

DVP Le groupe $\mathcal{SO}_2(\mathbb{F}_q)$

Antoine DEQUAY

21 septembre 2022

Notes

- Prof : .
- Leçons : 104, 106, 120, 123, 162, 190.
- Références :
 - H2G2 tome 2.

Théorème 1 Soit q une puissance d'un nombre premier impair, on a l'isomorphisme :

$$\mathcal{SO}_2(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré de } \mathbb{F}_q^*, \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon.} \end{cases}$$

Preuve. Commençons par décrire le groupe auquel on s'intéresse :

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

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

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

forment un système linéaire de déterminant $a^2 + b^2 = 1$, donc la solution évidente $(c, d) = (-b, a)$ est l'unique solution et elle vérifie bien $c^2 + d^2 = 1$. On a donc :

$$\mathcal{SO}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{M}_n(\mathbb{F}_q), a^2 + b^2 = 1 \right\}.$$

En notant $\mathbf{S}^1(\mathbb{F}_q)$ le "cercle unité" de $\mathbb{F}_q^2$, on a accès à la bijection :

$$\begin{pmatrix} \mathbf{S}^1(\mathbb{F}_q) & \xrightarrow{\sim} & \mathcal{SO}_2(\mathbb{F}_q) \\ (a, b) & \mapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{pmatrix}.$$

Comptons donc les points du cercle.

Supposons que -1 soit résidu quadratique modulo q . On se donne ω une de ses racines, on peut écrire $a^2 + b^2 = (a + \omega b)(a - \omega b)$, et on a alors :

$$\begin{cases} x = a + \omega b \\ y = a - \omega b \end{cases} \iff \begin{cases} a = \frac{x+y}{2} \\ b = \frac{x-y}{2\omega} \end{cases} \quad (\text{licite car } 2 \neq 0, \text{ car } q \text{ est impair}).$$

Par changement de variable, on a donc :

$$|\mathcal{SO}_2(\mathbb{F}_q)| = |\mathbf{S}^1(\mathbb{F}_q)| = |\{(x, y) \in \mathbb{F}_q^2, xy = 1\}|.$$

Pour $x \in \mathbb{F}_q^*$, on a un unique $y = x^{-1}$ correspondant, d'où $|\mathcal{SO}_2(\mathbb{F}_q)| = q - 1$. On note :

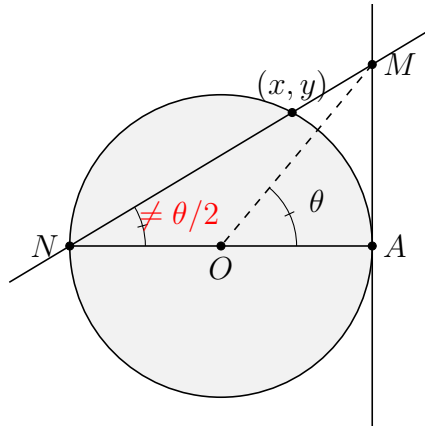
$$\psi : \left(\begin{array}{ccc} \mathcal{SO}_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^* \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \longmapsto & a + \omega b \end{array} \right).$$

L'application ψ est un morphisme, par analogie avec le corps des complexes. Elle est bien injective, car si $\psi(A) = 1$, alors $x = a + \omega b = 1$, puis $y = a - \omega b = \frac{a^2 + b^2}{a + \omega b} = 1$, et il vient $a = 1$ et $b = 0$.

Par égalité des cardinaux, ψ est bien un isomorphisme de $\mathcal{SO}_2(\mathbb{F}_q)$ sur le groupe cyclique $\mathbb{F}_q^*$. D'où :

$$\mathcal{SO}_2(\mathbb{F}_q) \cong \mathbb{Z}/(q-1)\mathbb{Z}.$$

Supposons à présent que -1 ne soit pas un résidu quadratique modulo q . On raisonne graphiquement par analogie avec les réels.



A dire en même temps qu'on dessine : On note $N = (-1, 0)$, $M = (1, 2t)$ pour $t \in \mathbb{F}_q$. On note $p(t) \neq N$ l'intersection de $\mathbf{S}^1(\mathbb{F}_q)$ et de la droite (NM) (dans le cas des réels, $t = \tan(\theta/2)$ par théorème de l'angle inscrit).

Le point $p(t)$ existe bien ! C'est une propriété sur les coniques, que l'on redémontre ici : (MN) admet pour équation $y = t(x + 1)$ (car $2 \neq 0$). On cherche donc à résoudre l'équation aux abscisses $(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0$. Comme $1+t^2 \neq 0$ (car -1 n'est pas résidu quadratique modulo q), l'équation admet deux solutions. La solution évidente, -1 , correspondant à N est écartée. Par relation coefficients-racines, on obtient :

$$x = -\frac{t^2 - 1}{1 + t^2} \text{ et } y = t(x + 1) = \frac{2t}{1 + t^2}.$$

Inversement, Pour tout point $M' = (x, y) \neq N$ du cercle unité, (NM') coupe la droite $X = 1$ en un unique point $\left(1, \frac{2y}{x+1}\right)$ qui existe car $x \neq -1$ car $M' \neq N$. Ainsi, on a bien une

bijection de $\mathbf{S}^1(\mathbb{F}_q) \setminus \{N\}$ sur $\mathbb{F}_q$, donc

$$|\mathcal{SO}_2(\mathbb{F}_q)| = |\mathbf{S}^1(\mathbb{F}_q)| = q + 1.$$

Il reste à voir que $\mathcal{SO}_2(\mathbb{F}_q)$ est bien cyclique. Pour cela, on note :

$$\psi : \left(\begin{array}{ccc} \mathcal{SO}_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_{q^2}^* \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \longmapsto & a + \omega b \end{array} \right),$$

où ω est une racine carrée de -1 dans $\mathbb{F}_{q^2}^*$, vu comme extension de $\mathbb{F}_q^*$. L'élément ω existe bien : $X^2 - 1$ est irréductible dans $\mathbb{F}_q[X]$ (sans racine de degré 2), donc $L := \mathbb{F}_q[X]/\langle X^2 + 1 \rangle$ est une extension de $\mathbb{F}_q$ de degré 2, contenant une racine carrée de -1 . Par unicité, il vient $\mathbb{F}_{q^2} = L$ (l'argument fonctionne pour tout élément non carré!).

Comme précédemment, ψ est bien un morphisme injectif. Son image est donc en particulier un sous-groupe du groupe multiplicatif de $\mathbb{F}_{q^2}^*$. Comme $\mathbb{F}_{q^2}^*$ est un corps fini, son groupe multiplicatif est cyclique, et ses sous-groupes le sont donc également. Donc $\mathcal{SO}_2(\mathbb{F}_q)$ est bien cyclique, ce qui achève la preuve. □

Remarque

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

$$\text{la formule : } N = \sum_{k|N} |\{g \in G \mid \text{ord}(g) = k\}| = \sum_{k|N} N_k \quad (\clubsuit).$$

Soit $g \in G$ avec $\text{ord}(g) = k$ et $k \mid N$. On a $|\langle g \rangle| = k$ et $\langle g \rangle \cong_{\text{isom}} \mathbb{Z}/k\mathbb{Z}$. 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 $k \mid N$: $N_k \in \{0, \varphi(k)\}$ $(\spadesuit)$

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

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