Structure de $\mathrm{SO}_2(\mathbb{F}_q)$

[On trouvera cette démonstration dans le Caldero & Germoni, *Nouvelles histoires hédonistes de groupes et de géométrie, Tome II* p.50.]

Soit q une puissance d'un nombre premier impair.

Lemme 2.1

Posons $C^1(\mathbb{F}_q) \overset{\text{def}}{=} \left\{(a,b) \in \mathbb{F}_q \mid a^2+b^2=1\right\}$.

$$\mathrm{SO}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ (a,b) \in C^1(\mathbb{F}_q) \right\}$$

Théorème 2.2

$$\mathrm{SO}_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}\big/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré de } \mathbb{F}_q, \\ \mathbb{Z}\big/(q+1)\mathbb{Z} & \text{si } -1 \text{ n'est pas un carré de } \mathbb{F}_q \end{cases}$$

Structure de la démonstration :

1 ▸ *Démontrer le Lemme,*

2 ▸ *Montrer que* $\mathrm{SO}_2(\mathbb{F}_q)$ *est toujours cyclique,*

3 ▸ *Montrer que* $\mathrm{SO}_2(\mathbb{F}_q)$ *a même cardinal que* $C^1(\mathbb{F}_q)$*,*

4 ▸ *Déterminer* $\#C^1(\mathbb{F}_q)$ *dans les deux cas.*

---

1 ▸ Par définition,

$$\begin{aligned} \mathrm{SO}_2(\mathbb{F}_q) &= \left\{A \in \mathcal{M}_2(\mathbb{F}_q) \mid {}^tAA = I_2,\ \det(A)=1\right\} \\ &= \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \ : \ (a,b,c,d) \in \mathbb{F}_q^4,\ a^2+b^2=c^2+d^2=ad-bc=1,\ ac+bd=0 \right\} \\ &= \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \ : \ (c,d) \in S_{\mathbb{F}_q}(S_{a,b}),\ (a,b) \in C^1(\mathbb{F}_q) \right\} \end{aligned}$$

où $S_{\mathbb{F}_q}(S_{a,b})$ est l'ensemble des solutions sur $\mathbb{F}_q$ du système d'inconnues c et d :

$$S_{a,b} : \begin{cases} ac+bd=0 \\ ad-bc=1 \end{cases} \iff \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Comme $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2+b^2 = 1$, c'est un système de Cramer dont la solution est $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix}$, ce qui au passage justifie que la condition $c^2+d^2=1$ est automatique pour le passage à la troisième égalité ci-dessus. Ainsi,

$$\mathrm{SO}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ (a,b) \in C^1(\mathbb{F}_q) \right\}$$

2 ▸ Montrons que $\mathrm{SO}_2(\mathbb{F}_q)$ est cyclique :

- Supposons qu'il existe $i \in \mathbb{F}_q$ tel que $i^2 = -1$. Posons $\varphi : \begin{array}{ccc} \mathrm{SO}_2(\mathbb{F}_q) & \to & \mathbb{F}_q^\times \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \mapsto & a + ib \end{array}$ est un morphisme de groupes : déjà, $\forall (a,b) \in C^1(\mathbb{F}_q^2)$, $(a+ib)(a-ib) = a^2+b^2 = 1 \neq 0$ donc $a+ib \neq 0$, *i.e.* $a+ib \in \mathbb{F}_q^\times$ par intégrité, et on vérifie par un calcul direct que l'image d'un produit est le produit des images. Montrons que φ est injectif : soit $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{Ker}(\varphi)$. Alors $1 = a^2 + b^2 + (a+ib)(a-ib) = 1 \times (a-ib)$. L'application $(a,b) \in \mathbb{F}_q^2 \mapsto (a+ib, a-ib)$ est bijective, de réciproque $(x,y) \in \mathbb{F}_q^2 \mapsto \left(\frac{x+y}{2}, \frac{x-y}{2i}\right)$ (car $i \neq 0$ par intégrité, et $2 \neq 0$ car q est impair) *(Remarque : il faut penser aux nombres complexes, c'est même plus qu'une analogie !)*, *a fortiori* $a = \frac{(a+ib)+(a-ib)}{2} = 1$ et $b = \frac{(a+ib)-(a-ib)}{2i} = 0$, *i.e.* $A = I_2$.
  On dispose ainsi d'une injection $\mathrm{SO}_2(\mathbb{F}_q) \hookrightarrow \mathbb{F}_q^\times$, mais tout sous groupe du groupe multiplicatif d'un corps fini est cyclique, donc $\mathrm{SO}_2(\mathbb{F}_q)$ est cyclique.
- Supposons que -1 n'est pas un carré dans $\mathbb{F}_q$. Alors $X^2+1 \in \mathbb{F}_q[X]$ est irréductible (car de degré 2 sans racines sur un corps), donc $\mathbb{F}_q[X]\Big/\langle X^2+1\rangle \simeq \mathbb{F}_{q^2}$. De là, -1 est un carré dans $\mathbb{F}_{q^2}$, et d'après les injections $\mathrm{SO}_2(\mathbb{F}_q) \hookrightarrow \mathbb{F}_q^\times \hookrightarrow \mathbb{F}_{q^2}^\times$ et le même argument que précédemment, $\mathrm{SO}_2(\mathbb{F}_q)$ est cyclique.

