P. Maurer

ENS Rennes

Recasages : *120, 121, 123, 126, 170*

Référence : Caldero-Germoni, H2G2.

Loi de réciprocité quadratique

On commence par des rappels sur le symbole de Legendre. On se donne p un nombre premier et $q = p^n$ avec $n \geq 1$.

Proposition 1. *Si $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p > 2$, on a $|\mathbb{F}_q^2| = \dfrac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \dfrac{q-1}{2}$.*

Démonstration. Si $p = 2$, $\mathbb{F}_q$ est de caractéristique 2, le morphisme de Frobenius $x \mapsto x^2$ est bijectif de $\mathbb{F}_q$ sur $\mathbb{F}_q^2$. On en déduit le résultat.

Supposons désormais $p > 2$. On pose $\varphi : \begin{cases} \mathbb{F}_q^* \to \mathbb{F}_q^{*2} \\ x \mapsto x^2 \end{cases}$. Le premier théorème d'isomorphisme donne

$$\mathbb{F}_q^{*2} \simeq \mathbb{F}_q^* / \operatorname{Ker} \varphi,$$

où $\operatorname{Ker} \varphi = \{x \in \mathbb{F}_q^* : x^2 = 1\} = \{-1, 1\}$. On en déduit que $|\mathbb{F}_q^{*2}| = |\mathbb{F}_q^*| / 2 = \dfrac{q-1}{2}$, puis que $|\mathbb{F}_q^2| = \dfrac{q+1}{2}$. □

Proposition 2. *On suppose $p > 2$ et on se donne $a \in \mathbb{F}_q^*$. Alors*

$$a^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}.$$

Démonstration. On pose $X = \left\{ a \in \mathbb{F}_q^{*2} : a^{\frac{q-1}{2}} = 1 \right\}$. Alors $|X| \leq \dfrac{q-1}{2}$ car un polynôme de degré $\dfrac{q-1}{2}$ a au plus $\dfrac{q-1}{2}$ racines. Par ailleurs, si $a \in \mathbb{F}_q^{*2}$, il existe $x \in \mathbb{F}_q^*$ tel que $a = x^2$ et on a donc $a^{\frac{q-1}{2}} = x^{2 \times \frac{q-1}{2}} = x^{q-1} = 1$, donc $a \in X$. Ainsi, on a l'inclusion $\mathbb{F}_q^{*2} \subset X$, et $|X| \leq |\mathbb{F}_q^{*2}|$ d'après la proposition 1. Ceci conclut que $\mathbb{F}_q^{*2} = X$.

Par ailleurs, pour tout $a \in \mathbb{F}_q^*$, on a $\left(a^{\frac{q-1}{2}}\right)^2 = 1$, donc $a^{\frac{q-1}{2}} \in \{-1, 1\}$. Ceci termine la preuve. □

Définition 3. *On définit le symbole de Legendre pour $p > 2$ et $a \in \mathbb{F}_p$ par*

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

Proposition 4. *Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. On a*

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

Démonstration. On distingue deux cas.

- Si a est un carré, alors il existe $y \in \mathbb{F}_p^*$ tel que $a = y^2$ et on a $ax^2 = 1 \iff (yx)^2 = 1 \iff xy \in \{-1, 1\}$ donc $|\{x \in \mathbb{F}_p : ax^2 = 1\}| = 2$, et d'autre part $\left(\frac{a}{p}\right) = 1$ donc $1 + \left(\frac{a}{p}\right) = 2$.

- Supposons que a n'est pas un carré. Pour $x \in \mathbb{F}_p^*$, on a $ax^2 = 1 \iff a = (x^{-1})^2$, et il est clair que $a0^2 \neq 1$. On en déduit que $|\{x \in \mathbb{F}_p : ax^2 = 1\}| = 0$, et d'autre part on a $\left(\frac{a}{p}\right) = -1$ donc $1 + \left(\frac{a}{p}\right) = 0$. □

Théorème 5. *(Loi de réciprocité quadratique)*

Soit p et q deux nombres premiers impairs distincts. Alors on a

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

Démonstration.

Notons $d = \dfrac{p-1}{2}$. On va calculer le cardinal modulo p de la sphère X de $\mathbb{F}_q^p$ de deux manières :

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

Etape 1 : par l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X.

On fait agir $\mathbb{Z}/p\mathbb{Z}$ par permutation des indices sur $\mathbb{F}_q^p$, de sorte que pour $k \in \mathbb{Z}/p\mathbb{Z}$, on ait

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

les indices étant vus modulos p : $x_{\ell+p} = x_\ell$ pour tout ℓ.

