2.7 Étude du groupe $\mathcal{SO}_2(\mathbb{F}_q)$

Théorème : Soit $p \in \mathbb{P}$, $p \neq 2$, $n \in \mathbb{N}^*$ et $q = p^n$ avec $n \in \mathbb{N}^*$

$$\mathcal{SO}_2(\mathbb{F}_q) \underset{\text{isom}}{\simeq} \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \in \mathbb{F}_q^{*(2)} \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{si } -1 \notin \mathbb{F}_q^{*(2)} \end{cases}$$

Démonstration : $\mathcal{SO}_2(\mathbb{F}_q) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \middle\backslash \ \det(A) = 1 \ , \ A^t A = \mathrm{I}_2 \right\}$

Cette description fournit : $\mathcal{SO}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \middle\backslash \ ad - bc = a^2 + b^2 = c^2 + d^2 = 1 \ , \ ac + bd = 0 \right\}$

Soit $(a, b) \in (\mathbb{F}_q)^2$ tel que $a^2 + b^2 = 1$ et soit le système : $(S) = \begin{cases} ac + bd = 0 \\ ad - bc = 1 \end{cases} \Leftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Ce système a pour déterminant $\delta = a^2 + b^2 = 1 \neq 0$ donc il y a une unique solution, qu'on trouve aisément comme étant $(c, d) = (-b, a)$. On vérifie ainsi aussi l'égalité $c^2 + d^2 = 1$.

Notons $\mathcal{C}^1(\mathbb{F}_q) = \{(a, b) \in (\mathbb{F}_q)^2 \ \backslash \ a^2 + b^2 = 1\}$. Par ce qui précède, il y a donc une bijection donnée par

$$f \left| \begin{array}{ccc} \mathcal{C}^1(\mathbb{F}_q) & \longrightarrow & \mathcal{SO}_2(\mathbb{F}_q) \\ (a, b) & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array} \right.$$

1) Premier cas : $-1 \in \mathbb{F}_q^{*(2)} = \left\{x^2 \ \backslash \ x \in \mathbb{F}_q^*\right\}$. Soit $\omega \in \mathbb{F}_q^*$ tel que $\omega^2 = -1$
$a^2 + b^2 = 1 \Leftrightarrow (a + \omega b)(a - \omega b) = 1$ et puisque $p \neq 2$, on peut poser le changement de variables :

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

La bijection f permet de dire : $|\mathcal{SO}_2(\mathbb{F}_q)| = |\mathcal{C}^1(\mathbb{F}_q)| = |\{(x, y) \in (\mathbb{F}_q)^2 \ \backslash \ xy = 1\}| = q - 1$ [24]

Soit l'application $\varphi \left| \begin{array}{ccc} \mathcal{SO}_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^* \\ A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \longmapsto & a + \omega b \end{array} \right.$. C'est un morphisme de groupes (facile à vérifier).

- Si $\varphi(A) = a + \omega b = 1$, alors $y = a - \omega b = \dfrac{a^2 + b^2}{a + \omega b} = 1$ donc $a = 1$ et $b = 0$: φ est injectif
- Il y a égalité des cardinaux par ce qui précède, d'où la surjectivité.

On conclut que φ est bien un isomorphisme.

2) Second cas : $-1 \notin \mathbb{F}_q^{*(2)} = \left\{x^2 \ \backslash \ x \in \mathbb{F}_q^*\right\}$ *(Faire le dessin, figure 3.1 page 52 de la référence)*
Notons $N = (-1, 0)$ dans le plan $(\mathbb{F}_q)^2$. Soit $t \in \mathbb{F}_q$, on note $M = (1, 2t)$. On voit que la droite (NM) coupe le cercle en N et en un second point $p(t)$ (paramétrage de x, y), donc démontrons-le.

- La droite (NM) a pour équation $y = t(x + 1)$ et le cercle a pour équation : $x^2 + y^2 = 1$

Cela nous donne : $x^2(1 + t^2) + 2t^2 x + (t^2 - 1) = 0$, qui est une équation de degré 2 (car $-1 \notin \mathbb{F}_q^{*(2)}$)

24. La dernière égalité provient du fait que fixer x impose automatiquement la valeur $y = 1/x$.

Elle possède deux solutions, $x = -1$ est la première [25], et la seconde est donnée par la formule :
$x(-1) = \dfrac{t^2-1}{1+t^2}$ d'où un $y = \dfrac{2t}{1+t^2}$

• Inversement, si on se donne $M'(x,y) \in \mathcal{C}^1(\mathbb{F}_q)$, avec $M' \neq N$, on a $x \neq -1$.
Ainsi, $(NM') \cap \{x = 1\}$ est réduite à 1 point, ce qui fait que p établit une bijection $\mathbb{F}_q \longrightarrow \mathcal{C}^1(\mathbb{F}_q)\setminus\{N\}$ et donc $|\mathcal{C}^1(\mathbb{F}_q)\setminus\{N\}| = q$

In fine, on a $|\mathcal{SO}_2(\mathbb{F}_q)| \underbrace{=}_{f} |\mathcal{C}^1(\mathbb{F}_q)| \underbrace{=}_{p} q+1$. Il reste alors à montrer que $\mathcal{SO}_2(\mathbb{F}_q)$ est cyclique.

