9 Isométries directes sur $\mathbb{F}_q^2$

Leçons 120, 123, 190, (104, 106, 125)

Ref : [H2G2 Tome 1] VIII Prop 3.5

Ce développement consiste à déterminer le groupe des isométries directes sur $\mathbb{F}_q^2$.

Théorème 1 Soit $p \in \mathfrak{P}$ un nombre premier impair, $n \in \mathbb{N}^*$ et $q = p^n$. Alors le groupe spécial orthogonal $SO_2(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ si -1 est un carré dans $\mathbb{F}_q^*$, et à $\mathbb{Z}/(q+1)\mathbb{Z}$ sinon.

On note dans la suite $\mathbb{F}_q^{*(2)} := \left\{x^2, \quad x \in \mathbb{F}_q^*\right\}$ les carrés de $\mathbb{F}_q^*$.

Démonstration. Étape 1. Description du groupe spécial orthogonal analogue au cas réel.

On commence par décrire $SO_2(\mathbb{F}_q)$. On rappelle que les éléments A de ce groupe sont caractérisés dans $\mathcal{M}_2(\mathbb{F}_q)$ par la relation ${}^tAA = I_2$ et par le fait que leur déterminant est 1. Ainsi, on a

$$SO_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (a,b,c,d) \in \mathbb{F}_q^4, \ ad - bc = a^2 + b^2 = c^2 + d^2 = 1, ac + bd = 0 \right\}.$$

Soit $(a,b) \in \mathbb{F}_q^2$ tel que $a^2 + b^2 = 1$. On étudie le système

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

d'inconnue $(c,d) \in \mathbb{F}_q^2$. Alors (S) est équivalent à

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Mais comme la matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est inversible (car de déterminant non nul par hypothèse sur (a,b)), ce système a une unique solution, et elle est donnée par $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix}$. On a alors également $c^2 + d^2 = 1$. Réciproquement, si une matrice est de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $a^2 + b^2 = 1$, alors on vérifie que c'est un élément de $SO_2(\mathbb{R})$. L'application

$$\Phi : \left| \begin{array}{ccc} \mathbb{S}^1(\mathbb{F}_q) & \longrightarrow & SO_2(\mathbb{F}_q) \\ \begin{pmatrix} a \\ b \end{pmatrix} & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array} \right. ,$$

où $\mathbb{S}^1(\mathbb{F}_q)$ désigne la sphère unité de $\mathbb{F}_q$, est donc une bijection.

Étape 2. Cas où -1 est un carré dans $\mathbb{F}_q^*$.

On se donne $\omega \in \mathbb{F}_q^*$ tel que $\omega^2 = -1$, et $(a,b) \in \mathbb{F}_q^2$. On a alors

$$(a,b) \in \mathbb{S}^1(\mathbb{F}_q) \iff a^2 + b^2 = 1 \iff (a + b\omega)(a - b\omega) = 1.$$

On effectue alors le changement de variable

$$\begin{cases} x = a + b\omega \\ y = a - b\omega \end{cases},$$

qui est licite puisque le changement de variable inverse est donné par

$$\begin{cases} a = \dfrac{x+y}{2} \\ b = \dfrac{x-y}{2\omega} \end{cases},$$

où ω et 2 sont bien inversibles dans $\mathbb{F}_q$ (on est en caractéristique différente de 2). On a donc

$$(a,b) \in \mathbb{S}^1(\mathbb{F}_q) \iff xy = 1.$$

Comme les ensembles considérés sont tous finis et en bijection, on a

$$|SO_2(\mathbb{F}_q)| = \left|\mathbb{S}^1(\mathbb{F}_q)\right| = \left|\left\{(x,y) \in \mathbb{F}_q^2, \quad xy = 1\right\}\right| = q - 1,$$

où la dernière égalité vient du fait que l'on peut choisir x quelconque dans $\mathbb{F}_q^*$ et que y est alors fixé ($y = x^{-1}$).

