

Soient p premier impair, $r \geq 1$ et $q = p^r$. On note $\mathbb{F}_q^{x(2)}$ l'ensemble des carrés de $\mathbb{F}_q^*$.

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \in \mathbb{F}_q^{x(2)} \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Rappelons que $SO_2(\mathbb{F}_q) = \{A \in M_2(\mathbb{F}_q) \mid {}^tAA = I_2 \text{ et } \det(A) = 1\}$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_q) \mid ad - bc = a^2 + b^2 = c^2 + d^2 = 1 \text{ et } ac + bd = 0 \right\}.$$

Pour tout $(a, b) \in \mathbb{F}_q^2$, le système $(S_{a,b}) : \begin{cases} ad - bc = 1 \\ ac + bd = 0 \end{cases} \Leftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ d'inconnues c et d est de déterminant $a^2 + b^2$. Si $(a, b) \in C^1(\mathbb{F}_q) := \{(a, b) \in \mathbb{F}_q^2 \mid a^2 + b^2 = 1\}$, alors ce système admet une unique solution, qui est $(c, d) = (-b, a)$ (qui vérifie $c^2 + d^2 = 1$). Ainsi, l'application $f: C^1(\mathbb{F}_q) \rightarrow SO_2(\mathbb{F}_q)$, $(a, b) \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est bien définie, et $g: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b)$ est injective sur $SO_2(\mathbb{F}_q)$ (si $g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = g\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)$, alors $a' = a$ et $b' = b$, mais $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2(\mathbb{F}_q)$ et $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SO_2(\mathbb{F}_q)$, donc (c, d) est solution de $(S_{a,b})$ et (c', d') est solution de $(S_{a,b'})$, et $a^2 + b^2 = a'^2 + b'^2 = 1$, donc $(c', d') = (-b', a') = (-b, a) = (c, d)$). Comme f est clairement injective et $C^1(\mathbb{F}_q)$ et $SO_2(\mathbb{F}_q)$ sont finis, f est bijective (de réciproque g).

1^{er} cas : $-1 \in \mathbb{F}_q^{x(2)}$: Soit $w \in \mathbb{F}_q^*$ tel que $w^2 = -1$. Pour tout $(a, b) \in \mathbb{F}_q^2$, $a^2 + b^2 = 1 \Leftrightarrow (a + wb)(a - wb) = 1$. Comme $p \neq 2$, l'application $(a, b) \mapsto (a + wb, a - wb)$ est une bijection de $\mathbb{F}_q^2$ (de réciproque $(x, y) \mapsto (\frac{x+y}{2}, \frac{x-y}{2w})$), donc $C^1(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 \mid xy = 1\}$, donc $\#SO_2(\mathbb{F}_q) = \#C^1(\mathbb{F}_q) = q - 1$.

Posons $\varphi: SO_2(\mathbb{F}_q) \rightarrow \mathbb{F}_q^*$, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + wb$. C'est un morphisme de groupes $\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{pmatrix}$, $(a + wb)(c + wd) = (ac - bd) + w(ad + bc)$. Soit $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \text{Ker}(\varphi)$. Alors

$1 = \varphi(A) = a + wb = \frac{a^2 + b^2}{a - wb} = \frac{1}{a - wb}$, donc $a - wb = 1$, donc $2a = 2$ et $2wb = 0$, mais $p \neq 2$ donc $2 \neq 0$, donc $a = 1$ et ($w \neq 0$ donc) $b = 0$, donc $A = I_2$. Ainsi, φ est injectif, mais $\#SO_2(\mathbb{F}_q) = q - 1 = \#\mathbb{F}_q^*$, donc φ est un isomorphisme, donc $SO_2(\mathbb{F}_q) \simeq \mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

