

Loi de réciprocité quadratique.

Référence : Nouvelles histoires hédonistes de groupes et de géométries, chapitre V, annexe C, Caldero-Germoni.

Leçons : 120, 121, 123, 126, 170, 190.

Théorème : Soient p et q deux nombres premiers impairs distincts.

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

Preuve :

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

“On va calculer le cardinal de X modulo p de deux manières différentes, et on va en déduire la loi de réciprocité quadratique.”

“Considérons l'action de groupe suivante de $\mathbb{Z}/p\mathbb{Z}$ sur X :

$\varphi : \begin{cases} \mathbb{Z}/p\mathbb{Z} \times X & \rightarrow X \\ (k, (x_1, \dots, x_p)) & \mapsto (x_{k+1}, \dots, x_{k+p}) \end{cases}$ (“où $+$ désigne l'addition dans $\mathbb{Z}/p\mathbb{Z}$, $1, \dots, p$ désignant ici les éléments de $\mathbb{Z}/p\mathbb{Z}$ ”).

(φ est à valeurs dans X parce que $(x_{k+1}, \dots, x_{k+p}) \in (\mathbb{F}_q)^p$ et $\sum_{i=1}^p x_{k+i}^2 = 1$.)

($\varphi((k+k', (x_1, \dots, x_p))) = \varphi((k, (\varphi((k', (x_1, \dots, x_p))))))$ et $\varphi((0, (x_1, \dots, x_p))) = (x_1, \dots, x_p)$.)

D'après la formule des classes on a : $|X| = \sum_{i \in I} |O_i| = \sum_{i \in I} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|S_i|}$ (“où les $O_i, i \in I$ sont les orbites de X et les S_i les stabilisateurs associés”) qui est congru au nombre d'orbites réduites à un élément de X modulo p (car les S_i sont des sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ donc d'ordre 1 ou p).

Or l'orbite de $(x_1, \dots, x_p) \in X$ est réduite à un élément si et seulement si $x_1 = \dots = x_p$, et pour tout $x \in \mathbb{F}_q$, $(x, \dots, x) \in X$ si et seulement si $px^2 = 1$, donc le nombre d'orbite réduites à un élément de X est le nombre de solutions de $px^2 = 1$ dans $\mathbb{F}_q$, donc 2 si p est un carré modulo q et 0 sinon, donc $1 + \left(\frac{p}{q}\right)$.

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

Montrons à présent que $|X| = (q^{\frac{p-1}{2}} + (-1)^{\frac{(p-1)(q-1)}{4}})q^{\frac{p-1}{2}}$.

Remarquons que $X = \{x \in (\mathbb{F}_q)^p, {}^t x x = 1\}$.

$$\text{Or } \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } A := \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \\ & & & & & (-1)^{\frac{p-1}{2}} \end{pmatrix} \text{ sont symétriques}$$

et congruentes (car inversibles et de même discriminant, cf. classification des formes quadratiques dans les corps finis) donc X est en bijection avec $X' = \{y \in (\mathbb{F}_q)^p, {}^t y A y = 1\}$.

$$X' = \{(y_1, z_1, \dots, y_d, z_d, t) \in (\mathbb{F}_q)^p, 2 \sum_{i=1}^d y_i z_i + at^2 = 1\} \text{ (où } d = \frac{p-1}{2} \text{ et } a = (-1)^d).$$

Soit $(y_1, z_1, \dots, y_d, z_d, t) \in (\mathbb{F}_q)^p$.

Si $y_1 = \dots = y_d = 0$ alors on a équivalence entre $(y_1, z_1, \dots, y_d, z_d, t) \in X'$ et $at^2 = 1$ donc l'ensemble des $(y_1, z_1, \dots, y_d, z_d, t) \in X'$ tels que $y_1 = \dots = y_d = 0$ est de cardinal $q^d(1 + a^{\frac{q-1}{2}}) = q^d(1 + (-1)^{\frac{(p-1)(q-1)}{4}})$ (choix de $z_1, \dots, z_d$ et nombre de solutions à $at^2 = 1$, même raisonnement que plus haut).

Sinon, il y a $q^d - 1$ choix pour les y_j , et si $y_i \neq 0$ (ce qui implique $2y_i \neq 0$ puisque $q \neq 2$) $2 \sum_{i=1}^d y_i z_i + at^2 = 1$ se réécrit $z_i = (-2y_i)^{-1}(\sum_{j \neq i} y_j z_j + at^2)$ donc on peut choisir t et les z_j ($j \neq i$) quelconques dans $\mathbb{F}_q$ et z_i est alors fixé, ce qui fait que l'ensemble des $(y_1, z_1, \dots, y_d, z_d, t) \in X'$ tels qu'on n'a pas $y_1 = \dots = y_d = 0$ est de cardinal $(q^d - 1)q^d$.

$$X', \text{ et donc } X, \text{ est donc de cardinal } q^d(1 + (-1)^{\frac{(p-1)(q-1)}{4}}) + (q^d - 1)q^d = q^d((-1)^{\frac{(p-1)(q-1)}{4}} + q^d) \equiv \left(\frac{q}{p}\right) ((-1)^{\frac{(p-1)(q-1)}{4}} + \left(\frac{q}{p}\right)) \pmod{p} \equiv \left(\frac{q}{p}\right) (-1)^{\frac{(p-1)(q-1)}{4}} + 1 \pmod{p}.$$

Avec ce qui précède on a donc $1 + \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) (-1)^{\frac{(p-1)(q-1)}{4}} + 1 \pmod{p}$ d'où $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \pmod{p}$ (car $\left(\frac{p}{q}\right)$ est son propre inverse). Or ces termes sont égaux à 1 ou -1 et $p \neq 2$ donc l'égalité est vraie dans $\mathbb{Z}$.