Musterlösung Serie 22

Endliche Körper, Separable Körpererweiterungen

1. Finde für $p^r = 8, 9, 16$ das Minimalpolynom über $\mathbb{F}_p$ eines Erzeugenden von $\mathbb{F}_{p^r}^\times$.

   Lösung: Sei $p^r = 8$. Da $X^3 + X + 1$ ein irreduzibles Polynom vom Grad 3 über $\mathbb{F}_2$ ist, folgt $\mathbb{F}_8 \cong \mathbb{F}_2[X]/(X^3 + X + 1)$. Ausserdem ist $\mathbb{F}_8^\times$ 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 dann $X^3 + X + 1$.

   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 $\mathbb{F}_9^\times$ 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 $\mathbb{F}_2$; also ist $\mathbb{F}_{16} = \mathbb{F}_2(a)$ für ein Element a mit Minimalpolynom $X^4 + X + 1$ über $\mathbb{F}_2$. Da $\mathbb{F}_{16}^\times$ 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 von $X^3 - 1$ oder $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$, wohingegen aus Gradgründen jedes dieser Polynome teilerfremd zum irreduziblen Polynom $X^4 + X + 1$ ist. Dies kann also nicht sein, und a ist ein Erzeuger von $\mathbb{F}_{16}^\times$ mit dem Minimalpolynom $X^4 + X + 1$.

2. (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 algebraischen Abschluss von $\mathbb{F}_5$ und $\mathbb{F}_{125} := \mathbb{F}_5(\alpha)$. Berechne die Darstellungsmatrix des Frobeniusautomorphismus $\mathrm{Frob}_5 \colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der geordneten 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 $\mathbb{F}_{125}^\times$ 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 over $\mathbb{F}_5$.

(b) Since α is a root of f, we have

$$\begin{aligned} \alpha^3 &= -3\alpha - 3 = 2(\alpha + 1), \\ (\alpha + 1)^3 &= \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3(\alpha^2 + 1), \quad \text{and} \\ \alpha^9 &= (2(\alpha + 1))^3 = 8 \cdot 3(\alpha^2 + 1) = -\alpha^2 - 1. \end{aligned}$$

To compute the matrix of $\mathrm{Frob}_5 : x \mapsto x^5$ with respect to the basis $(1, \alpha, \alpha^2)$, 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:

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

The matrix associated to Frob_5 with respect to the basis $B := (1, \alpha, \alpha^2)$ is therefore

$$ {}_B[\mathrm{Frob}_5]_B \;=\; \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}. $$

(c) We know that $\beta = \lambda + \mu\alpha + \nu\alpha^2$ for some $\lambda, \mu, \nu \in \mathbb{F}_5$. The equation $1 = \beta(1 - \alpha)$ 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 the system of linear equations

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

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

(d) The group $\mathbb{F}_{125}^\times$ 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 $\mathrm{ord}_{\mathbb{F}_{125}^\times}(\alpha) = 124$, 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. We easily find that $\alpha^4 = 2(\alpha^2 + \alpha) \neq 1$, so that we must check that $\alpha^{62} \neq 1$. For this we note that

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

Using the formulas in (b) we now compute

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

Hence

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

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

3. Sei K ein Körper der Charakteristik $p > 0$ und sei $a \in K$.

   (a) Zeige, dass das Polynom $f(X) := X^p - X - a \in K[X]$ separabel ist.

   (b) Sei α eine Nullstelle von f in einem algebraisch abgeschlossenen Oberkörper L von K. Zeige

   $$\big\{\beta \in L : f(\beta) = 0\big\} \;=\; \big\{\alpha + x : x \in \mathbb{F}_p\big\}.$$

   (c) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Körpererweiterung $K(\alpha)/K$ den Grad p hat. Was geschieht im Fall $a \in \{y^p - y : y \in K\}$?

   (d) Zeige, dass im Fall $a \notin \{y^p - y : y \in K\}$ die Gruppe $\mathrm{Aut}_K(K(\alpha))$ zyklisch der Ordnung p ist.

   (e) Konstruiere auf diese Weise für $K = \mathbb{F}_p$ einen Körper der Ordnung p^p.

   Lösung: (a) We proved in the lecture that f is separable if and only if f and f' are coprime. Since $f'(X) = pX^{p-1} - 1 = -1$ is a unit in $K[X]$, this is indeed the case.

   (b) Since f is separable of degree p, it has exactly p roots in L. Therefore, both sets have the same finite cardinality p, and to show that they are equal it suffices to show that one is included in the other. Recall that the Frobenius of degree p is a field endomorphism of L which is the identity on $\mathbb{F}_p$. Thus for all $x \in \mathbb{F}_p$ we have

   $$f(\alpha + x) = (\alpha+x)^p - (\alpha + x) - a = \alpha^p + x^p - \alpha - x - a = f(\alpha) + x^p - x = 0.$$

   Hence $\{\beta \in L : f(\beta) = 0\} \supset \{\alpha + x : x \in \mathbb{F}_p\}$ and the equality follows.

