Anaël Marit ENS Rennes

FORMES QUADRATIQUES SUR LES CORPS FINIS

- 101, 123, 148, 170 –

—

Le groupe linéaire agit de plusieurs façons sur les ensembles de matrices, et savoir caractériser les orbites sous ces actions forme un ensemble de problèmes qu'il est intéressant de savoir résoudre. Dans le cas de l'action d'équivalence, le pivot de Gauss fournit une réponse immédiate. Pour l'action de similitude, c'est le théorème de réduction de Frobenius qui fournit les invariants. Mais pour l'action de congruence sur les matrices symétriques, il n'y a pas de réponse dans le cas général (du moins pas à ma connaissance).

On va répondre ici à ce problème dans le cas des matrices à coefficients dans un corps fini en classifiant les classes d'isométrie des espaces quadratiques, problème qui est équivalent à déterminer les orbites de congruence. On aura en chemin besoin d'étudier le groupe des carrés sur un corps fini, en déployant pour cela des outils assez variés pour répondre à notre problème.

Soit p un nombre premier impair et q une puissance non triviale de p. On fixe $\mathbb{F}_q$ un corps fini à q-éléments ainsi que (E, φ) un $\mathbb{F}_q$-espace quadratique de dimension d finie avec φ non nulle. Nous allons montrer :

Théorème 1 (Réduction des formes quadratiques, corps finis ([2], theo 16.19)). *Soit $\alpha \in \mathbb{F}_q$ un élément non carré. Il existe un unique entier r et un unique $\delta \in \{1, \alpha\}$ tels que, dans une certaine base $\mathscr{B}$ de E, on ait :*

$$Mat_{\mathscr{B}}(\varphi) = \begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & 0_{d-r} \end{pmatrix} \tag{1}$$

Cette forme réduite caractérise entièrement la classe d'isométrie de φ.

Groupe de carrés de $\mathbb{F}_q$

On va dans un premier temps donner quelques résultats sur les carrés de $\mathbb{F}_q$. On notera dans toute la suite :

$$K := \{x^2,\ x \in \mathbb{F}_q\} \quad K^\times = K \setminus \{0\} \tag{2}$$

Proposition 2. *$K^\times$ est un sous-groupe de $\mathbb{F}_q^\times$ d'indice 2.*

Contactez-moi en cas de coquille à prénom.nom@ens-rennes.fr !

Démonstration. $K^\times$ est l'image de $\mathbb{F}_q^\times$ par le morphisme de groupes $f : x \mapsto x^2$. C'est donc un sous-groupe de $\mathbb{F}_q^\times$. Par ailleurs, le noyau du morphisme f est exactement l'ensemble des racines de $X^2 - 1$. Comme $\mathbb{F}_q$ est un corps de caractéristique impaire [(i)] , ce polynôme a exactement deux racines données par 1 et -1. Donc $K^\times$ est de cardinal $\dfrac{q-1}{2}$: il est bien d'indice 2. □

Lemme 3. *Soient $(a, b) \in (\mathbb{F}_q^\times)^2$ et $c \in \mathbb{F}_q$. L'équations*

$$ax^2 + by^2 = c \tag{3}$$

d'inconnues $(x, y) \in \mathbb{F}_q^2$ admet au moins une solution.

Démonstration. On commence par isoler x dans l'équation :

$$x^2 = \frac{c - by^2}{a} \tag{4}$$

Ainsi, l'ensemble des valeurs envisageables pour x^2 est donné par :

$$Z := \left\{ \frac{c - bz}{a} \mid z \in K \right\} \tag{5}$$

Pour que notre équation ait des solutions, il faut et il suffit que Z contienne un élément qui soit un carré. Nous allons montrer que $Z \cap K$ est non vide par dénombrement.

Tout d'abord, comme a et b sont inversibles dans $\mathbb{F}_q^\times$, l'application $z \mapsto a^{-1}(c - bz)$ est bijective. Z a donc même cardinal que K, c'est-à-dire $\dfrac{q+1}{2}$ (puisque $K^\times$ est d'indice 2 dans $\mathbb{F}_q^\times$ et que K contient exactement un élément supplémentaire). Mais la formule du crible donne :

$$|K \cup Z| = |Z| + |K| - |Z \cap K| = q + 1 - |Z \cap K| \tag{6}$$

comme $K \cup Z$ est un sous-ensemble de $\mathbb{F}_q$, son cardinal est majoré par q, d'où :

$$|K \cap Z| \geqslant 1 \tag{7}$$

Il suffit de prendre pour x une racine carrée d'un élément de $K \cap Z$: il existe alors $y \in \mathbb{F}_q$ tel que (x, y) est solution de l'équation par construction. □

Réduction des formes quadratiques

Ces quelques résultats en poche, on va prouver le théorème de réduction. Commençons par remarquer que pour $\alpha \in \mathbb{F}_q \setminus K$ fixé, le couple $\{1, \alpha\}$ forme un système de représentants des éléments de $\mathbb{F}_q^\times$ modulo le groupe des carrés inversibles (puisque celui-ci est d'indice 2), observation qui aura son importance.

(i). En caractéristique 2, $1 = -1$ et ce morphisme est bijectif : c'est le Frobenius !

