G. Nebe, M. Kirschmer

Lösung 10

Aufgabe 1.

(a) Aus (c) folgt, daß σ_x bijektiv ist. Für $e \in E$ ist $q(\sigma_x(e)) = q(e - \frac{b_q(e,x)}{q(x)}x) = q(e) - \frac{b_q(e,x)}{q(e)} \cdot b_q(e,x) + \frac{b_q(e,x)^2}{q(e)^2} \cdot q(x)^2 = q(e)$. Also ist $\sigma_x \in O(E,q)$. Weiter ist $\sigma_x(x) = x - \frac{b_q(x,x)}{q(x)}x = x - 2x = -x$.

(b) Ist $y \in E$ mit $b_q(x,y) = 0$, so ist $\sigma_x(y) = y - \frac{b_q(y,x)}{q(x)}x = y - 0 \cdot x = y$.

(c) Für $e \in E$ ist

$$\begin{aligned}\sigma_x(\sigma_x(e)) &= \sigma_x(e - \frac{b_q(e,x)}{q(x)}x) = e - \frac{b_q(e,x)}{q(x)}x - \frac{b_q(e - \frac{b_q(e,x)}{q(x)}x, x)}{q(x)}x = e - \frac{b_q(e,x)}{q(x)}x - \frac{b_q(e,x)}{q(x)}x \\ &= e - 2\frac{b_q(e,x)}{q(x)}x + \frac{b_q(e,x)}{q(x)}\frac{b_q(x,x)}{q(x)}x = e - 2\frac{b_q(e,x)}{q(x)}x + 2\frac{b_q(e,x)}{q(x)}x = e\,.\end{aligned}$$

(d) Nach Teil (a) ist $S(E)$ eine Untergruppe von $O(E,q)$. Wir behaupten $g \circ \sigma_x \circ g^{-1} = \sigma_{g(x)}$ für alle $g \in O(E,q)$. Hieraus folgt dann die Behauptung.

Für Für $e \in E$ ist

$$\begin{aligned}(g \circ \sigma_x \circ g^{-1})(e) &= g(g^{-1}(e) - \frac{b_q(g^{-1}(e),x)}{q(x)}x) = e - \frac{b_q(g^{-1}(e),x)}{q(x)}g(x) = e - \frac{b_q(e,g(x))}{q(g(x))}g(x) \\ &= \sigma_{g(x)}(e)\,.\end{aligned}$$

Aufgabe 2.

Sicher ist $\mathrm{ind}(E,q) \in \{0,1\}$. Im Fall $\mathrm{ind}(E,q) = 1$ spaltet also eine hyperbolische Ebene von (E,q) ab, was aus Dimensionsgründen $(E,q) = \mathbb{H}(\mathbb{F}_\ell)$ impliziert.

Sei nun also $\mathrm{ind}(E,q) = 0$. Dann ist $q(e) \neq 0$ für alle $e \in E - \{0\}$. Denn: Ist $q(e) = 0$ mit $e \neq 0$ so ist $\langle e \rangle$ scharf primitiv (da es ein $f \in E$ mit $b_q(e,f) = 1$ geben muss). Es spaltet somit eine hyperbolische Ebene von (E,q) ab (vgl. Bem. 8.29). Dies widerspricht $\mathrm{ind}(E,q) = 0$.
Sei (e,f) eine Basis von E. Dann ist $q(xe+f) = x^2q(e) + b_q(e,f)x + q(f) \neq 0$ für alle $x \in \mathbb{F}_\ell$. Damit ist also $p(X) := X^2 + \frac{b_q(e,f)}{q(e)}X + \frac{q(f)}{q(e)}$ irreduzibel über $\mathbb{F}_\ell$. Wir setzen $K := \mathbb{F}_\ell[X]/p(X)$. Dann ist K eine quadratische Erweiterung von $\mathbb{F}_\ell$ und es existiert ein $\alpha \in K$ mit $p(\alpha) = 0$. Damit ist $p(X) = (X-\alpha)(X-\alpha^\ell)$. Insbesondere ist $\alpha^{\ell+1} = \frac{q(f)}{q(e)}$ und $-\alpha - \alpha^\ell = \frac{b_q(e,f)}{q(e)}$.
Bezeichne $N\colon K \to \mathbb{F}_\ell, z \mapsto z^{\ell+1}$ die zugehörige Norm. Ist $\langle \beta \rangle = K^* \cong C_{\ell^2-1}$, so hat $N(\beta) = \beta^{\ell+1}$ die Ordnung $(\ell^2-1)/(\ell+1) = \ell - 1$; ist also ein Erzeuger von $\mathbb{F}_\ell^*$. Damit ist die Normform $N\colon K \to \mathbb{F}_\ell$ surjektiv. Also existiert ein $\gamma \in K$ mit $N(\gamma) = q(e)$. Mit $(1, -\alpha)$ ist dann auch $(\gamma, -\gamma\alpha)$ linear unabhängig über $\mathbb{F}_\ell$ und es folgt:

