Classification des formes quadratiques sur $\mathbb{F}_q$

Léo Gayral

2017-2018

ref : Perrin – Cours d'algèbre – p.130

Soient $\mathbb{F}_q$ un corps de caractéristique différente de 2, et $E \cong \mathbb{F}_q^n$ un espace vectoriel. On fixe également $a \in \mathbb{F}_q^*$ qui n'est pas un carré.

Lemme 1. On pose $\mathbb{F}_q^{2*} := \{x^2, x \in \mathbb{F}_q^*\}$. C'est un sous-groupe multiplicatif de $\mathbb{F}_q^*$ d'indice 2. En particulier, $a \notin \mathbb{F}_q^{2*}$ donc $\mathbb{F}_q^* = \mathbb{F}_q^{2*} \sqcup a\mathbb{F}_q^{2*}$.

Démonstration.
F_q^{2*} est clairement un sous-groupe en tant qu'image de $\mathbb{F}_q^*$ par le morphisme de groupes $\phi : x \mapsto x^2$. De plus, $\ker(\phi)$ est l'ensemble des racines de $X^2 - 1 = (X-1)(X+1)$, d'où $\ker(\phi) = \{\pm 1\}$ à deux éléments et donc F_q^{2*} d'indice 2.

Ce sous groupe ne rencontre pas l'ensemble translaté $a\mathbb{F}_q^{2*}$ d'où la partition de F_q^*. □

Remarque 1. Dans le cas de caractéristique 2, $x \mapsto x^2$ est le morphisme de Frobenius, de noyau trivial, donc tous les éléments de F_q sont des carrés.

Lemme 2. $\forall(\lambda, \mu) \in \left(\mathbb{F}_q^*\right)^2, \exists(x, y) \in (\mathbb{F}_q)^2, \lambda x^2 + \mu y^2 = 1.$

Démonstration.
Soient $A = \{1 - \lambda x^2, x \in \mathbb{F}_q\}$ et $B = \{\mu y^2, y \in \mathbb{F}_q\}$. $|A| = |B| = \frac{q+1}{2}$ donc $|A| + |B| > q = |\mathbb{F}_q|$; il en découle $A \cap B \neq \emptyset$. □

Définition 1. Soient $q, q' \in Q(E)$ deux formes quadratiques. On dit que q et q' sont semblables s'il existe $\phi \in GL(E)$ telle que $q' = q \circ \phi$; de façon équivalente, du point de vue matriciel, on a $P \in GL_n(\mathbb{F}_q)$ telle que $\mathrm{Mat}(q') = P^T \mathrm{Mat}(q) P$.

Lemme 3. I_n et $\mathrm{diag}(1,\dots,1,a)$ ne sont pas semblables.

Démonstration.
Si on avait $\mathrm{diag}(1,\dots,1,a) = P^T I_n P = P^T P$ alors on aurait

$$a = \det(\mathrm{diag}(1,\dots,1,a)) = \det\left(P^T P\right) = \det(P)^2 \in \mathbb{F}_q^{2*} \ ,$$

ce qui est exclu. □

Théorème 1 (Cas non dégénéré)**.** Soit $q \in Q(E)$ une forme quadratique non dégénérée. Dans une base orthogonale adaptée, $\mathrm{Mat}(q) = \mathrm{diag}(1,\dots,1,\lambda)$ avec $\lambda \in \{1, a\}$.

Démonstration.
Le résultat en dimension 1 découle du premier lemme. En effet, en fixant un vecteur de base e on va avoir $\mathrm{Mat}_e(q) = \lambda \in \mathbb{F}_q^*$. Si $\lambda = \delta^2 \in \mathbb{F}_q^{2*}$ alors dans la base $f = \delta e$ on aura $\mathrm{Mat}_f(q) = 1$. Sinon $\lambda = a\delta^2 \in a\mathbb{F}_q^{2*}$ et dans la base $f = \delta e$ on aura $\mathrm{Mat}_f(q) = a$.

Considérons maintenant le cas spécifique de la dimension 2, qui servira de base à notre schéma de récurrence. Comme on travaille en caractéristique différente de 2, on peut trouver de façon effective une base orthogonale $e = (e_1, e_2)$ avec l'algorithme de réduction de Gauss. Dans cette base, on a $q(x_1, x_2) = \lambda x_1^2 + \mu x_2^2$. D'après le second lemme, on a donc $f_1 = (x_1, x_2) \neq 0$ tel que $q(f_1) = 1$. Soit $f_2 \in f_1^\perp$ non nul. En particulier, on a $f = (f_1, f_2)$ libre en dimension 2, une base orthogonale de (E, q). Dans cette base, on a $q(y_1, y_2) = y_1^2 + \lambda y_2^2$. On peut alors appliquer le cas de dimension 1 à $q' = q|_{\mathrm{Vect}(f_2)}$.

Supposons le résultat vrai en dimension inférieure ou égale à n et $\dim(E) = n+1$. Par réduction de Gauss, on se place dans une base orthogonale $(e_i)_{0\leq i\leq n}$. On commence par appliquer le cas de dimension 2 à $q|_{\mathrm{Vect}(e_0,e_1)}$, et on en déduit une nouvelle base (f_0, e_1') du sous-espace telle que $q(f_0) = 1$. En raisonnant par blocs, on applique le cas de dimension n à $q|_{\mathrm{Vect}(e_1',e_2,\dots,e_n)}$, ce qui donne une base $(f_1,\dots,f_n)$ du sous-espace, de sorte que $\mathrm{Mat}_{f_0,\dots,f_n}(q) = \mathrm{diag}(1,\dots,1,\lambda)$ avec $\lambda \in \{1, a\}$. □

Remarque 2 (Cas dégénéré)**.** Dans le cas général, les matrices de la forme $M = \mathrm{diag}(0,\dots,0,\overbrace{1,\dots,1,\lambda}^{r})$ avec $0 \leq r \leq n$ et $\lambda \in \{1, a\}$ forment un système de représentants des classes de congruence.