf{F}_4[X]$ nicht irreduzibel sein, wenn alle seine Koeffizienten in $\mathbf{F}_2$ liegen. Denn ein solches Polynom wäre auch irreduzibel in $\mathbf{F}_2[X]$, und hätte somit $\mathbf{F}_4$ als Zerfällungskörper, was nicht geht.

Der Frobenius-Automorphismus $\mathrm{F} : \mathbf{F}_4 \longrightarrow \mathbf{F}_4$, $\xi \longmapsto \xi^2$, koeffizientenweise angewandt, bildet ein irreduzibles Polynom auf ein irreduzibles Polynom ab. Die Frobenius-Bahnen in $\mathbf{F}_4$ sind $\{0\}$, $\{1\}$, $\{\alpha, 1+\alpha\}$.

Ferner kann ein Polynom der Form $X^2 + u$ mit $u \in \mathbf{F}_4$ nicht irreduzibel sein, da es ein $v \in \mathbf{F}_4$ mit $v^2 = u$ gibt, und somit $X^2 + u = (X+v)^2$ folgt.

Es genügt wegen Frobenius, Polynome der Form $X^2 + X + \xi$ und $X^2 + \alpha X + \xi$ mit $\xi \in \mathbf{F}_4$ zu betrachten. Im ersteren Fall genügt ferner die Betrachtung von $\xi = \alpha$.

- Das Polynom $X^2 + X$ nimmt die Werte $\{0,\ 1\}$ an.

  Es ist $X^2 + X + \alpha$ irreduzibel, und damit auch $X^2 + X + (1+\alpha)$.

- Das Polynom $X^2 + \alpha X$ nimmt die Werte $\{0,\, 1+\alpha\}$ an.

  Es ist $X^2 + \alpha X + 1$ irreduzibel, und damit auch $X^2 + (1+\alpha)X + 1$.

  Es ist $X^2 + \alpha X + \alpha$ irreduzibel, und damit auch $X^2 + (1+\alpha)X + (1+\alpha)$.

Und in der Tat gibt es nach Übungsaufgabe 58 (2) gerade $(4^{(2^1)} - 4^{(2^0)}) \cdot 2^{-1} = 6$ irreduzible normierte Polynome von Grad 2 in $\mathbf{F}_4[X]$.

Aufgabe 5.

Wir haben zu zeigen, daß p den Grad $[E:K] = |\operatorname{Gal}(E|K)|$ der Erweiterung teilt, da eine endliche Gruppe, deren Ordnung durch p geteilt wird, ein Element der Ordnung p enthält. Dazu genügt es nun, zu zeigen, daß es einen Zwischenkörper $E|L|K$ gibt mit $[L:K] = p$.

Sei $a \in E$ eine Nullstelle von $f(X)$ und setze $L = K(a)$. Da $f(X) = \mu_{a,K}(X)$, ist $[L:K] = \deg(\mu_{a,K}) = \deg(f) = p$.

Aufgabe 6.

1. Lösung.

Wir führen eine Induktion nach m. Es wird

$$\begin{aligned}
\Phi_{2m}(X) &= \frac{X^{2m}-1}{\Bigg(\prod\limits_{\substack{d\,|\,2m\\ d\equiv_2 0\\ d\neq 2m}} \Phi_d(X)\Bigg)\Bigg(\prod\limits_{\substack{d\,|\,2m\\ d\not\equiv_2 0}} \Phi_d(X)\Bigg)} = \frac{X^{2m}-1}{\Bigg(\prod\limits_{\substack{d\,|\,m\\ d\neq m}} \Phi_{2d}(X)\Bigg)\Bigg(X^m - 1\Bigg)} \\
&= \frac{X^m+1}{\Bigg(X+1\Bigg)\Bigg(\prod\limits_{\substack{d\,|\,m\\ d\notin\{1,m\}}} \Phi_d(-X)\Bigg)} = \frac{(-X)^m-1}{\Bigg(\prod\limits_{\substack{d\,|\,m\\ d\neq m}} \Phi_d(-X)\Bigg)} \\
&= \Phi_m(-X)\,.
\end{aligned}$$

2. Lösung.

Sei m ungerade, und $m \geq 3$. Zu zeigen ist $\Phi_{2m}(X) = \Phi_m(-X)$. Wir behaupten zunächst, daß $\Phi_m(-X)$ normiert ist, d.h. daß der Grad von $\Phi_m(X)$ gerade ist. Dies folgt mit Induktion nach m aus der Definition $\Phi_m(X) = (X^m - 1)/(\prod_{d\,|\,m,\, d\neq m} \Phi_d(X))$, da der Grad von $X^m - 1$ und von $\Phi_1(X)$ ungerade ist, alle anderen Faktoren aber nach Induktionsvoraussetzung geraden Grad haben.

