

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

Théorème

Soient $k = \mathbb{F}_q$ un corps fini tel que $\text{car}(k) \neq 2$ et E un k -espace vectoriel de dimension n . Soit $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.

Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E , de matrices :

$$Q_1 = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \quad \text{ou} \quad Q_2 = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha \end{pmatrix}.$$

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

Lemme 1

Le groupe $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$, en particulier il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.

Preuve :

On considère le morphisme de groupes :

$$\begin{aligned} \chi : \mathbb{F}_q^* &\rightarrow \mathbb{F}_q^* \\ x &\mapsto x^2. \end{aligned}$$

Son image est $\mathbb{F}_q^{*2}$ et son noyau est $\{-1, 1\}$ ainsi :

$$|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}$$

Donc $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$ et il y a $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ 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 $\mathbb{F}_q$.

Preuve :

On vient de voir qu'il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$. La quantité $\frac{1-by^2}{a}$ prend donc $\frac{q+1}{2}$ valeurs quand y parcourt $\mathbb{F}_q$, comme

$$\frac{q+1}{2} + \frac{q+1}{2} > q$$

l'un de ces valeurs est nécessairement un carré.

L'équation admet donc des solutions dans $\mathbb{F}_q$.

Démonstration :

On va montrer par récurrence sur $n = \dim E$ que toute forme quadratique Q sur E a une matrice du type annoncé.

- **Initialisation :** $n = 1$, soit $e \in \mathbb{F}_q^*$, $Q(e) \neq 0$ puisque Q est non dégénérée. On distingue deux cas :

- Si $Q(e) \in \mathbb{F}_q^{*2}$, il existe $\lambda \in \mathbb{F}_q^*$ tel que $Q(e) = \lambda^2$, alors $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = 1$$

- Sinon $Q(e) \notin \mathbb{F}_q^{*2}$ comme $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$ il existe $\lambda \in \mathbb{F}_q^*$ tel que $Q(e) = \alpha\lambda^2$, alors $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = \alpha$$

- **Hérédité :** on suppose le résultat vrai au rang n , montrons le au rang $n + 1$.
Soit $(e_1, \dots, e_{n+1})$ une base Q -orthogonale de E . Notons $H = \text{Vect}(e_1, e_2)$. Il existe $a, b \in \mathbb{F}_q^*$ tels que :

$$Q|_H = \langle a, b \rangle$$

Or, d'après le lemme 2, l'équation $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$. Il existe donc $\varepsilon_1 \in H$ tel que $Q(\varepsilon_1) = 1$. On applique alors l'hypothèse de récurrence à $H^\perp$ et on obtient la matrice voulue.

Ce qui achève la récurrence.

Comme α n'est pas un carré, les deux formes quadratiques précédentes ne sont pas équivalentes car leurs discriminants ne sont pas égaux modulo les carrés et donc il y a bien deux classes d'équivalences de formes sur $\mathbb{F}_q$.

Bonus

Théorème (Classification générale)

Une forme quadratique Q est caractérisée par son rang et par le discriminant réduit $\overline{\delta(Q)}$ qui est le discriminant de la forme quadratique obtenue en quotientant E par $\text{Ker}(Q)$.

Démonstration :

Soit Q une forme quadratique sur E de rang r . On note $\overline{\delta(Q)} = \varepsilon \in \{1, \alpha\}$.

Soit $(e_1, \dots, e_{n-r})$ une base de $\text{Ker}(Q)$, et soit U un supplémentaire de $\text{Ker}(Q)$ dans E alors $Q|_U$ est non dégénérée et il existe une base $\mathcal{B}_U$ de U telle que :

$$\text{Mat}_{\mathcal{B}_U}(Q|_U) = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon \end{pmatrix}$$

En recollant les bases on obtient le résultat cherché.

Références

- Daniel Perrin, *Cours d'algèbre*
- Philippe Caldero, Jérôme Germoni, *Histoires hédonistes de groupes et géométries*