Loi de réciprocité quadratique

ref: Histoire hédonistes de groupes et de géométries, Caldero-Germani p 319.
Perrin, Cours d'Algèbre p 74.

Objectif: Étude général des carrés dans $\mathbb{F}_q$.

On considère p un nombre premier et $q=p^n$. On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x=y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition:

1) Pour $p=2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$.
2) Pour $p>2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Preuve:

1) Pour $p=2$, $\mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^2$ est un automorphisme donc surjectif ainsi $\mathbb{F}_q^2 = \mathbb{F}_q$.

2) Pour $p>2$, on a le morphisme de groupe : $\varphi: \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$, $x \longmapsto x^2$

par le théorème d'iso: $\frac{\mathbb{F}_q^*}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi) = \mathbb{F}_q^{*2}$.

Or on a: $\ker(\varphi) = \{x \in \mathbb{F}_q \mid x^2 = 1\} = \{-1, 1\}$ car polynôme à 2 racines distinctes sur le corps commutatif $\mathbb{F}_q$.

Donc :

$$|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q|}{2} = \frac{q-1}{2}.$$

Et $\mathbb{F}_q^2 = \mathbb{F}_q^{*2} \cup \{0\}$ d'où $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

□

Proposition: (Caractérisation des carrés)

On suppose que $p>2$, alors on a: $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Preuve: On pose $X = \{x \in \mathbb{F}_q \mid x^{\frac{q-1}{2}} = 1\}$. On a $|X| \leq \frac{q-1}{2}$ (car un polynôme de degré $\frac{q-1}{2}$ a au plus $\frac{q-1}{2}$ racines).
D'autres part, si x est dans $\mathbb{F}_q^{\times 2}$ on a $x = y^2$ donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ et donc $\mathbb{F}_q^{\times 2} \subset X$. Pour une raison de cardinal, il en résulte $X = \mathbb{F}_q^{\times 2}$. ∎

Rmq:

1) On a la suite exacte : $1 \longrightarrow \mathbb{F}_q^{\times 2} \longrightarrow \mathbb{F}_q^{\times} \longrightarrow \{1, -1\} \longrightarrow 1$.

$$x \longmapsto x^{\frac{q-1}{2}}$$

En effet si x est dans $\mathbb{F}_q^{\times}$, $y = x^{\frac{q-1}{2}}$ vérifie $y^2 = 1$ donc $y = \pm 1$, le reste est clair avec la prop précédente.

2) La proposition fournit un critère pour savoir si un élément de $\mathbb{F}_q$ est un carré.
Par exemple, si $q = 7$ donc $\mathbb{F}_q = \mathbb{Z}/7\mathbb{Z}$, on a $\frac{q-1}{2} = 3$ et $\ell^3 = 8 = 1 \bmod 7$, de sorte que ℓ est un carré, $3^3 = 27 = -1 \bmod 7$ et 3 n'est pas carré.

Corollaire: Soit p un nombre premier impair et on pose $q = p^n$. Alors, -1 est un carré dans $\mathbb{F}_q$ ssi $q \equiv 1 \bmod 4$.

Preuve: $-1 \in \mathbb{F}_q^{\times 2} \iff (-1)^{\frac{q-1}{2}} = 1 \iff \frac{q-1}{2}$ pair $\iff q \equiv 1 \bmod 4$. ∎

Application:
Il existe une infinité de nombres premiers de la forme $4m+1$.

Preuve:
Soit n un entier et p un facteur premier de $(n!)^2 + 1$. On a $p > n$ car sinon $p \mid n!$. D'autre part dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ on a $(n!)^2 + 1 = 0$ donc $-1 = (n!)^2$ donc -1 est un carré.
Par le corollaire $p \equiv 1 \bmod 4$ donc $p = 4m+1$.
En faisant augmenter on a le résultat. ∎

Définition : Symbole de Legendre

Pour p un nombre premier impair et $q = p^\alpha$. Pour $a \in \mathbb{F}_q$ on définit le symbole de Legendre de a par :

$$\left(\frac{a}{q}\right) = \begin{cases} 1 \text{ si } a \text{ est un carré de } \mathbb{F}_p^\times \\ -1 \text{ si } a \text{ n'est pas un carré de } \mathbb{F}_p^\times \\ 0 \text{ si } a = 0 \end{cases}$$

Proposition : On a $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}}$ donc $\left(\frac{\cdot}{q}\right) : \mathbb{F}_q^\times \longrightarrow \{-1, 1\}$ est un morphisme de groupe.

