Loi de réciprocité quadratique par les formes quadratiques

Leçon: 121, 170, 123
Réf: H2G2, tome 1

On va prouver le théorème suivant:

Théorème 1

Soit p et q deux nombres premiers impairs distincts. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}$$

Les rappels du symbole de Legendre sont à la fin.

Preuve

idée: calculer de deux façons différentes le cardinal modulo p de la "sphère" sur $\mathbb{F}_q$:
$$X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p : \sum_{i=1}^{p} x_i^2 = 1\}.$$

→ d'une part, avec une action de groupe
→ d'autre part, en étudiant la forme quad.

1) $\mathbb{Z}/p\mathbb{Z} \curvearrowright \mathbb{F}_q^p$ avec:
$$\begin{array}{|l} \mathbb{Z}/p\mathbb{Z} \times X \longrightarrow X \\ (k, (x_1, \dots, x_p)) \mapsto k\cdot(x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k}) \end{array}$$

où les indices sont vus modulo p, $\forall l \in [\![1, p]\!]$, $x_{l+p} = x_l$.

~~• Soit $x \in \mathbb{F}_q$ et $(x, \dots, x) \in X$.~~
~~Alors $\mathrm{Orb}_{\mathbb{Z}/p\mathbb{Z}}(x, \dots, x) = \{(x, \dots, x)\}$.~~

~~Si $(x_1, \dots, x_p) \in X$, avec $i \neq j$, $x_i \neq x_j$.~~

~~alors $\mathrm{Stab}_{\mathbb{Z}/p\mathbb{Z}}(x_1, \dots, x_p) = \{k \in \mathbb{Z}/p\mathbb{Z},\ k \cdot (x_1, \dots, x_p) = (x_1, \dots, x_p)\}$~~

~~et $\mathrm{Stab}_{\mathbb{Z}/p\mathbb{Z}}(x, \dots, x) = \mathbb{Z}/p\mathbb{Z}$.~~

~~Ainsi le nombre d'orbites à stabilisateur trivial~~

Il y a deux sortes d'orbites :

type 1 $\to$ celle dont le stabilisateur est $\mathbb{Z}/p\mathbb{Z}$, elles sont de la forme $\{(x, \dots, x)\}$ où $x \in \mathbb{F}_q$. On a donc

$$p x^2 = 1.$$

type 2 $\to$ les autres, dont le stabilisateur est un sg strict de $\mathbb{Z}/p\mathbb{Z}$, donc est forcément trivial.

Par l'équat° aux classes :

$$|X| = \sum_{\text{orbites}} |\text{orbite}| = \sum_{\substack{\text{orbite} \\ \text{de type 1}}} |\text{Orbite}| + \sum_{\substack{\text{orbite} \\ \text{de type 2}}} |\text{Orbite}|$$

relat° orbite / stabilisateur

$$= \sum_{\substack{x \in \mathbb{F}_q, \\ p x^2 = 1}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} + \underbrace{\sum \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{1\}|}}_{= 0 \text{ modulo } p}$$

et $|\{x \in \mathbb{F}_q, p x^2 = 1\}| = 1 + \left(\frac{p}{q}\right)$ (lemme)

$\to$ preuve après

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

2) On va étudier une forme quadratique.

Les matrices $I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ et $A = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 & \\ & & & & & 1 & 0 & \\ & & & & & & & a \end{pmatrix}$

ceci $a = (-1)^{(p-1)/2} = (-1)^d$ avec $d = \frac{p-1}{2}$ sont congruentes car

→ symétriques
→ m̂ rang (p)
→ m̂ déterminant, donc même discriminant.

) sur $\mathbb{F}_p$.

(Thm de classificat° des formes quadratiques).

Donc X s'identifie par un chgt linéaire de variables à

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

On distingue deux types de points:

- les points tq $y_1 = \dots = y_d = 0$, alors $at^2 = 1$
  $\rightarrow$ il y en a $q^d\left(1 + \left(\frac{a}{q}\right)\right) = \left(1 + \left(\frac{(-1)^{(p-1)/2}}{q}\right)\right)q^d$
  $= \left(1 + \left(\frac{a}{q}\right)\right)q^d$

- s'il existe un y_i non nul $\rightarrow (y_1, \dots, y_d)$ vecteur non nul de $\mathbb{F}_q^d$
  il y en a $q^d - 1$. Le choix de t est quelconque et alors une fois t et les y_i fixés les $(z_1, \dots, z_d)$ vivent dans un hyperplan affine de $\mathbb{F}_q^d$ $\rightarrow$ il y en a q^{d-1}!

  Au total: $\underbrace{(q^d - 1)}_{\text{les } y_i} \times \underbrace{q}_{t} \times \underbrace{q^{d-1}}_{\text{les } z_j}$

Ainsi $|X| = |X'| = q^d\left(1+\left(\frac{a}{q}\right)\right) + (q^d-1)qq^{d-1}$

$$= q^d\left[1+\left(\frac{a}{q}\right) + q^d - 1\right]$$

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

Au final, comme $\cancel{q^d\left(\left(\frac{a}{p}\right) + q^d\right) =}$

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

$$\iff \left(\frac{q}{p}\right)\left[\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right] \equiv \left(\frac{p}{q}\right) + 1 \; [p]$$

$$\iff \cancel{\left(\frac{q}{p}\right)} + \underbrace{(-1)^{\frac{p-1}{2}\frac{q-1}{2}}}_{\in \pm 1} = \underbrace{\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)}_{\in \pm 1} + \cancel{\left(\frac{q}{p}\right)} \; [p]$$

donc on a égalité dans $\mathbb{Z}$,

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

$\square$