Prérequis : • action, relation orbite stabilisateur
• forme quad et représentat° matricielle, discriminant, classificat° sur un corps fini.
• hyperplan et forme linéaire
• symbole de Legendre et critère d'Euler.

16'24 en commençant au thm. → faut vraiment aller vite

15' en allant vite.

Duverney p64

Def : Pour p un nombre premier et $n \in \mathbb{Z}$, on définit le symbole de Legendre par

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } n \equiv 0 [p] \\ 1 \text{ si } n \not\equiv 0 [p] \text{ et } n \text{ est un carré modulo } p. \\ -1 \text{ sinon}. \end{cases}$$

Critère d'Euler : On a $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} [p]$. pour p impair.

Dém : Si $n \equiv 0 [p]$, c'est évident. On suppose donc maintenant $n \not\equiv 0 [p]$.

D'après le petit thm de Fermat, $\forall x \in \mathbb{F}_p^\times \; x^{p-1} \equiv 1 [p]$ i.e. $(x^{\frac{p-1}{2}})^2 - 1 \equiv 0 [p]$.

Or $\mathbb{F}_p$ est un corps donc $X^2 - 1$ n'a que ± 1 comme racines donc

$\forall x \in \mathbb{F}_p^\times \quad x^{\frac{p-1}{2}} \equiv \pm 1 [p]$.

On sait qu'il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^\times$ et $\frac{p-1}{2}$ non carrés.

Si x est un carré, $x^{\frac{p-1}{2}} = y^{p-1} = 1$ donc $X^{\frac{p-1}{2}} - 1$ a au moins $\frac{p-1}{2}$ racines distinctes dans $\mathbb{F}_p$: les carrés.
Si x n'est pas un carré alors $x^{\frac{p-1}{2}} \equiv -1 [p]$ car $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines car $\mathbb{F}_p$ est un corps.

└

Lemme Soient q un nombre premier impair et $b \in \mathbb{Z}^\times$. Alors

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

Dém : On a $\{x \in \mathbb{F}_q \, , \, bx^2 = 1\} = \{x \in \mathbb{F}_q \, , \, x^2 = b^{-1}\}$

Or b est un carré modulo q ssi b^{-1} l'est.
Donc le cardinal de cet ensemble vaut 0 ssi b^{-1} n'est pas un carré ssi b n'est pas un carré ssi $\left(\frac{b}{q}\right) = -1$

et 2 sinon.

└

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

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

L'idée est de calculer son cardinal modulo p de deux façons différentes.

On commence par définir $q : (x_1, .., x_p) \in \mathbb{F}_q^p \longmapsto \sum_{i=1}^p x_i^2$ qui est une forme quadratique.

$1^{ère}$ façon : On fait agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire

- $\forall k \in \mathbb{Z}/p\mathbb{Z}$ $\forall (x_1,..,x_p) \in \mathbb{F}_q^p$ $k.(x_1,..,x_p) = (x_{k+1},...,x_{k+p})$ où les indices sont pris modulo p. On remarque que si $(x_1,..,x_p) \in X$ alors $k.(x_1,..,x_p) \in X$ donc l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X est bien définie.

- Le stabilisateur d'un élément est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, donc par théorème de Lagrange, son cardinal divise p. Or p est premier donc on a deux types de stabilisateurs :

  + ceux de cardinal p, donc égaux à $\mathbb{Z}/p\mathbb{Z}$: $Stab(x) = \mathbb{Z}/p\mathbb{Z}$ ssi $\begin{cases} x = (a,..,a),\ a \in \mathbb{F}_q \\ \text{et } q(x) = 1 \end{cases}$

    si $\exists i \neq j$ $x_i = x_j$, soit $k \in \mathbb{Z}/p\mathbb{Z}$ tq $i+k = j\ [p]$ alors $k \notin Stab(x)$.
    Réciproque ok.

    ssi $\begin{cases} x = (a,..,a) \\ pa^2 = 1 \end{cases}$

  + ceux de cardinal 1, donc égaux à $\{e\}$.

- Soit $\{x_i\}_{1 \le i \le r}$ une famille de représentants des orbites distinctes, alors,

$$|X| = \sum_{i=1}^{r} |Orb(x_i)| = \sum_{|Stab(x_i)|=1} |Orb(x_i)| + \sum_{|Stab(x_i)|=p} |Orb(x_i)|$$ car les orbites forment une partition de X.

Or d'après la relation orbite-stabilisateur, $|Orb(x_i)| = \dfrac{|\mathbb{Z}/p\mathbb{Z}|}{|Stab(x_i)|}$ $1 \le i \le r$.
donc,

$$|X| = \sum_{|Stab(x_i)|=1} p + \sum_{|Stab(x_i)|=p} 1 \equiv |\{1 \le i \le r,\ |Stab(x_i)| = p\}|\ [p].$$

$\equiv |\{x \in X,\ |Stab(x)| = p\}|\ [p]$ car si $|Stab(x)| = p$ alors $|Orb(x)| = 1$.

