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

ref : Perrin

THÉORÈME 18.1 *Soit E un espace vectoriel de dimension finie sur un corps fini $\mathbb{F}_q$ de caractéristique différente de 2. Soit q une forme quadratique sur E. Pour $a \in \mathbb{F}_q$ qui n'est pas un carré, il existe une base dans laquelle la matrice de q est de la forme* $\mathrm{diag}(0,\dots,0,1,\dots,1)$ *ou* $\mathrm{diag}(0,\dots,0,1,\dots,1,a)$.

PREUVE.

On peut supposer q non dégénérée :

Si q est dégénérée, elle a un noyau N. On prend un supplémentaire quelconque H de N et la restriction de q à H est alors non dégénérée. En choisissant une base adaptée à la décomposition orthogonale $E = N \oplus H$, on a une matrice diagonale par blocs avec un bloc nul et un bloc non dégénéré.

Cas de la dimension 2 : heuristique + carrés dans $\mathbb{F}_q$

En dimension 2, dans une base orthogonale la matrice de q est de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Pour mettre un 1 en haut à gauche, il faut donc trouver un couple $(x,y) \neq (0,0)$ tel que $ax^2 + by^2 = 1$. Comme le cardinal du corps est fini, on va montrer l'existence abstraite de solutions en dénombrant les carrés.

LEMME 18.2 *L'ensemble des carrés non nuls $\mathbb{F}_q^{*2}$ est d'indice 2 dans le groupe $\mathbb{F}_q^*$: pour $a \in F_q^*$ non carré, on a $\mathbb{F}_q^* = F_q^{*2} \cup aF_q^{*2}$. Le nombre de carrés dans $\mathbb{F}_q$ est donc $\frac{q+1}{2}$. Pour $a, b \neq 0$, l'équation $ax^2 + by^2 = 1$ a toujours des solutions $(x,y) \neq (0,0)$.*

PREUVE. On a un morphisme de groupes multiplicatifs $\mathbb{F}_q^* \to \mathbb{F}_q^*$ donné par l'élévation au carré. Son noyau est le sous-groupe $\{\pm 1\}$ qui est d'ordre 2 car on est en caractéristique différente de 2. L'ensemble des carrés non nuls qui est l'image de ce morphisme est donc un sous-groupe d'indice 2. Il y a donc $\frac{q-1}{2}$ carrés non nuls, en y ajoutant 0, on trouve $\frac{q+1}{2}$. Les parties $\{\frac{1-by^2}{a}$ pour $y \in F_q\}$ et $\{x^2$ pour $x \in \mathbb{F}_q\}$ sont de cardinal $\frac{q+1}{2}$, dans un ensemble de cardinal q, donc doivent s'intersecter pour un couple (x,y) qui est forcément différent de $(0,0)$ qui n'est pas solution de l'équation. □

Récurrence : $n = 1$: Pour $x \in E \setminus 0$, $q(x)$ est ou non un carré. Quitte à multiplier x par un scalaire non nul, on se ramène à $q(x) = 1$ ou a.

$n \geq 2$: On prend un plan non isotrope P dans E engendré par un vecteur non isotrope e et un vecteur non isotrope f dans l'hyperplan orthogonal au premier. Dans la base (e,f), q s'écrit $ax^2 + by^2$ avec $a, b \neq 0$ et le lemme permet alors de trouver un vecteur $v = xe + yf$ non nul tel que $q(v) = 1$. L'orthogonal de v est alors un supplémentaire qui est non isotrope pour q auquel on peut appliquer l'hypothèse de récurrence.

Il reste à vérifier que les deux formes de matrices non dégénérées sont non congruentes. C'est à cause de l'invariance du discriminant : le déterminant d'une matrice symétrique est invariant par congruence modulo les carrés. On fabrique alors un invariant d'équivalence pour les formes quadratiques non dégénérées par $\det(q) \in K^*/K^{*2}$. □

Leçons concernées : corps finis, formes quadratiques.