

Lösung 14

Aufgabe 56.

- (1) Schreibe $\mu_{a,K}(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in E[X]$, mit $\alpha_i := \sigma_i(a)$ paarweise verschieden, was wegen $E|K$ galoisch möglich ist. Nach der Produktregel ist $\mu'_{a,K}(X) = (X - \alpha_2) \cdots (X - \alpha_n) + (X - \alpha_1)h(X)$ für ein $h(X) \in E[X]$. Somit wird wegen $a = \alpha_1$

$$\mu'_{a,K}(a) = (a - \alpha_2) \cdots (a - \alpha_n),$$

und also

$$f(X) = \frac{(X - \alpha_2) \cdots (X - \alpha_n)}{(a - \alpha_2) \cdots (a - \alpha_n)}.$$

Insbesondere sehen wir nun, daß $f(a) = 1$ und $f^{\sigma_i}(a) = \sigma_i(f(\sigma_i^{-1}(a))) = \sigma_i(f(\alpha_{i'})) = 0$, wobei $\sigma_{i'} := \sigma_i^{-1}$.

- (2) Seien $i, j \in [1, n]$, und sei $i \neq j$.

Der Eintrag der Matrix $\left(f^{\sigma_i^{-1} \circ \sigma_j}(a)\right)_{i, j \in [1, n]}$ an Position (i, i) ist $f(a) = 1$ nach (1).

Der Eintrag der Matrix $\left(f^{\sigma_i^{-1} \circ \sigma_j}(a)\right)_{i, j \in [1, n]}$ an Position (i, j) ist $f^{\sigma_i \circ \sigma_j^{-1}}(a) = f^{\sigma_k}(a) = 0$, da mit $\sigma_k := \sigma_i \circ \sigma_j^{-1}$ sicher $k \in [2, n]$ liegt, womit das Resultat aus (1) folgt.

Da nun $d(a) \neq 0$, kann $d(X) \in E[X]$ nicht gleich 0 sein.

- (3) Es hat $d(X) \in E[X]$ als Polynom von Grad $\leq n(n-1)$ höchstens $n(n-1)$ verschiedene Nullstellen in E , und a fortiori nur endlich viele Nullstellen in K . Somit können wir uns ein $b \in K$ mit $d(b) \neq 0$ wählen. Sei $c := f(b)$. Wir behaupten, daß

$$(\sigma_1(c), \dots, \sigma_n(c))$$

linear unabhängig ist über K , und damit eine Basis von E über K , eine sogenannte *Normalbasis*.

Seien $\lambda_1, \dots, \lambda_n \in K$ mit

$$\lambda_1 \sigma_1(c) + \cdots + \lambda_n \sigma_n(c) = 0$$

gegeben. Wir haben zu zeigen, daß alle λ_i verschwinden. Anwendung von σ_i^{-1} gibt, daß

$$\begin{aligned} 0 &= \sigma_i^{-1}(\lambda_1 \sigma_1(c) + \cdots + \lambda_n \sigma_n(c)) \\ &= \lambda_1 (\sigma_i^{-1} \circ \sigma_1)(f(b)) + \cdots + \lambda_n (\sigma_i^{-1} \circ \sigma_n)(f(b)) \\ &= \lambda_1 f^{\sigma_i^{-1} \circ \sigma_1}(b) + \cdots + \lambda_n f^{\sigma_i^{-1} \circ \sigma_n}(b) \end{aligned}$$

für alle $i \in [1, n]$, wobei im letzten Schritt zu beachten ist, daß $b \in K \subseteq E$ gewählt wurde und damit unter allen Automorphismen über K fest bleibt. Nun zeigt die Invertierbarkeit der Matrix $\left(f^{\sigma_i^{-1} \circ \sigma_j}(b)\right)_{i, j \in [1, n]}$, welche aus $d(b) \neq 0$ resultiert, daß in der Tat $\lambda_1 = \cdots = \lambda_n = 0$.

- (4) Man kann nun entweder wie in (2, 3) zunächst $d(X)$ bestimmen, sowie ein b aus dem Grundkörper, welches keine Nullstelle von d darstellt. Oder aber, man vertraut auf sein Geschick und findet ein passendes c durch Probieren – das ist meist schneller.