   (c) We start with the easy case: If $a = y^p - y$ for some $y \in K$, then $\alpha = y \in K$ is a root of $f(X) = X^p - X - (y^p - y)$. By (b), any root of f is in K. This means that $K(\alpha) = K$ and f decomposes into linear factors over K.

   Now assume that $a \notin \{y^p - y : y \in K\}$, i.e. $\forall y \in K\colon y^p - y \neq a$. Then all the roots $\alpha + x$ of f lie outside K, and we claim that f is irreducible. This claim then

implies that f ist the minimal polynomial of α over K, so that $K(\alpha)$ has degree p over K.

To prove our claim, consider any monic factor $g \in K[X]$ of f. Then by (b) we have

$$g(X) = \prod_{x \in I} (X - \alpha - x)$$

in $L[X]$ for some nonempty subset $I \subseteq \mathbb{F}_p$. Set $d := |I| = \deg(g)$, which by construction satisfies $0 < d \leqslant p$. Then the coefficient of X^{d-1} in g is

$$-\sum_{x \in I} (\alpha + x) = -d\alpha - \sum_{x \in I} x.$$

This coefficient must lie in K, and since $\sum_{x \in I} x \in \mathbb{F}_p \subseteq K$, this implies $d\alpha \in K$. As $\alpha \notin K$, this is only possible if $p|d$, which implies $d = p$. Thus any factor of f has degree $p = \deg(f)$ and is therefore equal to f. This makes f irreducible.

(d) Nach (c) ist $K(\alpha)$ ein Stammkörper des irreduziblen Polynoms f über K. Nach §6.2 der Zusammenfassung und (b) steht folglich die Menge der Homomorphismen $\varphi\colon K(\alpha) \to K(\alpha)$ über K in Bijektion zu der Menge $\{\alpha + x : x \in \mathbb{F}_p\}$ der Wurzeln von f in $K(\alpha)$. Wegen $[K(\alpha)/K] < \infty$ ist ausserdem jeder solche Endomorphismus bereits ein Automorphismus. Die Gruppe $\mathrm{Aut}_K(K(\alpha))$ steht also in Bijektion zu $\mathbb{F}_p$ und hat deshalb die Ordnung p. Da p eine Primzahl ist, kann $\mathrm{Aut}_K(K(\alpha))$ dann nur zyklisch sein.

(Tatsächlich ist die Bijektion zwischen $\mathrm{Aut}_K(K(\alpha))$ und $\mathbb{F}_p$ bereits ein Gruppenisomorphismus. Denn zu jedem $x \in \mathbb{F}_p$ sei φ_x der eindeutige Endomorphismus mit $\varphi_x(\alpha) = \alpha + x$. Für alle $x, y \in \mathbb{F}_p$ gilt dann

$$\varphi_x(\varphi_y(\alpha)) = \varphi_x(\alpha + y) = \varphi_x(\alpha) + \varphi_x(y) = (\alpha + x) + y = \alpha + (x + y) = \varphi_{x+y}(\alpha).$$

Die Eindeutigkeit der Bijektion zeigt dann $\varphi_x \circ \varphi_y = \varphi_{x+y}$; somit ist die Bijektion ein Homomorphismus und folglich ein Isomorphismus.)

(e) Nach (c) genügt es, das Element a in der Menge $\mathbb{F}_p \setminus \{y^p - y : y \in \mathbb{F}_p\}$ zu wählen. Diese Menge ist gleich $\mathbb{F}_p \setminus \{0\}$; also tut es zum Beispiel $a = 1$. Somit ist $X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel, und jeder Stammkörper davon ist eine Erweiterung von $\mathbb{F}_p$ vom Grad p, also ein Körper der Ordnung p^p.

4. Seien p eine Primzahl und K ein endlicher Körper der Ordnung p^n mit $n > 0$. Zeige:

   (a) Im Fall $p = 2$ ist jedes Element von K ein Quadrat.

   (b) Jedes Element von K ist eine Summe von zwei Quadraten.

   (c) Für $p > 2$ ist ist -1 ein Quadrat in K genau dann, wenn $p^n \equiv 1 \mod 4$ ist.

Lösung:

(a) Da alle endlichen Körper perfekt sind, ist die Frobenius-Endomorphismus Frob_p bijektiv. Im Fall $p = 2$ ist dieser gleich der Quadratabbildung.

