Groupe $SO_2(\mathbb{F}_q)$

[CALDERO 2, p 50]

ÉNONCÉ :

Théorème : Soit q une puissance d'un nombre premier impair. On a un isomorphisme :

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si -1 est un carré de } \mathbb{F}_q^* \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{si -1 n'est pas un carré de } \mathbb{F}_q^* \end{cases}$$

DÉVELOPPEMENT :

Démonstration. Le groupe se décrit par :

$$\begin{aligned} SO_2(\mathbb{F}_q) &= \{A \in GL_2(\mathbb{F}_q) \mid det(A) = 1,\ {}^tAA = I_2\} \\ &= \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mid ad - bc = a^2 + b^2 = c^2 + d^2 = 1, ac + bd = 0 \right\} \end{aligned}$$

Fixons $(a, b) \in \mathbb{F}_q^2$ tel que $a^2 + b^2 = 1$. Les équations :

$$\begin{cases} ac + bd = 0 \\ -bc + ad = 1 \end{cases}$$

forment un système linéaire de déterminant $a^2 + b^2 = 1$. La solution évidente $(c, d) = (-b, a)$ est donc la seule, et on a bien $c^2 + d^2 = 1$. Ainsi on obtient :

$$SO_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{F}_q,\ a^2 + b^2 = 1 \right\}$$

On a ainsi une bijection :

$$\begin{aligned} S^1(\mathbb{F}_q) &\longrightarrow SO_2(\mathbb{F}_q) \\ (a, b) &\longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{aligned}$$

Il s'agit donc de compte les points du cercle. On distingue 2 cas :

- $\underline{-1 \in (\mathbb{F}_q^*)^2}$: Soit $\omega \in \mathbb{F}_q^*$ tel que $-1 = \omega^2$. On a alors $a^2 + b^2 = (a - \omega b)(a + \omega b)$. Un changement de variables donne :

$$\begin{cases} x = a + \omega b \\ y = a - \omega b \end{cases} \iff \begin{cases} a = \frac{x+y}{2} \\ b = \frac{x-y}{2\omega} \end{cases}$$

D'où l'égalité des cardinaux :

$$|SO_2(\mathbb{F}_q)| = |S^1(\mathbb{F}_q)| = |\{(x, y) \in \mathbb{F}_q^2,\ xy = 1\}| = q - 1$$

Il suffit de vérifier que l'application :

$$\begin{aligned} SO_2(\mathbb{F}_q) &\longrightarrow \mathbb{F}_q^* \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} &\longmapsto a + \omega b \end{aligned}$$

est un isomorphisme de groupes. En effet, c'est un morphisme de groupes (vérification immédiate) et si $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in SO_2(\mathbb{F}_q)$ est telle que $a + \omega b = 1$, alors $x = 1$ et $y = a - \omega b = \frac{a^2+b^2}{a+\omega b} = 1$ d'où $a = 1$ et $b = 0$, d'où l'injectivité. L'égalité des cardinaux nous permet de conclure.

- $\underline{-1 \notin (\mathbb{F}_q^*)^2}$: Soient $N = (-1, 0) \in \mathbb{F}_q^2, t \in \mathbb{F}_q$ et $M = (1, 2t)$. La droite (NM) coupe le cercle $S^1(\mathbb{F}_q)$ en N et en un deuxième point $p(t)$. (NM) admet pour équation $y = t(x + 1)$ d'où l'équation

aux abscisses : $(1+t^2)x^2+2t^2x+t^2-1=0$. Comme $1+t^2\neq 0$, c'est une équation du second degré ayant pour solution (autre que $x=-1$) $x=\frac{1-t^2}{1+t^2}$ ce qui donne $y=t(x+1)=\frac{2t}{1+t^2}$. Inversement, pour tout point M' de $S^1(\mathbb{F}_q)$ distinct de N, la droite (NM') coupe la droite $X=1$ en un point. Ainsi, p établit une bijection de $\mathbb{F}_q$ sur $S^1(\mathbb{F}_q)\setminus\{N\}$. On en déduit :

$$|SO_2(\mathbb{F}_q)|=|S^1(\mathbb{F}_q)|=q+1$$

. Il suffit désormais d'injecter $SO_2(\mathbb{F}_q)$ dans $\mathbb{F}_{q^2}^*$ (extension dans laquelle -1 possède une racine carrée ω). Comme tout sous-groupe d'un groupe cyclique est cyclique, on en déduit le résultat. □

Remarques :

- On a utilisé les faits que $(\mathbb{F}_q^*,\times)\simeq\mathbb{Z}/(q-1)\mathbb{Z}$ et que tout sous-groupe d'un groupe cyclique est cyclique : il faut savoir les démontrer.
- Lorsque $q=2^n$, on a que : $O_2(\mathbb{F}_q)\simeq SO_2(\mathbb{F}_q)\simeq(\mathbb{Z}/2\mathbb{Z})^n$.