- (i) Mit $a = i$ wird $f(X) = (X+i)/(2i) \in \mathbf{C}[X]$, und somit $d(X) = -iX$. Sei also z.B. $b = 1$, und somit $f(b) = \frac{1+i}{2i}$. Wir können einen solchen Normalbasiserzeuger durch ein \mathbf{R} -Vielfaches ersetzen, und somit stattdessen z.B. $c := 2f(b) = 1 - i$ wählen. Und in der Tat ist $(\sigma_1(c), \sigma_2(c)) = (1 - i, 1 + i)$ eine \mathbf{R} -Basis von \mathbf{C} .

- (ii) Schreibe $\zeta := \zeta_8$ und bezeichne $\sigma_1 := \text{id} : \zeta \mapsto \zeta$, $\sigma_2 : \zeta \mapsto \zeta^3$, $\sigma_3 : \zeta \mapsto \zeta^5 = -\zeta$ und $\sigma_4 : \zeta \mapsto \zeta^7 = -\zeta^3$. Verwende $a = \zeta$. Stellen wir zunächst einmal fest, daß $(\zeta^1, \zeta^3, \zeta^5, \zeta^7)$ linear abhängig über \mathbf{Q} ist, da z.B. $\zeta^1 + \zeta^5 = 0$.

Es wird

$$f(X) = \frac{(X - \zeta^3)(X - \zeta^5)(X - \zeta^7)}{(\zeta - \zeta^3)(\zeta - \zeta^5)(\zeta - \zeta^7)} = \frac{X^3 + \zeta X^2 + \zeta^2 X + \zeta^3}{4\zeta^3},$$

und

$$\begin{aligned}
 d(X) &= 4^{-4} \cdot \det \begin{pmatrix} 1-\zeta^3 X - \zeta^2 X^2 - \zeta^1 X^3 & 1-\zeta^1 X + \zeta^2 X^2 - \zeta^3 X^3 & 1+\zeta^3 X - \zeta^2 X^2 + \zeta^1 X^3 & 1+\zeta^1 X + \zeta^2 X^2 + \zeta^3 X^3 \\ 1-\zeta^1 X + \zeta^2 X^2 - \zeta^3 X^3 & 1-\zeta^3 X - \zeta^2 X^2 - \zeta^1 X^3 & 1+\zeta^1 X + \zeta^2 X^2 + \zeta^3 X^3 & 1+\zeta^3 X - \zeta^2 X^2 + \zeta^1 X^3 \\ 1+\zeta^3 X - \zeta^2 X^2 + \zeta^1 X^3 & 1+\zeta^1 X + \zeta^2 X^2 + \zeta^3 X^3 & 1-\zeta^3 X - \zeta^2 X^2 - \zeta^1 X^3 & 1-\zeta^1 X + \zeta^2 X^2 - \zeta^3 X^3 \\ 1+\zeta^1 X + \zeta^2 X^2 + \zeta^3 X^3 & 1+\zeta^3 X - \zeta^2 X^2 + \zeta^1 X^3 & 1-\zeta^1 X + \zeta^2 X^2 - \zeta^3 X^3 & 1-\zeta^3 X - \zeta^2 X^2 - \zeta^1 X^3 \end{pmatrix} \\
 &= \frac{1}{2}(X^8 - X^4).
 \end{aligned}$$

Verwendbar ist also jedes $b \in \mathbf{Q} \setminus \{-1, 0, 1\}$. Nehmen wir $b = 2$, und als ein rationales Vielfaches von $f(b)$ erhalten wir $c := 4f(b) = -2\zeta^3 - 4\zeta^2 - 8\zeta + 1$, und somit die Normalbasis

$$(-2\zeta^3 - 4\zeta^2 - 8\zeta + 1, -2\zeta + 4\zeta^2 - 8\zeta^3 + 1, 2\zeta^3 - 4\zeta^2 + 8\zeta + 1, 2\zeta + 4\zeta^2 + 8\zeta^3 + 1).$$

- (iii) Zunächst halten wir die Basis $(1, X_3, X_3^2, X_2, X_2X_3, X_2X_3^2)$ von $\mathbf{Q}(X_1, X_2, X_3)$ über $\mathbf{Q}(s_1, s_2, s_3)$ fest. Um ein geeignetes c zu finden, hilft hier sinnvolles Probieren. Wir behaupten, daß mit $c = X_2X_3^2$ das aus der \mathcal{S}_3 -Bahn dieses Elementes bestehende Tupel

$$(X_2X_3^2, X_3X_2^2, X_1X_3^2, X_3X_1^2, X_1X_2^2, X_2X_1^2)$$

eine Normalbasis von $\mathbf{Q}(X_1, X_2, X_3)$ über $\mathbf{Q}(s_1, s_2, s_3)$ darstellt. Dazu verwenden wir die wie in 54 (1) hergeleiteten Relationen

