Loi de réciprocité quadratique

Dorian Cacitti-Holland

2020-2021

Références.

1. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
2. Algèbre et géométrie de Jean-Etienne Rombaldi

Leçons.

1. 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$, applications
2. 121 Nombres premiers, applications
3. 123 Corps finis, applications
4. 126 Exemples d'équations en arithmétique
5. 150 Exemples d'actions de groupes sur des espaces de matrices
6. 170 Formes quadratiques sur un espace vectoriel de dimension finie, orthogonalité, isotropie, applications

Lemme. Soit $a \in \mathbb{Z}^*$ et $q \in \mathcal{P}\backslash\{2\}$ tel que q ne divise pas a, alors

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

Démonstration.
On a $a \in \mathbb{F}_q^2 \iff a^{-1} \in \mathbb{F}_q^2$
Donc si $a \in \mathbb{F}_q^2$ alors il existe $x \in \mathbb{F}_q$ tel que $x^2 = a^{-1}$, d'où x et $-x$ sont deux racines distinctes (car $q \neq 2$) de $aX^2 - 1$ dans $\mathbb{F}_q$.
Réciproquement si $aX^2 - 1$ a deux racines distinctes dans $\mathbb{F}_q$ alors il existe $x \in \mathbb{F}_q$ tel que $ax^2 = 1$, donc $a^{-1} \in \mathbb{F}_q^2$, puis $a \in \mathbb{F}_q^2$.
Par conséquent

$$\left|\left\{x \in \mathbb{F}_q, ax^2 = 1\right\}\right| = \left|\left\{x \in \mathbb{F}_q, (aX^2 - 1)(x) = 0\right\}\right| = \left\{ \begin{array}{cccc} 0 & si & a \notin \mathbb{F}_q^2 \\ 2 & si & a \in \mathbb{F}_q^2 \end{array} \right. = 1 + \left(\frac{a}{q}\right)$$

□

Théorême. Soit $(p, q) \in (\mathcal{P}\backslash\{2\})^2$ distincts, alors

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

Démonstration. On considère

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

Etape 1 : Calcul de $|X|$ par une forme quadratique

On considère $f \in Q(\mathbb{F}_q^p)$ définie dans la base canonique b de $\mathbb{F}_q^p$ par

$$Mat_b(f) = I_p$$

On pose $d = \frac{p-1}{2}, a = (-1)^d, J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et on considère la forme quadratique $g \in Q(\mathbb{F}_q^p)$ définie par

$$Mat_b(g) = diag(J, ..., J, a) =: M$$

Alors $rg(M) = p = rg(I_p)$, ie f et g sont non dégénérées.
De plus

$$det(M) = det(J)^d a = (-1)^d(-1)^d = 1 = det(I_p)$$

Ainsi, pour toute base e de E et P la matrice de passage entre b et e,

$$\frac{\Delta_e(f)}{\Delta_e(g)} = \frac{det(P)^2\Delta_b(f)}{det(P)^2\Delta_b(g)} = 1 \in \mathbb{F}_q^2$$

Donc par classification des formes quadratiques sur les corps finis, M et I_p sont congruentes. Ainsi

$$|X| = \left|f^{-1}(\{1\})\right| = |g^{-1}(\{1\})| = \left| \left\{ (y_1, z_1, ..., y_d, z_d, x) \in \mathbb{F}_q^p, 2\sum_{i=1}^{d} y_i z_i + ax^2 = 1 \right\} \right|$$

Soit $(y_1, z_1, ..., y_d, z_d, x) \in \mathbb{F}_q^p$ tel que $2\sum_{i=1}^{d} y_i z_i + ax^2 = 1$, alors distinguons plusieurs cas :

- Si $y_1 = ... = y_d = 0$ alors $z_1, ..., z_d$ peuvent être quelconques (q^d choix possibles) mais $ax^2 = 1$, d'où d'après ce qui précède il y a $1 + \left(\frac{a}{q}\right)$ choix possibles pour x, d'où $q^d\left(1 + \left(\frac{a}{q}\right)\right)$ choix possibles pour $(y_1, z_1, ..., y_d, z_d, x)$.
- S'il existe $i \in [\![1, d]\!]$ tel que $y_i \neq 0$ alors $(y_1, ..., y_d)$ est un vecteur non nul de $\mathbb{F}_q^d$ pour lequel il y a $(q^d - 1)$ choix possibles.
  Puis en fixant $x \in \mathbb{F}_q$ (donc q choix possibles), alors $(z_1, ..., z_d)$ vit dans un hyperplan affine de $\mathbb{F}_q^d$, d'où q^{d-1} choix possibles pour $(z_1, ..., z_d)$.
  Finalement on a $(q^d - 1)qq^{d-1} = (q^d - 1)q^d$ choix possibles pour $(y_1, z_1, ..., y_d, z_d, x)$.

Par conséquent

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

Etape 2 : Calcul de $|X|$ par action de $\mathbb{F}_p$ sur $\mathbb{F}_q^p$

On considère l'action par permutation cyclique

$$\forall k \in \mathbb{F}_p, \forall x \in \mathbb{F}_q^p, k.x = (x_{1+k}, ...x_{p+k})$$

Où les indices sont vus modulo p, et on la restreint au sous-ensemble stable X.
Soit $x \in X$, alors :

— Si $Stab(x) = \mathbb{F}_p$ alors $Orb(x) = \{(x_1, ..., x_1)\}$ et

$$px_1^2 = f(x) = 1$$

— Sinon $Stab(x) \neq \mathbb{F}_p$, mais comme $Stab(x) < \mathbb{F}_p$, par théorème de Lagrange

$$|Stab(x)| \mid |\mathbb{F}_p| = p$$

avec p premier, d'où $Stab(x) = \{1\}$.

Par conséquent, d'après la formule des classes,

$$|X| = \sum_{Stab(x)=\mathbb{F}_p} |Orb(x)| + \sum_{Stab(x)\neq\mathbb{F}_p} \frac{|\mathbb{F}_p|}{|Stab(x)|} = |\{x_1 \in \mathbb{F}_q, px_1^2 = 1\}| + Np$$

D'où, grâce au lemme précédent,

$$|X| = 1 + \left(\frac{p}{q}\right) + Np \equiv 1 + \left(\frac{p}{q}\right) [p]$$

Etape 3 : Transitivité de la relation d'égalité dans $\mathbb{F}_p$

Par conséquent on a

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

Or $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}[p] = q^d[p]$ et $\left(\frac{a}{q}\right) = \left(\frac{(-1)^d}{q}\right) = \left(\frac{-1}{q}\right)^d = (-1)^{\frac{q-1}{2}d}$.

Donc

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

ie

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

D'où comme ces nombres sont $-1, 1$ et $p \neq 2$

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

□