Etude de $SO_2(\mathbb{F}_q)$

Réf:
- Histoires hédonistes de groupes et de géométries tome 1, J. Caldero

Leçons: 104, 120, 123, 125, 162, 190.

Théorème

Soit q une puissance d'un nombre premier impair.

Si -1 est un carré dans $\mathbb{F}_q$ alors on a

$$SO_2(\mathbb{F}_q) \simeq \frac{\mathbb{Z}}{(q-1)\mathbb{Z}}$$

Sinon on a

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

Preuve: on a la description suivante de $SO_2(\mathbb{F}_q)$

$$SO_2(\mathbb{F}_q) = \left\{ A \in GL_2(\mathbb{F}_q) \,/\, \det(A) = 1 \,,\, {}^tAA = I_2 \right\}$$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; (a,b,c,d) \in \mathbb{F}_q^4,\ ad-bc=1,\ a^2+b^2=1,\ c^2+d^2=1,\ ac+bd=0 \right\}$$

Soient a, b dans $\mathbb{F}_q$ tels que $a^2+b^2=1$. Alors le système d'équations linéaires

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

est un système de déterminant 1. Ainsi il y a une unique solution : c'est $(c,d) = (-b,a)$ et on a bien alors

$$c^2+d^2=1$$

On en déduit la bijection $S^1(\mathbb{F}_q) \xrightarrow{\varphi}{\sim} SO_2(\mathbb{F}_q)$ donnée par

$$\varphi(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Pour calculer $\#SO_2(\mathbb{F}_q)$ on se ramène à compter les points du cercle.

Etape 1 : Supposons que -1 soit un carré dans $\mathbb{F}_q$.
Soit $\omega \in \mathbb{F}_q^*$ tel que $-1 = \omega^2$. Soient a, b dans $\mathbb{F}_q$ tels que

$$a^2 + b^2 = 1$$

On peut alors factoriser de la façon suivante

$$(a + \omega b)(a - \omega b) = a^2 + b^2$$

Comme q est impair, l'application

$$(a, b) \longmapsto (a + \omega b, a - \omega b)$$

est alors bijective d'inverse $(x, y) \longmapsto \left(\frac{x+y}{2}, \frac{x-y}{2\omega}\right)$

On obtient alors

$$\#SO_2(\mathbb{F}_q) = \#S^1(\mathbb{F}_q) = \#\left\{(x, y) \in \mathbb{F}_q^2 \,/\, xy = 1\right\}$$

Le choix d'un x dans $\mathbb{F}_q^*$ détermine entièrement $y \in \mathbb{F}_q$ tel que $xy = 1$. D'où

$$\#SO_2(\mathbb{F}_q) = \#\mathbb{F}_q^* = q - 1$$

De plus, l'application

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

est un morphisme de groupes. Il est injectif. En effet, soit (a, b) dans $\mathbb{F}_q$ tels que $a^2 + b^2 = 1$ et $a + \omega b = 1$. Alors on obtient

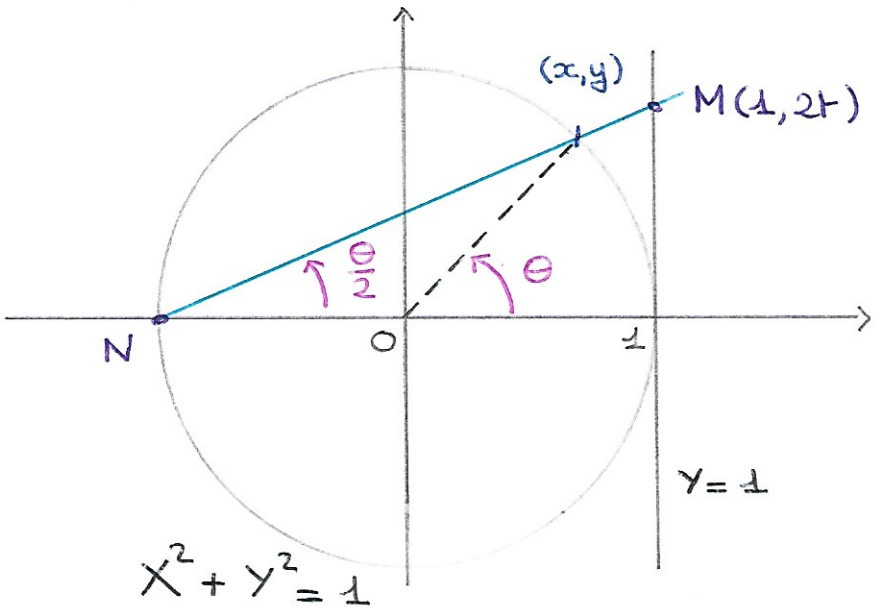
$$1 = \frac{a^2 + b^2}{a + \omega b} = a - \omega b$$

