11 Loi de réciprocité quadratique

Leçons 121, 123, 126, 170

Ref : [H2G2 Tome 1] V.C

Le but de ce développement est de montrer un résultat important de la théorie des corps finis, qui permet de relier le fait que deux nombres premiers impairs soient respectivement des carrés l'un modulo l'autre. Il utilise notamment le théorème de classification des formes quadratiques sur les corps finis.

On rappelle la définition suivante.

Définition 1 Soit p un entier premier impair et a un élément de $\mathbb{F}_p$. On définit le *symbole de Legendre* de a par

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0 \end{cases}.$$

Théorème 2 (Loi de réciprocité quadratique) Soient p et q deux entiers premiers impairs distincts. Alors on a

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

Démonstration. L'idée de la preuve consiste à calculer les cardinaux de deux sphères unités de $\mathbb{F}_q^p$ pour deux formes quadratiques équivalentes, et de montrer que ce sont les mêmes. On aura par ailleurs besoin du lemme suivant [1].

Lemme 3 Soit a un élément de $\mathbb{F}_p^*$ (où p désigne toujours un nombre premier impair). Alors on a

$$\left|\left\{x \in \mathbb{F}_p, \quad ax^2 = 1\right\}\right| = 1 + \left(\frac{a}{p}\right).$$

Démonstration. Le membre de gauche correspond au nombre de racine du polynôme $aX^2 - 1$, de degré 2, dans le corps $\mathbb{F}_p$. On distingue deux cas :

- si a n'est pas un carré modulo p, a^{-1} non plus et alors le polynôme n'a pas de racine dans $\mathbb{F}_p$: l'égalité est donc correcte
- si a est un carré, a^{-1} aussi, et on note alors ε une racine de a^{-1} ; ε et $-\varepsilon$ sont alors deux racines distinctes (car $\varepsilon \neq 0$) de $aX^2 - 1$, et comme ce polynôme est de degré, il ne peut en avoir d'autre, ce qui prouve que l'égalité tient aussi.

□

Étape 1. Dénombrement de la sphère unité de $\mathbb{F}_q^p$ modulo p.

On veut connaître le cardinal de la sphère unité de $\mathbb{F}_q^p$

$$S := \left\{(x_1, .., x_p) \in \mathbb{F}_q^p, \quad \sum_{i=1}^{p} x_i^2 = 1\right\}.$$

On fait agir le groupe $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique des coordonnées sur $\mathbb{F}_q^p$:

$$\forall k \in \mathbb{Z}/p\mathbb{Z},\ \forall (x_1, .., x_p) \in \mathbb{F}_q^p, \quad k \cdot (x_1, .., x_p) = (x_{k+1}, .., x_{k+p}),$$

où l'on voit bien sûr les indices modulo p. On étudie en particulier l'action de $\mathbb{Z}/p\mathbb{Z}$ sur S [2]. On classifie les orbites de S sous cette action : d'après la relation orbite-stabilisateur, on a pour tout $x \in S$

$$|O_x||\mathrm{Stab}_x| = |\mathbb{Z}/p\mathbb{Z}| = p,$$

et comme p est premier on en déduit que les orbites sont de deux types :

- le point $(x, .., x) \in S$ pour $x \in \mathbb{F}_q^p$ est sa propre orbite, et son stabilisateur est $\mathbb{Z}/p\mathbb{Z}$; de plus on a nécessairement $px^2 = 1$ puisque $(x, .., x) \in S$

1. En fonction du temps, on peut choisir de le démontrer ou de l'admettre.
2. Si $x \in S$, alors pour tout $k \in \mathbb{Z}/p\mathbb{Z}$, $k \cdot x$ est toujours un élément de S.

– les autres orbites sont de cardinal p et ont un stabilisateur trivial ; on note k le nombre de ces orbites.

Comme S est union disjointe de ses orbites, on a alors

$$|S| = \left|\left\{x \in \mathbb{F}_q, \quad px^2 = 1\right\}\right| \times 1 + k \times p.$$

Ainsi, d'après le lemme, comme p est inversible dans $\mathbb{F}_q$ puisqu'il est premier et différent de q, on en déduit

$$|S| \equiv \left(\frac{p}{q}\right) + 1 \quad [p].$$

Étape 2. Une seconde sphère unité de $\mathbb{F}_q^p$ équipotente à S.

On définit la forme quadratique φ par

$$\forall x = (x_1, .., x_p) \in \mathbb{F}_q^p, \quad \varphi(x) = 2\left(x_1x_2 + .. + x_{p-2}x_{p-1}\right) + ax_p^2$$

où $a = (-1)^{\frac{p-1}{2}}$. On note aussi $d = \dfrac{p-1}{2}$, et on définit $S' := \left\{x \in \mathbb{F}_q^p,\ \varphi(x) = 1\right\}$ la sphère unité pour φ. La matrice de φ dans la base canonique est

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

et son déterminant est $\det(A) = (-1)^d a = 1$. D'après le théorème de classification des formes quadratiques, les formes φ et $\displaystyle\sum_{i=1}^{p} x_i^2$ sont donc équivalentes, et le changement de variable linéaire qui permet de passer de l'un à l'autre fournit une bijection entre S et S'. On a donc $|S| = |S'|$.

Étape 3. Dénombrement de S' modulo p.

On distingue deux types de points dans S' :

– ceux pour lesquels $x_1 = x_3 = ..x_{p-2} = 0$; il suffit de choisir $x_p \in \left\{x \in \mathbb{F}_q, \quad ax^2 = 1\right\}$ $\left(1 + \left(\frac{a}{q}\right)\right.$ possibilités d'après le lemme) et on a alors q^d possibilités pour les coordonnées restantes

– si au moins l'une des coordonnées $x_1, x_3, .., x_{p-2}$ est non nulle ($q^d - 1$ possibilités) et que x_p est aussi fixé (q possibilités), il reste à choisir un point $(x_2, .., x_{p-1})$ dans un hyperplan affine de $\mathbb{F}_q^d$, soit q^{d-1} possibilités

On a donc

$$|S'| = q^d\left(1 + \left(\frac{a}{q}\right) + q^d - 1\right) = q^d\left(q^d + ((-1)^d)^{\frac{q-1}{2}}\right).$$

Or on a aussi $q^d = \left(\dfrac{q}{p}\right)$, donc en utilisant les résultats des deux premières étapes, on a :

$$\left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \equiv \left(\frac{p}{q}\right) + 1 \quad [p].$$

Or $\left(\dfrac{q}{p}\right)^2 = 1$, donc on peut simplifier les 1 de chaque côté. Il reste l'égalité suivante dans $\mathbb{Z}/p\mathbb{Z}$:

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

Or les deux membres de cette équation dans $\mathbb{Z}/p\mathbb{Z}$ sont dans $\{\pm 1\}$. Comme p est supérieur à 2, cette équation reste vraie dans $\mathbb{Z}$, et on en déduit la loi de réciprocité quadratique. □