

Réciprocité quadratique

Recasage: 101, 126, 170, 190 (voire 121)

Réf: Caldero - Germoni, NH262 Tome 1 p. 304

Lemme: p premier impair, $a \in \mathbb{F}_p^*$, alors $|\{x \in \mathbb{F}_p : ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$

Dém: a est un carré dans $\mathbb{F}_p^*$ $\Leftrightarrow a^{-1}$ est un carré dans $\mathbb{F}_p^*$
 $\Leftrightarrow ax^2 - 1 \in \mathbb{F}_p[X]$ a deux racines distinctes

Ainsi $|\{x \in \mathbb{F}_p : ax^2 = 1\}| = \begin{cases} 0 = 1 - 1 = 1 + \left(\frac{a}{p}\right) & \text{si } a \notin \mathbb{F}_p^{*2} \\ 2 = 1 + 1 = 1 + \left(\frac{a}{p}\right) & \text{si } a \in \mathbb{F}_p^{*2} \end{cases} \quad \square$

Théorème: $p \neq q$ premiers impairs, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Dém: On calcule de deux manières $|X| \bmod p$ où $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^p x_i^2 = 1\}$

* on fait agir $\mathbb{F}_p$ sur $\mathbb{F}_q^p$ par permutation cyclique :

$$\forall k \in \mathbb{F}_p, \forall (x_1, \dots, x_p) \in \mathbb{F}_q^p, k \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$$

où les indices sont vus mod p : $x_{p+p} = x_p$.

Le stabilisateur d'un élément est un sous-groupe de $\mathbb{F}_p$ donc par Lagrange, comme p est premier, on a que deux stabilisateurs possibles : $\{1\}$ et $\mathbb{F}_p$.

Si $\text{Stab}_u = \mathbb{F}_p$: $\forall k \in \mathbb{F}_p, k \cdot u = (u_{1+k}, \dots, u_{p+k}) = (u_1, \dots, u_p) = u$
 donc $u = (x, \dots, x)$ où $x \in \mathbb{F}_q$.

Donc $\begin{cases} u \in X \\ \text{Stab}_u = \mathbb{F}_p \end{cases} \Leftrightarrow u = (x, \dots, x), x \in \mathbb{F}_q : px^2 = 1 \text{ (dans } \mathbb{F}_q)$

D'après le lemme, il y a $1 + \left(\frac{p}{q}\right)$ tels éléments

$$\text{D'après l'équation aux classes, } |X| = \sum_{\substack{x \in \mathbb{F}_q \\ px^2 = 1}} \frac{|\mathbb{F}_p|}{|\mathbb{F}_p|} + \sum_{\substack{\text{stab} \\ \text{trivial}}} \frac{|\mathbb{F}_p|}{|\{0\}|}$$

$\underbrace{\hspace{1cm}}_{=1} \qquad \underbrace{\hspace{1cm}}_{=p}$

d' où $|X| = 1 + \left(\frac{p}{q}\right) \pmod{p}$.

* On remplace la forme quadratique $\sum_{i=1}^p x_i^2$ par une forme qui lui est congruente.

$\sum x_i^2$ est la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est I_p .

Soit $d = \frac{p-1}{2}$, $a = (-1)^d$ et $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_q)$ et on considère la forme quadratique dont la matrice dans la base canonique de $\mathbb{F}_q^p$ est

$$A = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \\ & & & a \end{pmatrix} \left\{ \frac{p-1}{2} \text{ blocs} \right\} \in M_p(\mathbb{F}_q).$$

rang p = inversible
pour le thm de classif.

discriminant = det.

modulo les carrés

du corps de base.

I_p et A sont symétriques, de même rang p et même déterminant $1 = (-1)^{(p-1)/2} \cdot a$ donc même discriminant donc par le théorème de classification des f.q sur $\mathbb{F}_q$, elles sont congruentes sur $\mathbb{F}_q$.

$$\exists P \in GL_p(\mathbb{F}_q) \text{ tq } A = {}^t P I_p P = {}^t P P$$

Si g est la forme quadratique associée à A, on identifie X à

$$X' = \{x \in \mathbb{F}_q^p : g(x) = 1\} \text{ i.e } X' = \{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p,$$

$$2(y_1 z_1 + \dots + y_d z_d) + a t^2 = 1\}$$

On distingue deux types de points de X' :

- ceux où $y_1 = \dots = y_d = 0$: chaque valeur de t telle que $a t^2 = 1$ détermine q^d points : $q^d (1 + a^{(q-1)/2}) = q^d (1 + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}})$
- ceux pour lesquels au moins un des $y_i \neq 0$ ($q^d - 1$ possibilités) : une fois fixés $(y_1, \dots, y_d)$ et t, il reste à choisir $(z_1, \dots, z_d)$ dans un hyperplan affine de $\mathbb{F}_q^d$ donc de cardinal q^{d-1} ce qui fait $(q^d - 1) q \cdot q^{d-1}$ tels points.