$$\begin{aligned}
 X_1 &= s_1 - X_3 - X_2 \\
 X_2^2 &= -s_2 + s_1X_3 - X_3^2 + s_1X_2 - X_2X_3 \\
 X_3^3 &= s_1X_3^2 - s_2X_3 + s_3 \\
 X_1^2 &= (s_1^2 - s_2) - s_1X_3 - s_1X_2 + X_2X_3. \\
 X_3^2 &= (-s_1s_2 + s_3) + s_1^2X_3 - s_1X_3^2 + (s_1^2 - s_2)X_2 - s_1X_2X_3
 \end{aligned}$$

Vorstehendes Tupel berechnet sich in der gewählten Basis zu

$$\begin{aligned}
 &(X_2X_3^2, -s_3 + s_1X_2X_3 - X_2X_3^2, -s_3 + s_2X_3 - X_2X_3^2, (s_1^2 - s_2)X_3 - s_1X_3^2 - s_1X_2X_3 + X_2X_3^2, \\
 &s_2X_2 - s_1X_2X_3 + X_2X_3^2, (s_1s_2 - s_3) - s_1^2X_3 + s_1X_3^2 - s_2X_2 + s_1X_2X_3 - X_2X_3^2),
 \end{aligned}$$

was der invertierbaren Matrix

$$\begin{pmatrix} 0 & -s_3 & -s_3 & 0 & 0 & s_1s_2 - s_3 \\ 0 & 0 & s_2 & s_1^2 - s_2 & 0 & -s_1^2 \\ 0 & 0 & 0 & -s_1 & 0 & s_1 \\ 0 & 0 & 0 & 0 & s_2 & -s_2 \\ 0 & s_1 & 0 & -s_1 & -s_1 & s_1 \\ 1 & -1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

entspricht. (Ihre Determinante ist übrigens $s_1^2s_2^2(3s_3 - s_1s_2)$.)

Ist für die analoge Frage in n Variablen $c = X_1^0X_2^1 \cdots X_n^{n-1}$ eine geeignete Wahl?

Aufgabe 57.

- (1) Es wird

$$\begin{aligned}
 \beta^0 &= 1 \\
 \beta^1 &= \beta \\
 \beta^2 &= \beta^2 \\
 \beta^3 &= 1 + \beta \\
 \beta^4 &= \beta + \beta^2 \\
 \beta^5 &= 1 + \beta + \beta^2 \\
 \beta^6 &= 1 + \beta^2 \\
 \beta^7 &= 1.
 \end{aligned}$$

(2) Wir können unsere Kandidatenliste wie folgt verkürzen.

Der konstante Koeffizient eines irreduziblen Polynoms ist ungleich 0.

Der Frobenius-Automorphismus $F : \mathbf{F}_8 \longrightarrow \mathbf{F}_8, \xi \longmapsto \xi^2$, koeffizientenweise angewandt, bildet ein irreduzibles Polynom auf ein irreduzibles Polynom ab. Die Frobenius-Bahnen in \mathbf{F}_8 sind $\{0\}, \{1\}, \{\beta, \beta^2, \beta + \beta^2\}, \{1 + \beta, 1 + \beta^2, 1 + \beta + \beta^2\}$.

Ein Polynom der Form $X^2 + u$ mit $u \in \mathbf{F}_8$ ist nicht irreduzibel, da es ein $v \in \mathbf{F}_8$ mit $v^2 = u$ gibt, und somit $(X + v)^2 = X^2 + u$ ist.

Unter Zuhilfenahme dieser Tatsachen führen wir einen Nullstellentest durch. Ein Polynom von Grad 2 ohne Nullstelle ist irreduzibel. Es genügt wegen Frobenius, Polynome der Form $X^2 + X + \xi, X^2 + \beta X + \xi$ und $X^2 + (1 + \beta)X + \xi$ mit $\xi \in \mathbf{F}_8$ zu betrachten.

