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

Mohamed NASSIRI

Références :

Cours d'algèbre, Daniel Perrin - p.130

Recasage :

• • • • • 150 : Exemples d'actions de groupes sur les espaces de matrices.
• • • • • 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
• • • • ○ 123 : Corps finis. Applications.
• • • ○ ○ 101 : Groupe opérant sur un ensemble. Exemples et applications.

Résumé :

Prérequis :

Formes quadratiques - Corps finis

Théorème : Soit $k = \mathbb{F}_q$ un corps fini de caractéristique différente de 2, et E un k-espace vectoriel de dimension n.
Soit $\alpha \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$. Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E, de matrices

$$Q_1 = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \quad \text{et} \quad Q_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix}$$

Démonstration.

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

Démonstration du lemme :
On a $|\mathbb{F}_q^2| = \frac{q+1}{2}$. En effet, on a le morphisme surjectif

$$\begin{aligned} c \ : \ \mathbb{F}_q^* &\to \mathbb{F}_q^* \\ x &\mapsto x^2 \end{aligned}$$

Son noyau est $\{-1, 1\}$ et son image est $\mathbb{F}_q^{*2}$, donc par le premier théorème d'isomorphisme, on a

$$\mathbb{F}_q^{*2} = \mathbb{F}_q^* / \{-1, 1\}$$

Ainsi, $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et comme $0^2 = 0$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
Les parties $A = \{\frac{1-by^2}{a}$ pour $y \in \mathbb{F}_q\}$ et $B = \{x^2$ 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 différent de $(0, 0)$ (car $(0, 0)$ n'est pas solution de l'équation).

□

Revenons à la démonstration du théorème.
On va procéder par récurrence sur $n \geq 2$:
• $n = 2$:
On choisit une base orthogonale pour Q dans laquelle $Q(x, y) = ax^2 + by^2$. Par le lemme, il existe un vecteur $e_1 = (x, y)$ tel que $Q(e_1) = 1$.
Soit e_2 un vecteur orthogonal à e_1 :
◦ Si $Q(e_2) = \lambda^2$, on remplace e_2 par $\frac{1}{\lambda}e_2$, donc on aura $Q = Q_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
◦ Si $Q(e_2)$ n'est pas un carré, comme $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$, on a $Q(e_2) = \lambda^2\alpha$, et on remplace e_2 par $\frac{1}{\lambda}e_2$, donc on aura $Q = Q_2 = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$

• $n > 2$:
On prend une base orthogonale $e_1, ..., e_n$. D'après le même lemme, il existe un vecteur ϵ_1 du plan $\langle e_1, e_2\rangle$ tel que $Q(\epsilon_1) = 1$.
On applique l'hypothèse de récurrence à l'hyperplan $H = \langle\epsilon_1\rangle^\perp$ et on obtient

$$Q = Q_1 = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \quad \text{ou} \quad Q = Q_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix}$$

Pour conclure, il reste à montrer que Q_1 et Q_2 ne sont pas semblables.
Si tel était le cas, il existerait $P \in GL_n(\mathbb{F}_q)$ telle que :

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix} = P^T \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} P = P^T P$$

mais alors on aurait :

$$\alpha = \det \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix} = \det(P^T P) = \det(P^2) \in \mathbb{F}_q^{*2}$$

Mais il se trouve que l'on a exclu ce cas ! □

Remarques :

- Plus d'explications sur "$\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$". Être d'indice 2, peut aussi se traduire comme "pour $a \notin \mathbb{F}_q^{*2}$, on a $\mathbb{F}_q^* = \mathbb{F}_q^{*2} \sqcup a\mathbb{F}_q^{*2}$.
- .
- Mises en garde sur le développement :
  Attention à ...