Algebra I

Musterlösung 15

Endliche Körper

Sei p eine Primzahl.

90. Sei $L := \mathbb{F}_p(t)$ der Körper der rationalen Funktionen über $\mathbb{F}_p$ in der Variablen t (d.h. der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$) und sei $K := \mathbb{F}_p(t^p)$.

Zeige: Das Polynom $X^p - t^p$ ist irreduzibel und inseparabel über K, und L ist sein Zerfällungskörper.

Lösung: Der Ring $\mathbb{F}_p[t^p]$ ist isomorph zum Polynomring $\mathbb{F}_p[Y]$ via eines Isomorphismus, der auf $\mathbb{F}_p$ die Identität ist und Y auf t^p abbildet. Da Y ein irreduzibles Element im Hauptidealring $\mathbb{F}_p[Y]$ ist, ist auch $t^p \in \mathbb{F}_p[t^p]$ irreduzibel. Nach dem Eisenstein-Schönemann-Kriterium ist nun $X^p - t^p$ ein irreduzibles Polynom in $\mathbb{F}_p[t^p][X]$, also ist es nach dem Lemma von Gauss irreduzibel in $\mathbb{F}_p(t^p)[X] = K[X]$. über L gilt $X^p - t^p = (X - t)^p$, also hat das Polynom die p-fache Nullstelle t und ist somit, da es irreduzibel ist, nicht separabel. Da $L = K(t)$ ist, ist L der Zerfällungskörper.

91. Sei K ein Körper der Charakteristik p und sei $K \to K, x \mapsto x^p$ der Frobeniushomomorphismus.

(a) Zeige: Der Frobeniushomomorphismus ist injektiv.

(b) Zeige: Der Frobeniushomomorphismus ist genau dann surjektiv, wenn jedes Polynom in $K[X]$ separabel ist.

Bemerkung: Ein Körper, über den jedes Polynom separabel ist, heisst *perfekt*.

Lösung: (a) Aus der Vorlesung wissen wir, dass der Frobeniushomomorphismus ein Körperhomomorphismus ist. Somit ist er injektiv.

(b) Wir nehmen zuerst an, der Frobeniushomomorphismus $K \to K$ sei surjektiv. Sei per Widerspruchsannahme $f \in K[X]$ inseparabel. Wir können o.B.d.A. annehmen, dass f irreduzibel ist. Wegen Insepabaribilität müssen f und f' mit Satz 16.1 einen gemeinsamen Teiler haben vom Grad ≥ 1 haben. Da f jedoch irreduzibel ist, folgt daraus, dass dieser Teiler gleich f ist. Dies impliziert aus Gradgründen $f' = 0$. Folglich hat f die Form $f = \sum_{i=0}^{n} a_i X^{pi}$. Da der Frobeniushomomorphismus surjektiv ist, können wir $a_i = b_i^p$ mit $b_i \in K$ schreiben. Also ist $f = \sum_{i=0}^{n} b_i^p X^{pi} = (\sum_{i=0}^{n} b_i X^i)^p$ und folglich nicht irreduzibel.

Für die Gegenrichtung nehmen wir an, der Frobeniushomomorphismus $K \to K$ sei nicht surjektiv. Sei also $b \in K$ nicht im Bild des Frobeniushomomorphismus. Dann hat das Polynom $X^p - b \in K[X]$ keine Nullstelle, seine irreduziblen Faktoren haben somit mindestens Grad 2. Sei a eine Nullstelle in einem Zerfällungskörper. Dann gilt $X^p - b = (X - a)^p$ in $K(a)[X]$, somit ist $K(a)$ der Zerfällungskörper. Somit hat jeder irreduzible Faktor von $X^p - b \in K[X]$ die mehrfache Nullstelle a. Also haben wir ein nichtseparables Polynom gefunden und K ist nicht perfekt.

92. Sei $q = p^n$ für eine positive ganze Zahl n.

(a) Zeige: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn sein Grad ein Teiler von n ist.

(b) Sei I_d die Menge der normierten, irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Beweise die Gleichung

$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Folgere daraus, dass $\sum_{d|n} \big(d \cdot |I_d|\big) = q$ gilt.

(d) Bestimme die Anzahl der irreduziblen Polynome vom Grad 6, 7, 8 in $\mathbb{F}_2[X]$.

Lösung: (a) Jedes irreduzible Polynom über einem endlichen Körper ist separabel. Also ist f genau dann ein Teiler von $X^q - X$, wenn f und $X^q - X$ eine gemeinsame Nullstelle α in einem Zerfällungskörper von $X^q - X$ haben. Aber die Nullstellen von $X^q - X$ sind genau die Elemente des Körpers $\mathbb{F}_q$ der Ordnung q. Für diese ist $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ ein Teiler von $[\mathbb{F}_q : \mathbb{F}_p] = n$. Damit ist gezeigt, dass aus $f | X^q - X$ tatsächlich $\deg(f) | n$ folgt.

