Loi de réciprocité quadratique

(inspiré de la version de Maxence Brévard)

Leçons : 121 ; 123 ; 126 ; 170 ; 190

Références : CALDERO–GERMONI, *Nouvelles Histoires Hédonistes de Groupes et Géométrie Tome 1* (p.304)[?]

Prérequis :

- la classification des formes quadratiques sur un corps fini
- le symbole de Legendre et la propriété $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
- définition d'un hyperplan affine
- les orbites d'une action sont disjointes
- la relation orbite/stabilisateur

Introduction :

La loi de réciprocité quadratique est un outil très puissant dans la théorie des corps finis car elle permet d'étudier le résidu quadratique d'un nombre premier q sur $\mathbb{F}_p$ en connaissant le résidu quadratique p sur $\mathbb{F}_q$.

Théorème 1 (Loi de réciprocité quadratique)**.** Soient p, q deux entiers premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Idée de la preuve : On construit une forme quadratique φ' sur $\mathbb{F}_q^p$ équivalente à la forme quadratique de matrice l'identité φ. On montre alors que leurs boules unités

$$X' = \{x \in \mathbb{F}_q^p, \varphi'(x) = 1\} \quad \text{et} \quad X = \{x \in \mathbb{F}_q^p, \varphi(x) = x_1^2 + \cdots + x_p^2 = 1\}$$

sont équipotentes. On dénombre X en faisant agir $\mathbb{F}_p$ sur X et X' en faisant apparaître un hyperplan affine de $\mathbb{F}_q^p$.

Nous aurons besoin du lemme combinatoire suivant :

Lemme 1. Soit p impair premier et $a \in \mathbb{F}_p^*$. Alors

$$|\{x \in F_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$$

Démonstration du lemme. Le polynôme $ax^2 - 1$ admet au plus deux racines dans le corps $\mathbb{F}_p$. Comme $a \in \mathbb{F}_p$ et $\mathbb{F}_p$ est un corps, on réécrit l'équation souhaitée : $x^2 = a^{-1}$. Distinguons deux cas :

— Si a n'est pas un carré, a^{-1} ne l'est pas non plus, il n'y a donc aucune solution. L'égalité est immédiate.

— Sinon a est un carré donc a^{-1} l'est aussi, on écrit $a^{-1} = \varepsilon^2$. On a donc deux solutions distinctes : ε et $-\varepsilon$. On vérifie alors l'égalité souhaitée

D'où le résultat. □

Démonstration de la loi de réciprocité quadratique. Considérons la forme quadratique définie pour tout $x = (x_1, \cdots, x_p) \in \mathbb{F}_q^p$ par $\varphi(x) = x_1^2 + \cdots + x_p^2$. Notons $X = \{x \in \mathbb{F}_q^p, \varphi(x) = 1\}$ la boule unité de $\mathbb{F}_q^p$.

Étape 1 : *Dénombrons X modulo p*

On fait agir le groupe $\mathbb{F}_p$ sur X par permutations circulaires des coordonnées.

$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_p \times X & \to X & \\ (\alpha, (x_1, x_2, \ldots, x_p)) & \mapsto & (x_{1+\alpha[p]}, x_{2+\alpha[p]}, \ldots, x_{p+\alpha[p]}) \end{array} \right.$$

La relation orbite-stabilisateur assure alors l'égalité :

$$\forall x \in \mathbb{F}_q^p, \ |Stab_x|.|Orb_x| = |\mathbb{F}_p| = p$$

Comme p est premier, il y a deux types d'orbites :

— des orbites de taille p, de stabilisateur $\{e\}$. On notera k le nombre d'orbites de taille p.

— des orbites de taille 1, de stabilisateur $\mathbb{F}_p$, qui sont de la forme : $\{(x, \cdots, x)\}, x \in \mathbb{F}_q$ avec $px^2 = 1$.[1] D'après le lemme, il y en a donc $1 + \left(\frac{p}{q}\right)$.

