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

Réf° Perrin p130.

Soit $\mathbb{K} = \mathbb{F}_q$ un corps fini de caractéristique différente de 2

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 : * si $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{2*}$, $\mathbb{F}_q^* = \mathbb{F}_q^{2*} \sqcup \alpha\mathbb{F}_q^{2*}$.
* il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.

Lemme 2° L'équation (en x et y) $ax^2 + by^2 = 1$ avec $a, b \in \mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$.

Théorème° Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soit $d \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{2*}$. Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E, de matrices : $Q_1 = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ et $Q_2 = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & d \end{pmatrix}$

Une forme Q est de l'un ou l'autre type suivant que son discriminant $\delta(Q)$ est ou non un carré de $\mathbb{F}_q^*$.

* possible puisque car$(\mathbb{K}) \neq 2$.

Heuristique : Cas de la dimension 2 : on peut trouver une base orthogonale (grâce à l'algo de réduct° de Gauss*) tq dans cette base, $Q(x_1, x_2) = ax_1^2 + bx_2^2$ (de matrice $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$) et pour mettre un 1 en haut à gauche, on doit trouver (x_1, x_2) tq $Q(x_1, x_2) = 1$. D'où l'utilité du lemme 2 que l'on va ensuite montrer à l'aide du lemme 1 en dénombrant les carrés. On pourra ensuite raisonner par récurrence sur la dimension de l'espace.

Preuve du lemme 1° : On considère le morphisme de groupes : $\begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{F}_q^* \\ x & \longmapsto & x^2 \end{array}$
Son image est $\mathbb{F}_q^{2*}$ et son noyau est l'ensemble des racines de $X^2 - 1 = (X-1)(X+1)$, donc $\{\pm 1\}$ qui est de cardinal 2 puisque car$(\mathbb{K}) \neq 2$.
Ainsi d'après le 1er Thm d'isomorphisme (en considérant les cardinaux), on obtient $|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}$, ($\mathbb{F}_q^{2*}$ sous gpe d'indice 2).
On obtient alors directement la partition $\mathbb{F}_q^* = \mathbb{F}_q^{2*} \sqcup \alpha\mathbb{F}_q^{2*}$.
De plus, $\mathbb{F}_q^2 = \mathbb{F}_q^{*2} \cup \{0\}$ donc il y a $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.

Remarque° On voit tout de suite que le cas de caractéristique 2 ne fonctionne pas, puisque alors $x \mapsto x^2$ est le morphisme de Frobenius, qui est un automorphisme donc tout le monde est un carré.

Preuve du lemme 2° : On note $A = \{ax^2, x \in \mathbb{F}_q\}$ et $B = \{1 - by^2, y \in \mathbb{F}_q\}$
Alors puisque $\begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & ax \end{array}$ et $\begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ y & \longmapsto & 1 - by \end{array}$ sont des bijections, on a
$|A| = |B| = |\mathbb{F}_q^2| = \frac{q+1}{2}$.

Donc $|A \cap B| = |A| + |B| - |A \cup B| = q+1 - \underbrace{|A \cup B|}_{\leq q} \geq 1$

Donc il existe $(x,y) \in \mathbb{F}_q^2$, $ax^2 = 1 - by^2$.

Preuve du théorème : On va montrer le résultat par récurrence sur $n = \dim(E)$.

* $n=1$: Soit $e \in \mathbb{F}_q^*$ tel que $Q(e) \neq 0$, possible puisque Q est non dégénérée. On a alors $\mathrm{Mat}_e(Q) = \lambda \in \mathbb{F}_q^*$
  - Soit $\lambda = s^2 \in \mathbb{F}_q^{2*}$, alors dans la base $f = s^{-1}e$, on a bien $\mathrm{Mat}_f(Q) = 1$
  - Soit $\lambda = \alpha s^2 \in \alpha \mathbb{F}_q^{2*}$, alors dans la base $f = s^{-1}e$, on a bien $\mathrm{Mat}_f(Q) = \alpha$. (d'après le lemme 1)