En sommant, on trouve :

$$\begin{aligned} |X| = |X'| &= q^d (q^d - 1 + 1 + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}) \\ &= q^d (q^d + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}) \end{aligned}$$

On obtient: $|X| = \left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \right) q^{\frac{p-1}{2}} = \left(\frac{p}{q} \right) + 1 \pmod{p}$

d'où $|X| = \left(\left(\frac{q}{p} \right) + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \right) \left(\frac{q}{p} \right) = \left(\frac{p}{q} \right) + 1 \pmod{p}$

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

d'où $\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{p}.$

Or ces deux termes valent ± 1 et on est en caractéristique $p \neq 2$ donc l'égalité se relève dans $\mathbb{Z}$, ce qui conclut. $\square$

Détails

Hyperplan affine:

On a $y_1, \dots, y_d$ non tous nuls, on peut supposer $y_1 \neq 0$
 $t \in \mathbb{F}_q$ quelconque

Posons $F = \{ z = (z_1, \dots, z_d) \in \mathbb{F}_q^d : 2 \sum_{i=1}^d y_i z_i = 1 - at^2 \}$

Soit $f: \mathbb{F}_q^d \rightarrow \mathbb{F}_q$, c'est une forme linéaire sur $\mathbb{F}_q^d$
 $(z_1, \dots, z_d) \mapsto 2 \sum_{i=1}^d y_i z_i$

non identiquement nulle car $y_1 \neq 0$ donc $H = \ker f$ est un hyperplan de $\mathbb{F}_q^d$.

De plus, $z = (z_0, 0, \dots, 0) \in \mathbb{F}_q^d$ avec $z_0 = \frac{1-at^2}{2y_1}$ vérifie
 $f(z) = 1-at^2$.

Ainsi: $F = z + H$ est bien un hyperplan affine.

H est de dimension $d-1$ sur l'ex $\mathbb{F}_q$ donc de card. q^{d-1} .

Théorème de classification des formes quadratiques sur $\mathbb{F}_q$

$K = \mathbb{F}_q$ est un corps fini de cardinal impair, deux matrices symétriques inversibles $A, A' \in S_n(\mathbb{F}_q)$ sont congruentes si et seulement si elles ont le même discriminant.

Dém.

Plus précisément, on montre (Perrin p 130) que pour E un $\mathbb{F}_q$ -ev de dim n , $\alpha \in \mathbb{F}_q^*$ non carré, il y a exactement deux classes de formes quadratiques non dégénérées sur E , de matrices $\text{Diag}(1, \dots, 1)$ ou $\text{Diag}(1, \dots, 1, \alpha)$ et une forme q est de l'un ou l'autre type selon si $S(q)$ est ou non un carré de $\mathbb{F}_q^*$. Ici $S(A) = 1$ est un carré donc A est bien congruente à $\text{Diag}(1, \dots, 1) = I_p$.

Perrin p 130 Lemme:
Caldes p 330

$\forall a, b \in \mathbb{F}_q^*$, l'équation $ax^2 + by^2 = 1$ admet au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q$.

Dém.

on sait qu'il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$. Comme $a \neq 0$, $\exists \lambda \neq 0$ az est bijective donc il existe $\frac{q+1}{2}$ éléments de la forme ax^2 . Idem pour $1-by^2$. Ainsi $|\{ax^2 : x \in \mathbb{F}_q\}| + |\{1-by^2 : y \in \mathbb{F}_q\}| = q+1 > q$ donc leur intersection est non vide d'où le résultat. $\square$

Par récurrence, pour $n=2$ on choisit une base orthogonale pour q dans laquelle $q(x, y) = ax^2 + by^2$. Par le lemme, $\exists e_1 = (x, y)$ tq $q(e_1) = 1$. Soit e_2 orthogonal à e_1 .

• Si $q(e_2) = \lambda^2$, on remplace e_2 par $\frac{1}{\lambda} e_2$

• Si $q(e_2)$ n'est pas un carré, on a $q(e_2) = \lambda^2 \alpha$ et on remplace e_2 par $\frac{e_2}{\lambda}$

car $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$...

Pour $n > 2$, soit $(e_1, \dots, e_n)$ une base orthogonale et $H = \text{Vect}(e_1, e_2)$

Dans la base (e_1, e_2) de H , $q|_H$ s'écrit $ax^2 + by^2$ avec $(a, b) \neq (0, 0)$ et par le lemme, $\exists e_1 = (x, y) \in H$ tq $q(e_1) = 1$ et on applique l'HR à $\langle e_1 \rangle^\perp$.

