# Loi de réciprocité quadratique

Akita

ENS Rennes, 2013-2014

Référence : *Histoires hédonistes de groupes et de géométries*, Caldero-Germoni.

Développement pour les leçons :
- 101. Groupe opérant sur un ensemble. Exemples et applications.
- 103. Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
- 104. Groupes finis. Exemples et applications.
- 120. Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121. Nombres premiers. Applications.
- 123. Corps finis. Applications.
- 126. Exemples d'équations diophantiennes.
- 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 190. Méthodes combinatoires, problèmes de dénombrement.

Soient $p$ et $q$ deux nombres premiers impairs distincts.

**Définition :**

Pour $a \in \mathbb{F}_p$, 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 (loi de la réciprocité quadratique) :**

On a :

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

*Démonstration :*

On utilisera la propriété suivante : pour $a \in \mathbb{F}_p^*$, on a :

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

Posons :

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

L'idée de la preuve consiste à calculer le cardinal de $S$ de deux manières différentes pour arriver à nos fins. Dans un premier temps, faisons agir $\mathbb{Z}/p\mathbb{Z}$ sur $S$ de manière circulaire :

$$\forall \overline{k} \in \mathbb{Z}/p\mathbb{Z},\ \forall (x_1, \ldots, x_p) \in S,\ \overline{k}.(x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k}),$$

où les indices sont vus modulo $p$ : $x_{i+p} = x_i$. D'après la formule des classes, les orbites sont de deux types : soit elles sont de cardinal égal à 1 (ce sont les singletons $\{(x, \ldots, x)\}$, où $x \in \mathbb{F}_q$), soit elles sont de cardinal égal à $p$. Or le nombre d'orbites de type singleton est égal au nombre de solutions $x$ de l'équation $px^2 = 1$ dans $\mathbb{F}_q$. On en déduit la première égalité :

$$|S| = \left(\frac{p}{q}\right) + 1 \mod p.$$

Maintenant considérons les formes quadratiques suivantes :

$$q_1(x_1, \ldots, x_p) := \sum_{i=1}^{p} x_i^2$$

$$\text{et} \quad q_2(x_1, \ldots, x_p) := \sum_{i=1}^{\frac{p-1}{2}} 2\, x_{2i-1}\, x_{2i} + (-1)^{\frac{p-1}{2}} x_p^2.$$

Leurs matrices $p \times p$ à coefficients dans $\mathbb{F}_q$ sont respectivement :

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } A = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & 1 & \\ & & & & & 1 & 0 & \\ & & & & & & & (-1)^{\frac{p-1}{2}} \end{pmatrix}.$$

Or $I_p$ et $A$ ont même déterminant et donc même discriminant. D'après la classification des formes quadratiques sur $\mathbb{F}_q$, $q_1$ et $q_2$ sont équivalentes et on a alors :

$$|S| = |\tilde{S}| := \left| \left\{ (x_1, \ldots, x_p) \in \mathbb{F}_q^p,\ \sum_{i=1}^{\frac{p-1}{2}} 2\, x_{2i-1}\, x_{2i} + (-1)^{\frac{p-1}{2}} x_p^2 = 1 \right\} \right|.$$

Distinguons deux types de points de $\tilde{S}$ :
- les points tels que $x_1 = x_3 = \cdots = x_{p-2} = 0$ : chaque valeur de $x_p$ telle que $(-1)^{(p-1)/2}\, x_p^2 = 1$ détermine $q^{(p-1)/2}$ points, donc, d'après la propriété du début, on a $q^{(p-1)/2}(1 + (-1)^{(p-1)(q-1)/4})$ points de ce type,
- les points pour lesquels au moins un des $x_{2i-1}$ est non nul : une fois fixés les $x_{2i-1}$ ($q^{(p-1)/2} - 1$ choix possibles) et $x_p$ ($q$ choix possibles), il reste à choisir $(x_2, x_4, \ldots, x_{p-1})$ dans un hyperplan affine de $\mathbb{F}_q^{(p-1)/2}$ ($q^{(p-3)/2}$ choix possibles) : il y a donc $q^{(p-1)/2}(q^{(p-1)/2} - 1)$ points de ce type.

On obtient ainsi notre deuxième égalité et on en déduit :

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

D'où la formule voulue après simplification (multiplication par $\left(\frac{q}{p}\right)$).

Un mot sur le symbole de Legendre :

justification (pour $a \neq 0$) de $a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } a = 0 \end{cases}$ :

Considérons les morphismes de groupes $\chi : \begin{cases} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{cases}$ et $\lambda : \begin{cases} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longrightarrow & x^{(p-1)/2} \end{cases}$.
D'après le petit théorème de Fermat, le morphisme $\lambda \circ \chi = \chi \circ \lambda$ est trivial. On en déduit d'une part : $a^{(p-1)/2} = \pm 1$. D'autre part : $\mathrm{Im}\chi \subset \ker\lambda$. Or $|\mathrm{Im}\chi| = |\mathbb{F}_p^*|/|\ker\chi| = (p-1)/2$ et $|\ker\lambda| \leq (p-1)/2$ car $\ker\lambda = \{\text{racines de } X^{(p-1)/2} - 1\}$ (sur un corps commutatif). D'où : $\ker\lambda = \mathrm{Im}\chi$. The end !

**Remarques :**

- attention dans le C-G il y a plusieurs coquilles : dans la formule en-dessous de "En effet, faisons agir ...", l'indice du dernier $x_i$ est $p$ et pas $n$ ; il faut rajouter "non" après le premier "stabilisateur", enlever "non" après le deuxième (et le pan de phrase "nécessairement ...") et rajouter "non" devant le troisième,
- cf les remarques dans le C-G autour du symbole de Legendre.

**Annexe (Calcul de $\left(\frac{2}{p}\right)$) :**

Soit $\alpha$ une racine de $X^4+1$. C'est une racine $8^e$ primitive de l'unité dans une extension de $\mathbb{F}_p$, ie : $\alpha^8 = 1$ et $\alpha^4 = -1$, ou encore : $\alpha^2 = -\alpha^{-2}$.

Posons $\beta := \alpha + \alpha^{-1}$. Alors $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = 2$. Donc 2 est un carré dans $\mathbb{F}_p$ ssi $\beta \in \mathbb{F}_p$. Or $\beta \in \mathbb{F}_p \Leftrightarrow \beta^p = \beta$. Calculons : $\beta^p = \alpha^p + \alpha^{-p}$, d'où :

$$\text{pour } p \equiv \pm 1 \ [8],\ \beta^p = \alpha + \alpha^{-1} = \beta,\ \text{car } \alpha^8 = 1,$$

$$\text{pour } p \equiv \pm 3 \ [8],\ \beta^p = \alpha^3 + \alpha^{-3} = \alpha^{-1}(\alpha^4 + \alpha^{-2}) = \alpha^{-1}(-1 - \alpha^2) = -\beta,\ \text{car } \alpha^4 = -1.$$

D'où le résultat voulu. Référence : *Arithmétique*, Hindry.