Sandrine CARUSO

Formes quadratiques sur $\mathbb{F}_q$.

Référence : Francinou – Gianella – Nicolas, Oraux X-ENS, Algèbre 3

Théorème. *Soient p un nombre premier impair, q une puissance de p, $\mathbb{F}_q$ le corps à q éléments, et $\delta \in \mathbb{F}_q$ un élément qui ne soit pas un carré. Soit $n \in \mathbb{N}^*$. Il existe exactement deux classes d'équivalences de forme quadratiques sur $\mathbb{F}_q^n$: celles de $q_1(x) = x_1^2 + \cdots + x_n^2$ et de $q_2(x) = x_1^2 + \cdots + x_{n-1}^2 + \delta x_n^2$.*

Lemme 1. *Il y a exactement $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$. De plus, si l'on note C l'ensemble des carrés, on a $\mathbb{F}_q^* \backslash C = \delta C$.*

Démonstration. Soit $\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*$, $x \mapsto x^2$. C'est un morphisme de groupe de $\mathbb{F}_q^*$, son image est C, et son noyau est $\{-1, 1\}$ (car p est impair). Donc

$$\operatorname{Card} C = \frac{\operatorname{Card} \mathbb{F}_q^*}{\operatorname{Card} (\ker \psi)} = \frac{q-1}{2},$$

et $\operatorname{Card} (\mathbb{F}_q^* \backslash C) = \frac{q-1}{2}$. L'application $C \to \mathbb{F}_q^* \backslash C$, $x \mapsto \delta x$ est une bijection, d'où $\mathbb{F}_q^* \backslash C = \delta C$. □

Lemme 2. *Soient $a, b \in \mathbb{F}_q$. L'équation $ax^2 + by^2 = 1$ a au moins une solution dans $\mathbb{F}_q^2$.*

Démonstration. En comptant 0, il y a exactement $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$ d'après le lemme précédent. Soient $A = \{1 - ax^2, x \in \mathbb{F}_q\}$ et $B = \{by^2, y \in \mathbb{F}_q\}$. Les ensembles A et B sont en bijection avec $C \cup \{0\}$, et donc $\operatorname{Card} A = \operatorname{Card} B = \frac{q+1}{2}$. Ainsi, $\operatorname{Card} A + \operatorname{Card} B > \operatorname{Card} \mathbb{F}_q = q$, et ces ensembles ne peuvent donc être disjoints. Ce qui signifie exactement que l'équation $ax^2 + by^2 = 1$ a au moins une solution. □

Passons maintenant à la démonstration du théorème. Tout d'abord, q_1 et q_2 ne sont pas équivalentes, car si c'était le cas, il existerait $P \in \mathrm{GL}_n(\mathbb{F}_q)$ telle que

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \delta \end{pmatrix} = {}^tP \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} P,$$

et ceci entraînerait $\delta = (\det P)^2$. Pour montrer que toute forme quadratique est équivalente à l'une de ces deux-là, nous allons procéder par récurrence sur la dimension n de l'espace.

Tout d'abord, si $n = 1$, une forme quadratique q est de la forme $q(x) = ax^2$. Si a est un carré ($a = b^2$), le changement de variable $x' = ax$ donne l'équivalence entre q et q_1. Sinon, a est de la forme δb^2 et le « même » changement de variable donne $q \sim q_2$.

Nous allons également traiter le cas $n = 2$ qui nous servira de lemme pour établir l'hérédité dans notre récurrence. Soit q une forme quadratique. Quitte à faire un premier changement de coordonnées pour se placer dans une base orthogonale pour q, on peut supposer que $q(x) = a_1x_1^2 + a_2x_2^2$. D'après le lemme 2, il existe un vecteur $v^{(1)} = (v_1^{(1)}, v_2^{(1)})$ tel que $q(v^{(1)}) = 1$. Il est bien sûr non nul, soit $v^{(2)} \in (v^{(1)})^{\perp_q}$, non nul. Alors $(v^{(1)}, v^{(2)})$ est une base de $\mathbb{F}_q^2$ et dans cette base, $q(x_1v^{(1)} + x_2v^{(2)}) = x_1^2 + \alpha x_2^2$. On distingue encore deux cas selon que α soit un carré ou non : si α est un carré, alors $q \sim q_1$, sinon, $q \sim q_2$.

Soit maintenant $n \geqslant 2$, supposons le résultat vrai pour tout espace de dimension $n-1$. Soit q une forme quadratique sur $\mathbb{F}_q^n$. Quitte à changer de coordonnées pour une base orthogonale pour q, on suppose que $q(x) = a_1x_1^2 + \cdots + a_nx_n^2$. En appliquant le cas $n = 2$ à la restriction de q au sous-espace engendré par les deux premiers vecteurs de base, on se ramène à une forme quadratique du type $q(x) = x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$. On applique alors l'hypothèse de récurrence à la forme $q'(x) = a_2x_2^2 + \cdots + a_nx_n^2$ sur l'espace engendré par les $n-1$ derniers vecteurs, et on en déduit le résultat voulu.