Caractérisation des formes quadratiques sur $\mathbb{F}_q$.

Théorème : Soit $\mathbb{F}_q$ avec $\text{carac}(\mathbb{F}_q) \neq 2$. Soit E un $\mathbb{F}_q$-e.v. de dimension n, $\alpha \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. Il y a alors 2 classes d'équivalence de formes quadratiques non dégénérées sur E. Leur matrice dans une base adaptée est $Q_1 = I_n$ où $Q_2 : \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix}$.

De plus, Q est de type $Q_1 \iff \det(Q)$ est un carré dans $\mathbb{F}_q$.

Lemme : Si $(a,b) \in \mathbb{F}_q^\times$, l'équation $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$ ($\text{carac}(\mathbb{F}_q) \neq 2$).

Preuve du théorème : Si $n = 1$, par ce qui précède et par hypothèse, $\mathbb{F}_q^\times = (\mathbb{F}_q^\times)^2 \amalg \alpha(\mathbb{F}_q^\times)^2$

$Q = (\beta)$. Si $\beta = \gamma^2$, $Q = (\gamma)(1)(\gamma)$

Si $\beta = \alpha\gamma^2$, $Q = (\gamma)(\alpha)(\gamma)$

Si $n = 2$, choisissons une base orthogonale pour Q notée $(u;v)$. Si l'on note $Q(u) = a$ et $Q(v) = b$ et $(x;y)$ une solution de l'équation $ax^2 + by^2 = 1$, qui existe d'après le lemme, alors $Q(ux + vy) = 1$.

Posons $e_1 = ux + vy$ et e_2 un vecteur Q-orthogonal à e_1 qui n'est pas isotrope.

Si $Q(e_2) = \lambda^2$, alors dans la base $\mathcal{B} = (e_1; \frac{e_2}{\lambda})$, $\text{Mat}(Q;\mathcal{B}) = I_2$

Si $Q(e_2) = \alpha\lambda^2$, ——————————, $\text{Mat}(Q;\mathcal{B}) = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$.

Si la propriété est vraie pour $(n-1)$, $(n > 2)$, alors soient $(e_1; e_2)$ deux vecteurs Q-orthogonaux non isotropes et $(x;y)$ tels que $xe_1 + ye_2 = \varepsilon$ et $Q(\varepsilon) = 1$ (donné par le lemme).

Posons $H = \{e_1\}^\perp$. Alors $Q_{|H}$ admet une base orthogonale $\mathcal{B}'(\varepsilon_2 \dots \varepsilon_n)$ telle que $\text{Mat}(Q_{|H}; \mathcal{B}') = \widetilde{Q} = I_{n-1}$. Donc, si $\mathcal{B}(\varepsilon_1 \dots \varepsilon_n)$, alors

ou

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

$$\mathrm{Mat}(Q;\mathcal{B}) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \tilde{Q} \end{array}\right) = I_n \quad \text{ou} \quad \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

(les 0 étant là car $(\varepsilon_1 \dots \varepsilon_n)$ est Q-orthogonale).

Si Q_1 et Q_2 sont congruentes, alors $\det Q_2 = (\det P)^2 \det Q_1$.
Et $\alpha = (\det P)^2 \in (\mathbb{F}_q^\times)^2$, ce qui est impossible. Il y a donc exactement 2 classes de congruence.

Preuve du Lemme : 1) Soient $\phi : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$, $x \longmapsto x^2$ alors $(q-1) = \#\mathrm{Ker}\,\phi \, \#\mathrm{Im}\,\phi$.

Donc $\#\{\text{carrés de } \mathbb{F}_q^\times\} = \dfrac{q-1}{\#\mathrm{Ker}\,\phi} = \dfrac{q-1}{2}$. car $\left[\begin{array}{c}\mathrm{Card}(\mathbb{F}_q) \neq 2 \\ \text{donc } 1 \neq -1\end{array}\right]$

Donc $\#\{\text{carrés de } \mathbb{F}_q\} = \dfrac{q+1}{2}$.

2) Soit $\psi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $y \longmapsto (1-by^2)a^{-1}$; ψ est une composée de ϕ et de bijections.

Donc $\#\mathrm{Im}\,\psi = \dfrac{q+1}{2}$.

Si $(x;y)$ est solution de $ax^2 + by^2 = 1$, alors $z = x^2 \in (\mathbb{F}_q)^2 \cap [\mathrm{Im}\,\psi]$ et inversement la réciproque est vraie.

Donc $\#[\mathrm{Im}\,\psi \cap (\mathbb{F}_q)^2] \geq \#\mathrm{Im}\,\psi + \#(\mathbb{F}_q)^2 - \#[(\mathbb{F}_q)^2 \cup \mathrm{Im}\,\psi]$

$\geq \dfrac{q+1}{2} + \dfrac{q+1}{2} - q = 1$.

Donc cette équation admet au moins une solution.