- Das Polynom $X^2 + X$ nimmt die Werte $\{0, \beta, \beta^2, \beta + \beta^2\}$ an.
Somit ist $X^2 + X + 1$ irreduzibel.
Ferner ist $X^2 + X + (1 + \beta)$ irreduzibel, und damit auch die anderen Elemente seiner Frobenius-Bahn, nämlich $X^2 + X + (1 + \beta^2)$ und $X^2 + X + (1 + \beta + \beta^2)$.
- Das Polynom $X^2 + \beta X$ nimmt die Werte $\{0, 1 + \beta, 1 + \beta^2, \beta + \beta^2\}$ an.
Es ist $X^2 + \beta X + 1$ irreduzibel, und damit sind dies auch $X^2 + \beta^2 X + 1$ und $X^2 + (\beta + \beta^2)X + 1$.
Es ist $X^2 + \beta X + \beta$ irreduzibel, und damit sind dies auch $X^2 + \beta^2 X + \beta$ und $X^2 + (\beta + \beta^2)X + (\beta + \beta^2)$.
Es ist $X^2 + \beta X + \beta^2$ irreduzibel, und damit sind dies auch $X^2 + \beta^2 X + (\beta + \beta^2)$ und $X^2 + (\beta + \beta^2)X + \beta$.
Es ist $X^2 + \beta X + (1 + \beta + \beta^2)$ irreduzibel, und damit sind dies auch $X^2 + \beta^2 X + (1 + \beta)$ und $X^2 + (\beta + \beta^2)X + (1 + \beta^2)$.
- Das Polynom $X^2 + (1 + \beta)X$ nimmt die Werte $\{0, 1, \beta, 1 + \beta\}$ an.
Es ist $X^2 + (1 + \beta)X + \beta^2$ irreduzibel, und damit sind dies auch $X^2 + (1 + \beta^2)X + (\beta + \beta^2)$ und $X^2 + (1 + \beta + \beta^2)X + \beta$.
Es ist $X^2 + (1 + \beta)X + (1 + \beta^2)$ irreduzibel, und damit sind dies auch $X^2 + (1 + \beta^2)X + (1 + \beta + \beta^2)$ und $X^2 + (1 + \beta + \beta^2)X + (1 + \beta)$.
Es ist $X^2 + (1 + \beta)X + (\beta + \beta^2)$ irreduzibel, und damit sind dies auch $X^2 + (1 + \beta^2)X + \beta$ und $X^2 + (1 + \beta + \beta^2)X + \beta^2$.
Es ist $X^2 + (1 + \beta)X + (1 + \beta + \beta^2)$ irreduzibel, und damit sind dies auch $X^2 + (1 + \beta^2)X + (1 + \beta)$ und $X^2 + (1 + \beta + \beta^2)X + (1 + \beta^2)$.

Insgesamt erhalten wir $28 = (8^{(2^1)} - 8^{(2^0)}) \cdot 2^{-1}$ irreduzible Polynome von Grad 2, in Übereinstimmung mit 58 (2).

Sei nun z.B. $\mathbf{F}_{64} := \mathbf{F}_8(\alpha) = \mathbf{F}_2(\alpha, \beta)$ mit $\alpha^2 + \alpha + 1 = 0$.

(3) Sei α wie in (2). Die echten Zwischenkörper von \mathbf{F}_2 und \mathbf{F}_{64} ergeben sich zu

$$\begin{aligned} \mathbf{F}_8 &= \mathbf{F}_2(\beta) \\ \mathbf{F}_4 &= \mathbf{F}_2(\alpha) \end{aligned}$$

Man erhält z.B. $\beta = \alpha\beta + (\alpha\beta)^8$ und $\alpha = \alpha + \alpha^4 + \alpha^{16}$ auch über die jeweilige Spur.

(4) Wir verwenden das irreduzible Polynom $X^3 + X + \beta$ zur Konstruktion von $\mathbf{F}_{512} := \mathbf{F}_8(\gamma)$ mit $\gamma^3 = \gamma + \beta$.

Die Frobenius-Bahn des Elements γ über \mathbf{F}_2 ist gegeben durch

$$\{\gamma, \gamma^2, \gamma^4, \gamma^8, \gamma^{16}, \gamma^{32}, \gamma^{64}, \gamma^{128}, \gamma^{256}\} = \{\gamma, \gamma^2, \beta\gamma + \gamma^2, \beta\gamma + \gamma^2 + \beta^2\gamma^2, \gamma + \beta^2\gamma + \gamma^2 + \beta\gamma^2, \gamma + \beta\gamma^2, \gamma + \beta\gamma + \gamma^2 + \beta^2\gamma^2, \gamma + \beta^2\gamma + \beta\gamma^2, \gamma + \beta\gamma + \gamma^2 + \beta\gamma^2\}.$$

In anderen Worten, dieses Element bleibt unter keinem nichtidentischen Automorphismus von \mathbf{F}_{512} über \mathbf{F}_2 fest, und liegt folglich in keinem echten Teilkörper von \mathbf{F}_{512} . Sein Minimalpolynom bestimmt sich über die Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

deren Spalten die Potenzen von γ durchlaufen, zu

$$\mu_{\gamma, \mathbf{F}_2}(X) = X^9 + X^7 + X^5 + X + 1.$$

Dies ist ein irreduzibles Polynom von Grad 9 in $\mathbf{F}_2[X]$.

