Le groupe $SO_2(\overline{\mathbb{F}_q})$

Leçons: 104, (106, 123, 130)

Réf: NH2G2 Tome 2 p 50-52.

Prop: Si $p \neq 2$ est premier, $q = p^m$ avec $m \in \mathbb{N}^*$, on a l'isomorphisme:

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

Dém: Le groupe se décrit par $SO_2(\overline{\mathbb{F}_q}) = \{A \in GL_2(\overline{\mathbb{F}_q}) : \det A = 1 \text{ et } {}^tAA = I_2\}$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{array}{l} ad-bc = 1, \\ a^2+b^2 = c^2+d^2 = 1, \\ ac+bd = 0 \end{array} \right\}$$

Si on fixe $(a,b) \in (\overline{\mathbb{F}_q})^2$ tel que $a^2+b^2 = 1$, les équations $\begin{cases} ac+bd = 0 \\ ad-bc = 1 \end{cases}$ forment un système de déterminant $a^2+b^2 = 1 \neq 0$ donc la solution évidente $(c,d) = (-b,a)$ est la seule et on a bien $c^2+d^2 = 1$.

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

Notons $S^2(\overline{\mathbb{F}_q}) = \{(a,b) \in (\overline{\mathbb{F}_q})^2 : a^2+b^2 = 1\}$ la sphère unité de $\overline{\mathbb{F}_q}$ de sorte à ce qu'on ait la bijection suivante:

$$f : \begin{array}{ccc} S^1(\overline{\mathbb{F}_q}) & \xrightarrow{\sim} & SO_2(\overline{\mathbb{F}_q}) \\ (a,b) & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array}.$$

- **1er cas:** -1 est un carré de $\overline{\mathbb{F}_q}^*$: soit $\omega \in \overline{\mathbb{F}_q}^*$ $\omega_q - 1 = \omega^2$

On peut donc écrire $a^2+b^2 = 1 = (a+\omega b)(a-\omega b)$ et faire le changement de variables suivant: $\begin{cases} x = a+\omega b \\ y = a-\omega b \end{cases} \Leftrightarrow \begin{cases} a = \frac{x+y}{2} \\ b = \frac{x-y}{2\omega} \end{cases}$.

car on est en caract $\neq 2$

La bijectivité de f permet d'affirmer que $|SO_2(\mathbb{F}_q)| = |\mathbb{S}^1(\mathbb{F}_q)|$
$= |\{(x,y) \in (\mathbb{F}_q)^2 : xy = 1\}|$
$= q-1$.

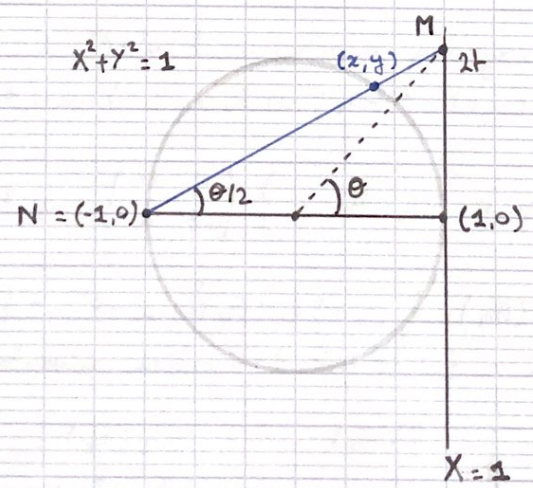
analogue de $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto x+iy$

Soit de plus φ : $SO_2(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^*$
$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a+\omega b$.

φ est un morphisme de groupes.
Si $\varphi(A) = a+\omega b = 1$, alors $y = \dfrac{a^2+b^2}{a+\omega b} = \dfrac{1}{1} = 1$ donc $\begin{cases} a = 1 \\ b = 0 \end{cases}$
d'où $A = I_2$.
φ est donc un morphisme injectif entre deux groupes de même cardinal : c'est un isomorphisme.
Ainsi : $SO_2(\mathbb{F}_q) \simeq \mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. (car $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$)

- 2e cas : -1 n'est pas un carré dans $\mathbb{F}_q^*$

Dessin à faire (dans le plan $\mathbb{F}_q^2$!)



Soit $t \in \mathbb{F}_q$ et $M = (1, 2t)$. La droite (NM) coupe le cercle $\mathbb{S}^1(\mathbb{F}_q)$ en N et en un deuxième point $p(t)$.

(carac $\neq 2$)

La droite (NM) admet pour équation $y = t(x+1)$
et le cercle $x^2+y^2 = 1$
ce qui donne $x^2(1+t^2) + 2t^2x + (t^2-1) = 0$

l'analogie avec les réels et la paramétrisation du cercle se fait nettement ressentir...

Comme -1 n'est pas un carré de $\mathbb{F}_q^*$, c'est une équation de degré 2. Une solution évidente est -1 (qui correspond à N), qui ne nous intéresse pas beaucoup. L'autre s'obtient par le produit des racines :

$$x(-1) = \frac{t^2-1}{1+t^2} \quad \text{d'où} \quad x = \frac{1-t^2}{1+t^2} \quad \text{et} \quad y = t(1+x) = \frac{2t}{1+t^2}.$$

Réciproquement, si $M' = (x,y)$ est un point de $\mathbb{S}^1(\mathbb{F}_q) \setminus \{N\}$, on a $x \neq -1$ donc la droite (NM') coupe la droite $X=1$ en un seul point. Ainsi p établit une bijection de $\mathbb{F}_q$ sur $\mathbb{S}^1(\mathbb{F}_q) \setminus \{N\}$.
Donc $|SO_2(\mathbb{F}_q)| = |\mathbb{S}^1(\mathbb{F}_q)| = |\mathbb{F}_q| + 1 = q+1$.

$\mathbb{F}_{q^2} = \mathbb{F}_q[X]/(X^2+1)$ car -1 non carré dans $\mathbb{F}_q^*$

Il reste à montrer que $SO_2(\mathbb{F}_q)$ est cyclique. Pour cela, on considère $\mathbb{F}_{q^2}$, extension de $\mathbb{F}_q$ de degré 2 dans laquelle -1 possède une racine. Si μ est une racine de -1 dans $\mathbb{F}_{q^2}^*$, on a alors :

$$\tilde{\psi} : SO_2(\mathbb{F}_q) \hookrightarrow SO_2(\mathbb{F}_{q^2}) \hookrightarrow \mathbb{F}_{q^2}^*$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a + \mu b$$

$SO_2(\mathbb{F}_q) \simeq \mathrm{Im}\,\tilde{\psi} \leq \mathbb{F}_{q^2}^*$

Par injectivité de $\tilde{\psi}$, $SO_2(\mathbb{F}_q)$ est (isomorphe à) un sous-groupe de $\mathbb{F}_{q^2}^*$, qui est cyclique. Comme tout sous-groupe d'un groupe cyclique est encore cyclique, $SO_2(\mathbb{F}_q)$ est cyclique et donc

$$SO_2(\mathbb{F}_q) \simeq \mathbb{Z}/(q+1)\mathbb{Z}.$$