Nimm umgekehrt $\deg(f) | n$ an. Sei α eine Nullstelle von f in einem Zerfällungskörper von f. Dann ist $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(f)$ und somit ist $\mathbb{F}_p(\alpha)$ der Zerfällungskörper von $X^{p^{\deg(f)}} - X$. Dies impliziert $\alpha^{p^{\deg(f)}} = \alpha$ und mit $\deg(f) | n$ folgt $\alpha^q = \alpha$.

(b) Wegen (a) teilt die rechte Seite die linke, denn die f sind alle zueinander teilerfremd. Sei umgekehrt $a \in \mathbb{F}_q$ eine Nullstelle von $X^q - X$. Sei $m_{a,\mathbb{F}_p}$ das normierte Minimalpolynom von a über F_p. Dann gilt $m_{a,\mathbb{F}_p} | X^q - X$ und $\deg(m_{a,\mathbb{F}_p}) \leq [\mathbb{F}_q : \mathbb{F}_p] = n$, also ist das Polynom auf der rechten Seite ein annullierendes Polynom für a und $m_{a,\mathbb{F}_p}$ muss einer der Faktoren sein. Da $X^q - X$ nur einfache Nullstellen hat, folgt die Aussage.

(c) Vergleiche den Grad auf der rechten und linken Seite in (b).

(d) Mit (c) gilt $2^6 = |I_1| + 2|I_2| + 3|I_3| + 6|I_6|$. Die irreduziblen Polynome von Grad 2 und 3 können wir schnell abzählen und wir finden $|I_6| = 9$.

Wieder gilt $2^7 = |I_1| + 7|I_7|$ und daher $|I_7| = \frac{128-2}{7} = 18$.

Es gilt $2^8 = |I_1| + 2|I_2| + 4|I_4| + 8|I_8|$, also $|I_8| = \frac{256-2-2-12}{8} = 30$.

93. Finde für $q = 8, 9, 16$ das Minimalpolynom über $\mathbb{F}_2$ *bzw.* $\mathbb{F}_3$ eines Erzeugers von $\mathbb{F}_q^*$.

Lösung: Sei $p^r = 8$. Dann ist $\mathbb{F}_8$ isomorph zu $\mathbb{F}_2[X]/(X^3 + X + 1)$, da $X^3 + X + 1$ ein irreduzibles Polynom vom Grad 3 über $\mathbb{F}_2$ ist. Ausserdem ist $\mathbb{F}_8^*$ zyklisch der Ordnung 7, also ist jedes von 1 verschiedene Element ein Erzeugendes. Zum Beispiel können wir das Bild von X in $\mathbb{F}_2[X]/(X^3+X+1)$ als erzeugendes Element wählen. Sein Minimalpolynom ist natürlich $X^3 + X + 1$.

Sei $p^r = 9$. Dann ist $\mathbb{F}_9$ isomorph zu $\mathbb{F}_3[X]/(X^2 + 1)$, da $X^2 + 1$ ein irreduzibles Polynom vom Grad 2 über $\mathbb{F}_3$ ist. Eine $\mathbb{F}_3$-Basis von $\mathbb{F}_9$ ist also $\{1, a\}$ mit $a^2 = -1$. Da $\mathbb{F}_9^*$ zyklisch der Ordnung 8 ist, suchen wir ein Element der Ordnung 8. Die Elemente der Ordnungen 1, 2 und 4 sind respektive 1, -1 und $\pm a$. Somit kann zum Beispiel $a + 1$ nur noch die Ordnung 8 haben. (Wir können dies auch direkt nachrechnen vermittels $(a + 1)^2 = 2a$ und $(a + 1)^4 = (2a)^2 = -4 = -1 \neq 1$.) Wegen $(a + 1)^2 + (a + 1) - 1 = 0$ und $a + 1 \notin \mathbb{F}_3$ ist $X^2 + X - 1$ das Minimalpolynom von $a + 1$ über $\mathbb{F}_3$.

Sei $p^r = 16$. Das Polynom $X^4 + X + 1$ ist irreduzibel vom Grad 4 über $\mathbb{F}_2$, folglich ist $\mathbb{F}_{16} = \mathbb{F}_2(a)$ für ein Element a mit Minimalpolynom $X^4 + X + 1$ über $\mathbb{F}_2$. Da $\mathbb{F}_{16}^*$ zyklisch der Ordnung $16 - 1 = 3 \cdot 5$ ist, ist schon a selbst ein Erzeuger, sofern nicht $a^3 = 1$ oder

$a^5 = 1$ ist. In diesem Fall wäre a eine Nullstelle des Polynoms $X^3 - 1$ oder des Polynoms $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. Allerdings ist aus Gradgründen jedes dieser Polynome teilerfremd zum irreduziblen Polynom $X^4 + X + 1$. Dies kann also nicht sein, und a ist ein Erzeuger von $\mathbb{F}_{16}^*$ mit dem Minimalpolynom $X^4 + X + 1$.

94. (a) Zeige, dass das Polynom $f(X) = X^3 + 3X + 3$ irreduzibel in $\mathbb{F}_5[X]$ ist.

