Classification des formes quadratiques non dégénérées sur un corps fini

Source : [Per] page 130.

Notions utilisées : formes quadratiques, corps finis,

Motivations

Déterminer les formes quadratiques non dégénérées sur tous les corps finis. Le nombre très restreint (deux) obtenu donne une idée un peu plus précise de ce que peut être une forme quadratique sur $\mathbb{F}_q$. Une application que l'on peut citer étant (une des nombreuses démonstrations de) la loi de réciprocité quadratique. On trouve aussi une application à la caractérisation des similitudes dans [Per].

Prérequis :

- $Card(\mathbb{F}_q^{\times 2}) = \dfrac{q-1}{2}$ (c.f premier lemme).
- $\forall a \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$, $\mathbb{F}_q^\times = \mathbb{F}_q^{\times 2} \sqcup a\mathbb{F}_q^{\times 2}$ (conséquence du th d'isomorphisme et du découpage en classes d'équivalence, c.f premier lemme).
- Existence de bases $f-$orthogonales pour f bilinéaire symétrique non dégénérée. (De Seguin Pazzis page 89 et en fait Réduction de Gauss p14)
- Conditions nécessaires d'équivalence de formes quadratiques (en particulier, si on veut avoir une chance d'être équivalent alors il faut que les déterminants soient égaux dans $\mathbb{K}^\times/\mathbb{K}^{\times 2}$

Notation : $\mathbb{F}_q^{\times 2} = \{x \in \mathbb{F}_p^\times, \exists y \in \mathbb{F}_p, x = y^2\}$ désigne les carrés de $\mathbb{F}_q^\times$.

On peut éventuellement prouver le lemme précédent avant le théorème :

Lemme 1. *Si $\mathbb{F}_q$ est de caractéristique 2, tout élément est un carré. Sinon, $Card(\mathbb{F}_q^{\times 2}) = \dfrac{q-1}{2}$.*

Preuve. On considère le morphisme de groupes multiplicatifs

$$\varphi : x \in \mathbb{F}_q^\times \mapsto x^2 \in \mathbb{F}_q^\times.$$

Le noyau de ce morphisme est, par définition, l'ensemble des racines du polynôme $X^2 - 1$ dans $\mathbb{F}_q$. En caractristique différente de 2, on obtient $\ker(\varphi) = \{-1, 1\}$. En caractéristique 2 on a $X^2 - 1 = (X-1)^2$ d'où $\mathrm{Ker}(\varphi) = \{1\}$. De plus, par définition, $\mathrm{Im}(\varphi) = \mathbb{F}_q^{\times 2}$. Ainsi, par théorème d'isomorphisme, $\mathbb{F}_q^{\times 2} \simeq$

$\mathbb{F}_q^\times / \ker(\varphi)$ qui est de cardinal $q-1$ (ce qui ne compte pas 0 qui est aussi un carré) pour le cas de la caractéristique 2 et $\dfrac{q-1}{2}$ sinon. □

Théorème 2. *Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2 et E un $\mathbb{F}_q$ espace vectoriel de dimension finie n. Alors il n'y a que deux classes d'équivalence (pour l'action de congruence) de formes quadratiques sur $\mathbb{F}_q$, données par les deux matrices*

$$I_q \text{ et } M_n := \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \alpha \end{pmatrix}$$

où $\alpha \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ est un élément non nul et non carré de $\mathbb{F}_q$.

Preuve. On procède par récurrence sur la dimension n de E. Commençons par le cas $n=2$ pour se fixer les idées. Soit Q une forme quadratique sur E de dimension 2 et f sa forme polaire associée. On considère $(\varepsilon_1, \varepsilon_2)$ une base $f-$ orthogonale, c'est à dire telle que $q(x\varepsilon_1 + y\varepsilon_2) = f(x,y) = ax^2 + by^2 + 0xy$. Ce que l'on souhaiterait est dans un premier temps changer $\mathcal{B}$ en une base de premier vecteur $e_1$telle que $f(e_1) = 1$. C'est pourquoi on est amenés à montrer le lemme suivant :

