Loi de réciprocité quadratique par les formes quadratiques

Leçons: 120, 121, 123, 126, 170.

Énoncé: si p et q sont des nombres premiers impairs : $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$, autrement dit

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \text{ si } p \equiv 1 [4] \text{ ou } q \equiv 1 [4] \\ -\left(\frac{q}{p}\right) \text{ si } p \equiv q \equiv 3 [4] \end{cases}.$$

Preuve.

- D'abord on vérifie (lemme) que si p premier impair et $a \in \mathbb{F}_p^\times$: $|\{x \in \mathbb{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$.
En effet pour $x \in \mathbb{F}_p$, $ax^2 = 1 \Leftrightarrow x^2 = a^{-1}$: si a^{-1} est un carré il y a $2 = 1 + \left(\frac{a^{-1}}{p}\right)$ solutions, sinon il y en a $0 = 1 + \left(\frac{a^{-1}}{p}\right)$. On conclut car $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)$.

- On se fixe p, q premiers impairs. On pose $X = \left\{ x \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1 \right\}$: on va estimer son cardinal de deux manières.
D'abord on considère l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X déf par $k \cdot (x_1, \cdots, x_p) = (x_{1+k}, \cdots, x_{p+k})$, où l'on voit les indices modulo p. Si $\mathrm{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$, $x = (y, \cdots, y)$ pour un certain $y \in \mathbb{F}_q$, et $1 = \sum_{i=1}^{p} x_i^2 = p y^2$.
Sinon $\mathrm{Stab}(x) = \{0\}$ et $\frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathrm{Stab}(x)|} = p$; la formule des classes donne donc :

$$|X| \equiv \sum_{py^2=1} 1 \equiv 1 + \left(\frac{p}{q}\right) \ [p] \text{ d'après le lemme.}$$

- On remarque que $X = \{ x \in \mathbb{F}_q^p \mid Q(x) = 1 \}$ avec Q la forme quadratique sur $\mathbb{F}_q^p$ de matrice I_p dans la base canonique. On pose les notations suivantes : $d = \frac{p-1}{2}$, $\varepsilon = (-1)^d$, $J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{F}_q)$,

$$M = \begin{bmatrix} J & & \\ & \ddots & \\ & & J \\ & & & \varepsilon \end{bmatrix} \in M_p(\mathbb{F}_q) \text{ où } J \text{ apparaît } d \text{ fois (on a bien } 2d+1 = p). \quad \det M = (\det J)^d \cdot \varepsilon$$

$= (-1)^d (-1)^d = 1 = \det I_p$. Alors on prend Q' la forme quadratique sur $\mathbb{F}_q^p$ de matrice M dans la base canonique : Q et Q' sont non dégénérées et ont même discriminant, donc sont équivalentes d'après le th de classification des formes quadratiques sur un corps fini de caractéristique impaire.
Si on écrit $Q' = Q \circ \varphi$ avec $\varphi \in GL(\mathbb{F}_q^p)$, en notant $X' = \{x \in \mathbb{F}_q^p \mid Q'(x) = 1\}$: pour $x \in \mathbb{F}_q^p$,
$x \in X' \Leftrightarrow Q'(x) = 1 \Leftrightarrow Q(\varphi(x)) = 1 \Leftrightarrow \varphi(x) \in X \Leftrightarrow x \in \varphi^{-1}(X)$. X et $X' = \varphi^{-1}(X)$ sont en bijection donc $|X| = |X'|$.
Par définition de Q', $X' = \left\{ (x_1, y_1, \cdots, x_d, y_d, z) \in \mathbb{F}_q^p \mid 2\sum_{i=1}^{d} x_i y_i + \varepsilon z^2 = 1 \right\}$. On écrit

$$X' = X'_1 \sqcup X'_2 \text{ avec } \begin{cases} X'_1 = \{(x_1, y_1, \cdots, x_d, y_d, z) \in X' \mid \forall 1 \le i \le d, \ x_i = 0\} \\ X'_2 = \{(x_1, y_1, \cdots, x_d, y_d, z) \in X' \mid \exists 1 \le i \le d, \ x_i \neq 0\} \end{cases}.$$

Pour $(x_1, y_1, \cdots, x_d, y_d, z) \in X_1'$, les y_i sont quelconques, et $\varepsilon z^2 = 1$ donc il y a $1 + \left(\frac{\varepsilon}{q}\right)$ possibilités pour z : ainsi $|X_1'| = q^d \left(1 + \left(\frac{\varepsilon}{q}\right)\right)$.

Pour $(x_1, y_1, \cdots, x_d, y_d, z) \in X_2'$, $x \neq 0$ et z peuvent d'abord être pris quelconques, puis l'ens des y possibles est un hyperplan affine de $\mathbb{F}_q^d$ (un translaté du noyau de la forme linéaire non nulle sur $\mathbb{F}_q^d$ $y \mapsto \varepsilon \sum_{i=1}^{d} x_i y_i$). Donc $|X_2'| = (q^d - 1) \cdot q \cdot q^{d-1} = q^d (q^d - 1)$.

Finalement $|X'| = |X_1'| + |X_2'| = q^d \left(1 + \left(\frac{\varepsilon}{q}\right) + q^d - 1\right) = q^d \left(q^d + \left(\frac{\varepsilon}{q}\right)\right)$.

- On conclut. Rappelons que $d = \frac{p-1}{2}$: en particulier $q^d \equiv \left(\frac{q}{p}\right) [p]$ et $\left(\frac{\varepsilon}{q}\right) = \left(\frac{-1}{q}\right)^d = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.
  Alors : $1 + \left(\frac{p}{q}\right) \equiv q^d \left(q^d + \left(\frac{\varepsilon}{q}\right)\right) \equiv \left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \equiv 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) [p]$, d'où $\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) [p]$. Puisque les nombres valent ± 1 et que $p \geq 3$, cette congruence est en fait une égalité.

