

SO₂(F_q) est cyclique

CloudSea

Cadre

Soit q une puissance d'un nombre premier impair, on montre que

$$\mathrm{SO}_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}_q \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Recasages :

- [[106 Groupe linéaire]]
- [[123 Corps finis]]
- [[190 Dénombrement]]

Backup

- [[120 Anneau $\mathbb{Z}$ sur $n\mathbb{Z}$]] à mentionner dans le cas $q = p$ mais pas faire un dev

Référence : NH2G2 tome 1

Déroulé du développement

On note S^1 l'ensemble des $(a, b) \in \mathbb{F}_q^2$ tels que $a^2 + b^2 = 1$

Montrer que $\mathrm{SO}_2(\mathbb{F}_q)$ s'identifie à S^1

Soit $(a, b) \in S^1$ et $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice de $\mathrm{SO}_2(\mathbb{F}_q)$ dont la première colonne est (a, b)

On a

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

Donc (c, d) est solution d'un système linéaire de déterminant $a^2 + b^2 = 1$, donc ce système

admet une et une seule solution, à savoir

$$(c, d) = (-b, a)$$

Donc

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Réciproquement, il est clair qu'une telle matrice est bien dans $\text{SO}_2(\mathbb{F}_q)$, donc

$$\text{SO}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ; a, b \in \mathbb{F}_q \right\}$$

On a une bijection de S^1 dans $\text{SO}_2(\mathbb{F}_q)$

On va donc dénombrer S^1 pour dénombrer $\text{SO}_2(\mathbb{F}_q)$

Montrer que si -1 est un carré dans $\mathbb{F}_q$ alors $|\text{SO}_2(\mathbb{F}_q)| = q - 1$

Soit $\omega \in \mathbb{F}_q$ tel que $\omega^2 = -1$, on a

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

Or comme on est pas en caractéristique 2, on a

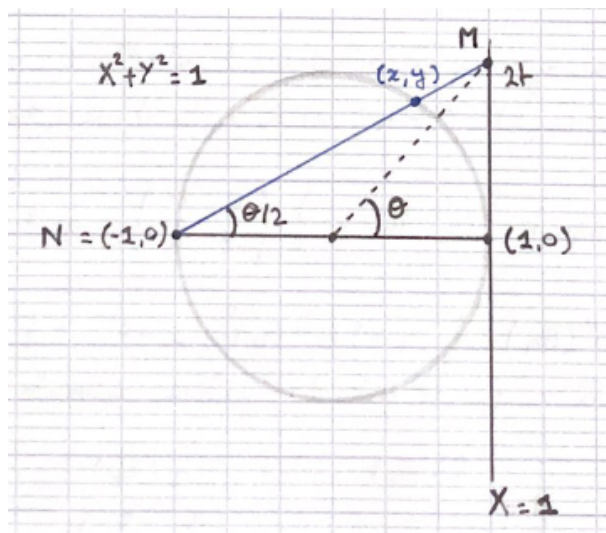
$$\begin{cases} x &= a + \omega b \\ y &= a - \omega b \end{cases} \Leftrightarrow \begin{cases} a &= \frac{x + y}{2} \\ b &= \frac{x - y}{2\omega} \end{cases}$$

Donc on a autant de $(a, b) \in S^1$ que de $(x, y) \in \mathbb{F}_q^2$ tels que $xy = 1$, à savoir $q - 1$, donc

$$|\text{SO}_2(\mathbb{F}_q)| = q - 1$$

Montrer que si -1 n'est pas un carré dans $\mathbb{F}_q$ alors $|\text{SO}_2(\mathbb{F}_q)| = q + 1$

Faisons un dessin (honteusement volé à Lavos sur agreg-maths)



Soit $t \in \mathbb{F}_q$, on considère $N = (-1, 0)$ et $M = (1, 2t)$ deux points de $\mathbb{F}_q^2$
 $2 \neq 0$ donc la droite (MN) a pour équation $y = t(x + 1)$
 Donc si $(x, y) \in (MN) \cap S^1$, on a