* Revenons au cas de l'heuristique : $n=2$ qui va nous donner une idée sur comment réaliser la récurrence
  ▷ ok car car $(\mathbb{F}_q) \neq 2$
  On a déjà vu que grâce à l'algo de réduct° de Gauss, il existe une base (e_1, e_2) orthogonale, telle que dans cette base, on ait donc $Q(x_1, x_2) = \lambda x_1^2 + \mu x_2^2$. D'après le lemme 2, il existe $f_1 = (x_1, x_2) \in \mathbb{F}_q^2$ tq $Q(x_1, x_2) = 1$ (nécessairement $(x_1, x_2) \neq (0,0)$). Soit $f_2 \in f_1^{\perp} \setminus \{0\}$ non isotrope. Alors (f_1, f_2) base orthogonale de (E, q), et dans cette base, $q(y_1, y_2) = y_1^2 + \lambda y_2^2$, et en faisant le même raisonnement que pour le cas $n=1$ sur $q(f_2)$, dans une certaine base (f_1, f_2),
  $\mathrm{Mat}_{(f_1,f_2)}(Q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ si $q(f_2) \in \mathbb{F}_q^{2*}$ et $\mathrm{Mat}_{(f_1,f_2)}(Q) = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$ sinon.

* Soit $n \geq 2$ tel que le résultat soit vrai en dimension inférieure ou égale à n, et soit E de dimension $n+1$ et Q forme quadratique sur E. Grâce à la réduction de Gauss, on peut prendre $(e_1, \dots, e_{n+1})$ une base orthogonale de Q. D'après le lemme, il existe $\varepsilon_1 \in \langle e_1, e_2 \rangle$ tel que $Q(\varepsilon_1) = 1$. On peut ensuite appliquer l'hypothèse de récurrence à $Q_{|\langle \varepsilon_1 \rangle^{\perp}}$: il existe une base orthogonale $(\varepsilon_2, \dots \varepsilon_n) = \tilde{\mathcal{B}}$ de $Q_{|\langle \varepsilon_1 \rangle^{\perp}}$ telle que $\mathrm{Mat}_{\tilde{\mathcal{B}}}(Q_{|\langle \varepsilon_1 \rangle^{\perp}}) = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & \alpha \end{pmatrix}$
  et alors pour $\mathcal{B} = (\varepsilon_1, \dots \varepsilon_n)$, on obtient bien $\mathrm{Mat}_{\mathcal{B}}(Q) = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & \alpha \end{pmatrix}$

Enfin, montrons que ces deux matrices ne sont pas congruentes : si elles l'étaient, on aurait existence d'une matrice $P \in GL_n(\mathbb{F}_q)$, telle que $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & \alpha \end{pmatrix} = {}^tP I_n P = {}^tPP$, donc en passant au déterminant :
$\alpha = \det({}^tPP) = \det(P)^2 \in \mathbb{F}_q^{2*}$, ce qui est une contradiction.

Corollaire : Soit E un $\mathbb{K}$-ev de dimension finie n et $d \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{2*}$. Soit Q une forme quadratique sur E, alors il existe une base dans laquelle la matrice de Q est de la forme $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 0 \end{pmatrix}$ ou $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 0 \end{pmatrix}$.

Preuve : Si q est non dégénérée, ok.
Sinon, q a un noyau N, on prend un supplémentaire H de N, et alors $q_{|H}$ est non dégénérée. En appliquant ce qui précède à $q_{|H}$, on obtient une matrice par blocs avec un bloc nul (sur N) et un bloc $\begin{pmatrix} 1 & (0) \\ (0) & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & (0) \\ (0) & d \end{pmatrix}$ sur H.

$\triangleright$ Cela montre qu'il y a 2 classes de formes non dégénérées, et $2n+1$ classes au total (la forme nulle, et sinon on choisit $r \in [\![1, n]\!]$ le rang puis λ parmi $\{1, d\}$).

Remarques : ✱ Si on reformule ça pour obtenir une classification plus générale : Si $\mathbb{K} = \mathbb{F}_q$ de caractéristique $\neq 2$, une forme quadratique Q est caractérisée par son rang et par son discriminant $\overline{S(Q)}$ réduit, qui est le discriminant de la forme obtenue en quotientant E par $\ker(Q)$ (cf H262)

✱ Comparons ce résultat aux autres classifications :
- sur $\mathbb{C}$ (ou $\mathbb{C}_p$ généralement $\mathbb{K}$ algébriquement clos de car $\neq 2$), les formes quadratiques sont uniquement déterminées par le rang (tout le monde est un carré !)
- sur $\mathbb{R}$, elles sont caractérisées par leur rang et leur signature (± 1 représentant les 2 classes modulo les carrés !)
- sur $\mathbb{Q}$, il existe une infinité de formes quadratiques 2 à 2 non équivalentes (et ce dès la dimension 1 : $Q(x) = px^2$ pour p premier n'est pas congrue à $Q(x) = x^2$ (sinon $p = s^2$ pour $s \in \mathbb{Q}$) et ce $\forall p$ premier)

✱ Exemple d'application : prouver la réciprocité quadratique. (cf H262)