2nd cas : $-1 \notin \mathbb{F}_q^{x(2)}$: Posons $N = (-1, 0) \in \mathbb{F}_q^2$. Soit $t \in \mathbb{F}_q$, posons $M = (1, 2t) \in \mathbb{F}_q^2$. La droite (NM) a pour équation $y = \frac{y_M - y_N}{x_M - x_N} (x - x_N) + y_N = t(x + 1)$. Elle intersecte le cercle unité $C^1(\mathbb{F}_q)$ en 2 points exactement : en effet, soit $(x, y) \in (NM)$ tel que $x^2 + y^2 = 1$. Alors $(1 + t^2)x^2 + 2t^2x + (t^2 - 1) = 0$, mais $-1 \notin \mathbb{F}_q^{x(2)}$ donc $1 + t^2 \neq 0$, $p \neq 2$ et $(2t^2)^2 - 4(1 + t^2)(t^2 - 1) = 4 = 2^2 \in \mathbb{F}_q^{x(2)}$, donc $x = \frac{-2t^2 \pm 2}{2(1 + t^2)} = \pm \frac{t^2 - 1}{t^2 + 1} \in \{-1, \frac{t^2 - 1}{t^2 + 1}\}$. Si $x = -1$, alors $y = 0$, i.e. $(x, y) = N$. Sinon, $y^2 = 1 - x^2 = \frac{(t^2 + 1)^2 - (t^2 - 1)^2}{(t^2 + 1)^2} = \frac{4t^2}{(t^2 + 1)^2} = \left(\frac{2t}{t^2 + 1}\right)^2$, donc $y = \pm \frac{2t}{t^2 + 1}$, mais $y = t(x + 1)$ donc $y = \frac{2t}{t^2 + 1}$.

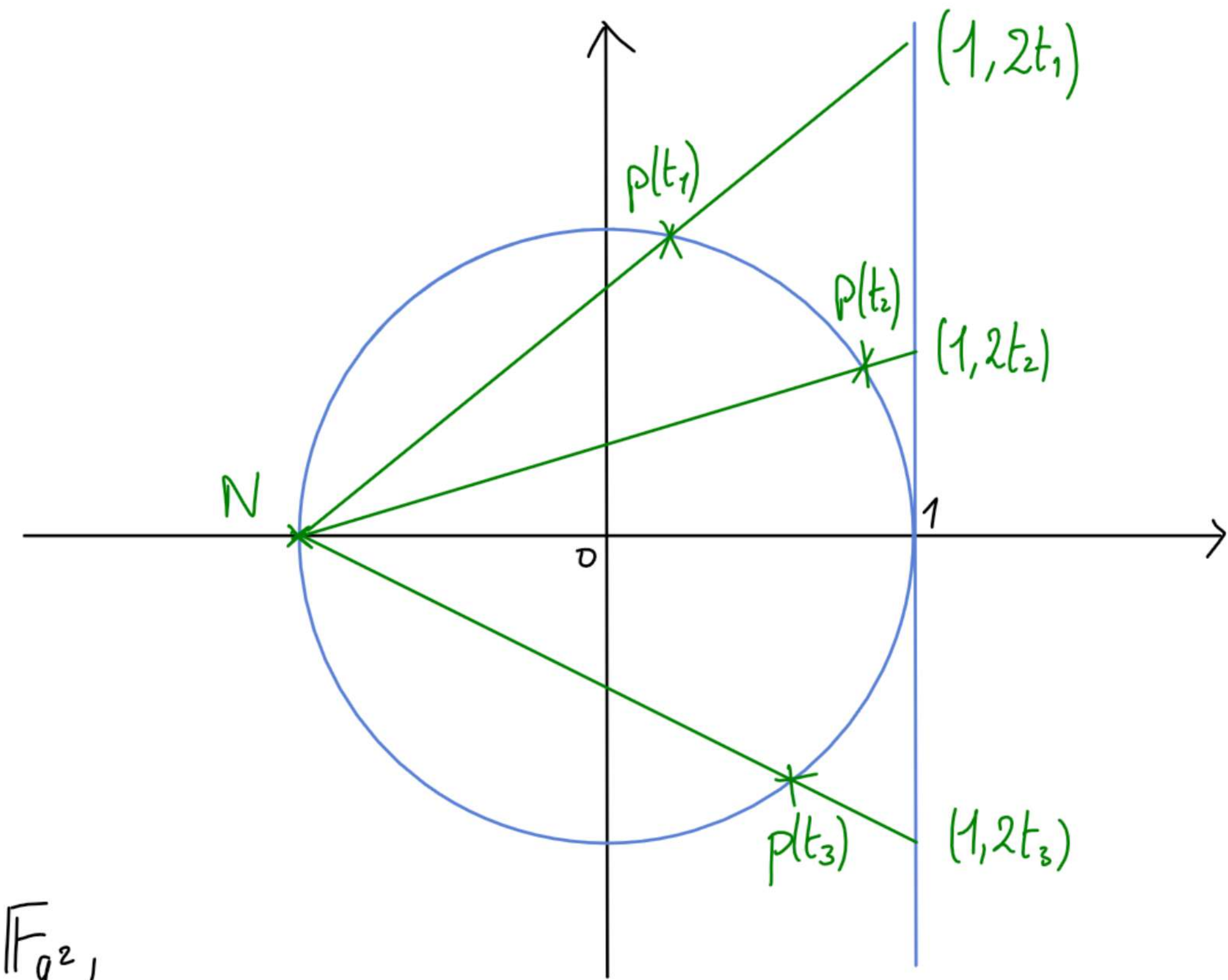
Posons $p: \mathbb{F}_q \longrightarrow C'(\mathbb{F}_q) \setminus \{N\}; t \longmapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1} \right)$: on a montré que p est injective. Réciproquement,