Ceci induit une action de $\mathbb{Z}/p\mathbb{Z}$ sur X, pour laquelle il y a alors deux types d'orbites : les singletons $\{(x, \ldots, x) : x \in X\}$, dont le stabilisateur est $\mathbb{Z}/p\mathbb{Z}$ tout entier et dont l'orbite est triviale, et les autres orbites, dont le stabilisateur est trivial.[1]

Au vu de la définition de X, on a $|\{(x, \ldots, x) : x \in X\}| = |\{x \in \mathbb{F}_q : px^2 = 1\}|$, donc d'après la proposition 4, il y en a $1 + \left(\frac{p}{q}\right)$. Par ailleurs, si $(x_1, \ldots, x_p)$ est dans une orbite non triviale, on a

$$|\mathrm{Orb}(x_1, \ldots, x_p)| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathrm{Stab}(x_1, \ldots, x_p)|} = p.$$

1. On rappelle que $|\mathrm{Stab}(x)|$ divise $|\mathbb{Z}/p\mathbb{Z}| = p$ qui est premier, donc $\mathrm{Stab}(x)$ est soit trivial soit égal à $\mathbb{Z}/p\mathbb{Z}$ tout entier. Il est clair que si $(x_1, \ldots, x_p) \in X^p$ ne vérifie pas $x_1 = \cdots = x_p$, son stabilisateur ne peut être $\mathbb{Z}/p\mathbb{Z}$ tout entier, il est donc trivial.

D'après la formule des classes, il vient $|X| = 1 + \left(\frac{p}{q}\right) + pk$, où k est le nombre d'orbites non triviales. Modulo p, ceci donne

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

Etape 2 : par congruence de deux formes quadratiques.

Notons Q la forme quadratique définie par $Q(x) = \sum_{i=1}^{p} x_i^2$ sur $\mathbb{F}_q^p$. Alors Q est représentée par la matrice I_p, qui est congruente à

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

où $a = (-1)^{\frac{p-1}{2}} = (-1)^d$. En effet, on a $\det(A) = (-1)^{\frac{p-1}{2}} \times a = (-1)^{p-1} = 1$, donc A et I_p ont même déterminant, donc même discriminant dans $\mathbb{F}_q^* / \mathbb{F}_q^{*2}$. Le théorème de classification des formes quadratiques sur $\mathbb{F}_q$ permet alors d'affirmer que Q et la forme quadratique Q' définie par

$$Q'(y_1, \dots, y_d, z_1, \dots, z_d, t) := 2\,(y_1\, z_1 + \cdots + y_d\, z_d) + a t^2$$

sont congruentes. Autrement dit, il existe une application linéaire bijectife ϕ telle que $Q \circ \phi = Q'$. En posant $X' = \{(y_1, \dots, y_d, z_1, \dots, z_d, t) \in \mathbb{F}_q^p :\ 2\,(y_1\, z_1 + \cdots + y_d\, z_d) + a t^2 = 1\}$, on a alors

$$X' = \phi^{-1}(X).$$

Comme ϕ^{-1} est bijective, on en déduit que $|X'| = |X|$, et cette égalité est en particulier vraie modulo p.

Etape 3 : calcul de $|X'|$ et conclusion.

On distingue deux types d'éléments de la forme $(y_1, \dots, y_d, z_1, \dots, z_d, t)$ dans X'.

- D'une part, les éléments tels que $y_1 = \cdots = y_d = 0$. Pour $t \in \mathbb{F}_q$ tel que $at^2 = 1$, il suffit alors de choisir $(z_1, \dots, z_d)$, et il y a q^d manières de le faire. La proposition 4 permet de conclure qu'il y a $q^d\Big(1 + \left(\frac{a}{q}\right)\Big) = q^d\Big(1 + a^{\frac{q-1}{2}}\Big)$ éléments de ce type.

- D'autre part, les éléments tels qu'au moins un y_i est non nul pour $i \in [\![1, d]\!]$. Il y a alors $q^d - 1$ manière de choisir le d-uplet $(y_1, \dots, y_d)$, q manières de choisir t, et une fois ces éléments fixés, choisir $(z_1, \dots, z_d)$ de sorte que $2\,(y_1\, z_1 + \cdots + y_d\, z_d) + a t^2 = 1$ revient à les choisir dans un hyperplan affine de $\mathbb{F}_q^d$. Le cardinal d'un tel hyperplan est q^{d-1}.

  Aussi, il y a un total de $(q^d - 1) q q^{d-1} = (q^d - 1)\, q^d$ éléments de ce type.

On en déduit que $|X'| = q^d\Big(q^d - 1 + 1 + a^{\frac{q-1}{2}}\Big) = q^d\Big(q^d + a^{\frac{q-1}{2}}\Big) = q^d\Big(q^d + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\Big)$. Par ailleurs, $|X| \equiv |X'|\,[p]$, donc d'après le résultat de l'étape 1, il vient

$$1 + \left(\frac{p}{q}\right) \ \equiv\ q^d\Big(q^d + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\Big)\ [p]$$

Par ailleurs, $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$ par définition du symbole de Legendre. On en déduit

$$\begin{aligned} 1+\left(\frac{p}{q}\right) &\equiv \left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right)+(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\right)[p] \\ &\equiv \left(\frac{q}{p}\right)^2+\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}[p] \\ &\equiv 1+\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}[p] \end{aligned}$$

En effet, on a $\left(\frac{q}{p}\right)^2 = \left(q^{\frac{p-1}{2}}\right)^2 = q^{p-1} = 1$, puisque $q \in \mathbb{F}_p^*$ (on a supposé $q \neq p$ dans les hypothèses du théorème). On en déduit finalement que

$$\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}[p],$$

donc en multipliant de part et d'autre par $\left(\frac{q}{p}\right)$,

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

Cette égalité modulo p étant dans $\{-1, 1\}$, elle est encore vraie sur $\mathbb{Z}$, et ceci conclut la preuve du théorème. □