3 ▸ D'après le Lemme, l'application $f : C^1(\mathbb{F}_q) \to \mathrm{SO}_2(\mathbb{F}_q)$, $(a,b) \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est bien définie et bijective., d'où $\#\mathrm{SO}_2(\mathbb{F}_q) = \#C^1(\mathbb{F}_q)$.

4 ▸ Déterminons $\#C^1(\mathbb{F}_q)$:

- Supposons qu'il existe $i \in \mathbb{F}_q$ tel que $i^2 = -1$. En utilisant le changement de variable $(a,b) \in \mathbb{F}_q^2 \mapsto (a+ib, a-ib)$ vu ci-dessus,

$$C^1(\mathbb{F}_q) = \left\{(a,b) \in \mathbb{F}_q^2 \mid 1 = a^2+b^2 = (a+ib)(a-ib)\right\} = \left\{(x,y) \in \mathbb{F}_q^\times \mid xy = 1\right\}$$

  donc $\#C^1(\mathbb{F}_q) = \#\mathbb{F}_q^\times = q-1$, et donc :

$$\boxed{\mathrm{SO}_2(\mathbb{F}_q) \simeq \mathbb{Z}\Big/(q-1)\mathbb{Z}}$$

- Supposons que -1 n'est pas un carré dans $\mathbb{F}_q$. Posons $N = (-1,0) \in \mathbb{F}_q^2$, et pour $t \in \mathbb{F}_q$, posons $M_t = (1,2t) \in \mathbb{F}_q^2$. La droite (NM_t) a pour équation (voir les commentaires plus bas : on va faire de la géométrie plane comme si on était dans $\mathbb{R}^2$, et ça va marcher) :

$$(NM_t) : y = \frac{y_M - y_N}{x_M - x_N}(x - x_N) + y_N = \frac{2t}{1-(-1)}(x+1) + 0 = t(x+1)$$

  De là, pour tout $(x,y) \in \mathbb{F}_q^2$,

$$\begin{aligned}
\begin{pmatrix} x \\ y \end{pmatrix} \in (NM_t) \cap C^1(\mathbb{F}_q) &\iff x^2+y^2 = 1 \quad \text{et} \quad y = t(x+1) \\
&\iff x^2 + t^2(x+1)^2 = 1 \quad \text{et} \quad y = t(x+1) \\
&\iff (t^2+1)x^2 + 2t^2x + t^2 - 1 = 0 \quad \text{et} \quad y = t(x+1) \\
&\overset{(*)}{\iff} x = \frac{-2t^2 \pm 2}{2(1+t^2)} \quad \text{et} \quad y = t(x+1) \\
&\iff x \in \left\{-1, \frac{1-t^2}{1+t^2}\right\} \quad \text{et} \quad y = t(x+1) \\
&\iff (x,y) = N \quad \text{ou} \quad (x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)
\end{aligned}$$

$(*)$: comme -1 n'est pas un carré, $1+t^2 \neq 0$, et $\Delta = (2t^2)^2 - 4(t^2+1)(t^2-1) = (2t^2)^2 - 4((t^2)^2-1) = 4 = 2^2$. De plus, q est impair donc $2 \neq 0$.

