Loi de réciprocité quadratique par les formes quadratiques

Nico

Prérequis : Formule aux classes, invariants de l'action par congruences dans un corps fini.

Notations :

1. $\mathbb{F}_p$ un corps fini de cardinal p où p est un nombre premier impair.
2. $\mathbb{F}_p^{[2]} = \{x^2 : x \in \mathbb{F}_p\}$
3. Pour $a \in \mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = 1$ si $a \in \mathbb{F}_p^{*[2]}$, -1 sinon. Il s'agit d'un morphisme de groupe de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.
4. Soit $A \in GL_n(\mathbb{F}_q) \cap \mathcal{S}_n(\mathbb{F}_q)$, où q est impair, on note $\delta(A)$ le discriminant de A, défini comme étant le reste modulo $\mathbb{F}_q^{[2]}$ de $\det(A)$.

J'énonce le résultat utilisé dans la preuve, qui selon moi, est le moins évident. Je donnerai des éléments de démonstration en annexe pour comprendre le résultat :

Thm 1. *Soit q impair. Soient $A, B \in \mathcal{S}_n(\mathbb{F}_q)$ inversibles. Alors A et B sont congruentes, si et seulement si, $\delta(A) = \delta(B)$*

On énonce le résultat qu'on démontrera :

Loi de réciprocité quadratique : Soient p, q deux nombre premiers impair distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Plan d'attaque : On souhaite calculer de deux manières différentes le cardinal de la "sphère" X définie par :

$$X = \{(x_0, \ldots, x_{p-1}\} \in \mathbb{F}_q^p : x_0^2 + \ldots + x_{p-1}^2 = 1\}$$

Le premier calcul utilise les actions de groupe par une méthode similaire de la preuve du théorème de Cauchy :

Démonstration. On considère l'action $\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ définie par :

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times X & \longrightarrow & X \\ (k, x_1, \ldots, x_p) & \longmapsto & (x_{0+k}, \ldots, x_{p-1+k}) \end{array}$$

Où par un abus de notation, "$n + k$" où $k \in \mathbb{Z}/p\mathbb{Z}$ désigne le reste modulo p de $n+$ un représentant de k.

Par équation des classes, pour tout $x \in X$, $p = |\mathbb{Z}/p\mathbb{Z}| = |Stab(x)|\ |Orb(x)|$. Donc $|Orb(x)| = 1$ ou p. On sait que les orbites des éléments de X forment une partition de X. Notons $X = \bigsqcup O_i$. Alors :

$$|X| = \sum_{|O_i|=1} |O_i| + \sum_{|O_j|=p} |O_j|$$

Notons $X^{\mathbb{Z}/p\mathbb{Z}} = \{x \in X : \forall k \in \mathbb{Z}/p\mathbb{Z},\ kx = x\}$ l'ensemble des éléments de X qui fixent $\mathbb{Z}/p\mathbb{Z}$. Il s'agit aussi de l'ensemble des éléments qui n'ont qu'un seul élément dans leur orbite. D'où le cardinal de X, modulo p est :

$$|X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \pmod{p}$$

Or $x \in X^{\mathbb{Z}/p\mathbb{Z}} \iff x_1 = \ldots = x_p$. D'où $|X^{\mathbb{Z}/p\mathbb{Z}}| = |\{x \in \mathbb{F}_q : px^2 = 1\}| = 2$ si $p^{-1} \in \mathbb{F}_q^{[2]}$, 0 sinon. D'où :

$$|X| \equiv \left(\frac{p^{-1}}{q}\right) + 1 \pmod{p} \equiv \left(\frac{p}{q}\right) + 1 \pmod{p}$$

D'où $\left(\frac{p}{q}\right) = |X| - 1$ dans $\mathbb{F}_p$. □

Le deuxième calcul consiste à étudier la forme quadratique $Q(x) = x_0^2 + \ldots + x_{p+1}^2$

Démonstration. On considère deux matrices de $M_p(\mathbb{F}_q)$:

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } A = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \\ & & & & & & & a \end{pmatrix}$$

Où $a = (-1)^{\frac{p-1}{2}}$.

Il s'agit de deux matrices inversibles, symétriques, et de même déterminant. En effet, A étant triangulaire par blocs (même diagonale par blocs), on a que :

$$\det A = a \times \det\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)^{\frac{p-1}{2}} = (-1)^{p-1} = 1 = \det I_p$$

Car p est impair. D'où $\delta(I_p) = \delta(A)$. D'où A et I_p sont congruentes par théorème 1.

On considère alors $P \in GL_p(\mathbb{F}_q)$ telle que $I_p = {}^tPAP$.

Il vient que $\forall x \in \mathbb{F}_q^p,\ Q(x) = {}^txx = {}^tx({}^tPAP)x = {}^t(Px)A(Px)$

Puisque $x \mapsto Px$ est bijective, on peut alors identifier l'ensemble $X = \{x \in \mathbb{F}_q^p : {}^txx = 1\}$ à

$$X' = \{x' \in \mathbb{F}_q^p : {}^txAx = 1\}$$

Or pour tout $u = (x, y) \in \mathbb{F}_q^2$, ${}^tu\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}u = \begin{pmatrix} y & x \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 2xy$.