On pose alors

$$\varphi : \left| \begin{array}{ccc} SO_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^* \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \longmapsto & a + b\omega \end{array} \right. .$$

On peut vérifier que φ est un morphisme de groupes. De plus, si $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est dans le noyau de φ, alors $a + b\omega = 1$, et donc $a - b\omega = \dfrac{a^2 + b^2}{a + b\omega} = 1$, ce qui montre que $a = 1$ et $b = 0$, et donc que A est l'identité. Ainsi, φ est injectif. Il est donc bijectif puisque les cardinaux des deux groupes sont les mêmes. Ainsi, c'est un isomorphisme. Comme $\mathbb{F}_q^*$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ [1], on en déduit le théorème dans le cas où -1 est un carré dans $\mathbb{F}_q^*$.

Étape 3. Cas où -1 n'est pas un carré dans $\mathbb{F}_q^*$.

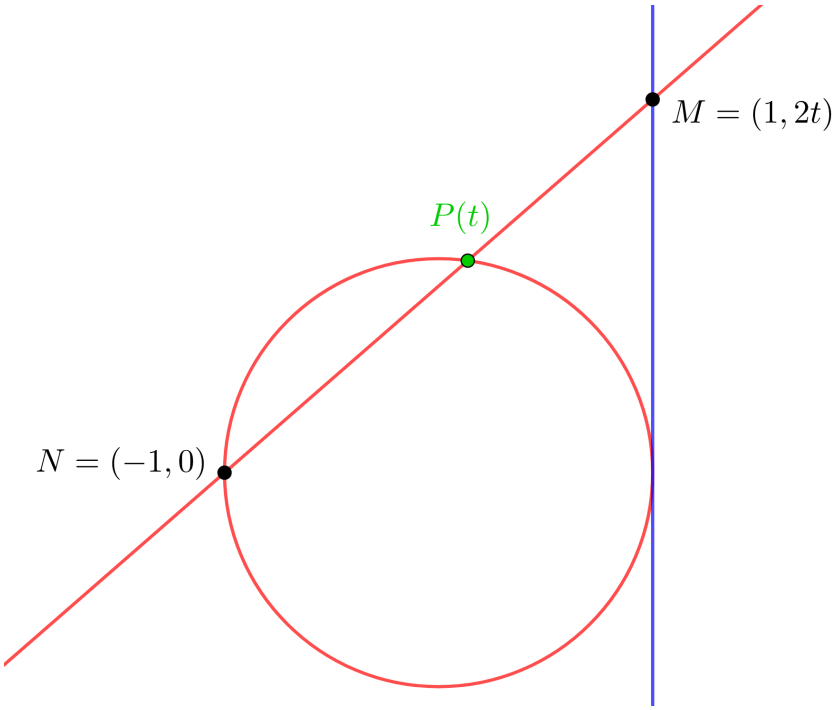

FIGURE 9.1 – Projection stéréographique de $\mathbb{S}^1(\mathbb{R})$

On utilise ici la projection stéréographique du cercle sur la droite $x = 1$ (voir figure 9.1 pour la situation analogue dans le cas du corps des réels). Notons $N = (-1, 0) \in \mathbb{F}_q^2$, et $M = (1, 2t) \in \mathbb{F}_q$ pour un certain $t \in \mathbb{F}_q$. Alors la droite (NM) coupe le cercle unité en N et en un second point $P(t)$. En effet, la droite a pour équation $y = t(x + 1)$ dans le plan $\mathbb{F}_q^2$ [2], et le cercle a pour équation $x^2 + y^2 = 1$. Ainsi, l'équation de leur intersection est

$$\left\{ \begin{array}{l} y = t(x+1) \\ x^2(1+t^2) + 2t^2x + (t^2 - 1) = 0 \end{array} \right. .$$

Comme -1 n'est pas un carré dans $\mathbb{F}_q^*$, la seconde équation, celle qui détermine x, est de degré 2 en x. Le calcul du discriminant montre qu'elle admet deux solutions, $x = -1$ et $x = \dfrac{1 - t^2}{1 + t^2}$. Le premier cas

