Formes quadratiques sur $\mathbb{F}_q$.

Benjamin Hellouin

Perrin, chap.5

Théorème 1. *Soit $\mathbb{F}_q$ un corps de caractéristique $\neq 2$ et E un $\mathbb{F}_q$-ev de dimension n. Il y a deux classes de congruence de formes quadratiques non dégénérées sur E, de matrices :*

$$Q_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & \\ 0 & & 1 \end{pmatrix} \quad et \quad Q_2 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & \alpha \end{pmatrix},$$

avec α un élément qui ne soit pas un carré sur $\mathbb{F}_q$.

En admettant l'existence d'un tel α, on voit que ces deux matrices ne sont pas congruentes. Si $Q_2 = {}^tPQ_1P$, on a $\alpha = (\det P)^2$, ce qui est contradictoire.

Lemme 1. *L'équation $ax^2 + by^2 = 1$ avec $a, b \in \mathbb{F}_q^*$, admet au moins une solution en x, y.*

Preuve du lemme. On va commencer par dénombrer les carrés de $\mathbb{F}_q$. Le morphisme de groupes $\begin{matrix} \mathbb{F}_q^* \to \mathbb{F}_q^* \\ x \mapsto x^2 \end{matrix}$ admet comme noyau $\{\pm 1\}$ ($x^2 = 1 \Rightarrow (x+1)(x-1) = 0$). Donc $|(\mathbb{F}_q^*)^2| = \frac{|\mathbb{F}_q^*|}{2}$ puisque $-1 \neq 1$, et on en déduit $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

Par conséquent, $\frac{1-by^2}{a}$ prend $\frac{q+1}{2}$ valeurs différentes. Comme $\frac{q+1}{2} + \frac{q+1}{2} > q$, par le principe des tiroirs, cette quantité prend une valeur qui est un carré, et on a donc $ax^2 + by^2 = 1$ en cette valeur.

Preuve du théorème. Soit q une forme quadratique sur E, on va prouver le résultat par récurrence.

$\mathbf{n = 2}$. On choisit une base orthogonale pour q, autrement dit une base dans laquelle $q(x_1, x_2) = ax_1^2 + bx_2^2$. Le lemme implique l'existence d'un vecteur x tel que $q(x) = 1$; soit y orthogonal à x. On distingue les cas suivant si $q(y)$ est un carré ou non. Si $q(y) = \lambda^2$, on se place dans la base $(x, y/\lambda)$ dans laquelle la matrice de q est l'identité. Sinon, comme $(\mathbb{F}_q^*)^2$ est d'indice 2 dans $\mathbb{F}_q^*$, αy est un carré est on a une base où la matrice de q est $\mathrm{Diag}(1, \alpha)$.

$\mathbf{n > 2}$. Supposons le résultat vrai jusqu'au rang $n-1$ et soit $(e_1 \dots e_n)$ une base orthogonale pour q. Comme précédemment, on peut trouver un vecteur $x_1 \in Vect(e_1, e_2)$ tel que $q(x_1) = 1$. On conclut en appliquant l'hypothèse de

récurrence à $(x_1)^\perp$.

Enfin, dans le cas où $\mathbb{F}_q$ est de caractéristique 2, la démonstration est valable mais tout élément est un carré et il n'y a qu'une seule classe d'équivalence.