D'où un calcul par blocs fournit que, si l'on note $d = \dfrac{p-1}{2}$:

$$X' = \left\{(x_1, y_1, \ldots, x_d, y_d, z) \in \mathbb{F}_q^p : \sum_{i=1}^{d} 2x_iy_i + az^2 = 1\right\}$$

Soit $x = (x_1, y_1, \ldots, x_d, y_d, z) \in X'$:

- Si $x_1 = \ldots = x_d = 0$, alors il y a $|\mathbb{F}_q^d \times \{z \in \mathbb{F}_q : az^2 = 1\}| = q^d(1 + \left(\dfrac{a}{q}\right)) = q^d(1 + \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}) = q^d(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})$ éléments.
- Si il existe un x_i non nul : on fixe $(x_1, \ldots, x_d : q^d - 1$ choix possibles. On fixe un $z : q$ choix. Soient alors $x = (x_1, \ldots, x_d)$ fixé, z fixé. On cherche à résoudre l'équation $Q(x_1, y_1, \ldots, x_p, y_p, z) = 1$ d'inconnue $(y_1, \ldots, y_d)$. Il s'agit d'une équation d'un hyperplan affine de $\mathbb{F}_q^d$, il y a alors q^{d-1} choix possible. D'où il y a $q(q^d - 1)q^{d-1} = q^d(q^d - 1)$ éléments.

Finalement,

$$|X'| = q^d(q^d - 1 + 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}) = q^{2d} + q^d(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

En regroupant tout ce qu'on a fait : Il vient que, dans $\mathbb{F}_p$:

$$1 + \left(\frac{p}{q}\right) = q^{2d} + q^d(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

On rappelle que $d = \dfrac{p-1}{2}$, et $\left(\dfrac{a}{p}\right) = a^{\frac{p-1}{2}}$, et $a^{p-1} = 1$ dans $\mathbb{F}_p$. d'où :

$$1 + \left(\frac{p}{q}\right) = 1 + \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

D'où dans $\mathbb{F}_p$:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

□

On fait d'ailleurs remarquer que cette égalité reste vraie dans $\mathbb{Z}$ car le symbole de legendre vaut ± 1, donc puisque $p \neq 2$, si on enlève le modulo p, nécessairement le quotient de la division euclienne du terme de gauche par p est nul.

On se propose de calculer la valeur de $\left(\dfrac{2}{p}\right)$, qui ne se trouve pas par le théorème puisque 2 n'est pas un premier impair

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Démonstration. On cherche à savoir si 2 est un carré dans $\mathbb{F}_p$. Autrement dit, on cherche à savoir si $X^2 - 2$ admet une racine dans $\mathbb{F}_p$.

On considère le corps de décomposition de $X^2 - 2$ noté $\mathbb{F}_p(\alpha)$ où α est une racine de $X^2 - 2$. On considère ζ une racine 8ème primitive de l'unité de $\mathbb{F}_p$. On a que :

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2\zeta\zeta^{-1} + \zeta^{-2} = 2$$

Car $\zeta^{-2} = -\zeta^2$. On peut supposer alors $\alpha = \zeta + \zeta^{-1}$ (quitte à regarder $-\alpha$ sinon).

- Si $p \equiv \pm 1[8]$. Soit alors k tel que $p = \pm 1 + 8k$, alors par Frobenius :

  $$\alpha^p = (\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p} = \zeta^{\pm 1}\zeta^{8k} + \zeta^{\mp 1}\zeta^{8k} = \zeta + \zeta^{-1} = \alpha.$$

  D'où $\alpha \in \mathbb{F}_p$

- Si $p \equiv \pm 3[8]$, soit alors k tel que $p = \pm 3 + k$. Alors :

  $$\alpha^p = \zeta^p + \zeta^{-p} = \zeta^{\pm 3}\zeta^{8k} + \zeta^{\mp 3}\zeta^{8k} = \zeta^3 + \zeta^{-3} = \zeta^5 + \zeta^{-5} = -(\zeta + \zeta^{-1}) \neq \alpha$$

  Car $p \neq 2$. D'où $2 \in \mathbb{F}_p^{[2]}$, si et seulement si, $p \equiv \pm 1[8]$, si et seulement si, $p^2 \equiv 1[8]$. D'où :

  $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

□

Annexe

Preuve du théorème 1 :

Le sens direct est assez simple : Si A et B sont congruentes, alors il existe P inversible tel que $A = {}^tPBP$. Alors $\det A = \det(P)^2 \det B$. D'où $\delta(A) = \delta(B)$ puisque $\det(P)^2 \in \mathbb{F}_q^{*[2]}$. (1)

Sens indirect :

Soit A une matrice symétrique inversible de $\mathbb{F}_q$. On lui associe une forme quadratique non dégénérée Q sur $\mathbb{F}_q^n$. Par le processus d'orthogonalisation, il existe une base de $\mathbb{F}_q^n$ qui est $Q-$orthogonale. Ie, Q s'écrit dans cette base :

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^2$$

D'où A est congruente à la matrice $\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$.

