Mathematisches Institut
der Universität München
Andreas Fackler

Sommersemester 2009
Lösungsvorschlag für Übungsblatt 8

Klausurenkurs Algebra

Aufgabe 1 (Frühjahr 2007, Thema 1, Aufgabe 2)

(a) Wegen $f(0) = 1$, $f(1) = 3$, $f(2) = 1$, $f(3) = 1$ und $f(4) = 4$ hat f keine Nullstelle, ist also irreduzibel. Folglich ist das von f erzeugte Ideal (f) prim und damit maximal, also ist $K[X]/(f)$ ein Körper. Nun gilt $\alpha^3 + \alpha + 1 = 0$, also $\alpha^3 = -\alpha - 1$. Für jedes Element $a_n X^n + \ldots + a_0 X^0 + (f) = a_n\alpha^n + \ldots a_0\alpha^0$ von K mit $n \geq 3$ gilt also: $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0\alpha^0 = a_n\alpha^{n-3}(-\alpha - 1) + a_{n-1}\alpha^{n-1} + \ldots + a_0\alpha^0$. Mit Induktion folgt hieraus, dass sich jedes Element von K als ein Polynom vom Grad höchstens 2 in α darstellen lässt, also in der Form $a_2\alpha^2 + a_1\alpha + a_0$. $(1, \alpha, \alpha^2$ ist also ein Erzeugendensystem von K über $\mathbb{F}_5$. Sei nun $a_2\alpha^2 + a_1\alpha + a_0 = 0$, also $a_2X^2 + a_1X + a_0 \in (f)$. Da f Grad 3 hat, muss jedes Vielfache von f entweder 0 sein oder ebenfalls mindestens Grad 3 haben. Also ist $a_2X^2 + a_1X + a_0 = 0$ und damit $a_2 = a_1 = a_0 = 0$, womit auch die lineare Unabhängigkeit bewiesen ist.

(b) Auf $\mathbb{F}_5$ ist der Frobenius-Automorphismus die Identität. Es gilt also:

$$\begin{aligned} F(1) &= 1 \\ F(\alpha) &= \alpha^5 = \alpha^2(-\alpha - 1) = -\alpha^3 - \alpha^2 = -\alpha^2 + \alpha + 1 = 4\alpha^2 + \alpha + 1 \\ F(\alpha^2) &= \alpha^{10} = \alpha(-\alpha - 1)^3 = -\alpha(\alpha^3 + 3\alpha^2 + 3\alpha + 1) \\ &= -\alpha(3\alpha^2 + 2\alpha) = -3\alpha^3 - 2\alpha^2 = -2\alpha^2 + 3\alpha + 3 = 3\alpha^2 + 3\alpha + 3 \end{aligned}$$

Damit erhalten wir als darstellende Matrix:

$$M = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 3 \\ 0 & 4 & 3 \end{pmatrix}$$

(c) Wir müssen das zu der Matrix $M - 1$ gehörende homogene Gleichungssystem lösen. Hierzu wenden wir das Gauß-Verfahren an:

$$\begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 3 \\ 0 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 3 \\ 0 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Der Eigenraum ist also eindimensional und hat die Basis $(1, 0, 0)$ – dargestellt bezüglich $(1, \alpha, \alpha^2)$ –, das heißt: 1.
Alternative Lösung: Der Frobenius-Homomorphismus lässt nur den Grundkörper $\mathbb{F}_5$ selbst fest; dieser hat etwa die Basis 1.

Aufgabe 2 (Frühjahr 2007, Thema 3, Aufgabe 1)

Ein Element von $\mathbb{F}_{2^8}$ ist genau dann primitiv, wenn es in keinem echten Unterkörper enthalten ist. Die Unterkörper von $\mathbb{F}_{2^8}$ sind genau $\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^4} \subset \mathbb{F}_{2^8}$. $\mathbb{F}_{2^4}$ hat 2^4 Elemente. Die Zahl der primitiven Elemente von $\mathbb{F}_{2^8}$ ist also $2^8 - 2^4 = 256 - 16 = 240$.

Aufgabe 3 (Frühjahr 2007, Thema 3, Aufgabe 2)

(a) Wegen $f(0) = f(1) = 1$ hat f keine Nullstelle. Wäre f reduzibel, wäre es also produkt irreduzibler Polynome vom Grad 2. Es gibt aber nur ein irreduzibles Polynom vom Grad 2, nämlich $X^2 + X + 1$, und $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq f$.

(b) Es ist $x^5 = x^4 \cdot x = (-x^3 - x^2 - x - 1) \cdot x = -x^4 - x^3 - x^2 - x = (x^3 + x^2 + x + 1) - x^3 - x^2 - x = 1$, also ist die Ordnung von x ein Teiler von 5. Da $X - 1$ kein Vielfaches von f ist, ist $X + (f) \neq 1 + (f)$, also $x \neq 1$. Daher hat x Ordnung 5.

Aufgabe 4 (Herbst 2004, Thema 2, Aufgabe 4)

(a) Angenommen, $\mathbb{Q}(\sqrt{p})$ ist isomorph zu $\mathbb{Q}(\sqrt{q})$. Dann ist die Gleichung $X^2 - q = 0$ in $\mathbb{Q}(\sqrt{p})$ lösbar, das heißt, es gibt $a, b \in \mathbb{Q}$ mit $(a + b\sqrt{p})^2 = q$. Hierbei kann a nicht null sein, da sonst $q = pb^2$, also $b = \sqrt{\frac{q}{p}} \notin \mathbb{Q}$ wäre. Ebenso kann b nicht 0 sein, da q kein Quadrat in $\mathbb{Q}$ ist. Also ist $a^2 + 2ab\sqrt{p} + b^2 p = q$, das heißt, $\sqrt{p} = \frac{q - b^2 p - a^2}{2ab} \in \mathbb{Q}$, ein Widerspruch.

(b) Nach Teilaufgabe (a) ist $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ ein echter Erweiterungskörper von $\mathbb{Q}(\sqrt{p})$, und zwar der Zerfällungskörper des Polynoms $X^2 - q$. Da dieses Grad 2 hat und auch $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ ist, hat die Erweiterung den Grad $2 \cdot 2 = 4$.

(c) Es gilt $\alpha^2 = p + q + 2\sqrt{pq}$, also $(\alpha^2 - p - q)^2 - 4pq = 0$. α ist also Nullstelle des Polynoms $X^4 - 2(p+q)X^2 + (p+q)^2 - 4pq = X^4 - 2(p+q)X^2 + (p-q)^2$. Um zu zeigen, dass dies irreduzibel, also das Minimalpolynom von α, ist, genügt es nach Teilaufgabe (b) zu zeigen, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ ist, dass sich also $\sqrt{p}$ und $\sqrt{q}$ durch α ausdrücken lassen. Dies folgt aber aus $\sqrt{p} - \sqrt{q} = \frac{p-q}{\alpha}$.