

Pierre Lissy

May 5, 2010

Lemme 1. *On peut se ramener au cas des formes quadratiques non dégénérées. Autrement dit, deux formes quadratiques sont équivalentes ssi elles ont même rang et qu'elles sont équivalentes sur l'orthogonal de leur noyau.*

Proof. La seule forme quadratique équivalente à la forme quadratique nulle est elle-même. On peut donc se ramener aux cas des formes quadratiques non nulles. On considère deux formes quadratiques non nulles équivalentes. Alors notamment elles ont le même rang, donc la dimension des noyaux est la même. De plus, comme $q(u) = q'$ on a nécessairement que u envoie le noyau de q' sur celui de q (le noyau est l'ensemble des x tel que pour tout y , $q(x + y) = q(x - y)$), et donc on n'a plus qu'à déterminer u sur l'orthogonal de ce noyau. Inversément, si l'on considère deux formes quadratiques qui ont un noyau de même dimension et dont les restrictions aux orthogonaux sont équivalentes, alors on complète l'isomorphisme obtenu en envoyant $\text{Ker}(q')$ sur $\text{Ker}(q)$ et le tour est joué. $\square$

Théorème 1. *On a deux classes d'équivalences de formes quadratiques non dégénérées sur les corps finis: celles dont le discriminant est un carré dans F_q et celles dont le discriminant n'est pas un carré. Ces classes d'équivalences correspondent aux deux situations distinctes où on peut rendre la matrice de la forme quadratique diagonale égale à Id ou avec le dernier coef qui n'est pas un carré dans F_q^* , égal à un certain α fixé.*

Proof. On commence par rappeler un fait bien connu.

Lemme 2. *L'équation $ax^2 + by^2 = 1$ a toujours des solutions dans F_q . (avec a, b non nuls)*

En effet, il y a $(q + 1)/2$ carrés dans F_q , donc la quantité $(1 - by^2)/a$ prend $(q + 1)/2$ valeurs distinctes et donc l'une d'elles est un carré car si aucune en est on obtient $q + 1$ éléments dans F_q ce qui est absurde.

Raisonnons maintenant par récurrence sur n . Pour $n = 2$ la forme quadratique est $ax^2 + by^2$, pour une base orthogonale (qui existe). Donc notamment d'après le lemme il existe e_1 tel que $q(e_1) = 1$. On considère un vecteur e_2 orthogonal à e_1 . On rappelle que les carrés inversibles forment un sous-groupe multiplicatif de F_q^* d'indice 2 (puisque'il y a $(q-1)/2$ carrés non nuls). Ainsi, comme $q(e_2) \in F_q^2$ soit c'est un carré dans F_q soit ce n'en est pas un, donc soit on l'écrit sous la forme λ^2 soit sous la forme $\lambda^2\alpha$, et dans les deux cas on divise par λ notre vecteur e_2 et on obtient la matrice dans la base annoncée. En dimension supérieure, c'est très simple. On considère une BON. On regarde le plan engendré par les deux premiers vecteurs et on considère dans ce plan un ε tel que $Q(\varepsilon) = 1$ (on vient d'expliquer comment faire). On applique l'hypothèse de récurrence à $\text{Vect}(\varepsilon)^\perp$ et dans une base adaptée la matrice de q est bien celle voulue.

Enfin, remarquons que les deux classes obtenues sont bien distinctes puisqu'évidemment le discriminant n'est pas le même modulo F_q^2 .

Par la remarque préliminaire, on a donc un total de $2n - 1$ classes d'équivalences de formes quadratiques: celle de rang 0, et toutes celles de rang i dont le discriminant est un carré, toutes celles de rang i dont le discriminant n'est pas un carré. $\square$

Théorème 2. *On considère maintenant un corps algébriquement clos k . Il n'y a qu'une seule classe d'équivalence de formes quadratiques non dégénérées, donc toute forme quadratique non dég est Id dans une certaine base.*

Proof. On considère une base orthogonale pour q . Dans cette base, $q(\sum x_i e_i) = \sum a_i x_i^2$. Mais k est algébriquement clos, donc le polynôme $X^2 - a_i$ a au moins une racine dans k , notée b_i . Du

coup $q(\sum x_i e_i) = \sum (b_i x_i)^2$. il suffit alors de changer notre base e_i en une base e_i/b_i pour obtenir que la matrice de q dans cette base est l'identité.

On en déduit qu'il y a exactement n classes d'équivalence de formes quadratiques, paramétrées uniquement par le rang. $\square$