G. Nebe Besprechung am 09.11.2016

Quadratische Formen, WS 2016/17

Blatt 3

Aufgabe 1.

a) Sei K ein endlicher Körper mit ungerader Charakteristik und $E = N(K)$ ein zweidimensionaler quadratischer Raum ausgestattet mit der Normform. Berechnen Sie $\det(E)$ und folgern Sie, dass zwei reguläre quadratische Räume über K genau dann isometrisch sind, wenn Dimension und Determinante übereinstimmen.

b) Wir wissen aus der Vorlesung, dass $N(K) \perp N(K) \cong \mathbb{H}(K) \perp \mathbb{H}(K)$ gilt. Geben Sie für $K = \mathbb{F}_2$ und $K = \mathbb{F}_3$ jeweils die Isometrie explizit an.

Aufgabe 2.
Ein **linearer Code** C über einem endlichen Körper K der **Länge** n ist ein linearer Teilraum $C \leq K^n$. Auf K^n definiert man die symmetrische Bilinearform $b(x, y) := \sum_{i=1}^n x_i y_i$. Der **duale Code** zu C ist $C^\perp := \{x \in K^n \mid b(x, c) = 0 \ \forall\ c \in C\}$. C heißt **selbstdual**, falls $C = C^\perp$ und **selbstorthogonal**, falls $C \subseteq C^\perp$. Das **Gewicht** eines $c \in C$ ist $\mathrm{wt}(c) := \#\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}$.

(a) Sei $K = \mathbb{F}_{p^m}$ für eine ungerade Primzahl p. Für welche p und n existieren selbtduale Codes in (K^n, b)?

(b) Bezeichne $\mathbf{1} := (1, \ldots, 1) \in K^n$, $E := \mathbf{1}^\perp$.

Sei jetzt $K = \mathbb{F}_2$, $V = K^n$ und $C \leq K^n$ ein Code.

Der Code C heißt **gerade** bzw. **doppelt gerade**, falls $\mathrm{wt}(c) \in 2\mathbb{Z}$ bzw. $\mathrm{wt}(c) \in 4\mathbb{Z}$ für alle $c \in C$.

Zeigen Sie:

1) (V, b) ist nicht ausgeartet.
2) Ist $C \subseteq C^\perp$, dann ist $\mathrm{wt}(c)$ für alle $c \in C$ gerade und deshalb ist $C \subseteq \mathbf{1}^\perp = \{c \in C \mid \mathrm{wt}(c) \text{ gerade }\}$.
3) Ist C doppelt gerade, dann ist C selbstorthogonal.
4) Enthält (V, b) einen doppelt geraden selbstdualen Code, dann ist $n \in 4\mathbb{Z}$.
5) Wir definieren eine quadratische Form $q : E \to \mathbb{F}_2, q(c) = \frac{\mathrm{wt}(c)}{2} + 2\mathbb{Z}$. Zeigen Sie, dass b_q die Einschränkung von b auf E ist.
6) Ist n gerade, dann gilt $E^\perp = \langle \mathbf{1} \rangle$, und (E, q) ist halbregulär wenn $n \notin 4\mathbb{Z}$.
7) Ist n ungerade, dann ist (E, q) regulär and $(V, b) = E \perp \langle \mathbf{1} \rangle$.

8) Schreibe $n = 8m + a$ mit $m \in \mathbb{N}_0$, $a \in \{1, 2, 3, 4, 5, 6, 7, 8\}$. Dann ist $(E, q) \cong \mathbb{H}(\mathbb{F}_2)^{4m} \perp\!\!\!\perp A$ mit

$$A \cong \begin{cases} \{0\} & a = 1 \\ [1] & a = 2 \\ N(\mathbb{F}_2) & a = 3 \\ N(\mathbb{F}_2) \perp\!\!\!\perp [0] & a = 4 \\ \mathbb{H}(\mathbb{F}_2) \perp\!\!\!\perp N(\mathbb{F}_2) & a = 5 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp\!\!\!\perp [1] & a = 6 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp\!\!\!\perp N(\mathbb{F}_2) & a = 7 \\ \mathbb{H}(\mathbb{F}_2)^3 \perp\!\!\!\perp [0] & a = 8 \end{cases}$$

Hinweis: liste die Elemente von E explizit auf.

9) Doppelt gerade selbstduale Codes existieren in V genau dann wenn $n \in 8\mathbb{Z}$.

Aufgabe 3.
Sei $K = \mathbb{F}_{p^m}$ ein endlicher Koerper, $F = \mathbb{F}_{p^{2m}}$ der eindeutige Erweiterungskörper vom Grad 2 und $V = F^n$. Auf V definieren wir das **hermitesche Spur-Skalarprodukt** als

$$b((v_1, v_2, \ldots, v_n), (w_1, w_2, \ldots, w_n)) = \mathrm{Tr}(\sum_{i=1}^{n} v_i w_i^{p^m}),$$

wobei Tr die Spur von F über K sei. Somit wird (V, b) zu einem billinearen K-Vektorraum der Dimensison $2n$.

a) Zeigen Sie, dass b symmetrisch ist und bestimmen Sie eine Gram-Matrix.

b) Sei nun $p = 2$. Zeigen Sie, dass dann $(V, q_b) \cong \mathbb{H}^n$ gilt. Folgern Sie, dass für alle n selbstduale $\mathbb{F}_2$-lineare Codes in V existieren.

c) Sei nun $K = \mathbb{F}_2$, $F = \mathbb{F}_4$ mit primitivem Element w, $n = 4$ und es sei $C = \langle b_1, b_2, b_3, b_4 \rangle \leq V$ mit

$$\begin{aligned} b_1 &= \begin{pmatrix} w+1 & w & 0 & 1 \end{pmatrix} \\ b_2 &= \begin{pmatrix} w & 1 & w & 1 \end{pmatrix} \\ b_3 &= \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ b_4 &= \begin{pmatrix} w+1 & 1 & 0 & w \end{pmatrix} \end{aligned}$$

Zeigen Sie, dass C selbstdual ist.