$\equiv |\{x = (a,..,a),\ a \in \mathbb{F}_q,\ pa^2 = 1\}|\ [p]$

$\equiv |\{a \in \mathbb{F}_q,\ pa^2 = 1\}|\ [p]$ $\equiv 1 + \left(\frac{p}{q}\right)\ [p]$ d'après le lemme.

6min

$2^{ème}$ façon : On remplace q par une forme quadratique qui lui est congruente et pour laquelle $|X|$ est plus facile à trouver.

- On a défini q précédemment, c'est une forme quadratique. Sa matrice dans la base canonique de $\mathbb{F}_q^p$ est I_p.

Si on considère $M = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \\ & & & a \end{pmatrix}$ $\updownarrow p$ où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_q)$, $d = \frac{p-1}{2}$ $a = (-1)^d$

intérêt de p impair

. M représente la forme quadratique $\tilde{q} : (y_1, z_1, .., y_d, z_d, t) \mapsto 2\sum_{i=1}^{d} y_i z_i + at^2$ dans la base canonique de $\mathbb{F}_q^p$.

- Or $rg(M) = p = rg(I_p)$ et $\det M = (\det J)^d \times a = (-1)^d (-1)^d = 1 = \det I_p$ donc M et I_p ont même discriminant.
Donc d'après la classification des formes quadratiques sur un corps fini,

M et I_p sont congruentes : il existe $P \in GL_p(\mathbb{F}_q)$ telle que $M = {}^tP I_p P = {}^tPP$

On introduit $X' = \{ (x_1, \dots, x_p) \in \mathbb{F}_q^p,\ \tilde{q}(x_1, \dots, x_p) = 1 \}$

$= \{ x \in \mathbb{F}_q^p \quad {}^tx Mx = 1 \} = \{ x \in \mathbb{F}_q^p \quad {}^tx\, {}^tP P x = 1 \}$

or $x \mapsto Px$ est une bijection donc associe X' à X.

donc $|X'| = |X|$. On est donc ramené à calculer $|X'|$

- On a $X' = \{ (y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p,\ 2\sum_{i=1}^{d} y_i z_i + at^2 = 1 \}$

Il y a deux types de points dans X'

+ les points tels que $y_1 = \dots = y_d = 0$. , alors $\tilde{q}(y_1, z_1, \dots, y_d, z_d, t) = at^2$.

Or $at^2 = 1$ admet $1 + \left(\frac{a}{q}\right)$ solutions d'après le lemme et le choix des z_i est quelconque. Il y a donc $\left[1 + \left(\frac{a}{q}\right)\right] q^d$ tels points.

+ les points pour lesquels au moins un des y_i est non nul. (Il y a $q^d - 1$ choix pour les y_i)

Une fois fixés les y_i et t (q choix pour t), il reste à choisir les éléments $(z_1, \dots, z_d)$ qui vivent dans $\{ (z_1, \dots, z_d),\ 2\sum_{i=1}^{d} y_i z_i = 1 - at^2 \}$ qui est hyperplan affine de $\mathbb{F}_q^d$. car $(z_1, \dots, z_d) \mapsto 2\sum_{i=1}^{d} y_i z_i$ est une forme linéaire non nulle sur $\mathbb{F}_q^d$ car $(y_1, \dots, y_d) \neq (0, \dots, 0)$.

$\mathbb{F}_q^d$ est un e.v. de dimension d, donc cet hyperplan est de dimension $d-1$

On a donc q^{d-1} choix pour $(z_1, \dots, z_d)$

Donc $q^{d-1} \times q \times (q^d - 1)$ tels points en tout.

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

Conclusion:

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

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

i.e. $1 + \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\left[\left(\frac{q}{p}\right) + \left(\frac{a}{q}\right)\right]\ [p]$

en multipliant par $\left(\frac{q}{p}\right)$ des 2 côtés

i.e. $\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\left(\frac{a}{q}\right)\ [p]$ car $\left(\frac{q}{p}\right)^2 = 1$ et même $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv \left(\frac{a}{q}\right)\ [p]$

Comme les deux membres sont à valeurs dans ± 1, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{a}{q}\right)$ dans $\mathbb{Z}$

Si $a, b \in \{\pm 1\}$ et $a \equiv b\ [p]$ alors, on suppose $a \geq b$ quitte à échanger donc, $a - b = kp$, $k \in \mathbb{N}$ or $p \neq 2$ donc $k = 0$ ou $a - b \geq p \geq 3$ donc $k = 0$. donc $a = b$

donc $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv \left(\frac{a}{q}\right) [q]$ or par critère d'Euler, $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} [q]$

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

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

Et comme chaque membre est à valeurs dans ± 1, cette égalité est vraie sur $\mathbb{Z}$:

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

L