$$\begin{aligned}N(\gamma) &= q(e) \\ N(-\gamma\alpha) &= q(e)(-\alpha)^{\ell+1} = q(e)(-1)^{\ell+1} \cdot q(f)/q(e) = q(f) \\ b_N(\gamma, -\gamma\alpha) &= N(\gamma(1-\alpha)) - N(\gamma) - N(-\gamma\alpha) = q(e)(1-\alpha)(1-\alpha)^\ell - q(e) - q(f) \\ &= q(e)(1 - \alpha^\ell - \alpha + \alpha^{\ell+1}) - q(e) - q(f) = b_q(e,f)\end{aligned}$$

Damit ist $\varphi\colon (E,q) \to (K,N),\ xe + yf \mapsto \gamma(x - y\alpha)$ eine bijektive Isometrie zwischen (E,q) und (K,N).

Ist K' eine weitere quadratische Erweiterung von $\mathbb{F}_\ell$ mit zugehöriger Normform N', so existiert ein $\mathbb{F}_\ell$-linearer Isomorphismus $\tau\colon K \to K'$. Dieser erfüllt dann $N'(\tau(x)) = \tau(x)^{\ell+1} = \tau(x^{\ell+1}) = x^{\ell+1} = N(x)$ für alle $x \in K$, da $x^{\ell+1} \in \mathbb{F}_\ell$. Also ist τ eine Isometrie zwischen (K,N) und (K',N').

Aufgabe 3.

Ist (E, q) ein quadratischer K-Vektorraum mit Basis $(b_1, \dots, b_n)$ so liegt $\sigma \in \mathrm{Aut}_K(E)$ genau dann in $O(E, q)$, falls $q(b_i) = q(\sigma(b_i))$ und $b_q(b_i, b_j) = b_q(\sigma(b_i), \sigma(b_j))$ für alle $1 \le i < j \le n$ gelten.
Denn für jedes $e \in E$ ist $q(e)$ eine Linearkombination von $q(b_i)$ und $b_q(b_i, b_j)$ und umgekehrt ist auch $b_q(b_i, b_j) = q(b_i + b_j) - q(b_i) - q(b_j)$.

(a) Sei $H = \mathbb{F}_\ell$ erzeugt von (e, f) mit $b_q(e, f) = 1$ und $q(e) = q(f) = 0$. Dann ist $q(xe + yf) = xy$ für alle $x, y \in \mathbb{F}_\ell$. Insbesondere bildet $\sigma \in O(H)$ die Vektoren e und f auf Elemente in $\{xe \mid x \in \mathbb{F}_\ell^*\} \cup \{yf \mid y \in \mathbb{F}_\ell^*\}$ ab.

Im Fall $\sigma(e) = xe$ mit $x \in \mathbb{F}_\ell^*$ ist $\sigma(f) = yf$ mit $y \in \mathbb{F}_\ell^*$.

Im Fall $\sigma(e) = yf$ mit $y \in \mathbb{F}_\ell^*$ ist $\sigma(f) = xe$ mit $x \in \mathbb{F}_\ell^*$.

In beiden Fällen muß weiter gelten $1 = b_q(e, f) = b_q(\sigma(e), \sigma(f)) = b_q(xe, yf) = xy$ also $y = x^{-1}$.

Also existiert ein $x \in \mathbb{F}_\ell^*$ mit entweder $\sigma(e) = xe$ und $\sigma(f) = x^{-1}f$ oder aber $\sigma(e) = xf$ und $\sigma(f) = x^{-1}e$. Nach der vorgegangenen Bemerkung ist umgekehrt jede lineare Abbildung die dieser Bedingung genügt in $O(H)$. Insbesondere ist $|O(H)| = 2(\ell - 1)$.