Preuve : Directe. □

Proposition : Soit p un nombre premier impair et soit $a \in \mathbb{F}_p^\times$. On a :

$$\left|\{x \in \mathbb{F}_p \mid ax^2 = 1\}\right| = 1 + \left(\frac{a}{p}\right).$$

Preuve : On sait que $a \in \mathbb{F}_p^{\times 2} \iff a^{-1} \in \mathbb{F}_p^{\times 2}$ donc

$$\left|\{x \in \mathbb{F}_p \mid ax^2 = 1\}\right| = \left|\{x \in \mathbb{F}_p \mid x^2 = a^{-1}\}\right| = \begin{cases} 2 \text{ si } a \text{ carré } (y \text{ et } -y) \\ 0 \text{ sinon} \end{cases} = 1 + \left(\frac{a}{p}\right).$$

□

Rmq : Calcul pratique du symbole de Legendre.

Soit $p > 2$ premier et $n = \pm \prod_{i=1}^{r} q_i^{\alpha_i}$, le fait que le symbole de Legendre est un morphisme de groupe nous donne :

$$\left(\frac{n}{p}\right) = (-1)^{\frac{p-1}{2}} \prod_{i=1}^{r} \left(\frac{q_i}{p}\right)^{\alpha_i}$$

Il suffit donc de savoir calculer $\left(\frac{q}{p}\right)$ où q et p sont des nombres premier impairs, c'est l'objectif de la loi de réciprocité quadratique.

Théorème : Loi de réciprocité quadratique

Soit p et q deux nombres premiers impairs distincts. Alors :

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

Preuve: L'idée est de dénombrer de deux façons différentes le cardinal modulo p de la sphère de $\mathbb{F}_q^p$ i.e

$$X = \left\{ (x_1, x_2, \dots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1 \right\}$$

Méthode 1: On fait agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ sur X.

En effet on fait agir par permutation des coordonnées:

$$\forall k \in \mathbb{Z}/p\mathbb{Z},\ \forall (x_0, \dots, x_{p-1}) \in X,\ k.(x_0, \dots, x_{p-1}) = (x_k, \dots, x_{p-1+k})$$

où les indices sont vus modulo p : $x_{\ell+p} = x_\ell$ pour tout ℓ.

Soit $x \in X$ sont stabilisateur étant un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ on a deux possibilités.

- $\mathrm{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$ alors $x = (x_1, \dots, x_1)$ avec $x_1 \in \mathbb{F}_q$ donc $p x_1^2 = 1$.
  → comme chaque x est seul dans son orbite il y en a $1 + \left(\frac{p}{q}\right)$ d'après le lemme.
- $\mathrm{Stab}(x) = \{1\}$, alors son orbite est de cardinal p.

Donc par l'équation aux classes,

$$|X| = |X^{\mathbb{Z}/p\mathbb{Z}}| \bmod p \text{ donc } |X| = 1 + \left(\frac{p}{q}\right) \bmod p. \quad (1)$$

Méthode 2: Forme quadratique sur $\mathbb{F}_q^p$.

On a: $X = \{ x \in \mathbb{F}_q^p \mid f(x) = 1 \}$ où f est la forme quadratique associée à I_p dans la base canonique.

On veut trouver une autre forme quadratique congruente à f où le calcul du cardinal sera plus simple. Pour cela on pose :

$$A = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \\ & & & a \end{pmatrix} \text{ avec } J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ répété } d = \frac{p-1}{2} \text{ fois et } a = (-1)^{\frac{p-1}{2}}$$

qui est symétrique i.e définie une forme bilinéaire symétrique.

Alors il est clair que $\mathrm{rg}(M) = p = \mathrm{rg}(I_p)$

$$\det(M) = (\det J)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} = 1 = \det(I_p)$$

Ainsi M et I_p ont même rang et même discriminant, donc d'après la classification des formes quadratiques sur $\mathbb{F}_q$, M et I_p sont congruentes.

Il existe donc $P \in GL_p(\mathbb{F}_q)$ tel que : $A = {}^tP I_p P = {}^tPP$.