Comme les orbites sont disjointes, on a

$$|X| = \sum |\Omega_p| + \sum |\Omega_1| = \left(1 + \left(\frac{p}{q}\right)\right) \times 1 + k \times p \equiv 1 + \left(\frac{p}{q}\right) \ [p]$$

$$\boxed{|X| = 1 + \left(\frac{p}{q}\right) \ [p]}$$

Étape 2 : *Étudions un autre ensemble : X'*

On définit la forme quadratique φ' pour $x \in \mathbb{F}_q^p$ par

$$\varphi'(x_1, x_2, \ldots, x_{p-2}, x_{p-1}, x_p) = 2(x_1x_2 + \cdots + x_{p-2}x_{p-1}) + (-1)^{\frac{p-1}{2}} x_p^2$$

On notera X' l'ensemble $\{x \in \mathbb{F}_q^p, \varphi'(x) = 1\}$, la boule unité de $\mathbb{F}_q^p$ pour φ'. On pose $d = \frac{p-1}{2}$ et $a = (-1)^d$. La matrice de φ' dans la base canonique est :

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

Comme $det(\varphi') = det(A) = (-1)^d a = 1 = det(\varphi)$, d'après le théorème de **classification des formes quadratiques** sur les corps finis, φ et φ' sont équivalentes. Il existe un isomorphisme linéaire $u \in \mathcal{L}(\mathbb{F}_q)$ tq $\varphi' = \varphi \circ u$. Cet isomorphisme fournit une bijection entre les deux sphères X' et X. Ainsi

$$\boxed{|X| = |X'|}$$

1. car il faut que $\phi(\alpha, x) = x$ pour tout $\alpha \in \mathbb{F}_p$ et que $\varphi(x) = 1$

Étape 3 : *Dénombrons X' modulo p*

— Si $(x_1, x_3, \ldots, x_{p-2}) = (0, \ldots, 0)$, on choisit indifféremment le vecteur $(x_2, x_4, \ldots, x_{p-1})$ dans $\mathbb{F}_q^d$ (q^d choix possibles). On choisit ensuite $x_p \in \mathbb{F}_q$ vérifiant $ax_p^2 = 1$. D'après le lemme, il y a $1 + \left(\frac{a}{q}\right)$ possibilités.

— Sinon, on choisit les $x_1, x_3, \ldots, x_{p-2}$ ($q^d - 1$ choix). On choisit $x_p \in \mathbb{F}_q$ (q possibilités). Enfin, le vecteur $(x_2, x_4, \ldots, x_{p-1})$ est alors un élément quelconque de l'hyperplan affine

$$H = \left\{2(x_1x_2 + \cdots + x_{p-2}x_{p-1}) + ax_p^2 - 1 = 0\right\}$$

de cardinal $|H| = q^{d-1}$.

Donc

$$|X'| = q^d\left(1 + \left(\frac{a}{q}\right)\right) + (q^d - 1)qq^{d-1}$$

$$\boxed{|X'| = q^d\left(\frac{a}{q}\right) + q^{2d}}$$

Comme $|X| = |X'|$ et en faisant le calcul dans $\mathbb{F}_p$, on obtient finalement :

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

Or $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$ et par petit théorème de Fermat, $q^{2d} = q^{p-1} = 1[p]$.

D'autre part, $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}}$. Ainsi on obtient l'égalité suivante :

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

$$\boxed{\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}}$$

On a cette égalité dans $\mathbb{F}_p$, or le symbole de Legendre est un élément de $\{-1, +1\}$ et $p \neq 2$, donc les deux membres sont des éléments de $\{-1, +1\}$. Ains l'égalité est vraie dans $\mathbb{Z}$. □

Remarques :

Il y a beaucoup de preuves différentes de ce résultat.

Astuces de l'agrégatif :

En fonction du temps, je ne démontre pas le lemme qui est une simple étude de cas, parfois je fais une application pour trouver une condition nécessaire sur p pour que 3 soit un carré modulo p (utile dans le critère de primalité des nombres de Mersenne)

Condition nécessaire pour que 3 soit un carré modulo p avec p premier.

On utilise la loi de réciprocité quadratique avec 3 et p.

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

On suppose que 3 est un carré modulo p. Donc $\left(\frac{3}{p}\right) = 1$.

Ainsi si $p \equiv 1$ [3], on a $\left(\dfrac{p}{3}\right) = 1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être pair, d'où $p \equiv 1$ [4]. Par le lemme chinois, on a $p \equiv 1$ [12].

Et si $p \equiv 2$ [3], on a $\left(\dfrac{p}{3}\right) = -1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être impair, d'où $p \equiv 3$ [4]. Par le lemme chinois, on a $p \equiv -1$ [12].

Donc si 3 est un carré modulo p, on a nécessairement $p \equiv \pm 1$ [12].