Aufgabe 1 (Herbst 2003)**.** Es seien p und q Primzahlen. Warum zerfällt das Polynom

$$f = X^{p^q} - X$$

über dem Körper $\mathbb{F}_p$ mit p Elementen in p verschiedene Faktoren vom Grad 1 und $\frac{p^q-p}{q}$ verschiedene irreduzible Faktoren vom Grad q?
Hinweis: Die Faktoren müssen nicht angegeben werden! Zum Einstieg in die Aufgabe überlege man, daß die Nullstellen von f einen Körper bilden.

Lösung. Betrachte $f = X^{p^q} - X \in \mathbb{F}_p[X]$. Wir wissen bereits, daß die Menge der Nullstellen von f in einem algebraischen Abschluß einen Körper mit p^q Elementen $\mathbb{F}_{p^q}$ bilden. Unter diesen Nullstellen befinden sich bereits die Elemente von $\mathbb{F}_p$, also $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Das heißt f spaltet die entsprechenden Linearfaktoren ab, und wir können eine Zerlegung von f in irreduzible Polynome angeben als

$$f = X(X-\overline{1})\cdots(X-\overline{p-1})g_1\cdots g_r.$$

Da $\mathbb{F}_p[X]$ ein euklidischer Ring bezüglich der Gradabbildung ist, gilt aus Gradgründen $\deg(g_1\cdots g_r) = p^q - p$. Es bleibt also zu zeigen, daß $\deg(g_i) = q$ für alle $i = 1, \ldots, r$ und damit folgt automatisch $r = \frac{p^q-p}{q}$. Sei α Nullstelle eines g_i, dann ist

$$\mathbb{F}_p \subsetneq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^q}$$

ein Zwischenkörper mit $\alpha \notin \mathbb{F}_p$. Da aber der Grad $[\mathbb{F}_{p^q} : \mathbb{F}_p] = q$ ist, und q eine Primzahl ist, folgt

$$\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^q}$$

für jede Nullstelle eines der g_i. Es folgt, daß $\deg(g_i) = q$ für alle i.

Aufgabe 2 (Frühjahr 2007)**.** Betrachten Sie den endlichen Körper $\mathbb{F}_5$ mit funf Elementen, das Polynom $f(X) = X^3 + X + 1 \in \mathbb{F}_[X]$ und den Quotientenring $K = \mathbb{F}_5[X]/f((X))$. Weiter bezeichne α die Restklasse von X modulo $(f(X))$.

(a) Zeigen Sie, daß K eine Körper mit 125 Elementen und daß $(1, \alpha, \alpha^2)$ eine $\mathbb{F}_5$-Basis von K ist.

(b) Bestimmen Sie die Matrix $M \in \mathbf{GL}_3(\mathbb{F}_5)$, die den Frobenius-Automorphismus $F : K \to K$, $x \mapsto x^5$ bezüglich der Basis $(1, \alpha, \alpha^2)$ darstellt.

(c) Bestimmen Sie eine Basis für den Eigenraum von F zum Eigenwert 1.

Lösung. **Zu (a):** Das Polynom f hat Grad 3 und keine Nullstelle in $\mathbb{F}_5$:

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 1, \quad f(3) = 1, \quad f(4) = 4.$$

Also ist es irreduzibel in $\mathbb{F}_5[X]$. Damit ist das von f erzeugte Ideal (f) ein Primideal und da $\mathbb{F}_5[X]$ ein Hauptidealring ist, ist es auch maximal. Folglich ist $\mathbb{F}_5[X]/(f)$ eine Körper.
Da $\alpha = X \mod (f)$ ist, gilt $\alpha^3 + \alpha + 1 = 0$, das heißt

$$\alpha^3 = -\alpha - 1.$$

Sei $a_nX^n + \ldots + a_1X + a_0 + (f) = a_n\alpha^n + \ldots + a_1\alpha + a_0 \in K$ ein beliebiges Element mit $n \geqslant 3$. Durch Substitution erhält man

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = a_n\alpha^{n-3}(-\alpha - 1) + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0$$

also einen Ausdruck in dem die höchste vorkommende Potenz von α (mindestens) um eins kleiner ist. Induktiv erhält man so einen Ausdruck in dem die höchste Potenz von α maximal zwei ist. Es folgt also, daß sich jedes Element in $\mathbb{F}_5[X]/(f)$ als Polynom in α von Grad höchstens 2 darstellen lässt. Das heißt jedes Element hat eine Darstellung der Form

$$a_2\alpha^2 + a_1\alpha + a_0,$$

mit $a_0, a_1, a_2 \in \mathbb{F}_5$. Und damit ist $(1, \alpha, \alpha^2)$ ein Erzeugendensystem des $\mathbb{F}_5$-Vektorraums $\mathbb{F}_5[X]/(f)$.