Da nun wegen des Automorphismus $\mathbf{Q}[X] \xrightarrow{\sim} \mathbf{Q}[X]$, $X \longmapsto -X$ mit $\Phi_m(X)$ auch $\Phi_m(-X)$ irreduzibel ist, genügt es für die Gleichheit $\Phi_{2m}(X) = \Phi_m(-X)$ wegen der Eindeutigkeit des Minimalpolynoms zu zeigen, daß $\Phi_m(-X)$ im algebraischen Abschluß $\bar{K}$ eine primitive $2m$te Einheitswurzel annulliert. Nun ist $-\zeta_m$ eine Nullstelle von $\Phi_m(-X)$, und die multiplikative Ordnung von $-\zeta_m$ ist gerade $2m$. In der Tat ist $\boldsymbol{\mu}_m \cap \boldsymbol{\mu}_2 = 1$ wegen $(-1)^m \neq 1$, so daß $\boldsymbol{\mu}_{2m} \simeq \boldsymbol{\mu}_m \times \boldsymbol{\mu}_2$, $-\zeta_m \longleftarrow\!\dashv (\zeta_m, -1)$, und letzteres Element hat Ordnung $2m$.

Aufgabe 7.

(1) Die Aussage ist richtig. Sei $R \xrightarrow{\varphi} R/\mathfrak{a}$, $x \longmapsto x + \mathfrak{a}$ die Restklassenabbildung.

1. Lösung.

Ist $\mathfrak{b} \subseteq R/\mathfrak{a}$ ein Ideal, so haben wir zu zeigen, daß es endlich erzeugt ist. Es ist $\varphi^{-1}(\mathfrak{b}) \subseteq R$ ein Ideal, und also endlich erzeugt, da R als noethersch vorausgesetzt ist. Schreibe etwa $\varphi^{-1}(\mathfrak{b}) = (x_1, \ldots, x_k)$. Wir behaupten, daß $\mathfrak{b} = (\varphi(x_1), \ldots, \varphi(x_k))$. Die Inklusion $\supseteq$ ist klar. Zeigen wir $\subseteq$. Sei $b \in \mathfrak{b}$. Sei $y \in R$ mit $\varphi(y) = b$. Es gibt nun $r_1, \ldots, r_k \in R$ mit $y = r_1 x_1 + \cdots + r_k x_k$. Anwenden von φ liefert

$$\varphi(y) \;=\; \varphi(r_1)\varphi(x_1) + \cdots + \varphi(r_k)\varphi(x_k) \;\in\; (\varphi(x_1), \ldots, \varphi(x_k))\,,$$

wie verlangt.

2. Lösung.

Sei angenommen, es gebe eine unendliche echt aufsteigende Kette von Idealen $\mathfrak{b}_1 \subsetneq \mathfrak{b}_2 \subsetneq \cdots$ in $R/\mathfrak{a}$. Da φ surjektiv ist, ist dann auch die Kette von Idealen $\varphi^{-1}(\mathfrak{b}_1) \subsetneq \varphi^{-1}(\mathfrak{b}_2) \subsetneq \cdots$ in R echt aufsteigend. Eine solche kann aber wegen R noethersch nicht existieren, und wir haben einen Widerspruch.

(2) Die Aussage ist falsch. Ist allgemein p eine Primzahl, und L ein Körper mit p^k Elementen, und ist $K \subseteq L$ ein Teilkörper, so ist L ein Vektorraum über K, und also gibt es ein $m \geq 1$ mit $p^k = |L| = |K|^m$. Es folgt, daß $m \mid k$ und daß $K = p^{k/m}$. In unserer Situation besagt dies, daß ein Teilkörper eines Körpers mit 2^5 Elementen entweder 2 oder 2^5 Elemente enthält, nicht jedoch 2^3.

(3) Die Aussage ist richtig. Denn sei a eine Nullstelle von $f(X)$ in E und sei $L = K(a)$ Wurzelkörper von $f(X)$. Dann ist wegen $\mathrm{Gal}(E|K)$ abelsch die Untergruppe $\mathrm{Gal}(E|L) \leq \mathrm{Gal}(E|K)$ ein Normalteiler, und folglich $L|K$ galoisch. Dann aber zerfällt $f(X)$ bereits in $L[X]$ in Linearfaktoren, d.h. die Nullstellen von $f(X)$ in E liegen sämtlich bereits in L (denn die Bilder von a unter den Elementen von $\mathrm{Gal}(L|K)$ sind paarweise verschieden und alle ebenfalls Nullstellen von $f(X)$; dies liefert uns $|\,\mathrm{Gal}(L|K)| = [L : K] = \deg(f)$ Nullstellen von f bereits in L). Da E von den Nullstellen von $f(X)$ erzeugt wird, folgt $E = L$.