(b) Sei $Q := \{a^2 \mid a \in K\}$ die Menge aller Quadrate in K. Diese ist die Vereinigung von $\{0\}$ mit dem Bild des Homomorphismus $K^\times \to K^\times$, $x \mapsto x^2$. Der Kern dieses Homomorphismus ist $\{\pm 1\}$ und hat daher die Ordnung $\leqslant 2$. Das Bild des Homomorphismus hat daher die Ordnung $\geqslant \frac{p^n-1}{2}$. Somit gilt $|Q| \geqslant \frac{p^n+1}{2}$. Für jedes $x \in K$ betrachte nun die Menge $x-Q := \{x-q \mid q \in Q\}$. Für diese gilt wieder $|x - Q| \geqslant \frac{p^n+1}{2}$, und daraus folgt

$$|Q \cap (x-Q)| \;=\; |Q| + |x-Q| - |Q \cup (x-Q)| \;\geqslant\; \tfrac{p^n+1}{2} + \tfrac{p^n+1}{2} - |K| \;\geqslant\; 1.$$

Also ist $Q \cap (x - Q)$ nicht leer. Somit existieren $a, b \in K$ mit $b^2 = x - a^2$, oder anders gesagt $x = a^2 + b^2$.

(c) Wegen $p > 2$ ist $-1 \neq 1$ in K, und wegen $(-1)^2 = 1$ ist -1 daher ein Element der Ordnung 2 in $K^\times$. Nun ist $K^\times$ zyklisch der Ordnung $p^n - 1$ und daher isomorph zu $\mathbb{Z}/(p^n - 1)\mathbb{Z}$. Ausserdem entspricht das Element $-1 \in K^\times$ für jeden Isomorphismus der Restklasse $[\frac{p^n-1}{2}] \in \mathbb{Z}/(p^n - 1)\mathbb{Z}$. Somit ist -1 ein Quadrat in K genau dann, wenn $[\frac{p^n-1}{2}] \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ ein Vielfaches von 2 ist. Dies ist genau dann der Fall, wenn $\frac{p^n-1}{2}$ gerade ist, das heisst, wenn $p^n \equiv 1 \mod 4$ ist.

5. Zeige, dass eine Primzahl $p > 2$ genau dann als Summe zweier Quadrate in $\mathbb{Z}$ geschrieben werden kann, wenn $p \equiv 1 \mod 4$ ist.

Hinweis: Untersuche die Primfaktorzerlegung von p in $\mathbb{Z}[i]$. Siehe auch Serie 13, Aufgabe 2.

Lösung: Wir wissen bereits, dass $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z} \cdot i$ ist, und nach Aufgabe 2 von Serie 13 ist dies ein euklidischer Ring mit der multiplikativen Norm $N(a+bi) := a^2 + b^2$. Insbesondere ist er faktoriell. Ausserdem gilt

$$\mathbb{Z}[i]^\times \;=\; \{x \in \mathbb{Z}[i] \mid N(x) = 1\} \;=\; \{\pm 1, \pm i\}.$$

Zuerst sei $p \equiv 1 \mod 4$. Nach obiger Aufgabe 5 (c) ist dann $-1 \in \mathbb{F}_p^\times$ ein Quadrat. Also existiert $c \in \mathbb{Z}$ mit $p|(c^2 + 1)$. Andererseits ist $c \pm i \notin p \cdot \mathbb{Z}[i]$ und daher $p \nmid (c \pm i)$. Wegen $c^2 + 1 = (c + i)(c - i)$ ist p daher kein Primelement in $\mathbb{Z}[i]$. Da es ausserdem keine Einheit ist und $\mathbb{Z}[i]$ faktoriell ist, besitzt p daher eine Primfaktorzerlegung der Länge > 1. Schreibe $p = ef$ mit Nicht-Einheiten $e, f \in \mathbb{Z}[i]$. Dann gilt $N(e) \cdot N(f) = N(ef) = N(p) = p^2$ und $N(e)$, $N(f) > 1$, was nur möglich ist mit $N(e) = p$. Schreiben wir $e = a + bi$ mit $a, b \in \mathbb{Z}$, so erhalten wir nun $p = N(e) = a^2 + b^2$, also ist p wie gewünscht eine Summe zweier Quadrate.

Sei nun $p \equiv 3 \mod 4$. Nach Aufgabe 2 von Serie 13 ist p dann prim in $\mathbb{Z}[i]$. Existierten $a, b \in \mathbb{Z}$ mit $a^2 + b^2 = p$, so wäre $(a+ib)(a-ib) = p$ eine Faktorisierung von p. Da $N(a+ib) = N(a-ib) = p$ gälte, wären beide Faktoren keine Einheiten, ein Widerspruch.