Aufgabe 58.

- (1) Es ist $\text{Gal}(\mathbf{F}_{q^{(l^m)}}|\mathbf{F}_q) = \langle F \rangle \simeq C_{l^m}$, wobei $F : \mathbf{F}_{q^{(l^m)}} \rightarrow \mathbf{F}_{q^{(l^m)}}$, $x \mapsto F(x) := x^q$ den Frobenius-Automorphismus bezeichnet. Es gibt in $\langle F \rangle$ genau die $m + 1$ Untergruppen $U_k := \langle F^{l^{m-k}} \rangle \simeq C_{l^k}$ für $k \in [0, m]$. Somit gibt es genau $m + 1$ Zwischenkörper, nämlich $\text{Fix}_{U_k} \mathbf{F}_{q^{(l^m)}} = \mathbf{F}_{q^{(l^{m-k})}}$ für $k \in [0, m]$.
- (2) Jedes normierte irreduzible Polynom von Grad l^m in $\mathbf{F}_q[X]$ tritt als Minimalpolynom über \mathbf{F}_q von genau l^m Elementen von $\mathbf{F}_{q^{(l^m)}} \setminus \mathbf{F}_{q^{(l^{m-1})}}$ auf (vgl. 59 (1)), und zwei verschiedene irreduzible Polynome haben keine gemeinsame Nullstelle ξ in $\mathbf{F}_{q^{(l^m)}}$, da sonst $(X - \xi)$ den ggT dieser beiden Polynome, genommen in $\mathbf{F}_q[X]$, in $\mathbf{F}_{q^{(l^m)}}[X]$ teilen würde, im Widerspruch zur Teilerfremdheit.

Elemente in $\mathbf{F}_{q^{(l^m)}} \setminus \mathbf{F}_{q^{(l^{m-1})}}$ gibt es gerade $q^{(l^m)} - q^{(l^{m-1})}$ Stück, und je l^m teilen sich ein Minimalpolynom. Also gibt es

$$(q^{(l^m)} - q^{(l^{m-1})})l^{-m} = (q^{l^{m-1}(l-1)} - 1)q^{l^{m-1}}l^{-m}$$

normierte irreduzible Polynome von Grad l^m in $\mathbf{F}_q[X]$.

- (3) Zunächst bemerken wir, daß wegen $(X^{q^{(l^m)}} - X)' = -1$ das Polynom $X^{q^{(l^m)}} - X$ in seinem Zerfällungskörper $\mathbf{F}_{q^{(l^m)}}$ gerade $q^{(l^m)}$ verschiedene Nullstellen besitzt, nämlich alle Elemente von $\mathbf{F}_{q^{(l^m)}}$. Nach der Bemerkung aus (2) zerfällt $X^{q^{(l^m)}} - X$ somit in ein Produkt paarweise verschiedener irreduzibler Polynome.

Jedes normierte irreduzible Polynom von Grad l^k für ein $k \in [0, m]$ zerfällt in $\mathbf{F}_{q^{(l^m)}}[X]$ in Linearfaktoren (cf. 59 (1)), und ist somit ein Teiler von $X^{q^{(l^m)}} - X$ in $\mathbf{F}_{q^{(l^m)}}[X]$, und dies dann auch bereits in $\mathbf{F}_q[X]$, wie Polynomdivision zeigt.

Umgekehrt ist ein normierter irreduzibler Faktor von $X^{q^{(l^m)}} - X$ das Minimalpolynom eines Elements in $\mathbf{F}_{q^{(l^m)}}$, und als solches von Grad l^k für ein $k \in [0, m]$, da besagtes Element über \mathbf{F}_q einen Zwischenkörper zwischen \mathbf{F}_q und $\mathbf{F}_{q^{(l^m)}}$ erzeugt.

Von Grad l^k gibt es nach (2) gerade $(q^{(l^k)} - q^{(l^{k-1})})l^{-k}$ normierte irreduzible Polynome falls $k \geq 1$. Von Grad $1 = l^0$ gibt es noch q normierte irreduzible Polynome.