(b) Sei $F\colon \mathbb{F}_{\ell^3} \to \mathbb{F}_{\ell^2},\ x \mapsto x^\ell$ der Frobeniusautomorphismus. Nach Dedekinds Lemma ist $(1, F)$ linear unabhängig über $\mathbb{F}_{\ell^2}$ im $\mathbb{F}_{\ell^2}$-Vektorraum $\mathrm{Hom}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}, \mathbb{F}_{\ell^2})$ und aus Dimensionsgründen somit eine $\mathbb{F}_{\ell^2}$-Basis.

Also ist $O((\mathbb{F}_{\ell^2}, N))$ eine Teilmenge von $\{\alpha + \beta F \mid \alpha, \beta \in \mathbb{F}_{\ell^2}\}$. Gesucht sind somit alle $(\alpha, \beta) \in \mathbb{F}_{\ell^2}^2$ mit

$$\begin{aligned} x^{\ell+1} = N(x) = N(\alpha x + \beta x^\ell) &= (\alpha x + \beta x^\ell)(\alpha x + \beta x^\ell)^\ell = (\alpha x + \beta x^\ell)(\alpha^\ell x^\ell + \beta^\ell x) \\ &= \alpha^{\ell+1} x^{\ell+1} + \alpha\beta x^2 + \alpha^\ell \beta x^{2\ell} + \beta^{\ell+1} x^{\ell+1} \end{aligned}$$

für alle $x \in \mathbb{F}_{\ell^2}$. Dies ist äquivalent zu

$$0 = (\alpha^{\ell+1} + \beta^{\ell+1} - 1) \cdot x^{\ell-1} + \alpha^\ell \beta \cdot x^{2\ell-2} + \alpha\beta^\ell \quad \text{für alle } x \in \mathbb{F}_{\ell^2}^* .$$

Die rechte Seite läßt sich als Polynom in x von Grad $2\ell - 2$ auffassen, was $\ell^2 - 1$ Nullstellen hat. Es folgt $\alpha^{\ell+1} + \beta^{\ell+1} - 1 = \alpha^\ell \beta = \alpha\beta^\ell = 0$. Damit ist entweder $\alpha = 0$ und $\beta^{\ell+1} = 1$ oder aber $\beta = 0$ und $\alpha^{\ell+1}$. Umgekehrt ist klar, das jedes solches Paar (α, β) eine bijektive Abbildung $\alpha + \beta F$ liefert. Damit ist

$$O((\mathbb{F}_{\ell^2}, N)) = \{\alpha \cdot \mathrm{id}_{\mathbb{F}_{\ell^2}} \mid \alpha \in \mathbb{F}_{\ell^2}^* \text{ und } \alpha^{\ell+1} = 1\} \cup \{\beta \cdot F \mid \beta \in \mathbb{F}_{\ell^2}^* \text{ und } \beta^{\ell+1} = 1\} .$$

Sicher ist $\{\alpha \cdot \mathrm{id}_{\mathbb{F}_{\ell^2}} \mid \alpha \in \mathbb{F}_{\ell^2}^* \text{ und } \alpha^{\ell+1} = 1\}$ ein Normalteiler in $O((\mathbb{F}_{\ell^2}, N))$ welcher trivialen Schnitt mit $\langle F \rangle$ hat. Also ist $O((\mathbb{F}_{\ell^2}, N)) \cong C_{\ell+1} \rtimes C_2$.

Aufgabe 4.

(a) Da (E, q) nicht anisotrop ist, existiert ein $e \in E - \{0\}$ mit $q(e) = 0$. Also ist $\langle e \rangle$ scharf primitiv. Daher spaltet eine hyperbolische Ebene von (E, q) ab. Aber die quadratische Form einer hyperbolischen Ebene ist bereits surjektiv.

(b) Sei $(F, q') = (E \oplus \langle f \rangle, q')$ mit $q'(e + xf) = q(e) - x^2 a$ für alle $e \in E$ und $x \in A$.

Ist $a \in A^*$ im Bild von q so existiert ein $e \in E$ mit $q(e) = a$. Also ist $q'(e+f) = 0$ aber $e+f \neq 0$. Damit ist (F, q') nicht anisotrop.

Ist umgekehrt (F, q') nicht anisotrop, so existieren $e \in E$ und $x \in A$ mit $e + xf \neq 0$ aber $0 = q'(e + xf) = q(e) - x^2 a$. Im Fall $x \neq 0$ ist $q(e/x) = q(e)/x^2 = a$. Im Fall $x = 0$ ist $q(e) = 0$. Daher ist (E, q) bereits nicht anisotrop. Aber dann ist $q\colon E \to A$ bereits surjektiv nach (a).