soit $M' = (x', y') \in C'(\mathbb{F}_q) \setminus \{N\}$. Nécessairement, $x' \neq -1$, donc (NM') et $\{x=1\}$ sont deux droites non parallèles du plan, donc s'intersectent en un unique point M . Comme $p \neq 2$, l'application $t \mapsto 2t$ est une bijection de $\mathbb{F}_q$, donc il existe $t \in \mathbb{F}_q$ tel que $M = (1, 2t)$. Mais alors $M' = p(t)$ par construction de $p(t)$, d'après ce qui précède.

Ainsi, p est une bijection de $\mathbb{F}_q$ dans $C'(\mathbb{F}_q) \setminus \{N\}$, donc $\# C'(\mathbb{F}_q) = \# \mathbb{F}_q + 1 = q + 1$.

Dans $\mathbb{F}_{q^2}^\times$, -1 est un carré: en effet, $-1 \in \mathbb{F}_q^{(2)}$ donc $X^2 + 1$ est de degré 2 sans racines dans $\mathbb{F}_q$, donc irréductible, donc $L := \frac{\mathbb{F}_q[X]}{\langle X^2 + 1 \rangle}$ est une extension de degré 2 de $\mathbb{F}_q$, donc

$L \simeq \mathbb{F}_{q^2}$ par unicité. Il s'en suit que $X^2 + 1$ a une racine dans $\mathbb{F}_{q^2}$, i.e. que $(-1) \in \mathbb{F}_q^{(2)}$. Notons $w \in \mathbb{F}_{q^2}$ une racine de -1 . D'après ce qui précède, on dispose des injections $SO_2(\mathbb{F}_q) \hookrightarrow SO_2(\mathbb{F}_{q^2}) \hookrightarrow \mathbb{F}_{q^2}^\times$ (par $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + wb$), donc $SO_2(\mathbb{F}_q)$ est isomorphe à un sous-groupe fini du groupe multiplicatif du corps $\mathbb{F}_{q^2}$, donc $SO_2(\mathbb{F}_q)$ est cyclique. Finalement, $SO_2(\mathbb{F}_q) \simeq \mathbb{Z}/(q+1)\mathbb{Z}$.



COMMENTAIRES:

- Soit (V, q) un espace quadratique non dégénéré sur un corps commutatif K . De manière générale:
 - Si $\dim(V) \geq 3$, alors $Z(SO(q)) = \{\pm \text{id}_V\} \cap SO(q)$ (NB: $-\text{id}_V \in SO(q) \iff \dim(V)$ est paire)
(ça demande pas mal de travail)
 - Si $\dim(V) = 2$ et (V, q) est un plan hyperbolique, alors $SO(q) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in K^\times \right\} \simeq K^\times$ est abélien (en confondant les isométries et leur matrice dans une base — on le montre directement)
 - Si $\dim(V) = 2$ et (V, q) est anisotrope, alors $SO(q)$ est abélien.
(ça demande pas mal de travail)

Dans tous les cas, $SO(q)$ est abélien. On peut avoir la même discussion pour $O(q)$:

- Si $\dim(V) \geq 3$ ou $\dim(V) = 2$ et (V, q) est anisotrope, alors $Z(O(q)) = \{\pm \text{id}_V\}$.
- Si $\dim(V) = 2$ et (V, q) est un plan hyperbolique:
 - Si $K = \mathbb{F}_3$, alors $O(q) = \{\pm I_2, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ est abélien,
 - Sinon, $Z(O(q)) = \{\pm \text{id}_V\}$
(exercice rapide, calcul direct avec le critère $M \in O(q) \iff {}^t M \cdot \text{Mat}(q) \cdot M = \text{Mat}(q)$.)

- À toutes fins utiles, rappelons que $SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\}$.