Also erhalten wir insgesamt

$$q + \sum_{k \in [1, m]} (q^{l^k} - q^{l^{k-1}})l^{-k}$$

irreduzible Faktoren von $X^{q^{(l^m)}} - X$ in $\mathbf{F}_q[X]$.

Aufgabe 59.

- (1) Die Aussage ist richtig, wie man z.B. wie folgt begründen kann. Sei K der Wurzelkörper von $f(X)$. Wegen $|K| = q^n$ gilt $\xi^{q^n} - \xi = 0$ für alle $\xi \in K$, und somit zerfällt $X^{q^n} - X$ in $K[X]$ in q^n verschiedene Linearfaktoren. Da $f(X)$ das Minimalpolynom eines Elementes von K , d.h. einer der Nullstellen von $X^{q^n} - X$, ist, teilt $f(X)$ das Polynom $X^{q^n} - X$ in $\mathbf{F}_q[X]$, und zerfällt somit seinerseits in n verschiedene Linearfaktoren in $K[X]$. Da K von einer Nullstelle von $f(X)$ erzeugt wird, und da sowohl $f(X)$ als auch $X^{q^n} - X$ in $K[X]$ in Linearfaktoren zerfallen, ist K Zerfällungskörper sowohl von $f(X)$ als auch von $X^{q^n} - X$. Nun ist aber auch \mathbf{F}_{q^n} (konstruiert auf eine beliebig gewählte Weise) Zerfällungskörper von $X^{q^n} - X$, und somit isomorph zu K über \mathbf{F}_q . Also zerfällt $f(X)$ auch in $\mathbf{F}_{q^n}[X]$ in n verschiedene Linearfaktoren, hat also n verschiedene Nullstellen.
- (2) Die Aussage ist falsch. Wir zeigen dazu allgemeiner für einen Körper K , daß ein algebraisches Element von $K(X)$ notwendig bereits in K liegt. Dies zeigt dann die benötigte Aussage, denn gäbe es einen Teilkörper von $\mathbf{F}_q(X)$ isomorph zu \mathbf{F}_{q^2} , so gäbe es auch ein Element in $\mathbf{F}_q(X)$, welches im isomorphen Bild von \mathbf{F}_{q^2} , nicht aber in \mathbf{F}_q läge, und welches somit algebraisch über \mathbf{F}_q wäre, was aber nicht sein kann.

Sei also $\frac{f(X)}{g(X)} \in K(X)$ mit $f(X), g(X) \in K[X] \setminus \{0\}$ teilerfremd (der Fall $f(X) = 0$ ist ohnehin klar), und sei

$$a_n \left(\frac{f(X)}{g(X)} \right)^n + \dots + a_0 \left(\frac{f(X)}{g(X)} \right)^0 = 0,$$

mit $a_i \in K$ für $i \in [0, n]$. Wir dürfen $a_n \neq 0$ und $a_0 \neq 0$ annehmen.

Aus

$$-a_0 g(X)^n = f(X) \left(\sum_{i \in [1, n]} a_i f(X)^{i-1} g(X)^{n-i} \right)$$

folgt, daß jeder irreduzible Faktor von $f(X)$ auch $g(X)$ teilt. Einen solchen irreduziblen Faktor gibt es mithin nicht, und wir erhalten $f(X) \in K \setminus \{0\}$.

Aus

$$-a_n f(X)^n = g(X) \left(\sum_{i \in [0, n-1]} a_i f(X)^i g(X)^{n-1-i} \right)$$

folgt, daß jeder irreduzible Faktor von $g(X)$ auch $f(X)$ teilt. Einen solchen irreduziblen Faktor gibt es mithin nicht, und wir erhalten $g(X) \in K \setminus \{0\}$.

Insgesamt folgt $\frac{f(X)}{g(X)} \in K$.

- (3) Die Aussage ist falsch. Sei z.B. $K = \mathbf{Q}$ und $E = \mathbf{Q}(i)$. Für $x = a + bi \in \mathbf{Q}(i)^*$ mit $a, b \in \mathbf{Q}$ ist $N_{\mathbf{Q}(i)|\mathbf{Q}}(a + bi) = a^2 + b^2 > 0$. Somit ist z.B. $-1 \in \mathbf{Q}^*$, aber nicht im Bild der angegebenen Abbildung, welche damit nicht als nicht surjektiv nachgewiesen ist.