Comme α n'est pas un carré, les deux formes précédentes ne sont pas équivalentes car leurs discriminants ne sont pas égaux mod. $\mathbb{F}_q^{*2}$ et le discriminant est invariant par congruence mod. $\mathbb{F}_q^{*2}$. $\square$

En fait si q est quelconque, il va exister une base de E dans laquelle la matrice de q est $\text{Diag}(0, \dots, 0, 1, \dots, 1)$ ou $\text{Diag}(0, \dots, 0, 1, \dots, 1, \infty)$.

En effet, on vient de montrer le cas non dégénéré. Si q est dégénérée, elle a un noyau N et on prend un supplémentaire quelconque H de N de sorte que $q|_H$ soit non dégénérée. En prenant une base adaptée à la décomposition orthogonale $E = N \oplus H$, on a une matrice diagonale par blocs avec un bloc nul correspondant au noyau et un bloc de la forme voulue grâce à ce qui précède.

Réciprocité quadratique : applications

Théorème: $\forall p, q$ premiers impairs distincts, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

A retenir:

- Si $p \equiv 1 \pmod{4}$ ou $q \equiv 1 \pmod{4}$, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- Si $p \equiv -1 \pmod{4}$ et $q \equiv -1 \pmod{4}$, on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Perrin p 75 * $\forall p > 2$ premier, $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1 \Leftrightarrow \left(\frac{x}{q}\right) = 1$

En effet, si $X = \{x \in \mathbb{F}_q : x^{\frac{q-1}{2}} = 1\}$, on a $|X| \leq \frac{q-1}{2}$ (nombre de racines d'un pol. de degré $\frac{q-1}{2}$ sur un corps) et $\mathbb{F}_q^{*2} \subset X$ par le théorème de Lagrange. Comme en caract. $\neq 2$ on a $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ on a $\mathbb{F}_q^{*2} = X$.

Perrin p 75 * $p > 2$ premier, $q = p^m$, $m \in \mathbb{N}^*$, alors $-1 \in \mathbb{F}_q^{*2}$ si: $q \equiv 1 \pmod{4}$
i.e. $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ si $q \equiv 1 \pmod{4}$.

$$-1 \in \mathbb{F}_q^{*2} \Leftrightarrow (-1)^{(q-1)/2} = 1 \Leftrightarrow \frac{q-1}{2} \text{ pair} \Leftrightarrow q \equiv 1 \pmod{4}$$

Autre démo: $q \equiv 1 \pmod{4} \Leftrightarrow |\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ est pair
i.e. d'après le théorème de Sylow, il existe un élément x d'ordre 2 dans $\mathbb{F}_q^{*2}$: $x^2 = 1$ et $x \neq 1$ donc $x = -1$
et donc $q \equiv 1 \pmod{4} \Leftrightarrow -1 \in \mathbb{F}_q^{*2}$.

$$* 2 \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv \pm 1 \pmod{8} \Leftrightarrow \left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$

Lemme: $\mathbb{K}$ corps de caract. $\neq 2$, ζ racine primitive 8^e de l'unité, alors $(\zeta + \zeta^{-1})^2 = 2$.

Dém: $(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2$, or $\zeta^8 = 1$ et $\zeta^4 \neq 1$ donc $\zeta^4 = -1$
car caract. $\neq 2$ et donc $\zeta^2 = -\zeta^{-2}$

Conséquence: 2 est un carré dans $\mathbb{K} \Leftrightarrow \zeta + \zeta^{-1} \in \mathbb{K}$.

Dans notre cas: soit ζ racine primitive 8^e de l'unité tq $\zeta \in \mathbb{F}_{q^2}$
 (q est impair donc $q^2 - 1 = (q-1)(q+1)$ produit de deux
 pairs consécutifs donc multiple de 8. Or $\mathbb{F}_{q^2}^*$ est cyclique
 d'ordre $q^2 - 1$ donc contient un élément d'ordre 8: ζ)

Soit $F: x \mapsto x^q$ morphisme de Frobenius

- si $q \equiv \pm 1 \pmod{8}$, $F(\zeta + \zeta^{-1}) = \zeta^q + \zeta^{-q} = \zeta + \zeta^{-1}$ donc $\zeta + \zeta^{-1}$ est
 fixé par F donc est dans $\mathbb{F}_q$ donc avec ce qui précède, 2 est un carré
 dans $\mathbb{F}_q$
- Si $q \equiv \pm 3 \pmod{8}$, $F(\zeta + \zeta^{-1}) = \zeta^3 + \zeta^{-3}$ donc si 2 est un carré dans
 $\mathbb{F}_q$, on a $\zeta + \zeta^{-1} \in \mathbb{F}_q$ donc $\zeta + \zeta^{-1} = F(\zeta + \zeta^{-1}) = \zeta^3 + \zeta^{-3}$
 donc $\zeta^4 + \zeta^{-2} = \zeta^2 + 1$ donc $-1 - \zeta^2 = \zeta^2 + 1$ donc $2\zeta^2 = -2$
 donc en caract $\neq 2$, $\zeta^2 = -1$ i.e $\zeta^4 = 1$ ce qui est impossible.