Donc la bijection $x \longmapsto P^{-1}x$ identifie $X = \{ x \in \mathbb{F}_q^p \mid {}^tx x = 1 \}$ à :

$$X' = \{ x' \in \mathbb{F}_q^p \mid {}^tx' A x' = 1 \} = \left\{ (y_1, z_1, y_2, z_2, \dots, y_d, z_d, t) \in \mathbb{F}_q^p \mid 2 \sum_{i=1}^{d} y_i z_i + a t^2 = 1 \right\}$$

Il nous reste à dénombrer X' pour cela on distingue deux types de points $(y_1, z_1, y_2, z_2, \dots, y_d, z_d, t)$ de X' :

→ Si $y_1 = \dots = y_d = 0$: Alors chaque valeur de t telle que $at^2 = 1$ détermine q^d tels points ce qui donne par le corollaire :

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

→ Si il existe i tel que $y_i \neq 0$: Il y a $q^d - 1$ possibilités pour $(y_1, \dots, y_d)$, q possibilités pour t et il reste à choisir un élément $(z_1, \dots, z_d)$ dans un hyperplan affine de $\mathbb{F}_q^d$ donc q^{d-1} possibilités au total on a donc :

$$(q^d - 1)\, q\, q^{d-1}.$$

Donc : $|X| = |X'| = q^d\left(1 + (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\right) + (q^d - 1)q^d = q^d\left(q^d + (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\right)$

où $d = \frac{p-1}{2}$.

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

$$= \left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\right) \quad (6).$$

En utilisant (1) et (2) on obtient : $\left(\frac{q}{p}\right) = 1$

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

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

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

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

Or les deux termes valent ± 1 dans $\mathbb{Z}$ donc l'égalité est aussi vrai dans $\mathbb{Z}$ d'où le résultat.

Rmq : Autre loi de réciprocité quadratique.

Proposition : Soit p nombre premier impair. Alors

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{et} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Preuve: Par definition $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

On commence par remarquer les points suivant:

- Comme $p \neq 2$, pour $\alpha \in \mathbb{F}_{p^n}$ tel que $\alpha^4 = -1$ est d'ordre 8 dans $\mathbb{F}_{p^n}^\times$.
- On a $\alpha^3 = -\alpha^{-1}$, $\alpha^{-3} = -\alpha$ et $\alpha^2 = -\alpha^{-2}$
- Comme p est impair, $8 \mid p^2 - 1$ et $p \equiv \pm 1 \bmod 8$ ssi $\frac{p^2-1}{8}$ est pair
  et $p \equiv \pm 3 \bmod 8$ ssi $\frac{p^2-1}{8}$ est impair.

Cas 1: $(-1)^{\frac{p^2-1}{8}} = 1$.

Alors $p \equiv \pm 1 \bmod 8$. Si α est une racine quatrième de -1 dans une extension de $\mathbb{F}_p$ alors α est d'ordre 8 et donc $\alpha^p = \alpha^{\pm 1}$ car $p \equiv \pm 1 \bmod 8$.

Ainsi $\alpha + \alpha^{-1}$ est racine de $X^p - X$, puisque:

$$(\alpha+\alpha^{-1})^p - (\alpha+\alpha^{-1}) = \alpha^p + (\alpha^p)^{-1} - \alpha - \alpha^{-1} = \alpha^{\pm 1} + \alpha^{\mp 1} - \alpha - \alpha^{-1} = 0$$

Donc $\alpha + \alpha^{-1} \in \mathbb{F}_p$. Or,

$$(\alpha+\alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2} = 2$$

Donc 2 est un carré de $\mathbb{F}_p$.

Cas 2: $(-1)^{\frac{p^2-1}{8}} = -1$ alors $p \equiv \pm 3$ modulo 8.

Soit α une racine 4-ième de -1 dans une extension $\mathbb{F}_{p^n}$ alors les racines de 2 sont $\pm(\alpha+\alpha^{-1})$ dans les extensions de $\mathbb{F}_p$.

Or $\alpha + \alpha^{-1} \notin \mathbb{F}_p$ en effet $\alpha^p = \alpha^{\pm 3}$ donc $\alpha + \alpha^{-1}$ n'est pas racine de $X^p - X$ et $\alpha + \alpha^{-1} \neq 0$.

Ainsi 2 n'est pas un carré dans $\mathbb{F}_p$.

∎