(b) Sei α eine Nullstelle von f in einem Zerfällungskörper von f. Sei $\mathbb{F}_{125} = \mathbb{F}_5(\alpha)$. Berechne die Darstellungsmatrix des Frobeniusautomorphismus $\mathrm{Frob}_5 \colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der Basis $(1, \alpha, \alpha^2)$.

(c) Schreibe das Element $\beta := 1/(1-\alpha) \in \mathbb{F}_{125}$ als $\mathbb{F}_5$-Linearkombination von $1, \alpha$ und α^2.

(d) Zeige, dass α die zyklische Gruppe $\mathbb{F}_{125}^*$ erzeugt.

Lösung: We denote elements of $\mathbb{F}_5$ just with integer numbers, so that $5 = 0$.

(a) Since the polynomial $f \in \mathbb{F}_5[X]$ has degree 3, every proper decomposition of f has a linear factor, which means that f is irreducible if and only if it has no root in $\mathbb{F}_5$. Since $f(0) = 3$, $f(1) = 2$, $f(2) = 2$, $f(3) = 4$ and $f(4) = 4$, we obtain that f has no root in $\mathbb{F}_5$, therefore it is irreducible in $\mathbb{F}_5$.

(b) Since α is a root of f, we have

$$\alpha^3 = -3\alpha - 3 = 2(\alpha + 1) \text{ and}$$
$$(\alpha+1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3(\alpha^2 + 1),$$

which implies in particular that

$$\alpha^9 = -\alpha^2 - 1.$$

To compute the matrix of $\mathrm{Frob}_5 : x \mapsto x^5$ with respect to the basis $(1, \alpha, \alpha^2)$, where α is a root of f, we write down the images of 1, α and α^2 as $\mathbb{F}_5$-linear combinations of 1, α and α^2. We get the following:

$$\begin{aligned}
\mathrm{Frob}_5(1) &= 1 \\
\mathrm{Frob}_5(\alpha) &= \alpha^5 = \alpha^2 \cdot 2 \cdot (\alpha + 1) = 2\alpha^3 + 2\alpha^2 = -1 - \alpha + 2\alpha^2 \\
\mathrm{Frob}_5(\alpha^2) &= \alpha \cdot \alpha^9 = -\alpha^3 - \alpha = -2 + 2\alpha
\end{aligned}$$

Then the matrix associated to Frob_5 with respect to the basis $(1, \alpha, \alpha^2)$ is

$$M_{\mathrm{Frob}_5} = \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

(c) Suppose that $\beta = \lambda + \mu\alpha + \nu\alpha^2$ for $\lambda, \mu, \nu \in \mathbb{F}_5$. Then the condition $1 = \beta(1-\alpha)$ gives

$$1 = \lambda + (\mu - \lambda)\alpha + (\nu - \mu)\alpha^2 - \nu\alpha^3 = \lambda + 3\nu + (3\nu + \mu - \lambda)\alpha + (\nu - \mu)\alpha^2,$$

which is equivalent to

$$\begin{cases} \lambda + 3\nu = 1 \\ 3\nu + \mu - \lambda = 0 \\ \nu - \mu = 0. \end{cases}$$

Solving the equations backwards we obtain $\mu = \nu$, $\lambda = 4\nu$ and $7\nu = 1$, so that the unique solution is $(\lambda, \mu, \nu) = (2, 3, 3)$, and $\beta = 2 + 3\alpha + 3\alpha^2$.

(d) The group $\mathbb{F}_{125}^*$ is cyclic of order $124 = 4 \cdot 31$, and by Lagrange's theorem applied to the subgroup $\langle \alpha \rangle$ we see that the order of α is a divisor of 124. We want to prove that indeed $\mathrm{ord}_{\mathbb{F}_{125}^*}(\alpha) = 124$, and this can be done by checking that α^4 and α^{62} both differ from 1, since every proper divisor of 124 divides either 4 or 62. Of course, $\alpha^4 = 2(\alpha^2 + \alpha) \neq 1$, so that we are left to check that $\alpha^{62} \neq 1$. We have

$$\alpha^{62} = \alpha^{-1}(\alpha^9)^7 = -\alpha^{-1}(\alpha^2 + 1)^7.$$

To proceed with the computation, notice that

$$\begin{aligned}
&(\alpha^2 + 1)^3 = \alpha^6 + 3\alpha^4 + 3\alpha^2 + 1 = 4(\alpha + 1)^2 + \alpha^2 + \alpha + 3\alpha^2 + 1 = 3\alpha^2 - \alpha, \\
&(\alpha^2 + 1)^6 = (3\alpha^2 - \alpha)^2 = -\alpha^4 - \alpha^3 + \alpha^2 = -\alpha^2 + \alpha - 2 \text{ and} \\
&(\alpha^2 + 1)^7 = (-\alpha^2 + \alpha - 2)(\alpha^2 + 1) = -\alpha^4 - \alpha^2 + \alpha^3 + \alpha - 2\alpha^2 - 2 = \alpha.
\end{aligned}$$

Then

$$\alpha^{62} = -\alpha^{-1}\alpha = -1 \neq 1,$$

and we can conclude that α generates $\mathbb{F}_{125}^*$.