Développement : Loi de réciprocité quadratique

Leçons : 101, 120, 121, 123, 170, 190.

Théorème. *Soient p, q deux nombres premiers impairs distincts. On a* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Démonstration.
On considère la sphère $S = \left\{(x_1, \cdots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\right\}$. On va calculer son cardinal de deux façons différentes.

Étape 1 : Calcul par action de groupes.
On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur S par $k\cdot(x_1, \cdots, x_p) = (x_{1+k}, \cdots, x_{p+k})$ (où les indices sont modulo p). Soit $(x_1, \cdots, x_p) \in S$.
- Si $x_1 = \cdots = x_p$, alors son orbite est un singleton et son stabilisateur est $\mathbb{Z}/p\mathbb{Z}$. De plus, on a $px_1^2 = 1$.
- Sinon, le stabilisateur est un sous-groupe propre de $\mathbb{Z}/p\mathbb{Z}$, donc $\{0\}$ par le théorème de Lagrange. L'orbite est donc de cardinal p.

Soit Ω une transversale de l'action, et Ω_s l'ensemble des singletons $\{y, \cdots, y\}$ de S. On écrit la formule des classes :

$$|S| = \sum_{x\in\Omega} |\mathrm{Orb}(x)| = \sum_{x\in\Omega_s} |\mathrm{Orb}(x)| + \sum_{x\in\Omega\setminus\Omega_s} |\mathrm{Orb}(x)| = \left|\{x_1 \in \mathbb{F}_q, px_1^2 = 1\}\right| + p|\Omega\setminus\Omega_s| \equiv 1 + \left(\frac{p}{q}\right) [p]$$

car $\left|\{x_1 \in \mathbb{F}_q, px_1^2 = 1\}\right| = 1 + \left(\frac{p}{q}\right)$ (se prouve en distinguant les cas p carré et p non carré).

Étape 2 : Calcul avec des formes quadratiques.
On pose $d = \dfrac{p-1}{2}$, et on considère les matrices carrées $p \times p$ de $\mathbb{F}_q$

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \qquad A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix}$$

avec $a = (-1)^d = (-1)^{\frac{p-1}{2}}$. Elles sont symétriques, de rang p et de déterminant 1. Il existe donc $P \in GL_p(\mathbb{F}_q)$ telle que $I_p = {}^tPAP$. Si $X \in \mathbb{F}_q^p$, on a $X \in S \Leftrightarrow {}^tXX = 1$, or ${}^tXX = {}^tXI_pX = {}^tX{}^tPAPX = {}^t(PX)A(PX)$.
Ainsi, si on pose $S' = \{Y \in \mathbb{F}_q^p, {}^tYAY = 1\}$, on a $|S| = |S'|$. Soit $Y = (y_1, z_1, \cdots, y_d, z_d, t) \in \mathbb{F}_q^p$. Alors
$Y \in S' \Leftrightarrow {}^tYAY = 1 \Leftrightarrow 2y_1z_1 + \cdots + 2y_dz_d + at^2 = 1$. Alors :
- Si $y_1 = \cdots = y_d = 0$, il y a $1 + \left(\frac{a}{q}\right)$ manières de choisir t, et q^d manières de choisir $(z_1, \cdots, z_d)$.
- Sinon, il y a $q^d - 1$ manières de choisir $(y_1, \cdots, y_d)$ et q manières de choisir t. Ce d-uplet et t étant fixés, il existe k tel que $y_k \neq 0$. On pose $z_k = (2y_k)^{-1}(1 - at^2)$. Alors $Y_k := (0, \cdots, 0, y_k, z_k, 0, \cdots, 0, t) \in S'$. Soit H l'hyperplan vectoriel de $\mathbb{F}_q^d$ d'équation cartésienne $2y_1Z_1 + \cdots + 2y_dZ_d = 0$. Ainsi, $(z_1, \cdots, z_d)$ convient si et seulement si il appartient à l'hyperplan affine $Y_k + H$, qui est de cardinal q^{d-1} (car H est de dimension $d-1$ sur $\mathbb{F}_q$). Il y a donc $(q^d - 1)qq^{d-1} = q^d(q^d - 1)$ possibilités.

On a donc $|S'| = q^d\left[1 + \left(\frac{a}{q}\right) + q^d - 1\right] = q^d\left[\left(\frac{a}{q}\right) + q^d\right] = q^d\left(\frac{a}{q}\right) + q^{p-1} = q^d\left(\frac{a}{q}\right) + 1$.

Étape 3 : Conclusion.
On a $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}}$. Par ailleurs, on a $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$. D'où, modulo p, on a
$|S| = |S'| \Leftrightarrow 1 + \left(\frac{p}{q}\right) = 1 + \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}} \Leftrightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$, en notant que $\left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)$. □

Références

P. Caldero, J. Germoni, Histoires hédonistes de groupes et de géométrie, Calvage & Mounet, p. 185.

Notes personnelles

Joli, original, se recase bien, mais attention, ça utilise un résultat fort (la classification des formes quadratiques sur les corps finis).