Loi de réciprocité quadratique

Riffaut Antonin

2013-2014

Lemme 1. *Soient p un nombre premier impair et $a \in \mathbb{F}_p^*$. Alors*

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

Théorème 2 (Loi de réciprocité quadratique)**.** *Soient p et q deux nombres premiers impairs distincts. Alors*

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

Démonstration. Considérons l'ensemble

$$X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p\,;\, x_1^2 + \cdots + x_p^2 = 1\}.$$

Nous allons dénombrer les éléments de X de deux manières différentes :

Méthode 1. Faisons agir le groupe $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire des coordonnées. Pour cette action, il y a deux types d'orbites : d'une part, les singletons de la forme $\{(x, \dots, x)\}$ avec $x \in \mathbb{F}_p$, dont les stabilisateurs sont égaux à $\mathbb{Z}/p\mathbb{Z}$; d'autre part, toutes les autres orbites ont nécessairement un stabilisateur trivial. Le nombre d'orbites de la forme $\{(x, \dots, x)\}$ avec $x \in \mathbb{F}_p$, est égal au nombre de solutions de l'équation $px^2 = 1$ d'inconnue $x \in \mathbb{F}_p$, qui vaut $1 + \left(\frac{p}{q}\right)$ d'après le lemme 1. Chacune des autres orbites est de cardinal p d'après la relation orbite-stabilisateur.

En partitionnant X par les orbites distinctes de cette action, on en déduit que

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

Méthode 2. Les formes quadratiques $Q : (x_1, \dots, x_p) \longmapsto x_1^2 + \cdots + x_p^2$ et $Q' : (y_1, z_1, \dots, y_d, z_d, t) \longmapsto 2(y_1z_1 + \cdots + y_dz_d) + at^2$, avec $d = \frac{p-1}{2}$ et $a = (-1)^d$, sont équivalentes sur $\mathbb{F}_q^p$: en effet, leurs matrices respectives sont I_p et

$$\begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & a \end{pmatrix},$$

de même rang et de même discriminant (elles sont toutes deux de déterminant 1), donc elles sont congruentes en vertu de la classification des formes quadratiques sur les corps finis. Ainsi, le cardinal de X est égal au cardinal de l'ensemble

$$X' = \{(y_1, \dots, y_d, z_1, \dots, z_d, t) \in \mathbb{F}_q^p\,;\, 2(y_1z_1 + \cdots + y_dz_d) + at^2 = 1\}.$$

Dénombrons les éléments de X'. Soit $(y_1, \dots, y_d, z_1, \dots, z_d, t) \in X'$.

- Si $y_1 = \cdots = y_d = 0$, alors $at^2 = 1$. Il y a donc q possibilités pour chaque z_i, et $1 + \left(\frac{a}{q}\right)$ possibilités pour t par le lemme 1, soit un total de $q^d \left(1 + \left(\frac{a}{q}\right)\right)$ possibilités.
- Sinon, il existe au moins un y_i non nul. À $y_1, \ldots, y_d$ et t fixés, les z_i possibles forment un hyperplan affine de $\mathbb{F}_q^d$, il y a donc q^{d-1} possibilités. Au total, il y a $(q^d - 1)qq^{d-1} = (q^d - 1)q^d$ possibilités.

On en déduit que $|X| = q^d \left(q^d + \left(\frac{a}{q}\right)\right)$.

Finalement, en recoupant les deux méthodes, on obtient

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

d'où il s'ensuit la loi de réciprocité quadratique après simplification. ■

Complément : classification des formes quadratiques sur les corps finis

Théorème 3. *Soient $K = \mathbb{F}_q$ un corps fini de caractéristique différente de 2, et V un K-espace vectoriel de dimension finie n. Dans une base adaptée, toute forme quadratique non dégénérée sur V a une matrice de la forme I_n ou*

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \alpha \end{pmatrix},$$

avec $\alpha \in K$ non carré (il y a donc exactement deux classes de congruence de formes quadratiques sur V).

Démonstration. Procédons par récurrence sur n. Si $n = 1$, le résultat est immédiat. Supposons que $n \geq 2$, et que le résultat soit vrai au rang $n - 1$. Soient Q une forme quadratique non dégénérée sur V, et $(e_1, \ldots, e_n)$ une base de V orthogonale pour Q. Pour tous $\lambda, \mu \in K$,

$$Q(\lambda e_1 + \mu e_2) = \lambda^2 Q(e_1) + \mu^2 Q(e_2).$$

Montrons qu'il existe $\lambda, \mu \in K$ tels que $\lambda^2 Q(e_1) + \mu^2 Q(e_2) = 1$. Comme K contient $\frac{q+1}{2}$ carrés, les ensembles $E = \{\lambda^2 Q(e_1)\,;\, \lambda \in K\}$ et $F = \{1 - \mu^2 Q(e_2)\,;\, \mu \in K\}$ sont tous deux de cardinal $\frac{q+1}{2}$ ($Q(e_1), Q(e_2) \neq 0$ car Q est non dégénérée). Ainsi, $|E| + |F| = q + 1 > q = |K|$, donc par le principe des tiroirs, $E \cap F \neq \emptyset$.

On pose alors $e_1' = \lambda e_1 + \mu e_2$. On a $Q(e_1') = 1$. L'hypothèse de récurrence appliquée à la forme quadratique non dégénérée Q' induite par Q sur $\mathrm{Vect}(e_1')^\perp$ permet de conclure. ■

Références

[Cal] Philippe Caldero, Jérôme Germoni, *Histoires hédonistes de groupes et de géométries.*