# Loi de réciprocité quadratique

**Leçons : 101, 120, 121, *123, 126*, 170, 190**

**Définition 1**

*Soit $p$ premier impair. Le symbole de Legendre associé à $p$ est $\left(\frac{\cdot}{p}\right) : a \in \mathbb{F}_p^* \mapsto a^{\frac{p-1}{2}}$. Il vaut $1$ si $a$ est un carré modulo $p$ et $-1$ sinon.*

**Théorème 2**

*Si $p$ et $q$ sont deux premiers impairs distincts, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

**Lemme 3**

*Si $a \in \mathbb{F}_q^*$, l'équation $ax^2 = 1$ a $1 + \left(\frac{a}{q}\right)$ solutions.*

**Démonstration.** Soit $X = \left\{(x_1, \dots, x_p) \in \mathbb{F}_q^p : \sum_{i=1}^{p} x_i^2 = 1\right\}$. On va compter le nombre d'éléments de $X$ de deux manières différentes.

**Étape 1 : dénombrement par la formule des classes.**

$\mathbb{Z}/p\mathbb{Z}$ agit sur $X$ par permutation circulaire via $\overline{a} \cdot (x_1, \dots, x_p) = (x_{1+a}, \dots, x_{p+a})$, les indices étant considérés modulo $p$.

Le stabilisateur d'un élément $x$ étant un sous groupe de $\mathbb{Z}/p\mathbb{Z}$, il est soit trivial soit le groupe tout entier. Dans le second cas, cela signifie que toutes les composantes de $x$ sont égales et que $px_1^2 = 1$ dans $\mathbb{Z}/q\mathbb{Z}$. Selon le lemme, il y a donc $1 + \left(\frac{p}{q}\right)$ orbites réduites à un singleton.

Ainsi, selon la formule des classes, si $x^1, \dots, x^r$ sont les représentants des orbites non triviales,

$$|X| = 1 + \left(\frac{p}{q}\right) + \sum_{i=1}^{r} \frac{p}{|\mathrm{Stab}(x^i)|} \equiv 1 + \left(\frac{p}{q}\right) [p]$$

**Étape 2 : dénombrement "géométrique".**

On remarque que $X = \left\{x \in \mathbb{F}_q^p : q(x) = 1\right\}$ où $q(x) = \sum_{i=1}^{p} x_i^2$. Cette forme quadratique est représentée dans la base canonique $\mathscr{B}$ par $I_p$.

Introduisons la forme quadratique $r : (y_1, \dots, y_d, z_1, \dots, z_d, t) \mapsto 2\sum_{i=1}^{d} y_i z_i + at^2$ où $d = \frac{p-1}{2}$ et $a = (-1)^{\frac{p-1}{2}}$. Quitte à écrire $(y_1, \dots, y_d, z_1, \dots, z_d, t)$ sous la forme $(y_1, z_1, \dots, y_d, z_d, t)$, on peut supposer que la matrice $A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix}$ représente $r$ dans $\mathscr{B}$. Or, $\det A = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} = 1$ donc selon la classification des formes quadratiques dans un

corps fini, $r$ et $q$ sont équivalentes. Si on fixe $u \in \mathrm{GL}_p(\mathbb{F}_q)$ tel que $r = q \circ u$, on constate que $u$ induit une bijection de $X$ sur $X' = \left\{(y_1, \dots, y_d, z_1, \dots, z_d, t) : 2\sum_{i=1}^{d} y_i z_i + at^2 = 1\right\}$. Il s'agit donc de dénombrer $|X'|$.

Il y a deux types de points dans $X'$ :

- Ceux qui vérifient $y_1 = \cdots = y_d = 0$ : il y en a $q^d$ (choix de $z$) multiplié par $1 + \left(\frac{a}{p}\right) = 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (nombre de solutions de $at^2 = 1$).
- Les autres : une fois choisi $(y_1, \dots, y_d)$ non nul ($q^d - 1$ choix) et $t$ ($q$ choix), $z$ est déterminé par l'équation $2\sum_{i=1}^{d} y_i z_i + at^2 = 1$ est celle d'un hyperplan affine de $\mathbb{F}_q^d$ ; il y a donc $q^{d-1}$ possibilités pour $z$.

Ainsi, $X'$ a pour cardinal $q^d\left(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) + (q^d - 1) \times q \times q^{d-1} = q^d\left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)$.

**Étape 3 : Conclusion**

En comparant les deux calculs précédents modulo $p$, on a $1 + \left(\frac{p}{q}\right) \equiv q^{p-1} + q^d(-1)^{\frac{p-1}{2}\frac{q-1}{2}} [p]$

Or, dans $\mathbb{F}_p$, $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$, et $q^{p-1} = 1$ (Fermat) donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, ce qui n'est autre que la loi de réciprocité quadratique.

□

**Théorème 4**

*Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur $\mathbb{F}_q^n$, représentées par $I_n$ et $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ & & 1 \\ (0) & & a \end{pmatrix}$ où $a \in \mathbb{F}_q^*$ n'est pas un carré.*

**Référence :** Philippe CALDERO et Jérome GERMONI (2013). *Histoires hédonistes de groupes et de géométrie*. T. 1. Calvage et Mounet, pp. 185-186