Wir zeigen noch, daß es auch linear unabhänging ist. Sei also

$$a_2\alpha^2 + a_1\alpha + a_0 = 0.$$

Das bedeutet $g := a_2X^2+a_1X+a_0 \in (f)$, insbesondere ist f ein Teiler von g. Da $\deg(f) = 3$, aber $\deg(g) \leqslant 2$, ist $g = 0$, also $a_2 = a_1 = a_0 = 0$.

Zu (b): Wir müssen den Frobenius auf der Vektorraumbasis $(1, \alpha, \alpha^2)$ bestimmen und dies wieder in der Basis ausdrücken. Man beachte, daß seine Einschränkung auf $\mathbb{F}_5$ die Identität ist $F|_{\mathbb{F}_5} = \mathrm{id}_{\mathbb{F}_5}$.

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

Wir lesen die darstellende Matrix ab

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

Zu (c): Der Eigenraum für den Eigenwert 1, ist genau der Unterraum, auf dem der Frobenius als Identität operiert. Dies ist nur für den Grundkörper $\mathbb{F}_5$ der Fall, also für den Unterraum, der von der 1 erzeugt wird. Dies ist bereits eine Basis.

Alternative: Es ist klar, daß 1 ein Eigenwert der Matrix M ist. (Das charakteristische Polynom ist $\chi_M = (X-1)(X^2-4X-9) = (X-1)(X^2+X+1)$ und X^2+X+1 ist irreduzibel. Also ist 1 der einzige Eigenwert und hat Vielfachheit 1. Der Eigenraum dazu ist eindimensional und wird von der Basis $(1, 0, 0)$ aufgespannt bezüglich der Basis $(1, \alpha, \alpha^2)$, das heißt 1 ist eine Basis.

Aufgabe 3 (Frühjahr 2007)**.** Sei $K = \{0, 1\}$ der Körper mit zwei Elementen, und sei E ein Erweiterungskörper von K mit $|E| = 2^8$ Elementen.
Wieviele primitive Elemente besitzt E? Begründen Sie Ihre Antwort.

Lösung. Der Körper E ist isomorph zu $\mathbb{F}_{2^8}$. Es genügt all die Aufgabe für $\mathbb{F}_{2^8}$ zu beantworten. Ein Element von $\mathbb{F}_{2^8}$ ist genau dann primitiv, wenn es in keinem echten Unterkörper enthalten ist. Die Erweiterung $\mathbb{F}_{2^8}/\mathbb{F}_2$ hat Grad 8. Nach der Gradformel gilt für jeden Zwischenkörper $\mathbb{F}_2 \subset L \subset \mathbb{F}_{2^8}$ daß $[L : \mathbb{F}_2] | 8$. Also sind die Zwischen körper genau

$$\mathbb{F}_2 \subsetneq \mathbb{F}_{2^2} \subsetneq \mathbb{F}_{2^4} \subsetneq \mathbb{F}_{2^8}.$$

Die Zahl der primitiven Elemente ist also

$$|\mathbb{F}_{2^8}| - |\mathbb{F}_{2^4}| = 2^8 - 2^4 = 256 - 16 = 240.$$

Aufgabe 4 (Herbst 1999)**.** Der Körper K enthalte einen endlichen Teilkörper, der aus den n Elementen $a_1, \ldots, a_n$ bestehe. Man beweise: Für jedes Element $a \in K$ gilt

$$a^n - a = \prod_{i=1}^{n}(a - a_i).$$

Lösung. Sei $k = \{a_1, \ldots, a_n\} \subset K$. Da k ein endlicher Körper ist, gibt es eine Primzahl p und $r \in \mathbb{N}$ mit $k \cong \mathbb{F}_{p^r}$. Insbesondere ist $n = p^r$. Der endliche Körper $\mathbb{F}_{p^r}$ ist Zerfällungskörper des Polynoms $X^{p^r} - X$ über $\mathbb{F}_p$, die Elemente von $\mathbb{F}_{p^r}$ sind Nullstellen dieses Polynoms. Also sind in K die Elemente $a_1, \ldots a_n$ Nullstellen des Polynoms $X^{p^r} - X$ und es zerfällt

$$X^n - X = \prod_{i=1}^{n}(X - a_i).$$

Einsetzen eines beliebigen Elements $a \in K$ ergibt

$$a^n - a = \prod_{i=1}^{n}(a - a_i)$$

wie gewünscht.