2.10 Loi de réciprocité quadratique

Référence : P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 101, 121, 123, 150, 170, 190.

Définition 1. Pour p premier impair et $a \geqslant 1$, on définit le symbole de Legendre

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

Théorème 2 (Loi de réciprocité quadratique)**.** *Si p et q sont deux nombres premiers impairs distincts, alors*

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

Lemme 3. *Si p est premier impair et $a \in \mathbb{F}_p^*$, alors*

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

Démonstration. Cela résulte du fait que si a est un carré modulo p si et seulement si a^{-1} est un carré modulo p et du fait que si b est un carré, le polynôme $X^2 - b$ admet deux racines distinctes dans $\mathbb{F}_p$. □

Démonstration (Théorème). L'idée de la preuve est de calculer de deux façons différentes le cardinal de l'ensemble suivant :

$$X = \Big\{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1\Big\}.$$

La première méthode consiste à faire agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation sur les coordonnées : si $k \in \mathbb{Z}/p\mathbb{Z}$ et $(x_1, \ldots, x_p) \in X$,

$$k \cdot (x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k})$$

où les indices sont vus modulo p. On étudie alors les orbites de cette action. Puisque $\mathbb{Z}/p\mathbb{Z}$ n'a que des sous-groupes triviaux, les seuls stabilisateurs possibles d'un élément sont $\{1\}$ et $\mathbb{Z}/p\mathbb{Z}$. Les orbites dont le stabilisateur des éléments est $\mathbb{Z}/p\mathbb{Z}$ sont les singletons $\{(x, \ldots, x)\}$ avec $x \in \mathbb{F}_q$ tel que $px^2 = 1$, elles sont donc au nombre de $1 + \left(\frac{p}{q}\right)$ par le lemme. Par la relation orbite stabilisateur, les orbites dont le stabilisateur des éléments est trivial sont de cardinal $|\mathbb{Z}/p\mathbb{Z}|/|\{1\}| = p$. Ainsi, pas la formule des classes, $|X| \equiv 1 + \left(\frac{p}{q}\right) \mod p$.

On va maintenant utiliser une forme quadratique équivalente sur $\mathbb{F}_q^p$ à $f(x) = \sum_i x_i^2$ dont la matrice dans la base canonique est I_p. On considère pour cela la matrice

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

où on a posé $a = (-1)^d$ avec $d = (p-1)/2$. Les matrices A et I_p ont même rang p et même déterminant 1, donc même discriminant, elles définissent donc des formes quadratiques équivalentes. Si P est la matrice de changement de base pour passer de l'une à l'autre, on a alors $X' = PX$ et donc $|X| = |X'|$ où on a posé

$$X' = \{(y_1, \ldots, y_d, z_1, \ldots, z_d, t) \in \mathbb{F}_q^p \mid 2(y_1 z_1 + \cdots + y_d z_d) + at^2 = 1\}.$$

On distingue alors deux types d'éléments $(y_1, \ldots, y_d, z_1, \ldots, z_d, t)$ de X :

- Ceux dont tous les y_i sont nuls. Le choix de $(z_1, \ldots, z_d)$ est alors quelconque et donne donc q^d possibilités et celui de t donne, d'après le lemme, $1 + \left(\frac{a}{q}\right)$ possibilités, d'où $q^d \left(1 + \left(\frac{a}{q}\right)\right)$ éléments de X' de cette forme.
- Ceux dont au moins un des y_i est non nul. On choisit donc un vecteur non nul de $\mathbb{F}_q^d$: $q^d - 1$ possibilités, puis on choisit t de manière quelconque dans $\mathbb{F}_q$: q possibilités, il nous reste alors à choisir $(z_1, \ldots, z_d)$ dans l'hyperplan affine d'équation $2(y_1 z_1 + \cdots + y_d z_d) + at^2 - 1 = 0$, il y a donc q^{d-1} possibilités, et $q^d(q^d - 1)$ éléments de ce type dans X'.

On peut alors conclure :

$$q^q \left(1 + \left(\frac{a}{q}\right)\right) + q^d(q^d - 1) \equiv 1 + \left(\frac{p}{q}\right) \mod p$$

c'est-à-dire, avec $\left(\frac{a}{q}\right) = a^{(q-1)/2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, et $\left(\frac{q}{p}\right) = q^{(p-1)/2} = q^d$,

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

ainsi, en multipliant par $\left(\frac{q}{p}\right)$,

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

et on a alors l'égalité modulo p. Or les éléments en jeu sont égaux à ± 1, donc l'égalité est en fait dans $\mathbb{Z}$. □