On définit ainsi l'application $p : \mathbb{F}_q \to C^1(\mathbb{F}_q)\backslash\{N\},\ t \mapsto \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.

Celle-ci est injective car si $p(t) = p(t')$, alors d'après la suite d'équivalences précédente, $p(t) = p(t') \in C^1(\mathbb{F}_q) \cap (NM_t) \cap (NM_{t'})$. Or si $t \neq t'$, alors $(NM_t) \cap (NM_{t'}) = \{N\}$, mais $p(t) = p(t') \neq N$, donc $t = t'$. Inversement, p est surjective : en effet, soit $P \in C^1(\mathbb{F}_q)\backslash\{N\}$. Comme $P \neq N$, la droite (PN) intersecte la droite $\{x = 1\}$ et un unique point M. Comme q est impair, $2 \neq 0$ donc il existe $t \in \mathbb{F}_q$ tel que $M = M_t$. D'après la suite d'équivalences ci-dessus (autrement dit : par construction), $P = p(t)$.

De là, $\#C^1(\mathbb{F}_q) = \#C^1(\mathbb{F}_q)\backslash\{N\} + 1 = \#\mathbb{F}_q + 1 = q + 1$, et donc :

$$\boxed{\mathrm{SO}_2(\mathbb{F}_q) \simeq \mathbb{Z}\Big/(q+1)\mathbb{Z}}$$

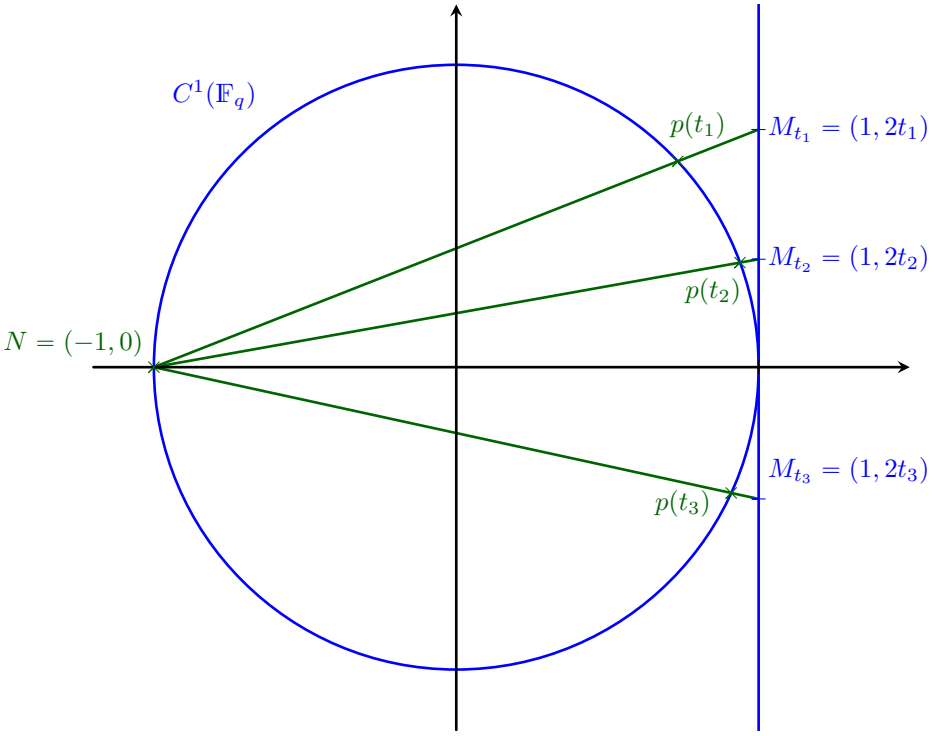

FIGURE 2.1 – Construction de $p(t)$

COMMENTAIRES

- Recasages : 106 (Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.), 123 (Corps finis. Applications.), éventuellement 104 (Groupes finis. Exemples et applications.) et 190 (Méthodes combinatoires, problèmes de dénombrement.)
- La démonstration complète est longue : on pourra admette le lemme et simplement énoncer le point 3 ▸ à l'oral.
- Concernant la géométrie euclidienne dans $\mathbb{F}_q^2$: on peut tout vérifier par le calcul :