1. Le groupe multiplicatif d'un corps fini est toujours cyclique.
2. On écrit que son équation est $y = \alpha x + \beta$, et on trouve α et β en inversant le système obtenu en observant que N et M vérifient cette équation. Notons qu'on a pour cela une nouvelle fois besoin de choisir $p \neq 2$.

correspond bien sûr au point N, et donc on a bien un second point d'intersection $P(t)$ donné par

$$P(t) = \begin{pmatrix} \dfrac{1-t^2}{1+t^2} \\ \dfrac{2t}{1+t^2} \end{pmatrix}.$$

Réciproquement, si $M' = (x, y) \in \mathbb{S}^1(\mathbb{F}_q)$ est différent de N, alors $x \neq -1$. Ainsi, la droite (NM') possède un unique point d'intersection avec la droite $\{x = 1\}$. Donc tout point de la droite correspond à un unique point du cercle, et réciproquement. Il y a donc une bijection entre $\mathbb{F}_q$ et $\mathbb{S}^1(\mathbb{F}_q)\backslash\{N\}$, ce qui montre que $\mathbb{S}^1(\mathbb{F}_q)$ est de cardinal $q+1$, et $SO_2(\mathbb{F}_q)$ aussi d'après de l'étape 1. Il reste alors à montrer que $SO_2(\mathbb{F}_q)$ est cyclique.

Pour cela, on injecte $SO_2(\mathbb{F}_q)$ dans $\mathbb{F}_{q^2}^*$. Le corps $\mathbb{F}_{q^2}$ est une extension de $\mathbb{F}_q$ de degré 2 dans laquelle -1 est un carré. En effet, X^2+1 est irréductible dans $\mathbb{F}_q[X]$ (car de degré 2 sans racine) donc $\mathbb{F}_q[X]/(X^2+1)$ est une extension de degré 2 de $\mathbb{F}_q$ qui est un corps de rupture de -1. Mais comme c'est un corps de cardinal q^2, par unicité des corps finis, ce corps de rupture est isomorphe à $\mathbb{F}_{q^2}$. On effectue alors un raisonnement analogue à celui de l'étape 2 : $SO_2(\mathbb{F}_q)$ s'injecte dans $\mathbb{F}_{q^2}^*$ en utilisant une racine carrée ω de -1 dans $\mathbb{F}_{q^2}^*$ et en produisant le même raisonnement que pour l'injectivité de φ. Ainsi, d'après le théorème d'isomorphisme, $SO_2(\mathbb{F}_q)$ est isomorphe (en tant que groupe) à son image par cette injection, qui est un sous-groupe du groupe cyclique $\mathbb{F}_{q^2}^*$. Donc $SO_2(\mathbb{F}_q)$ est cyclique[3], et est donc isomorphe à $\mathbb{Z}/(p+1)\mathbb{Z}$. □

La question naturelle qui suit cette démonstration est celle du cas $p = 2$. Je n'ai pas trouvé de livre traitant de cette question, mais elle n'est pas compliquée. On cherche à caractériser les éléments de $SO_2(\mathbb{F}_q)$, avec $q = 2^n$. Les équations décrites dans la première étape montrent que ce sont exactement les matrices de la forme $\begin{pmatrix} 1+b & b \\ b & 1+b \end{pmatrix}$, pour $b \in \mathbb{F}_q$. De plus, il se trouve que l'application qui associe l'élément b à cette matrice est un morphisme de groupes entre $SO_2(\mathbb{F}_q)$ et $\mathbb{F}_q$, surjectif par ce qui précède. Bien sûr, il est aussi injectif (étude du noyau). Finalement, on obtient

$$SO_2(\mathbb{F}_q) \simeq \mathbb{F}_q.$$

Ce résultat est très rapide à montrer donc peut permettre de combler si jamais il reste une ou deux minutes à la fin du développement. Dans tous les cas, je pense qu'il est bon de l'avoir en tête, cela me paraît être la question la plus évidente que le jury pourrait poser.

3. Tout sous-groupe d'un groupe cyclique est cyclique.