Pour cela, on procède de façon analogue, mais en injectant cette fois $\mathcal{SO}_2(\mathbb{F}_q) \hookrightarrow \mathbb{F}_{q^2}^\times$ [26] qui est une extension où -1 possède une racine [27].
Par théorème d'isomorphisme, on a donc : $\mathcal{SO}_2(\mathbb{F}_q)/\ker(\tilde{\varphi}) \underset{\text{isom}}{\simeq} \mathrm{Im}(\tilde{\varphi}) < \mathbb{F}_{q^2}^\times$
Or, le sous groupe mutiplicatif d'un corps fini est cyclique [28] , donc $\mathbb{F}_{q^2}^\times$ est cyclique, et tout sous-groupe d'un groupe cyclique est lui-même cyclique, ce qui achève la preuve, par injectivité de $\tilde{\varphi}$.

Référence : [CG18]
- Caldero-Germoni ; *Nouvelles histoires hédonistes de groupes et de géométries , Tome II* ; page 50-51

25. Que l'on écarte, car c'est N, et la N c'est pas très très gentil.

26. On note μ une racine de -1 dans $\mathbb{F}_{q^2}^\times$ et on a les injections
$$\begin{array}{ccccc} \mathcal{SO}_2(\mathbb{F}_q) & \hookrightarrow & \mathcal{SO}_2(\mathbb{F}_{q^2}) & \hookrightarrow & \mathbb{F}_{q^2}^\times \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \mapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \mapsto & a+\mu b \end{array}$$

27. Si $-1 \notin \mathbb{F}_q^{(2)}$, alors X^2+1 est irréductible dans $\mathbb{F}_q[X]$ (il est sans racines, et de degré 2), et donc $L = \mathbb{F}_q[X]/(X^2+1)$ est une extension de $\mathbb{F}_q$, avec $[L:\mathbb{F}_q] = \deg(X^2+1) = 2$. Par unicité, $L = \mathbb{F}_{q^2}$, et c'est un corps de rupture de X^2+1, ce qui assure que $-1 \in \mathbb{F}_{q^2}^{(2)}$. Notons d'ailleurs que cet argument fonctionne pour n'importe quel élément non carré.

28. Bien que classique, ce petit lemme mérite un peu d'attention :
Notons $|G| = N$. Par l'identité d'Euler : $N = \sum_{d|N} \varphi(d)$. On peut aussi compter avec les ordres respectifs, ce qui nous donne la formule : $N = \sum_{k|N} |\{g \in G \ \setminus \ \mathrm{ord}(g) = k\}| = \sum_{k|N} N_k$ (♣).
Soit $g \in G$ avec $\mathrm{ord}(g) = k$ et $k \mid N$. On a $|\langle g\rangle| = k$ et $\langle g\rangle \underset{\text{isom}}{\simeq} \mathbb{Z}/k\mathbb{Z}$. Par définition, $\langle g\rangle$ contient $\varphi(k)$ éléments d'ordre k.
Montrons que ce sont les éléments de $\langle g\rangle$. Par définition, les éléments de $\langle g\rangle$ sont racines de $(X^k-1) \in K[X]$. Il y a au plus k racines pour ce polynôme (K est un corps) et $|\langle g\rangle| = k$ donc les racines sont exactement $\langle g\rangle$.
Si g' est un élément d'ordre k, comme $(g')^k = 1$, il s'en suit que $g' \in \langle g\rangle$, et G contient donc toujours $\varphi(k)$ éléments d'ordre k, dès lors qu'il en existe un, ce qui signifie que pour $k \mid N$: $N_k \in \{0, \varphi(k)\}$ (♠)

$$N \underbrace{=}_{(\clubsuit)} \sum_{k|N} N_k \underbrace{\leqslant}_{(\spadesuit)} \sum_{k|N} \varphi(k) = N$$

Donc il y a égalité partout, ce qui force $N_k = \varphi(k)$ pour tout $k \mid N$. En particulier, $N_N = \varphi(N) \geqslant 1$. Il y a donc $\varphi(N)$ éléments d'ordre N, et il suffit d'en choisir un.