On introduit un premier lemme :

Lemme 2. *$\mathbb{F}_q^{*[2]}$ est un sous-groupe de $\mathbb{F}_q^*$, et $[\mathbb{F}_q^* : \mathbb{F}_q^{*[2]}] = 2$.*

Démonstration. Le fait que $\mathbb{F}_q^{*[2]}$ soit un sous-groupe découle du fait que $x \mapsto x^2$ est un morphisme de groupe pour la loi $\cdot$.
Si l'on considère l'application sur $\mathbb{F}_q^*$, $x \mapsto x^{\frac{q-1}{2}}$, q étant impair, elle est bien définie et est un morphisme de groupe. Par ailleurs, son noyau est $\mathbb{F}_q^{*[2]}$, d'image $\{-1, 1\}$. D'où par le premier théorème d'isomorphisme, $\mathbb{F}_q^*/\mathbb{F}_q^{*[2]} \simeq \{-1, 1\}$. Puisque $q \neq 2$, $\mathbb{F}_q^{*[2]}$ est d'indice 2. □

On considère alors ζ un élément de $\mathbb{F}_q^* \backslash \mathbb{F}_q^{*[2]}$. Il vient que pour tout $x \in \mathbb{F}_q^*$, x est congru à 1 ou ζ modulo $\mathbb{F}_q^{*[2]}$. On réduit alors la base Q-orthogonale modulo $\mathbb{F}_q^{*[2]}$, formant une base $(e_1, \ldots, e_n)$, et il vient que A est congruente à $\begin{pmatrix} \varepsilon_1 & & \\ & \ddots & \\ & & \varepsilon_n \end{pmatrix}$ Où $\varepsilon_i \in \{1, \zeta\}$.

Faisons encore mieux en introduisant un second lemme :

(1). On remarque qu'on a un aucun moment utilisé le fait qu'on soit sur un corps fini, il s'agit donc d'un invariant sur tout corps.

Lemme 3. *l'équation $ax^2 + by^2 = 1$, où $a, b \neq 0$, admet au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q$.*

Démonstration. Par le premier lemme, $|\mathbb{F}_q^{*[2]}| = \dfrac{q-1}{2}$. Donc $|\mathbb{F}_q^{*2]}| = \dfrac{q+1}{2}$. Puisque a est non nul, l'application $z \mapsto az$ est bijective dans $\mathbb{F}_q$. Il existe donc $\dfrac{q+1}{2}$ éléments qui s'écrivent sous la forme ax^2 où $x \in \mathbb{F}_q$. De même, en considérant l'application $z \mapsto 1 - bz$, on obtient qu'il existe $\dfrac{q+1}{2}$ éléments qui s'écrivent $1 - by^2$ dans $\mathbb{F}_q$. En considérant les cardinaux de l'union des ensembles $\{ax^2 : x \in \mathbb{F}_q\}$ et $\{1 - by^2 : y \in \mathbb{F}_q\}$, on a que $\dfrac{q+1}{2} + \dfrac{q+1}{2} = q+1 > q$. D'où l'intersection $\{ax^2 : x \in \mathbb{F}_q\} \cap \{1 - by^2 : y \in \mathbb{F}_q\}$ contient au moins un élément. Autrement dit, il existe $(x, y) \in \mathbb{F}_q^2$ tels que $ax^2 = 1 - by^2$. D'où le résultat souhaité. □

Ainsi, si $n \geq 2$, il existe $v \in \mathbb{F}_q^n$, avec deux composantes non nulles, tel que $Q(v) = 1$.

Alors pour tout (e_i, e_{i+1}), $1 \leq i \leq n-1$, on peut prendre un vecteur v_i de $\mathrm{Vect}(e_i, e_{i+1})$ non nul tel que $Q(v_i) = 1$. Alors A est congruente à $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \varepsilon_n \end{pmatrix}$

Où $\varepsilon_n \in \{1, \zeta\}$ car si n est impair, on se retrouve forcément à la fin avec un sous espace de dimension 1, et on ne peut donc pas appliquer le lemme.

C'est là où le discriminant intervient. On a que $\delta(A) = \det A \pmod{\mathbb{F}_q^{*[2]}}$. D'où ici, $\delta(A) = 1$ ou ζ, selon si $\varepsilon_n \in \{1, \zeta\}$. D'où le discriminant fournit une condition suffisante pour dire si deux matrices sont congruentes ou non.

Référence

Philippe Caldero, Jérôme Germoni (2019). *Nouvelles Histoires Hédonistes de Groupes et de Géométries tome 1.* Calvage & Mounet, p. 321.

Recasages

Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

Leçon 121 : Nombres premiers. Applications.

Leçon 123 : Corps finis. Applications.

Leçon 149 : Déterminant. Exemples et applications.

Leçon 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité. Applications.

Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.