Lemme 3. *Soient $a, b \in \mathbb{F}_q^\times$. Alors il existe $(x,y) \in \mathbb{F}_q$ tels que $ax^2 + by^2 = 1$.*

Preuve du lemme. On constate tout d'abord que $ax^2 + by^2 = 1 \iff y^2 = b^{-1}(1-ax^2)$ car b est inversible. Or a est inversible, donc pour $x_1, x_2 \in \mathbb{F}_q$ on a $b^{-1}(1-ax_1^2) = b^{-1}(1-ax_2^2)$ si et seulement si $x_1^2 = x_2^2$. Autrement dit, on a une bijection

$$\{b^{-1}(1-ax^2), x \in \mathbb{F}_q\} \simeq \{b^{-1}(1-az), z \in \mathbb{F}_q^{\times 2} \cup \{0\}\}$$

et cet ensemble est, d'après le premier lemme, de cardinal $\dfrac{q+1}{2}$. D'autre part, l'ensemble $\{y^2, y \in \mathbb{F}_q\}$ est de même cardinal $\dfrac{q+1}{2}$ par le même lemme. Ainsi, la réuinion $\{b^{-1}(1-ax^2), x \in \mathbb{F}_q\} \cup \{y^2, y \in \mathbb{F}_q\}$ étant de cardinal inférieur à q (car incluse dans $\mathbb{F}_q$) ne peut pas être disjointe [1]. On en déduit donc le résultat. □

1. On peut aussi dire que c'est l'intersection de deux ensembles de cardinaux dont la somme est supérieure au cardinal de l'ensemble total.

Retour à la preuve du théorème. Fort de ce lemme, on peut donc choisir un vecteur $e_1 = (x, y) \in E$ tel que $f(e_1) = 1$. Soit alors e_2 un vecteur orthogonal à e_1. Dès lors :

- Ou bien $f(e_2) = \lambda^2 \in \mathbb{F}_q^{\times 2}$ auquel cas on obtient I_2 en remplaçant e_2 par $\frac{1}{\lambda} e_2$.
- Ou bien $f(e_2) = \lambda^2 a$ avec $\lambda \in \mathbb{F}_q^{\times 2}$ auquel cas on obtient la seconde matrice en remplaçant e_2 par $\frac{1}{\lambda} e_2$.

On a donc traité le cas $n = 2$. Supposons le résultat vrai pour tout $2 \leq k \leq n-1$ pour un certain $n \in \mathbb{N}$ $n \geq 3$. Soit $\mathcal{B} = (\varepsilon_1, \ldots, \varepsilon_n)$ une base $f-$ orthogonale de E. D'après le lemme, il existe un vecteur $e_1 \in vect(\varepsilon_1, \varepsilon_2)$ tel que $f(e_1) = 1$. On applique alors l'hypothèse de récurrence sur la forme quadratique f restreinte à l'hyperplan $vect(e_1)^\perp$. Ainsi, f est bien de la forme annoncée.

Enfin, il faut vérifier que les deux matrices données correspondent à des formes quadratiques non équivalentes. On remarque que $\det(I_n) = 1$ d'une part et $\det(M_n) = a \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ (et donc différent de 1 modulo $\mathbb{F}_q$) d'autre part. Ainsi, les deux matrices sont de discriminants (déterminant modulo $\mathbb{F}_q^{\times 2}$) différents, donc ne peuvent pas être équivalentes. □

Remarque 4. *La classe de congruence de M_n est indépendante du choix de a car le discriminant est défini modulo $\mathbb{K}^{\times 2}$, en particulier il sera le même quel que soit le choix de $a \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$. On en déduit le résultat affirmant que deux formes quadratiques de même rang sont équivalentes si et seulement si leur discriminant est égal. (pour les corps finis) (pour $\mathbb{R}$ il faut être plus précis : c.f signature, qui ne donne pas juste la parité mais carrément le nombre de -1 sur la diagonale)*

Références

[Per] Daniel Perrin, Cours d'algèbre