- Équation de la droite passant par A et B tels que $x_A \neq x_B$:

$$\begin{aligned} M\begin{pmatrix}x\\y\end{pmatrix} \in (AB) &\iff \det(\vec{MA}, \vec{MB}) = 0 \\ &\iff \begin{vmatrix} x-x_A & x-x_B \\ y-y_A & y-y_B \end{vmatrix} = (x-x_A)(y-y_B) - (x-x_B)(y-y_A) = 0 \\ &\iff \cancel{xy} - x_A y - y_B x + x_A y_B = \cancel{xy} - x_B y - y_A x + x_B y_A \\ &\iff (x_B - x_A)y = (y_B - y_A)x + (y_B - y_A)x_A + (x_B - x_A)y_A \\ &\iff y = \frac{y_B - y_A}{x_B - x_A}(x - x_A) + y_A \end{aligned}$$

- Intersection de (NM_t) et $(NM_{t'})$:

$$\begin{aligned} M\begin{pmatrix}x\\y\end{pmatrix} \in (NM_t) \cap (NM_{t'}) &\iff y = t(x+1) = t'(x+1) \\ &\iff t = t' \quad \text{ou} \quad x = -1 \\ &\iff t = t' \quad \text{ou} \quad (x,y) = N \end{aligned}$$

- Rappelons que $\mathrm{SO}_2(\mathbb{R}) = \left\{ R(\theta) \overset{\text{def}}{=} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \ : \ 0 \leqslant \theta < 2\pi \right\} \simeq \mathbb{R}\Big/2\pi\mathbb{Z}$. En particulier, le complexe $\rho \mathrm{e}^{i\theta}$ correspond à la matrice $\rho R(\theta)$, dans le sens où $\rho \mathrm{e}^{i\theta}\rho' \mathrm{e}^{i\theta'} = \rho\rho' \mathrm{e}^{i(\theta+\theta')}$ et $\rho R(\theta)\rho' R(\theta') = \rho\rho' R(\theta+\theta')$, *i.e.* cette interprétation est compatible avec l'opération de multiplication complexe. C'est là le fondement de l'analogie mentionnée dans le développement.
- Le Lemme reste vrai si $q = 2^r$ est pair, et il faut dans ce cas remarquer que $(a,b) \in C^1(\mathbb{F}_{2^r}) \iff 1 = a^2 + b^2 = (a+b)^2$ en vertu du morphisme de Frobenius. De là,

$$\begin{aligned} \mathrm{SO}_2(\mathbb{F}_{2^r}) &= \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ (a,b) \in \mathbb{F}_{2^r}^2, \ a+b = \pm 1 = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & 1+a \\ 1+a & a \end{pmatrix} \ : \ a \in \mathbb{F}_{2^r} \right\} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \mathbb{F}_{2^r} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \end{aligned}$$

Remarquons que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ commutent, donc pour tout $a \in \mathbb{F}_{2^r}$,

$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 + a^2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^2 = I_2$$

(on utilise le binôme de Newton, et $2 \mid \binom{2}{1}$). Ainsi, tous les éléments de $\mathrm{SO}_2(\mathbb{F}_{2^r})$ sont d'ordre au plus 2. Automatiquement, $\mathrm{SO}_2(\mathbb{F}_{2^r})$ est abélien (soient A et B dans $\mathrm{SO}_2(\mathbb{F}_{2^r})$ d'ordre au plus 2. Comme *tous* les éléments sont d'ordre au plus 2, $BA = B^{-1}A^{-1} = (AB)^{-1} = AB$), d'où :

$$\boxed{\mathrm{SO}_2(\mathbb{F}_{2^r}) \simeq \left(\mathbb{Z}\Big/2\mathbb{Z}\right)^r}$$