

Loi de réciprocité quadratique
pour 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 $X = \{x \in \mathbb{F}_q^\uparrow \mid \sum_{i=1}^p x_i^2 = 1\}$: on va estimer son cardinal de deux manières.

D'abord on considère l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X définie par $k \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$, où l'on voit les indices modulo p . Si $\text{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$, $x = (y, \dots, y)$ pour un certain $y \in \mathbb{F}_q$, et $1 = \sum_{i=1}^p x_i^2 = py^2$.
Sinon $\text{Stab}(x) = \{0\}$ et $\frac{|\mathbb{Z}/p\mathbb{Z}|}{|\text{Stab}(x)|} = p$; la formule des classes donne donc:

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

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

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

$= (-1)^d (-1)^d = 1 = \det i_p$. Alors on prend Q' la forme quadratique sur \mathbb{F}_q^\uparrow 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 $\varphi \in GL(\mathbb{F}_q^\uparrow)$, en notant $X' = \{x \in \mathbb{F}_q^\uparrow \mid Q'(x) = 1\}$: pour $x \in \mathbb{F}_q^\uparrow$,
 $x \in X' \Leftrightarrow Q'(x) = 1 \Leftrightarrow Q(\varphi(x)) = 1 \Leftrightarrow \varphi(x) \in X \Leftrightarrow x \in \varphi^{-1}(X)$. X et $X' = \varphi^{-1}(X)$ sont en bijection donc $|X| = |X'|$.

Par définition de Q' , $X' = \{(x_1, y_1, \dots, x_d, y_d, z) \in \mathbb{F}_q^\uparrow \mid 2 \sum_{i=1}^d x_i y_i + \varepsilon z^2 = 1\}$. On écrit

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

Pour $(x_1, y_1, \dots, x_d, y_d, z) \in X_1'$, 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 $(x_1, y_1, \dots, x_d, y_d, z) \in X_2'$, $x \neq 0$ et z peuvent d'abord être pris quelconques, puis l'ens des y_i possibles est un hyperplan affine de \mathbb{F}_q^d (un translate 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 $d = \frac{r-1}{2}$: en particulier $q^d \equiv \left(\frac{q}{r}\right) [r]$ et $\left(\frac{\varepsilon}{q}\right) = \left(\frac{-1}{q}\right)^d = (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}}$.
 Alors: $1 + \left(\frac{\varepsilon}{q}\right) \equiv q^d \left(q^d + \left(\frac{\varepsilon}{q}\right)\right) \equiv \left(\frac{q}{r}\right) \left(\left(\frac{q}{r}\right) + (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}}\right) \equiv 1 + (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{r}\right) [r]$, d'où
 $\left(\frac{r}{q}\right) \equiv (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{r}\right) [r]$. Puisque les membres valent ± 1 et que $r \geq 3$, 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): $\beta: \begin{cases} \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times \\ x \mapsto x^2 \end{cases}$ est un morphisme de groupes de noyau $\{-1, 1\}$, d'où $|\text{Im } \beta| = \frac{|\mathbb{F}_p^\times|}{|\text{Ker } \beta|} = \frac{p-1}{2}$.

(ii): si $a \equiv 0$: 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 $J_n(\alpha) = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 & \\ & & & \alpha \end{bmatrix}$ de $M_n(\mathbb{F}_q)$. Ces classes sont caractérisées par le discriminant (qui appartient à $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 2} = \{1, \alpha\}$).

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 , $\frac{1-bx^2}{a}$ 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.

