

Th: Soit \mathbb{F}_q un cap fini de car $\neq 2$

E un \mathbb{F}_q -ev de dim n

$\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$

Q une fq sur E de rg r .

Alors, ds une certaine base, Q a pour matrice

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \text{ ou } \begin{pmatrix} I_{r-1} & 0 \\ 0 & \alpha & 0 \end{pmatrix}$$

desminime n si pas ou est un carré de \mathbb{F}_q

Dém :

OPS $r = n$ ie Q non dégénérée (sinon, on considère un suppl V de E^\perp ds E et on rq que Q a pour mat

$$\begin{pmatrix} [Q|_V] & 0 \\ 0 & 0 \end{pmatrix}$$

ds la réunion d'une base de V et d'une base de E^\perp avec $\dim V = r$ et $Q|_V$ non dég)

On fait une réc sur $n \geq 1$.

$n=1$:

On considère (e_1) une base de E .

On rq que $Q(e_1) \in \mathbb{F}_q^*$ (Q est non dég)

Mais $\mathbb{F}_q^* = \mathbb{F}_q^{*2} \cup \alpha \mathbb{F}_q^{*2}$. En effet, $\mathbb{F}_q^* \rightarrow \mathbb{F}_q^{*2}$
 $x \mapsto x^2$

est un morph de gres surj de noyau $\{-1, 1\}$ donc $|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{2}$

et donc $\mathbb{F}_q^* / \mathbb{F}_q^{*2} = \{1, \alpha\}$.

Donc soit $Q(e_1) = \lambda^2$ avec $\lambda \in \mathbb{F}_q^*$ et $[Q]_{\left(\frac{e_1}{\lambda}\right)} = (1)$

soit $Q(e_1) = \alpha \lambda^2$ avec $\lambda \in \mathbb{F}_q^*$ et $[Q]_{\left(\frac{e_1}{\lambda}\right)} = (\alpha)$

$n \geq 2$:

On considère (e_1, \dots, e_n) une Bo de E .

On note $a := Q(e_1) \in \mathbb{F}_q^*$

$b := Q(e_2) \in \mathbb{F}_q^*$

Li: $\exists x, y \in \mathbb{F}_q, ax^2 + by^2 = 1$

CcP: $\exists E_1 \in \langle e_1, e_2 \rangle, Q(E_1) = 1$

Mais $H = \langle E_1 \rangle^\perp$ est de dim $n-1$ (Q est non dég) donc il admet une base \mathcal{B} tq $[Q|_H]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 \\ & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 \\ & 1 \\ & & \alpha \end{pmatrix}$ (hyp réc)

et donc $[Q]_{(E_1, \mathcal{B})} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & & \\ & 1 & \\ & & \alpha \end{pmatrix}$ ($\langle E_1 \rangle \cap H = \{0\}$)

donc $E = \langle E_1 \rangle \oplus H$ et donc (E_1, \mathcal{B}) est une base de E

Qd y décrit \mathbb{F}_q , y^2 donc $\frac{1-by^2}{a}$ prend $\frac{q+1}{2}$ valeurs

($\text{Card}(\mathbb{F}_q^2) = 1 + |\mathbb{F}_q^{*2}| = \frac{q+1}{2}$) et donc

$\left\{ \frac{1-by^2}{a}, y \in \mathbb{F}_q \right\} \cap \mathbb{F}_q^2 \neq \emptyset$ (sinon, $\text{Card}(\mathbb{F}_q) \geq \frac{q+1}{2} + \frac{q+1}{2} > q$)

ie $\exists x, y \in \mathbb{F}_q, \frac{1-by^2}{a} = x^2$ ou encore $ax^2 + by^2 = 1$.