Commençons par prouver l'unicité de r et δ. La valeur de r ne fait pas mystère : il ne peut s'agir que du rang de φ. Supposons donnés $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et $\delta, \delta' \in \{1, \alpha\}^2$ tels que

$$Mat_{\mathscr{B}}(\varphi) = \begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & 0_{d-r} \end{pmatrix} \quad Mat_{\mathscr{B}'}(\varphi) = \begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta' & 0 \\ 0 & 0 & 0_{d-r} \end{pmatrix} \tag{8}$$

Dans ce cas, δ et δ' sont deux valeurs du discriminant de φ restreint à un supplémentaire de son radical (ou noyau). Puisque celui-ci est uniquement déterminé par φ, $\delta = \delta'$.

Intéressons-nous maintenant à l'existence. On raisonne par récurrence sur d. Pour $d = 1$, le résultat provient immédiatement du fait que tout élément de $\mathbb{F}_q$ est congrus à 1 ou α modulo les carrés. Supposons $d \geqslant 2$ et le résultat acquis pour toute dimension inférieure. Soit $\mathscr{B} = (e_1, \dots, e_d)$ une base φ-orthogonale de E fournie par le théorème de réduction de Gauss. Quitte à permuter, on suppose que $\varphi(e_i) \neq 0$ pour $1 \leqslant i \leqslant r$.

Si $r = 1$, alors il existe $\delta \in \{1, \alpha\}$ et $x \in \mathbb{F}_q^\times$ tels que $x^2\varphi(e_1) = \delta$ par réduction modulo les carrés. Ainsi, en remplaçant e_1 par xe_1, on obtient la forme souhaitée.

Sinon, le lemme précédent prouve qu'il existe $(x, y) \in \mathbb{F}_q^2$ tels que :

$$x^2\varphi(e_1) + y^2\varphi(e_2) = 1 \tag{9}$$

Posons $\varepsilon_1 := xe_1 + ye_2$. Par construction, on a $\varphi(\varepsilon_1) = 1$. Il suit que φ restreinte à $\mathrm{Vect}(\varepsilon_1)$ est non dégénérée. Ainsi, en notant H l'orthogonal de $\mathrm{Vect}(\varepsilon_1)$, H est un hyperplan de E, supplémentaire orthogonal de $\mathrm{Vect}(\varepsilon_1)$. Complétons alors ε_1 en une base $\mathscr{C}$ de E en prenant des vecteurs $(\varepsilon_2, \dots, \varepsilon_d)$ une base φ-orthogonale de H dans laquelle $\varphi_{|H}$ a la forme souhaitée, obtenue par hypothèse de récurrence. Par construction, la base $\mathscr{C}$ est φ-orthogonale, donc la matrice de φ dans cette base est diagonale, et a la forme souhaitée. □

Annexe - Et en pratique ?

Si ce théorème fournit, en théorie, un représentant canonique de la classe d'isométrie de φ, donnant ainsi une condition nécessaire et suffisante pour savoir si deux formes quadratiques sur $\mathbb{F}_q$ sont isométriques (ou, de façon équivalente, pour savoir si deux matrices symétriques à coefficients dans $\mathbb{F}_q$ sont congruentes), la mise sous forme réduite est en pratique un problème qui n'est pas aisé, car il nécessite de savoir réduire des éléments de $\mathbb{F}_q$ modulo les carrés. On va voir ici un algorithme pour répondre à ce problème dans la pratique.

Etant donnée φ une forme quadratique sur $\mathbb{F}_q$, on commence par calculer une base φ-orthogonale $\mathscr{B}$ grâce au théorème de réduction de Gauss (dont la preuve fournit un algorithme appliquable pour la construction de telles bases). On obtient alors :

$$Mat_{\mathscr{B}}(\varphi) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & \lambda_r & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix} \tag{10}$$

où les (λ_i) sont non nuls. L'entier r qui apparaît ici est le rang de φ : il s'agit du même r que celui qui apparaît dans la forme réduite. On calcule alors D le produit des λ_i, terme qui correspond au déterminant dans la base $\mathscr{B}$ tronquée de φ restreinte à un supplémentaire de son radical. D donc congrus à δ modulo les carrés. Reste à déterminer cette congruence...

Le problème se ramène en fait à savoir si D est ou non un carré de $\mathbb{F}_q$. Si $q = p$, ce problème se résout à l'aide de la loi de réciprocité quadratique (cf par exemple [1]). Dans le cas général, on peut montrer qu'un élément $D \in \mathbb{F}_q^\times$ est un carré si, et seulement si, $D^{\frac{q-1}{p-1}}$, qui appartient à $\mathbb{F}_p$, est un carré, problème qu'on sait résoudre encore grâce à la loi de réciprocité quadratique, mais ceci est un développement à part entière [(ii)].

Références

[1] Michel Demazure. *Cours d'algèbre*. Cassini, 2008. isbn : 978-2-84225-127-7.

[2] Jean-Etienne Rombaldi. *Mathématiques pour l'agrégation, Algèbre et géométrie*.

(ii). Par ici ! https ://agreg-maths.fr/developpements/1287