et donc $a = 1$ et $b = 0$.

Par égalité des cardinaux, on obtient

$$SO_2(\mathbb{F}_q) \simeq \mathbb{F}_q^\times \simeq \frac{\mathbb{Z}}{(q-1)\mathbb{Z}}$$

Etape 2 : Supposons que -1 ne soit pas un carré dans $\mathbb{F}_q$.



Soit $t \in \mathbb{F}_q$. On note M le point de $\mathbb{F}_q^2$ de coordonnées $(1,2t)$ et N le point $(-1,0)$. Alors (NM) est la droite d'équation

$$y = t(x+1)$$

Soit $(x,y) \in S^1(\mathbb{F}_q) \cap (NM)$. On a alors

$$t^2(x+1)^2 + x^2 = 1$$

c-à-d $$(t^2+1)x^2 + 2t^2x + t^2 - 1 = 0$$

C'est une équation polynomiale de degré 2 car $t^2+1 \neq 0$. On a

$$x^2 + \frac{2t^2}{t^2+1}x + \frac{t^2-1}{t^2+1} = 0$$

soit $$\left(x + \frac{t^2}{t^2+1}\right)^2 - \frac{t^4}{(t^2+1)^2} + \frac{t^2-1}{t^2+1} = 0$$

et $$\left(x + \frac{t^2}{t^2+1}\right)^2 - \frac{1}{(t^2+1)^2} = 0$$

Au final on obtient

$$\left(x - \frac{t^2-1}{t^2+1}\right)(x+1) = 0$$

Comme $x \neq -1$, on en déduit $x = \frac{t^2-1}{t^2+1}$ et donc $y = \frac{2t}{t^2+1}$

Inversement, pour tout point $(x,y) \in S^1(\mathbb{F}_q) \setminus \{N\}$ on a $x \neq -1$ et donc la droite (NM), où $M = (x,y)$, coupe la droite d'équation $Y = 1$ en un point.

Ainsi on obtient une bijection

$$\begin{array}{ccc} \mathbb{F}_q & \xrightarrow{\sim} & S^1(\mathbb{F}_q) \setminus \{N\} \\ t & \longmapsto & \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) \end{array}$$

d'où $\# SO_2(\mathbb{F}_q) = q+1$.

* Montrons que $SO_2(\mathbb{F}_q)$ est cyclique.

Etape 3 : on injecte $SO_2(\mathbb{F}_q)$ dans $\mathbb{F}_{q^2}$. Comme -1 n'est pas un carré dans $\mathbb{F}_q$, le polynôme X^2+1 est irréductible dans $\mathbb{F}_q[X]$ Alors il admet une racine μ dans $\frac{\mathbb{F}_q[X]}{(X^2+1)} \simeq \mathbb{F}_{q^2}$.

Ainsi le morphisme

$$SO_2(\mathbb{F}_q) \hookrightarrow SO_2(\mathbb{F}_{q^2}) \xrightarrow{\Psi_{q^2}} \mathbb{F}_{q^2}^*$$

est bien défini et injectif.

Ainsi $SO_2(\mathbb{F}_q)$ est isomorphe à un sous-groupe du groupe cyclique $\mathbb{F}_{q^2}^\times$: il est donc cyclique.

Cela conclut ∎