□

Complément 1 : propriétés élémentaires du symbole de Legendre - p premier impair, $a, b \in \mathbb{Z}$.

(i) Il y a exactement $\frac{p-1}{2}$ résidus quadratiques non nuls modulo p.

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

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 [4] \\ -1 & \text{si } p \equiv 3 [4] \end{cases}$.

Preuve. (i) : $\beta : \begin{cases} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ x \mapsto x^2 \end{cases}$ est un morphisme de groupes de noyau $\{-1, 1\}$, d'où $|\mathrm{Im}\,\beta| = \frac{|\mathbb{F}_p^\times|}{|\mathrm{Ker}\,\beta|} = \frac{p-1}{2}$.

(ii) : si $a = 0$: trivial. Si $a \equiv b^2 [p]$: $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) [p]$. Cela fournit les $\frac{p-1}{2}$ racines du polynôme $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$. Si a non résidu quadratique : $a^{p-1} \equiv 1 [p]$ donc $a^{\frac{p-1}{2}} \equiv \pm 1 [p]$. Or a non racine de $X^{\frac{p-1}{2}} - 1$ par ce qui précède : $a \not\equiv 1 [p]$ et $a \equiv -1 \equiv \left(\frac{a}{p}\right) [p]$.

(iii) et (iv) : découlent de (ii).

□

Complément 2 : Th de classification des formes quadratiques sur les corps finis de caractéristique impaire.

$\mathbb{F}_q$ un corps fini de caractéristique impaire, E un $\mathbb{F}_q$-ev de dim $n \geq 1$. On fixe $\alpha \in \mathbb{F}_q^\times$ non carré.

Il y a exactement deux classes d'équivalence de formes quadratiques non dégénérées sur E, respectivement associées aux matrices I_n et $J_n(\alpha) = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & \alpha \end{bmatrix}$ de $M_n(\mathbb{F}_q)$. Ces classes sont caractérisées par le discriminant (qui appartient à $\mathbb{F}_q^\times / \mathbb{F}_q^{2\times} = \{\bar{1}, \bar{\alpha}\}$).

Preuve.

- Lemme : pour $a, b \in \mathbb{F}_q^\times$, il existe $x, y \in \mathbb{F}_q$ tq $ax^2 + by^2 = 1$.

  En effet il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$ (même argument que dans le complément 1). x^2 prend $\frac{q+1}{2}$ valeurs qd x parcourt $\mathbb{F}_q$, $\frac{1 - by^2}{a}$ prend $\frac{q+1}{2}$ valeurs qd y parcourt $\mathbb{F}_q$. Puisque $\frac{q+1}{2} + \frac{q+1}{2} > q$, il existe une valeur commune, d'où le résultat.

- Soit Q une fq non dégénérée sur E : on montre par réc sur $n \geq 2$ qu'il existe une base de E dans laquelle la matrice de Q est I_n ou $J_n(\alpha)$ (pour $n=1$ c'est clair).

  Initialisation : $n=2$. Soit (e_1, e_2) une base Q-orthogonale de E : $Q(x) = a x_1^2 + b x_2^2$ avec $a, b \in \mathbb{F}_q^\times$. D'après le lemme il existe $x \in E$ tq $Q(x)=1$. Soit $y \neq 0$ orthogonal à x : (x,y) est une base orthogonale de E et Q est non dégénérée donc $Q(y) \neq 0$. Comme $Q(y) \in \mathbb{F}_q^\times$ et $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 2} = \{\bar{1}, \bar{\alpha}\}$, $Q(y) = \lambda^2$ ou $Q(y) = \lambda^2 \alpha$ avec un $\lambda \in \mathbb{F}_q^\times$. Dans les deux cas on pose $y = \lambda^{-1} y$: (x,y) est une base orthogonale qui convient.

  Hérédité : on suppose que c'est bon au rang n, où $n \geq 2$ fixé. Soit $(e_1, \dots, e_{n+2})$ une base Q-orthogonale de E : comme pour le cas $n=2$, le lemme donne l'existence de $x \in \mathrm{Vect}(e_1, e_2)$ tq $Q(x)=1$. On applique l'HR à $x^\perp$ pour obtenir une base ; en concaténant x et cette base de $x^\perp$ on obtient une base de E qui convient.

- Les discriminants des fq de matrices I_n et $J_n(\alpha)$ dans une base donnée sont $\bar{1} \neq \bar{\alpha}$: elles ne sont pas équivalentes. Il y a donc exactement deux classes d'équivalence. □

Réf : • HHGG1 : ↑185 (th).
• Perrin : ↑93 (complément 1), ↑130 (complément 2).
• Rombaldi : ↑428 (complément 1), ↑432 (th), ↑483 (complément 2).

↳ Cette preuve de la LRQ n'est pas la plus directe (on pense par exemple à la preuve utilisant les résidus minimaux absolus et leurs signes, ou celle utilisant les sommes de Gauss), mais elle a le mérite d'être très recasable.

↳ Autre propriété importante du symbole de Legendre : la loi complémentaire : $\left(\frac{2}{\uparrow}\right) = (-1)^{\frac{\uparrow^2-1}{8}} = \begin{cases} 1 & \text{si } \uparrow \equiv \pm 1 \,[8] \\ -1 & \text{si } \uparrow \equiv \pm 3 \,[8] \end{cases}$.
On peut la démontrer facilement via les résidus minimaux absolus.

↳ Pas besoin d'avoir à la fois HHGG1 et Rombaldi. Cependant le second est utile car les compléments sont dedans.