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

ce qui se ré écrit

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

-1 n'étant pas un carré, on a $t^2 + 1 \neq 0$ donc c'est une équation de degré 2 en x
 On a vu que -1 est solution (coucou N), donc l'autre solution s'obtient avec un lien
 coefficient racines, c'est

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

qui donne donc

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

Réciproquement pour tout point $P = (x, y)$ de S^1 différent de N , comme $x \neq -1$, la
 droite (NP) coupe la droite $\{x = 1\}$ en un unique point $M = (1, 2t)$

Donc $t \mapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right)$ est une bijection de $\mathbb{F}_q$ dans $S^1 \setminus \{N\}$

Donc $|\text{SO}_2(\mathbb{F}_q)| = q + 1$

Montrer que $\mathrm{SO}_2(\mathbb{F}_q)$ s'injecte dans $\mathbb{F}_{q^2}^*$ et conclure

On se place sur $\mathbb{F}_{q^2}$

Soit ω une racine de -1

$$\varphi : \mathrm{SO}_2(\mathbb{F}_q) \rightarrow \mathbb{F}_{q^2}^* \quad \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + \omega b$$

φ est un morphisme (de groupes) injectif, donc $\mathrm{SO}_2(\mathbb{F}_q)$ est isomorphe à un sous groupe (fini) de $\mathbb{F}_{q^2}^*$, il est donc cyclique, ce qui conclut la preuve

Détail de certains points

Pourquoi -1 admet une racine dans $\mathbb{F}_{q^2}$?

On considère $P = X^2 + 1 \in \mathbb{F}_q[X]$

Si P est scindé sur $\mathbb{F}_q$, alors -1 admet une racine dans $\mathbb{F}_q$, donc à fortiori sur $\mathbb{F}_{q^2}$

Sinon, P est irréductible, donc soit K le corps de rupture de P , K est une extension quadratique de $\mathbb{F}_q$, donc un corps fini à q^2 éléments, donc $K = \mathbb{F}_{q^2}$

Donc -1 admet bien une racine dans $\mathbb{F}_{q^2}$

Justifier que φ est un morphisme injectif

On a

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -ad - bc \\ bc + ad & ac - bd \end{pmatrix}$$

Et

$$(a + \omega b)(c + \omega d) = ac - bd + \omega(bc + ad)$$

Donc φ est bien un morphisme

Et l'injectivité crève les yeux

Version révisions

Soit q une puissance d'un nombre premier impair, on se propose de montrer que

$$\mathrm{SO}_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}_q \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

On note S^1 l'ensemble des $(a, b) \in \mathbb{F}_q^2$ tels que $a^2 + b^2 = 1$

1. Exhiber une bijection de S^1 dans $\mathrm{SO}_2(\mathbb{F}_q)$
2. Montrer que si -1 est un carré dans $\mathbb{F}_q$, alors $|\mathrm{SO}_2(\mathbb{F}_q)| = q - 1$
3. On suppose que -1 n'est pas un carré dans $\mathbb{F}_q$, et on se donne $t \in \mathbb{F}_q$, $N = (-1, 0)$ et $M = (1, 2t)$
 - 3.1 Soit $(x, y) \in (MN) \cap S^1$, montrer que x est racine d'un polynôme de degré 2 dont les coefficients dépendent seulement de t
 - 3.2 -1 est solution (coucou N), déterminer l'autre racine et en déduire le 2e point d'intersection de (MN) et S^1
 - 3.3 Montrer que $t \mapsto (x, y)$ est une bijection de $\mathbb{F}_q$ dans $S^1 \setminus \{N\}$ et en déduire que $|\mathrm{SO}_2(\mathbb{F}_q)| = q + 1$
4. Montrer que $\mathrm{SO}_2(\mathbb{F}_q)$ est un sous groupe de $\mathbb{F}_{q^2}^*$ et en déduire que $\mathrm{SO}_2(\mathbb{F}_q)$ est cyclique